**Inventory**

I created a 3-year plan and visual diagram via Lucid charts, for my midsize Digital forensics lab that I will be running. The lab space will be within a precinct, preferably on a the main or a basement level so that it stands a better chance in the event of a natural disaster. The lab space will be secured because it’ll be requiring RFID key card to enter through the main entrance and into the conference room and a personal identification number to enter the lab (Being so no one other than technicians and the lab manager have access). There are also several cameras around the lab as an extra security measure in the lab along with adequate cooling and humidity controls to protect the equipment. There will be an appropriate number of desks, workbenches, chairs, etc. for the size, and all the forensic and administrative work that will be completed in here. There are also a few evidence lockers dispersed within every room of the lab to ensure there is plenty of room for storage. It is important to note that each room will have different levels of security ranking based off how sensitive the evidence is. The lockers also will require a key to access the evidence inside and must be logged in and out via sign in sheet and personal ID number. This is to ensure the person that signed out evidence can be confirmed and can be held accountable for anything that goes missing. Also, secure internet connection specifically for the lab obviously and an evidence storage room that will remain separate and can be accessed by authorized individuals via their individual ID number.

Let us move on to my plan for equipment needed within my forensics lab. It is an absolute necessity to have a large and powerful server due to the amount of data and evidence that will come through here (I have the server labeled as ‘database’ in my diagram). The server I choose is a FREDC that stores up to 1.2 petabytes which equals up to 1228.8 terabytes of secure storage. I believe this will be plenty for a midsize forensic lab as it is fast, has a secure evidence chain, scalable, highly responsive, and with an agnostic infrastructure. We will also require some write blockers that support all types of hard drives, and I opted for two that come with forensic imagers as well. The write blockers for three years will total to $13,224 with the two forensic imagers of course. A scanner and printer are also a requirement for the lab and luckily there are machines that do both and might range from 1500-3000k depending on size and brand.

To continue, we will also be needing an exam computer that we have plenty of RAM, preferably a dual or quad core, and a large monitor. These computers will need firewalls and virus protection to keep them safe for potential threats. Virus protection ranges around $350/year for a business level version of the application (allows the more devices to be on a single plan) this would total to $1050 for three years. The lab will also need a couple cell phones with data connectors and signal blockers for cell phone exams. Tape dives, network equipment (switching hubs, network cards, router, etc.). We will need a Forensic Suite of choice more than likely FTK because it is commonly used by law enforcement and averages around $2,227/year totaling $6,681 for 3 years. Other supplies needed include: cables, CD-Rs, DVD-Rs, Clamshells, Tapes, hard drives, flashlight, plastic static bags, labels (for CD/DVD/bags), printer cartridges, and paper. There are also a number for free forensic tools that my lab will take advantage of.

**Accreditation plan**

In order to achieve employment in a Digital Forensics Lab (DFL) you must have a specific minimum level of skills/accreditation. Prior to employment staff must undergo a background check to gain knowledge of any criminal record the individual has, if any. The staff must also undergo necessary security vetting to confirm security clearance needed. Once the staff is recruited, they must continue to improve their skills so they can be successful in executing everything that’s needed in a DFL. The main requirement for anyone working in a DFL is having basic computer forensic knowledge is needed along with basic/advanced data recovery (NW3C-BDRA, ADRA). Tool specific training is necessary, in our case in FTK and legal training considering our midsize lab is within a precinct. Legal training would include learning about search warrants, testifying, computer crime laws, and other issues concerning our country.

The field of work we are in is always evolving and technology is always changing and requires constant learning and testing. Each examiner should take and pass a competency test to prove they understand the policies and tools needed to execute the job.

**Staffing**

The Lab Manager is the one person in the DFL with control over the entire lab which includes: the setup, purchasing of needed hardware and software, and the labs functions and procedures. The Lab Manager is also in charge of leading the recruitment, the training, mentoring, and guidance of everyone in their unit. Also, they are the only individual with the authority to accept or reject a case and makes all final decisions pertaining to any cases they accept. He/she must have advanced technical skills/knowledge and a managing or supervising background. Must also follow the legislative requirements for processes, procedures, electronic evidence, and evidence in general.

The Technician is responsible for maintaining all forensic equipment. This means the Techs must stay on top of updating all the labs hardware and software. Along updating all the systems within the lab as updates are released, they must also manage software patches. Normally, there are a few technicians that work in a DFL at a time we’d probably need about three techs for our mid-size laboratory.

They have the important job of not only maintaining equipment but handling the evidence within the storage/evidence room. This job includes maintaining the records of evidence and efficiently checking items in and out. Maybe there is even a technician that is designated to the evidence room to monitor and maintain its security. I believe that having someone at a desk that stays in that room will make things such as checking evidence out operate smoothly. Not only do tech handle evidence but they are also in charge of evidence processing. What evidence processing is, is the registration, the acquisition, and the storage of evidence that comes through the lab. Considering our lab is not that large two of our three techs might be required to process our evidence.

It is a necessity that a Tech. has a strong technical and computing skills along with plenty of technical knowledge. Attention to detail and the ability to accurately and clearly document any actions conducted on evidence is crucial to the job as well.

**Maintenance plan**

Due to the constant advancement in technology the technology requirements are always changing. Therefore, the staff must always remain up to date with the knowledge and skills necessary to maintain the proficiency of the lab. Some ways the staff could practice doing so would be to require them to research new technology and test if it could be useful to their investigations. Another way would be to require them to attend technical related meetings every-so-often, conduct electronic evidence analyses, view product demonstrations, and/or annual retraining programs. The staff’s skills should be up to date with current technology, and they should be sure to check that doors, windows, locks, RFID cards are all operating properly and if needed replaced. Along with the doors, windows, etc. the cameras should be checked and after a certain period of time and thorough examination remove any footage that is useless in order to free space for more.