Requirements for a Computer Forensics Lab

Contents

- In this chapter, we will cover the following topics:
  - Digital Forensic Lab
  - Physical requirements
  - Environment controls
  - Digital Forensic equipment
  - Office electrical equipment
  - Networked devices

Digital Forensic Lab

- Today, banks, tech companies, retailers (such as Amazon and Walmart), and utility providers are all using their digital forensics labs to speed up the investigation process and cut down on the costs of digital investigation.
- Compared with police labs, private corporations have more freedom when it comes to buying the most up-to-date software and hardware for their labs.
- Some Law Enforcement Agency(LEA) labs may still be using old software versions because they do not have enough money or people who know how to use it.
- In most cases, in-house digital forensics analysts work with law enforcement to solve cases that are related to their businesses.
- People who find evidence of or witness illegal activity (for example, violating rules or industrial sabotage and leaking secrets) will call law enforcement and work with them to get the evidence and move the case to court.
- The reporting company's digital forensic investigators or the e-discovery team will work with them to get and analyze the evidence.

3

Digital Forensic Lab

- Accrediting a digital forensics lab is an important thing to think about, whether you want to set up an in-house lab for your company or you want tooutsource your digital forensics work to a third-party provider.
- Accreditation ensures that your lab, or the one you want to use, meets the standards set by the official body in terms of using reliable methods, the right tools (hardware and software), and the right people to do its job.
- You need to think about how much money you have when planning a digital forensics lab.
- You also need to think about what you want to do in the lab and what kind of equipment and software you need to do it.
- Among other things, big companies are spending money to build advanced labs that can handle all types of computers and cases such as malware, outside breaches and network, GPS, and mobile forensics.
- These labs have well-trained people who use the most up-to-date forensic software and other special hardware tools.

4

Physical requirements

- The following physical needs are very important to have in any digital forensic lab:
  - There must be at least one way.
  - It is better if there are no windows in the lab.
  - The lab must be soundproof, so no one can hear what people are talking about inside the lab. This can be done by putting soundproofing material on the ceiling and walls and carpet on the floor to make the room quieter.
  - There must be an alarm system at the entrance of the lab, as well as a biometric system to let people into the lab. People who use the biometric access system must be able to show that they have been to the lab. This log must be kept for a long time for auditing.
  - Surveillance cameras should cover the whole lab, especially the main entrance and the room where digital evidence will be kept. Keep the video recorder of the surveillance system in the lab's safest room, which is called the "evidence storage room", so it does not get broken into.
  - This can lead to the tempering of evidence and violation of data integrity.
  - Fire suppression systems must be in place for this to work.

5

Environment controls

- To keep forensic equipment and seized digital devices from being damaged, the lab environment must be kept very clean.
- The following controls must be in place for this to work.
  - First, an air cooling system to remove heat from workstations. Because forensic workstations can stay running for a long-time during evidence analysis (like cracking a password), they can get very hot. This is especially important in small spaces, where heat can build up quickly.
  - Second, the lab needs to be a good place to work and clean. It must have a healthy climate in terms of temperature, low humidity, and clean air so that it is safe for people to work there.
  - Third, there should be good lighting in the whole lab and each forensic workstation room. Electricity providers and UPS units to keep the lab running even if there is a sudden loss of power, as well as for forensic workstations, storage servers, and surveillance cameras

6

Digital forensic equipment

- Forensic hardware
  - Licensing the server (which is required by some digital forensics suites).
  - Storage server that is set up to use standard removable hard drives to store digital evidence images and data that has been processed and extracted from those images. This server must not be connected to the internet.
  - Forensic workstation.
  - A portable forensic computer number is used outside the lab to capture evidence and for doing some analysis.
  - Computers that can connect to the internet and the intranet.
  - The administrative computer is used to keep track of logs and other things.
  - Hardware Write Blocker: This is a piece of hardware that connects the media that holds digital evidence (like a hard drive) to a forensic workstation. The goal of this piece of hardware is to keep the data on the evidence drive from being changed during the acquisition process.
  - CD/DVD drive.
  - USB reader.
  - HDD and SSD cases with a USB 3.0 port.
  - SD card reader.
  - USB 2.0 and USB 3.0 thumb drives of different sizes.
  - Tape drives are used to store long-term data.
  - The following are the types of data cables and connectors: Ethernet cables (RJ-45), BNC adapters (such as modular adapters), ribbon cables (such as ribbon cables), DIN split cables, VGA split cables (such as VGA split cables), USB cables, audio cables (such as USB extension cables), cable extenders, HDMI and FireWire (IEEE 1394).
  - Other tools, such as screwdrivers, a multi-meter, and a flashlight.

