An Assignment Submitted by

Name of Student

Name of Establishment

Class, Section, Date

Evidence against Acer Tree Service

It is vital that the varieties of daises are categorized and recognized as well as appropriately handled to preserve the veracity of the crucial evidence whereas making sure that important systems are not wrecked in the process. The authenticity of the evidence assembled is essential for determining the eventual outcome of data recovery and criminal cases. When analyzing evidence, the lawyers or legal practitioners should utilize the evidence that is available through the proper management and seizure at the scene (Bunting, 2012). Moreover, another equally crucial step is the debriefing procedure. This process is usually neglected when the forensic investigation is being conducted. Debriefing is important in the forensic investigation since it ensures better efficiency in future investigations.

When conducting a forensic investigation, the chief investigator is supposed to present his briefings using a debriefing form. To ensure all the details are addressed, the chief investigator should take a debriefing form and do the following steps:

- Write a study title.
- Include the name of a person conducting the research and contact information, if pertinent, for follow-up questions (Garrie & Morrissy, 2014).
- Elaborate on what is researched (for instance, aim, hypothesis, and purpose). Use simple English that can be understood easily and avoid jargon.
- Elaborate on how the participants of the forensic investigator were interviewed and grilled;
- Elaborate on why you grilled the participants or suspects when carrying our forensic investigation and whether it was necessary (Garrie & Morrissy, 2014).
- Explain how the results of the of the forensic investigation will be evaluated.

- Provide the participants with an opportunity to withdraw their consent to participate or to withdraw their data from the study (Garrie & Morrissy, 2014).
- Offer the participants or witnesses the opportunity to withdraw their consent to participate in the investigation. This is important because it will ensure the participants will not claim that they were lured to provide information. Foreign investigation where the witness is lured to prove the information is doomed to fail from the beginning.
- If possible, elaborate on the observed or anticipated results so far.
- Offer to avail the study results to the relevant authorities (Garrie & Morrissy, 2014).
- Offer websites or references that people can refer to for further readings in the study.
- Offer a list of resources or references that participants could seek if they become stressed after they have participated in the forensic investigation.

According to the case study of Slatestone Land Development and Acer Tree Service, they face a criminal case. Gogolin (2012) observed that a criminal case is the one that usually involves private disputes between persons or organizations. Criminal cases involve an action that is considered to be harmful to the society as a whole. In the case study discussed, Acer Tree Service faces a criminal case of trespassing and destruction of private property. According to Gogolin (2012), trespassing into the private facility and destroying property is a criminal offense, and it is punishable by law.

In this scenario, Slatestone Land Development contracted a company, Acer Tree Service, to clear land for 18 new homes. After a private owner complained of trees being cut from their property, my company was hired to investigate the communication between the companies above and the new homeowners in the form of emails and text messages dating one month before the

accident as no party involved asserted the responsibility for the decision of cutting the trees in question.

To ensure a successful and edifying investigation is being conducted, the digital forensic incident response and analysis kit will be designed and presented. It is of the utmost importance that proper planning is executed to ensure the integrity of the evidence collected and the validity of the legal system (Garrie & Morrissy, 2014). If the proper procedure and steps are not followed when conducting the investigation, then the case may not have substantial evidence to prosecute the accused. Therefore, it is vital to ensure there is proper planning in place to seal all the loop-holes in the case.

Day 1 - 2

Ensuring Physical Requirements for the Forensic Lab

The first thing I will do is ensure that the lab where the data will be analyzed meets the requirements needed to maintain and secure the integrity of the data. The lab must be secured through installing various security measures; this helps to secure evidence from loss or corrupt damages. Lockers or storage rooms are necessary for safety evidence, and a secure locking system should be in place to ensure maximum safety.

Ideally, the lab facility must have evidence “locker or safe” to ensure and attest to the extent integrity of the evidence gathered with the following minimum requirements:

- The room is small and fitted with genuine floor-to-ceiling.
- The door of the small room is fitted with a reliable lock mechanism; it can be an identification card limited to the authorized users, combination lock, and regular key lock.
- Containers are secured to prevent easy access.

- The small room should have containers that are waterproof; this helps to prevent the evidence from being damaged in the incidences when there are water breakages in the room or from the rain.
- Visitor's log detailing all personnel with the access for daily production purposes (Nelson, Phillips, & Steuart, 2010).
- The small room should be fitted with sound alarm systems that go off when there is a breach of security or attempted burglary. The alarm system is important at night where buglers try to access the room.
- Despite the fitting alarm system, the small room that has evidence should be guarded by the police officer all through to reduce the risk of burglary.

Planning and Preparation

A detailed checklist is crucial to ensure that all aspects are considered and covered during the investigation process. The checklist should entail the methodology and equipment needed for the investigation. Also, the coordination between the personnel involved in the investigation is essential when conducting a forensic investigation. It is important to both members of the investigative team and individuals and organizations being investigated as passwords may be necessary to access vital information relevant to the investigation.

