# Mini-Project 30: Computer Forensic Lab

## Mini-Project Overview

**Time Estimate: 90 minutes**

This mini-project builds upon the previous one where you were asked to prepare a presentation for the Board of Directors on your main duties for the company and how your position could help achieve business goals based on security and confidentiality.

## Project Submission Steps

The Board of Directors really liked your presentation, and they have given you their blessing to build a computer forensics lab.

Write a four to five (4–5) page paper in which you:

1. Explain the steps you would take to plan a budget for the lab, keeping in mind the general business objective to avoid unneeded costs.

2. Recommend the physical requirements and controls that you would consider implementing in order to keep the lab safe and secure.

3. Identify at least three (3) hardware and software tools that you would include in the design of the lab and explain your reasons behind your choices.

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

There has been employee complaints of ongoing sexual harassment over email and instant messaging systems. A computer forensics lab will be built to investigate this misconduct. The computer forensic specialist will comply with the business goals based on security and confidentiality. That is, the lab will be safe and secure and comply with the code of ethics. Before planning the budget for the lab the forensic specialist will need to gather the following information from the Board of Directors:

- The nature of the investigation
- What digital evidence should be found at the location
- The details of the search warrant
- Who are the suspects and what roles do they play in the investigation

The forensic specialist needs to take important steps to plan a budget for the lab. The following should be considered :

- First, the forensic workstation should be a powerful computer with a fast CPU and a large amount of memory and storage. For example, the Falino workstation worth around $5,000 from Sumuri consists of the Intel 7800 K processor, 32 GB of RAM and 512 GB SSD of storage space. SSD's (Solid State Drives) have higher throughput than the typical hard drive.
- Secondly, the forensic lab should consist of a response kit that is used to collect digital evidence. Items that should be included in the kit are as follows:
    - ☐ Digital camera to document your actions on the scene as it was when you arrived
    - ☐ Latex gloves as to not leave your fingerprints
    - ☐ Notepad to document your actions on the scene
    - ☐ Property report for seizing evidence and listing exactly what was taken.
    - ☐ Antistatic bags to put containers of digital evidence
    - ☐ Extra storage media such as SSD or USB devices.The storage can be attached to the forensic workstation or it can be a NAS or SAN. It is recommended that it is at least 10 - 20 TB.
- Thirdly, a hardware write blocker, also known as forensic disk controllers, is an important tool used in the forensic environment. It is a physical device that is connected between the computer and the source device. It allows you to access a storage device without changing its contents by intercepting and preventing any modification to the source device.
- A forensic laptop is required since the forensic specialist will need to move to different locations within the company.
- Lastly, forensic software is required to perform the forensic investigation. This consists of both open source and commercial software. Some open source forensic tools that can be used are Autopsy and SIFT. Commercial tools that can be used are Encase, Forensic Toolkit (FTK) and Forensic Explorer (FEX). The key is to not select the right tool but to use the tools that were chosen to provide reliable results from the artifacts in the investigation.

One element the forensic specialist has to work on to secure the lab is to collect volatile data or evidence in a specific order from most volatile to least volatile. If the most volatile evidence is not collected first, the evidence the specialist is looking for might be destroyed. RAM is the most volatile data in any computer system, and therefore it should be collected first. The order of volatility is as follows:

- Live system
- Running
- Network
- Virtual
- Physical

Another element that should be practiced to keep the lab secure is to make sure the servers used as evidence are not powered down since the specialist needs to retrieve the decryption key in case there is full disk encryption. With disk encryption, data on the disk is encrypted at all times. Decryption occurs on demand when files are read and occurs as long as the machine is up and running. The decryption key is somewhere in RAM and it stays there. If the server is powered down the decryption key is lost.

The chain of custody is another way of securing the forensic lab. The chain of custody preserves and authenticates evidence by documenting all access to the evidence, who accessed it, when it was accessed, and for what purpose it was accessed.

In the analysis phase of the forensics investigation, the specialist will conduct several analyses. A few of these are:

- Time analysis which is critical. If the evidence comes from various time zones there might be confusion in the investigation. Setting the forensic machine and tools to use universal time as a standard frame of reference helps solve this problem.
- Hash analysis can help keep the forensic lab safe. The specialist can use hash analysis to verify the evidence has not changed. Also, there are hash sets that identify known good files. These files have no evidentiary value and can be excluded from the investigation.
- File signature analysis to determine if the evidentiary files have been changed. A user can change the file extension to hide the evidence. The purpose behind carrying out a file signature analysis is to determine whether file signature and file extension are a match.

The training of the forensic specialist is an important aspect of the forensic lab. The specialist should have training in the following areas :

- Computer hardware and networking

- Basic computer forensic knowledge
- Tool specific training such as Encase and Forensic Toolkit (FTK)
- Legal training such as search warrants, good communication skills for testifying and computer crime laws.