7

Digital forensic equipment

- Office electrical equipment
  - Each workstation, server, and network device needs to have an uninterruptible power supply(UPS).
  - A device for projecting things (in a conference room).
  - Scanner
  - Photocopier
  - A paper shredder is the sixth thing on the list
  - Digital cameras, such as video cameras, and their accessories.
  - Wireless
  - Wi-Fi access point
  - Headset
  - Symmetrical power source

8

Digital forensic equipment

- Office electrical equipment
  - Networked devices
    - It is important to note that there should be a separate network inside of the lab that connects forensic workstations to the server that stores digital evidence image copies.
    - The server must be put in the evidence room to keep people from getting to it.
    - This lab-specific network cannot connect to the internet. In the lab, forensic examiners may need to look up more information about their findings or work with other people, so an internet connection should only be available through a direct line to the computer(s) that need it.
    - Router and switch to connect forensic workstations to the storage server in the lab. The lab's internet network should not be connected to the lab's network.
    - The things you need are a firewall, a switch, a router (the three components can be combined in one device), and network cables and wires.

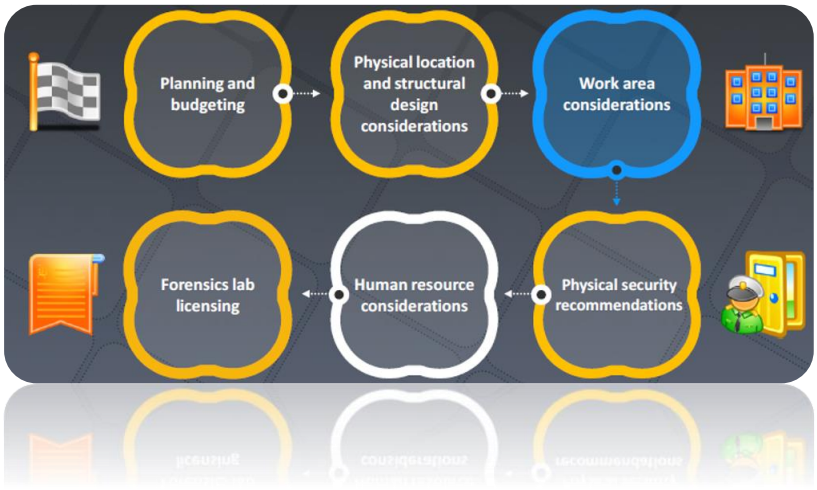
9

Forensic workstation

- There should be forensic workstations that have the most recent version of Windows OS (64-bit version) on them. Windows 10 Pro and Enterprise editions are recommended because they can run on high-end hardware and do a lot of work quickly.
- Both editions can have up to 6 TB of RAM and four processors. However, compared to modern Windows Server editions, which can have 24 TB of RAM, those two editions are cheaper because they belong to the Windows desktop product line.
- Now, let us talk about what kind of hardware is needed for forensic workstations. When working with digital evidence, you need a powerful computer to process and search through image files.
- Forensic computers need a lot of processing power and a lot of RAM. They also need a lot of storage space and a lot of expansion slots to connect different types of devices.
- Building a forensic workstation costs money, but it is still cheaper than buying a ready-made computer forensic workstation, which costs a lot more.
- For small businesses, this is still a good option. This is what you should have when you start from scratch and build a forensic workstation

10

Computer forensic lab



11

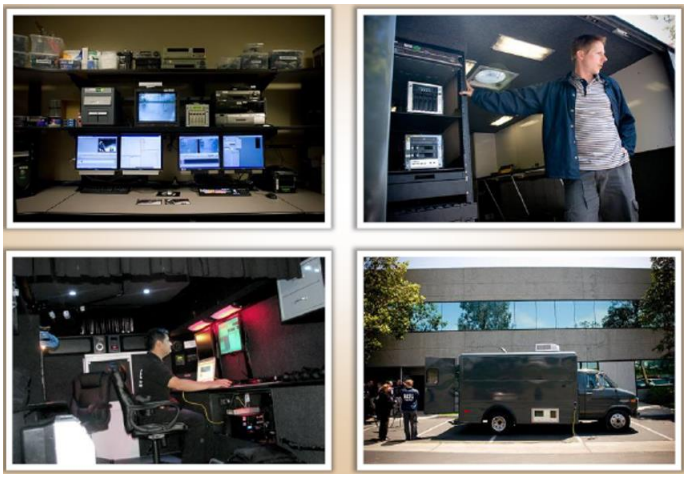
Forensic lab

12

Forensic lab

13

Forensic lab



14