Equipment

A vast array of equipment is necessary for performing a forensic investigation. The choice of the equipment is dependent on the devices being investigated. A checklist of the necessary equipment would include the following:

- Forensic Disk Imager — for performing a bit for bit replica of a device.

- Write Blocker — for converting a device into a read-only mode, making it impossible to tamper with the evidence during the imaging and analysis of the device.
- Cellebrite UFED Mobile Forensic Toolkit — for evidence extraction from mobile devices and storage in the USB stick.
- Dongles — for storage of the collected data or information.
- Faraday Bag or Cage — used for disabling the mobile device's network connection capability.
- Padded Pelican cases — for the transportation of items to the laboratory for analysis. This secures the items thereby ensuring that the integrity of the evidence collected is maintained.
- MacLockPick — for the collection of volatile data from Linux, Windows, and Macintosh operating systems.
- Evidence tape, antistatic bags, tags, indelible ink markers, and labels.
- Pens, field logbook or notebook, and pencils.
- Toolkits – contains key tools necessary for forensic investigation such as screwdrivers, suction cups, gloves cable ties, headlamp.
- PC reference guide.
- Digital camera for capturing live data on screens and the scene.
- Surge protectors, extension cords, and uninterruptible power supplies (UPSs).
- Hub or switch and network cables which can be used to establish a small network on the scene.

- Portable field imaging computer.
- Cables and adapters (Googlin, 2012).

Day 3 - 5

Collection of Data

After the planning, preparation, and checklists have been made, actual seizure and obtaining of the desired data is then done. During this process, it is paramount to secure the scene as this ensures the integrity of the evidence collected and the safety of the personnel involved. The task team is divided into two: one is a search and seizure team, and the other is an entry and security team (Garrie & Morrissy, 2014). The entry team's responsibility is securing the scene and establishing perimeter control as well as creating an ample environment for the other team to discharge their responsibilities. The search and seizure team conducts the search and collection of evidence.

During the collection of data photographs, detailed notes and recordings if necessary will be documented. Personal emails and all text messages from mobile devices will be accessed dating back to one month from the date of the incident (Bunting, 2012). Through the use of Faraday Bags to block wireless capabilities and Cellbrite UFEDs data from cell phones would be extracted and stored on the USB sticks to be further analyzed. Photographs of the screen in the process of accessing emails will serve as a form of capturing volatile data.

Inappropriate evidence transportation creates loopholes that might give rise to evidence tampering and loss of integrity. Once all relevant information is recorded and extracted, all evidence must be properly bagged and tagged for transportation to the forensic lab for the further analysis. The chain of command and recording of personnel transporting evidence are crucial to maintaining the integrity of the investigation (Garrie & Morrissy, 2014). Tagging is imperative

for associating evidence with the case, date, time, location, and seizing personnel. A chain of command ideally refers to a "Paper trail that tracks seizure, custody, control, transfer, analysis, and disposition of all evidence" (Bunting, 2012).

Day 6 - 8

Analyzing and Sorting Data

Once the evidence is transferred to the forensic lab, it is further analyzed. Forensic investigators can sort through the emails and text messages for evidence of the instructions of cutting down the trees marked with the red spray paint. It is vital for the admissibility of any findings that the investigation remains within the confines of the court order, analyzing the emails and text messages solely dating back one month from the date of the incident (Garrie & Morrissy, 2014). Breach of the court orders, in the aspect of evidence extraction and analysis beyond the expected period and underhand analysis of the evidence, leads to evidence inadmissibility.

Day 9 - 10

Digital Forensic Report

After the full analysis and sorting through the data, all relevant information is documented, and a thorough forensic report is written up by the investigator. The report should be extensive and conclusive, in which the details are subjectively outlined. The report would include a detailed account of the steps taken throughout the investigation as well as forensic images captured during the investigative process. The report would include an executive summary detailing the background information leading to the investigation, why a forensic investigator was necessary as well as a list of all personnel involved in the investigation and their respective roles. Once the Forensic Report is completed, the full document will be presented to the opposing counsel for review.

References

Bunting, S. (2012). EnCase computer forensics: The Official EnCE: EnCase certified examiner study guide. Indianapolis, IN John Wiley & Sons.

Garrie, D. B., & Morrissy, J. D. (2014). Digital Forensic Evidence in the Courtroom: understanding content and quality. Northwestern Journal of Technology and Intellectual Property, 12(2), 122-128.

Gogolin, G. (2012). Digital forensics explained. Boca Raton, FL: CRC Press.

Nelson, B., Phillips, A., & Steuart, C. (2010). Guide to computer forensics and investigations. Boston, MA: Course Technology Cengage Learning.