Digital Forensics Lab Scenario: Mid-Sized Police Department

Kaurice Woiwor

Old Dominion University

Digital Forensics Lab Scenario: Mid-Sized Police Department

Introduction

Forensic labs are essential to investigations. Evidence can be retrieved and examine within these labs. “Digital forensics is the process of uncovering and interpreting electronic data” (What is digital). Within these labs, analysts’ main goal is to preserve evidence in its original form (What is digital). They collect, identify and validate digital information. Professionals in this field must be attentive since digital forensics is held to higher standards (What is digital). Most federal agencies utilize digital forensics labs to conduct investigations on different cases. This case scenario asks me to create a brand-new digital forensics lab for a mid-sized police department. I have to create a diagram of the lab, an accreditation plan, a maintenance plan and create job descriptions for the potential staff. In this paper, I will discuss my layout for the lab, my accreditation plan, maintenance plan, job descriptions for the potential staff and equipment needed for the lab.

Digital Forensics Lab Diagram

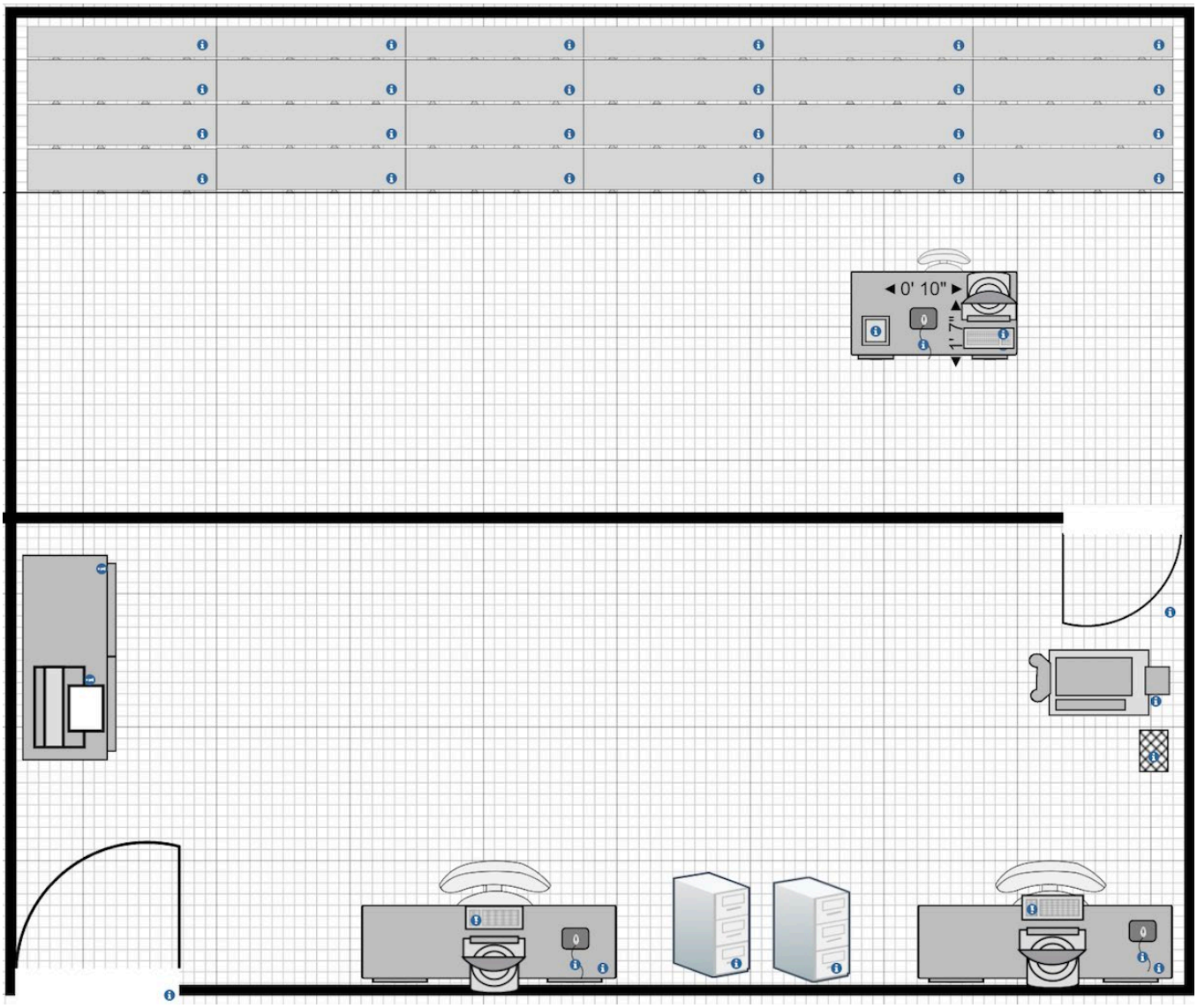
In the textbook, Guide to Computer Forensics and Investigations: Processing Digital Evidence, authors, Bill Nelson, Amerlia Phillips and Christopher Steuart state basic rules for forensic labs. According to the three, most labs tend to be small rooms (Nelson Phillips & Steuart, 2016). The labs should have locked doors to limited who has authorization to enter (book). They elaborated on the impotence of secure containers and visitors’ logs (Nelson Phillips & Steuart, 2016). They suggest containers with locks to prevent unwanted opening and visitor logs to keep track of traffic in and out of the lab (Nelson Phillips & Steuart, 2016)

