Hands-on Project 2-5

Justification

To conduct these investigations, a forensics lab is needed to handle and store all the evidence acquired. The law firm should be prepared for any case that may arise so as to appease their clients. This lab can be leveraged to advertise the services and capabilities of the law firm, potentially attracting more clients as well. The initial and sustaining budget for the lab will originate internally however, in the future, we may accept potential sponsors if the need to expand emerges.

Facility Cost

As most of the evidence expected to be received consists mainly of e-mail, spreadsheets, and documents, a singular lab that can hold two digital forensic examiners is sufficient. A room is needed to fit two forensic PCs, a workbench, and (two) storage lockers for physical evidence. The storage lockers are required to have a digital lock, like a numpad. This room should also have floor-to-ceiling walls and no windows to prevent unwanted passersby from viewing sensitive information. An example of the lab can be seen in the figure below:

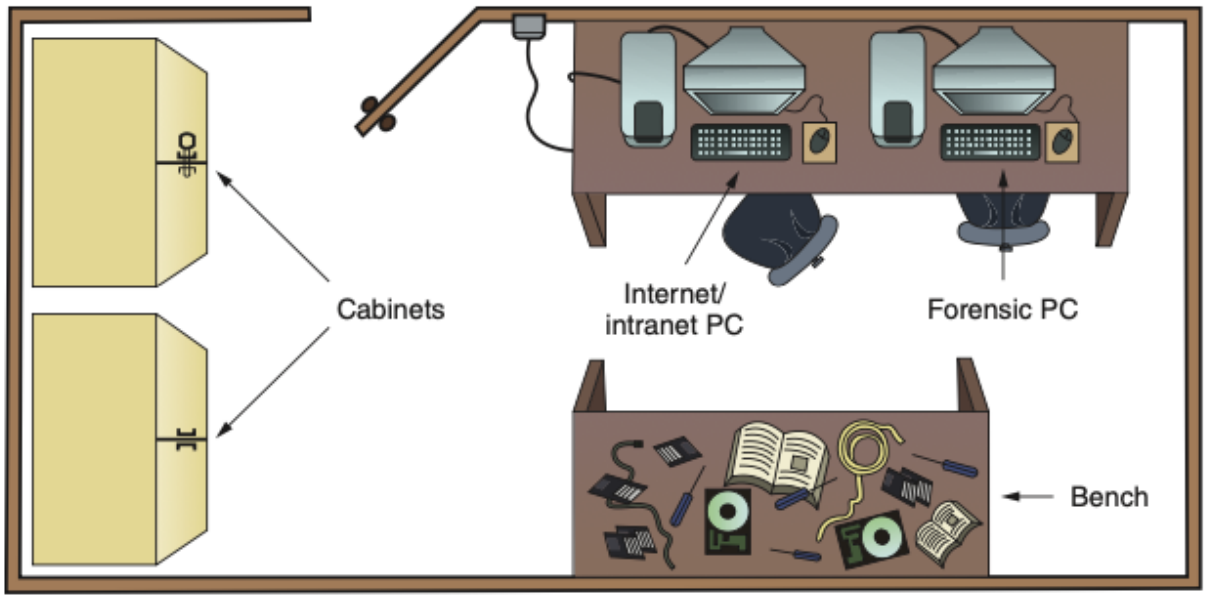

Figure 1: Forensics Lab Example

The door should be keycard-protected, which simultaneously logs those who enter (time they enter and time they exit) and only allows authorized personnel into the lab. Additionally, a security camera should be set up outside of the lab pointing at the door, so as to verify the logs of the keycard scanner.

The room should have adequate electrical power, as well as heating and ventilation to preserve evidence and also maintain temperature. A verified janitorial staff is allowed in for weekly maintenance, granted that the PCs and storage lockers auto-lock after a certain amount of time in case the examiners forget to.

Hardware Requirements

Considering hardware specifications, the clientele could potentially use any kind of computer system on the market. Thus, the forensic PCs should be Intel-based with the latest version of Windows, but have MacOS capabilities as well (integrated through a virtual machine) for any potential investigations that may require it. Each PC should have 2-3 terabytes of storage for all potential software needed as well as analyzing evidence for ongoing cases. Additionally, the lab should have an external storage drive of 30 terabytes to hold evidence from previous cases. The evidence can then be destroyed 6 months after the case is closed to make room for oncoming cases. Each high-end Intel-based PC will cost about $3,000 and the external hard drive will run about $500.

Software Requirements

The types of OSs that will be examined will mainly be Windows and MacOS. Older versions of these OSs must also be considered. The budget should allow for two copies of forensics software tools, one on each PC however, one tool is sufficient enough as the types of evidence expected to collect are not that complex. The forensics PCs should also have access to the internet.

Miscellaneous Budget Needs

The workbench and additional chairs can also be factored into the budget. A simple, sturdy table and ergonomic chairs can be considered. Computer peripherals are also needed, such as a monitor, keyboard, and mouse. Other accessories include HDMI cables, USB cables (type-A and type-C), thunderbolt cables, and desk lamps.