ITMS 538 Assign04a_rds

Alan Palayil Due Date: 10/09/2022

Case Project 2-3 (p.91 from Nelson Text)

Research your state, province, or neighboring states and provinces to determine whether digital forensics examiners require licenses. Write a one-page summary of the licensing requirements in the region you selected. If your region doesn't have any licensing requirements, research one of the following states: Michigan, Texas, or Georgia.

When it comes to the standard of operating procedures in computer forensics, every state has it own laws and procedures. In Illinois, the state is operating with regards to the Federal Rules of Civil Procedure Amendments. There are no additional state laws or regulations on the books in Illinois concerning computer forensics or data recovery. So, I will be writing about the licensing requirements of Michigan State. The policy of Michigan, states that departmentally acceptable certification or certified studies in computer forensics which comprises of two components.

The first component is a general information security certification which includes a peer review, common body of knowledge and the completion of 40 hours of general security continuing education per year for 3 consecutive years. The second component includes a 40-hour training of technical materials, search and seizure, preservation of evidence, best investigative practices, and legal aspects which are included in the State and Federal Acts; a written examination; and a practical exam or peer reviewed paper.

The requirements above are the technical requirements in order to get the license to be a digital forensics examiner. There are also other standard requirements to become a licensed professional examiner which includes being a U.S. citizen, not less than the age of 25, and have a high school education or its equivalent. That being said, you won't be able to receive the licensing if you have been convicted of a felony or misdemeanor such as assault, illegal use-or carry of weapons and drugs, two or more alcohol related offenses, and impersonating a law enforcement officer. Among other requirements, few departments also require you to have posted a $10,000 bond or insurance policy provided for in this act.

The licensing requirements do fall squarely on those individuals acting as independent consultants to the victimized organization. The implications for operating without a license are substantial, including fines up to $5,000 and an imprisonment up to 4 years.

ITMS 538 Assign04a_rds

Review Questions (p.135 from Nelson Text)

1.What's the main goal of a static acquisition?

- It is the preservation of digital evidence.

2. Name the three formats for digital forensics data acquisitions.

- Proprietary format
- Raw format
- Advanced Forensic Format

3.What are two advantages and disadvantages of the raw format?

- Advantages:
    1. The data transfer has faster speeds
    2. It can ignore minor data errors and most forensics analysis tools can read it.
- Disadvantages:
    1. It does not contain hash values in the file and needs a separate hash program to run to validate the data.
    2. It might not collect marginal (damaged) blocks and requires a target disk of equal or greater space.

4.List two features common with proprietary format acquisition files.

- It can eliminate the need to keep track of any additional validation files as case data can be added to the acquisition file.

- It can be segmented into smaller volumes without compromising the acquisition output and allow them to be archived to DVD or CD.

5.Of all the proprietary formats, which one is the unofficial standard?

- The unofficial standard is the Expert Witness which is used by Guidance Software EnCase.

7.What does a logical acquisition collect for an investigation?

- Logical acquisition only collects the specific files of interest to the investigation.

8. What does a sparse acquisition collect for an investigation?

- Sparse acquisition collects fragments of unallocated data in addition to the logical allocated data for the investigation.

9. What should you consider when determining which data acquisition method to use?

- The size of the source drive and if it retains as evidence along with the duration of the acquisition and its location.

10. Why is it a good practice to make two images of a suspect drive in a critical investigation?

- To have at least one good copy of the suspect drive, in case of any failures and not compromise the evidence of a critical investigation.

12. With newer Linux kernel distributions, what happens if you connect a hot swappable device, such a USB drive, containing evidence?

- The newer Linux kernel distribution automatically mounts the USB drive, that can alter the data on it.

13. In Linux, the fdisk -l command lists the suspect drive as /dev/hda1. Is the following dcfldd command correct?

```
dcfldd if=image_file.img
        of=/dev/hda1
```

- No, it’s not correct. The command reads the image_file.img file and writes it to the evidence drive's /dev/hda1 partition. The correct command is dcfldd if=/dev/hda1 of=image_file.img.

15. What’s a hashing algorithm?

- It is a program used to create a binary or hexadecimal number that represents the uniqueness of a file or disk.

20. Which forensics tools can connect to a suspect’s remote computer and run surreptitiously?

- ProDiscover Incident Response and EnCase Enterprise are few of the forensics tools which can connect to a suspect’s remote computer and run surreptitiously.

22. FTK Imager can acquire data in a drive’s host protected area. True or False?

- False

Casey et al, “**The Impact of Full Disk Encryption on Digital Forensics**”

Explain at least three ways in which Full Disk Encryption has forced an alteration of the approach toward preserving digital evidence.

Full Disk Encryption is designed for data decryption after a device startup as well as adaption by adversaries. It possesses adaptations in that it does not allow mobile gadgets to discharge(1q), and gettering passwords through keyloggers(2p), court orders as well as extraordinary actions. Full Disk Encryption (FDE) prevents computer recovery of digital evidence as its not possible to circumvent strong encryption without a passphrase or a key. It’s impossible to access data from a computer that has already been shut down. One effective approach to analyze an FDE protected system is to load the forensic duplicate into a virtual environment using tools such as LiveView. This approach is special case where integration has been integrated into the operating system, which can limit the use of other methods. Another approach is to acquire a forensic duplicate of storage media is to boot the evidentiary system from a forensic boot disk and to copy the data to other media.

In contrast to FDE, File-Level Encryption (FLE) is an encryption method, which takes place on the file system level. FDE and FLE are not mutually exclusive.