Only authorized personal will have access to the lab. The doors will be equipped with RFID card readers. To gain access to the lab, investigators will use their ID key cards. The reader on the door will allow those with access to enter. The lab space is divided into two sections, workspace, and evidence storage. There are two computer workstations in my diagram, but the lab will have four computer workstations. The other two workstations will be located against the dividing wall, across from the other workstations. Each workstation will have the necessary software download onto the computer. There will be a file cabinet located at each workstation. The file cabinets will hold basic office supplies, like pens, paper, notecards, folders, and a hidden safe.

There will be an all-in-one printer located on the right side of the room near the trash bin. This all-in-one printer has a copier, scanner, and printer. This will be used for work related to the investigations. The large file cabinet on the left will hold equipment used at investigation sites. There will be a keypad lock on the cabinet and personal will have the code to access the equipment. There is a printer located on the cabinet for regular printing usage. The evidence storage room will use ers RFID card readers as well. There will be a guard assigned to the evidence storage room. Personal will sign-in on the evidence room log. The evidence room log will have a time in, time out, item, print name, and signature slot. All of this information will be uploaded onto a digital log throughout the day and backed up every night. There will be a hard copy and a digital copy to ensure accountability and integrity.

There will be cameras in the evidence room for more security. Evidence will be stored with the crime scene security log. This will have information about who collected the evidence. Evidence will be stored in steel containers. If personal need evidence, the guard will get it for them. The containers will be labeled with the date of the investigation and the name of the case.

Diagram



Inventory of Equipment

There are many tools digital forensic labs use in aid to their investigations. There are certain tools in every lab, but labs can be tailored to the needs of the department. For my digital forensic lab, I choose a number of hardware and software items I felt would benefit the lab. Using the Customized Setup for Dedicated Cyber Investigation from Forensics Ware I was able to come with my inventory of equipment list.

Hardware

- Keypad
- RFID reader
- ID Keycards
- Four File cabinet
- Five mice
- Five chairs
- Five mouse pads
- Five desks
- Five computers
- Five Keyboards
- External drives
- Speakers for computers
- Audio listening and recording devices
- Digital voice recorder
- Hidden Safe
- Cameras
- All-in-one printer (printer, scanner and copier)
- Printer (regular office use)
- Large file cabinet
- Trash bin
- Steel storage containers
- Cat6 Ethernet cables
- Office Supplies
    - Paper, pens, notecards,
- Evidence log notebook
- Lights
- USB
- HDMI cables
- Router
- Switches
- Cat6 patch panels
- Memory cards
- Servers
- Workbench
- Write blocker device
- Faraday bag

Software

- Firewall
- Wireshark
- FTK Imager
- Caine
- Hex editor
- Kali Linux
- Password cracking
- Keylogger software
- GPS tracking
- Mobile phone tracking software
- Voice analysis software
- Data recovery software
- Data acquisition software
- Sleuth kit – autopsy
- Mobile field kit
- Windows XP
- Windows
- Mac OS
- Mobile data investigation kit
- Encryption/ Decryption tools
- Registry tools
- Antivirus
- Programming languages (C++, Java, Python)
- Open Source file viewer
- Cloud analyzer
- X- Way Forensics
- Office 365

Accreditation Plan

The accreditation plan I choose is the ISO/IEC 17025 plan. This plan is followed by many in the digital forensics' world. To become accredited the lab must follow the step to gain accreditation (Watson & Jones, 2013). The first step begins with the application process. Staff will have to get acclimated to the standard (Watson & Jones, 2013). The lab will go through the assessment phase to receive its accreditation (Watson & Jones, 2013). The lab will have to demonstrate it meets all the standards of ISO/IEC 17025 (Watson & Jones, 2013). Procedures, work instructions, documentation, records, and the manual will play big roles in the lab's accreditation (Watson & Jones, 2013).

