Computer Forensic Lab: Building a Computer Forensic Lab.

Vincent Kiweesi

Computer Forensic Lab

April 16, 2023

The steps to plan a budget for the lab would include analyzing the need for resources, technicians, hardware, and software. The cost of training the crew to set up and use the equipment. Also, it involves setting up the lab's security equipment Check, the cost of task execution. Determine the cost of labor needed to keep the lab in good working order. Divide costs into daily, weekly, monthly, and yearly expenses. To estimate anticipated future expenditures, use historical research costs. (*OAS*)  
  
A lab's costs include:   
- Hardware   
- Software  
- Facility space   
- Trained personnel  
  
Calculate how many computer cases your lab intends to look at.  
- Determine the kinds of computers you're likely to look at.   
  
- Consider technological advancements

You can determine the types of computer crimes that are most likely to occur using statistics, plan your lab expenses and requirements using this information.

Check out statistics from the Uniform Crime Report at www.fbi.gov/ucr/ucr.htm for federal reports.  
Identify crimes committed with specialized software.  
  
When setting up a lab for a private company, look at the following things:   
  
Hardware and software inventory  
- Problems reported last year  
- Future developments in computing technology   
- Time management is a big problem when choosing software and hardware to buy. (*OAS*)

It is crucial to implementing a Secure location that should maintain the integrity of the evidentiary data. A little space with actual floor-to-ceiling walls with a locking door, and secure container, a visitor's log also access levels for coworkers should be the same, I would inform the staff of the security policies, the lab can only be accessed by people you can trust you can accomplish this by equipping it with fingerprint scanners. All technicians using the lab should be given passwords. (*OAS*)

Include software and hardware into the lab's layout like a power station, which is used for high parallel processing and computation, and a forensic duplicator used to duplicate data forensically from disk to disk or disk to file for hardware. For Software I would include guidance software which helps to provide answers for computer forensics and investigations. Also, I would include Passware that covers solutions for password recovery, decryption, and analysis of encrypted evidence. (*OAS*)

Identify the high-level criteria that would be considered when selecting the forensic workstations to be utilized.

Depending on the needs and budget use multipurpose workstations for complex analysis activities and less powerful workstations for routine tasks.  
The most varied needs for computational investigation tools are found in forensic labs.  
Special interest groups (SIG), rule of thumb, one computer investigator per 250,000 residents of a region, and one multifunctional forensic workstation and one general-purpose workstation. (*OAS*)  
  
Finding requirements is simple by determining the atmosphere you work in. Assemble the necessary equipment to work in the designated environment like hardware platform and Operating system.  
Make a system memory and disk image, the images should be exported and imported into the forensic workstation. Put the tools to work by beginning with a disk image analysis and moving on to memory analysis. To fully understand the sequence of events, make a timeline of what happened and when. (*OAS*)

To fully understand and track the malicious behavior, compile a list of IOCs (indicators of compromise).  
REMNUX and the SANS SIFT Workstation stand out. There are a staggering number of open-source tools available on the SANS SIFT workstation that are made for digital forensic investigations. Like this, REMNUX offers a wide range of tools, especially for malware investigation. Both toolkits, however, only support Windows, and many helpful forensic tools are not available for Linux. A forensic analyst's day frequently involves switching between Windows and Linux platforms. Using Windows as the operating system for the forensic systems might be highly advantageous for the forensic analyst as there are probably more investigations and attacks on Windows systems. Thus, we prefer to use a Windows operating system with a lunix subsystem to get advantages of both (*OAS*).

Reference

*OAS*. (n.d.). Retrieved May 4, 2023, from https://www.oas.org/juridico/spanish/cyber/cyb32\_forensics\_lab\_en.pdf