The forensic specialist will need to analyze the email containing sexual harassment content. To understand how to perform a forensic analysis on email, the process of how it is transmitted through the network has to be understood. In the telecommunications company where the crime has been reported, a mail server is configured on the Windows server. The server contains a domain name and has SMTP ( port 25) installed to send and receive email messages from the client. POP3 (Post Office Protocol) is the protocol that allows the client to access their inbox and download emails. It utilizes port 110 on the network. The recipient has the option to leave the email on the server where a copy of the email will be saved in the database file of the email client. The IMAP protocol is a newer version of POP3 where the email client where a copy of the email stays on the server until the user purposely deletes it.

One problem with performing a forensic investigation on email to uncover a crime is how to decode the email dataset once you have acquired it. An email has global unique identifiers such as mailbox name, domain name and message ID in the email header that will allow a forensic specialist to serve a search warrant for any suspects of the crime. The E-Mail Header Analyzer available for download on https://blackhatethicalhacking.com can be used to parse email headers and convert them to a human readable format. It's primary use is to track someone or collect IP Addresses involved in the transmission of emails by identifying hop delays, the source of the email and hop country.

The telecommunications company uses Microsoft Outlook as the email client since most of the clients run on Windows and it comes preinstalled with the Microsoft Office suite. The forensic specialist can conduct an email examination by exporting the container used by the client and opening it with the email client installed on the forensic workstation. The user and forensic tools can use Microsoft Windows LIve Mail to view their email. The client stores email messages in **"\Users\$USER$\AppData\Local\Microsoft\Windows Live Mail"** directory path. The emails have an .eml file extension which is a standard text format.

For a forensic specialist to present evidence of the criminal email, they will have to generate a snapshot of the hard drive the email resides on. The first step is to use a write blocker which guarantees the data integrity of the suspect disk and is required in the chain of custody. The Tableau write-blocker is a hardware write-blocker that is stationed between the forensic workstation and the suspect drive. It's eSata connection on one side of it is fast and connects to the workstation. On the other side of the write-blocker is a SATA connection which connects to the suspect SATA drive. A SATA connector cable is used for the drive to write-blocker connection. The workstation will be able to read the disk but not write to it since the write blocker will make it write-protected. The specialist will then use Access Data FTK Manager on Windows to acquire the files on the disk. In other words, the specialist will perform forensic

acquisition. If the partition on the disk is something Windows recognized then it will be seen as an ordinary disk and shown as a drive in Windows Explorer. The MMC Console with the Disk Management snap-in can also be used to view the suspect disk. After it is confirmed that the disk can be seen by Windows, open the FTK Imager to acquire the disk by going to “file”, “create disk image”, select “physical drive” from the “Select the Source Evidence Type” pop-up. Selecting the physical drive will copy all the data from the suspect disk. Select “image file” after you make a copy of the disk since you never want to work with the original image file. Then, select the source suspect drive, the image destination, and the destination image type (Raw). After this the Evidence Item Information is entered and the disk image is saved in a file and folder that is created. The last step is to “Create Image” to create the snapshot of the disk.

The best operating system to use for forensic analysis is Kali LInux. That being said, there is an open source command line version of FTK Imager that can be installed on Linux. After the image is created and stored in a directory, a file carving tool such as bulk extractor can be used. This carving tool scans the disk image and extracts useful information without parsing the file system and it can process different parts of the disk in parallel.

The telecommunications company has also mentioned that there is sexual harassment in instant messaging. Mobile device forensics on which instant messaging occurs most frequently can be challenging since mobile device encryption is commonly used and it is mostly commercial forensic software. The specialist will want a Mobile Forensic Toolkit which will consist of a screwdriver or push pin-style tool to get access to the SIM card. Next, a Connection Cable Kit can be bought that contains 50 to 100 different types of cables that can connect to any phone on the market. The SIM card is important since it contains flash memory. When text messages are deleted from the cell phone it does not completely disappear. The flash memory doesn’t delete the file until it needs to open up space for something new. A tool then can be used to analyze the memory.

The forensic specialist is looking at Grayshift for it’s mobile forensic software and hardware. Grayshift produces the ‘Graykey’ box which uses an iPhone cracking technology shipped to police forces. The Graykey is a small box with two lightning cables for connecting iPhones. There are two versions: a $15,000 one which requires online connectivity and allows 300 unlocks and an offline one for $30,000 which cracks an unlimited number of iPhones. A four digit passcode can be cracked at the most 13 minutes and a six digit passcode can be cracked at most 22 hours. The devices uses a brute force attack to crack the passcodes. Combined with Graykey’s industry-leading mobile acquisition, AXIOM can gather and analyze data from IOS and Android devices quickly and easily. It can access memory images which contain important evidence such as suspect instant messaging.