There will be a documentation review to ensure everything is correct (Watson & Jones, 2013). After the lab has been walked through and activities have been examined, there could be one-on-one interviews with staff members (Watson & Jones, 2013). The closing briefing will discuss the things done right and wrong in the lab (Watson & Jones, 2013). If any corrective actions are needed, they will be taken care of. Once the corrective actions are complete and the lab meets the standards of ISO/IEC 17025 it will be accredited (Watson & Jones, 2013).

Maintenance Plan

To maintain this lab for the next three years, the lab must stay up to date with its accreditation plan. The lab will be subject to surveillance and the lab will have to pass the assessments given by the organization (Watson & Jones, 2013). Passing the assessments becomes a part of our maintenance plan. The lab will be maintained by having a lab audit every three months. During the audit, the facility's ceiling, floor, roof, and exterior walls will be inspected (CYSE 407). The lab's doors, door locks, visitor logs, and evidence container logs will

be examined. If there is damage to these items, repairs will begin immediately. The computers will be replaced every eighteen months (CYSE 407).

Training staff will be a part of the lab's maintenance plan. Training will happen every six months. Staff will be trained on the lab's policies and procedures. Staff will receive training on the latest information related to digital forensics. Having staff well versed in the new and old makes them more equip to handle different investigations. Budgets will be drafted yearly. Budgets will include expenses for training, hardware, software, facility repairs. Costs will be broken down into daily, quarterly and annual expenses (CYSE 407).

A risk assessment and business impact analysis will be a part of the lab's contingency plan. These assessments will be conducted yearly. The risk assessment will identify the risk and threats to the lab. The assessment will also point out and apply the measures needed to reduce or eliminate the risk (Watson & Jones, 2013). The business impact analysis examines the potential loss if a risk or threat occurred Watson & Jones, 2013). Completing the business impact analysis and risk assessment creates better results for the lab (Watson & Jones, 2013). The lab will complete both assessments yearly together.

Staffing

Staffing for the lab will include a lab manager, examiners, and guard for the evidence room. The duties of the lab manager will include case management, decision making, planning updates for the lab, assigning cases to investigators, briefing staff on policies, and conduct training (CYSE 407). The lab manager will be responsible for monitoring lab policies for staff, production schedules and enforce ethical standards among lab staff members (CYSE 407). Staff responsibilities will include performing tasks they are assigned, following policies and reporting

to the lab manager. The lab managers and staff are expected to have a degree related to digital forensics. A bachelor's degree in Computer Science, Information Systems, Engineering or Criminal justice. Both should have certifications in the field like the following CISSP, GIAC Certified Forensic Examiner GIAC Certified Forensic Analyst. Both should have at least two to three years of experience working in the field. Responsibilities of the guard include managing the evidence log, retrieving evidence, and updating the evidence log on the computer. The guard is a police officer in the department.

References

CYSE 407 Digital Forensics - Fall 2019. (n.d.). Retrieved from http://ple.odu.edu/courses/201910/cyse407/modules/1/2/2.

Forensicsware. (n.d.). Customized Setup for Dedicated Cyber Investigation. Retrieved from http://www.forensicsware.com/lab-setup.html.

Nelson, B., Phillips, A., & Steuart, C. (2016). *Guide to computer forensics and investigations: Processing digital evidence.* Boston, MA: Cengage Learning.

Watson, D. & Jones, A. (2013). Digital forensics processing and procedures. Retrieved from https://reader.elsevier.com/reader/sd/pii/B9781597497428000030?token=9A67A2AF84BDA54B178B187E674DCEAB3E43BB98B92E8BE346CF10A1F0242D15CA6DB0856EC7CE57DF77DEDE5E4BEE9F

What is Digital Forensics? - Definition from Techopedia. (n.d.). Retrieved from https://www.techopedia.com/definition/27805/digital-forensics.