Class: MBA- BIS 523

Date: March 21st, 2024

Teacher: Dr. Susan Helser

Student Name: Muhammad Zainul Zahid

**Introduction**

Following best practices is essential in the field of forensic investigations to guarantee the accuracy and dependability of the data gathered. The purpose of this paper is to present a thorough review of several best practices related to digital evidence collecting and forensic investigations. The report includes best practices for gathering digital evidence from a computer's memory and hard drive, high-level requirements for ediscovery, best practices for interviewing witnesses, guidelines for taking screenshots during an investigation, the importance of documenting a computer's time offset, and procedures for filming a crime scene.

**A) Procedure for Capturing Video of a Crime Scene**

One of the most important aspects of forensic investigations is filming the crime scene. It offers an impartial account of the incident, supporting the process of reconstructing the events and protecting important evidence. The steps listed below describe the ideal methods for taking video:

1. Preparation: Verify that the camera apparatus is operational and set up correctly before starting to record. To ensure that the entire crime scene is captured unhindered, use the right camera angle and position.

2. Record-keeping: First, note the location, time, and date of the surrounding area. With a slow pan, you may catch the full image while concentrating on important details like entry and exit points and points of interest.

3. Systematic Approach: Take meticulous notes at the crime scene, going from one location to another in a methodical fashion. Make sure there is enough light, and concentrate on taking pictures of specifics like bloodstains, tangible evidence, and pertinent items.

4. Storytelling: Talk while the video is being recorded to highlight important details of the scene, such as where the evidence is, what you noticed, and what you did. The video footage is better understood when this narration has been added.

5. custody chain: To ensure that the video recording remains intact as evidence, keep a thorough record of everyone who has access to or handled it.

**B) What to Take Screenshots of During an Investigation**

When gathering digital evidence for a case, screenshots are essential. They offer a still image of the information that was visible on a computer screen at a certain moment. Taking screenshots of the following is crucial when doing an investigation:

1. Take screen grabs of any digital communications, documents, or files that are relevant to the inquiry. Emails, chat logs, documents, and possibly even photos that hold proof fall under this category.

2. To determine the context of the evidence's discovery, document the system settings and configuration. This include taking screenshots of the network setups, installed software, and system properties.

3. Throughout the investigation, take screenshots to record any error messages, alerts, or other warnings that the system may display. Error messages could be important hints or signs of harmful behavior.

**C) The Significance of Recording a Computer’s Time Offset**

Keeping track of a computer's time offset is essential to preserving the accuracy of digital evidence. The time offset is the discrepancy between the actual time and the system time of the machine under analysis. It matters for the reasons listed below:

1. By keeping track of the time offset, investigators can precisely correlate events that occur on various systems or devices. Time stamp inconsistencies may be a sign of evidence tampering or manipulation.

2. Creating a precise chronology of events is crucial to forensic investigations. The time offset makes it easier to reconstruct chronological activity sequences by assisting in the alignment of timestamps from various sources.

3. Investigators can verify the timing of actions or events captured on the computer by recording the time offset. As a result, digital evidence used in court has greater evidentiary value.

**D) Best Practices in Collecting Digital Evidence from a Computer’s Memory and Hard Drive**

To retain the quality and dependability of the data, digital evidence collection from a computer's memory and hard drive necessitates strict adherence to best practices. Here are three recommended procedures:

1. To gather erratic data from the computer's memory, whenever feasible, perform live forensic analysis. This entails gathering data without affecting the system's current state from open network connections, active processes, and system logs.

2. Using specific instruments and methods, make forensic pictures of the computer's hard disk. By guaranteeing a bit-by-bit duplicate of the complete storage device, forensic imaging preserves the original data for analysis without compromising the integrity of the evidence.

3. Keep thorough records of the handling, storing, and transferring of all digital evidence that has been gathered, including the data from the computer. Establishing the integrity and admissibility of the evidence in court cases depends heavily on this paperwork.

**E) High-Level Requirements for Ediscovery**

The identification, preservation, and gathering of electronically stored information (ESI) for legal reasons is known as electronic discovery, or ediscovery. There are three primary prerequisites for eDiscovery:

1. Throughout the discovery process, take steps to maintain pertinent ESI in its original format to guarantee its validity and integrity. This entails putting legal holds on pertinent data and stopping ordinary data erasure procedures.

2. Create strong search and retrieval tools to find and get pertinent ESI quickly from large databases. Employ sophisticated search algorithms and indexing strategies to find relevant content more quickly.

3. Keep track of user actions, file attributes, timestamps, and other metadata related to electronic documents and files. Establishing the chain of custody and evidentiary value requires metadata, which gives the ESI important context and authenticity.

**F) Best Practices for Interviewing Witnesses**

One of the most important parts of forensic investigations is interviewing witnesses, which calls for a methodical and moral approach. Here are three recommended procedures:

1. Examine case documents, pinpoint important areas of investigation, and create a structured interview strategy in order to fully prepare for witness interviews. Prepare for probable obstacles and devise tactics to extract pertinent data.

2. Employ active listening strategies to ensure that witnesses are given uninterrupted time to completely convey their story during witness interviews. Keep an eye out for both verbal and nonverbal clues, and use open-ended inquiries to elicit thorough answers.

3. Refrain from using suggestive or leading questions during the interview process, and instead, remain objective and non-coercive. Let the witness tell you what they know voluntarily, and don't impose your own prejudices or presumptions.

**G) Best Practices for Testifying as an Expert Witness**

Proficiency in communication and in-depth knowledge of the legal procedure are prerequisites for testifying as an expert witness. Here are three recommended procedures:

1. Read through case materials, expert reports, and pertinent laws or regulations in order to thoroughly prepare for your testimony. Get familiar with the topic and prepare for any queries that lawyers could have.

2. Use language that the jury and judge can easily grasp to convey complicated technical facts in a clear and exact manner. Steer clear of jargon and technical terminology that could offend or confuse audiences who aren't experts.

3. Throughout your testimony, be objective and impartial while presenting the facts and your opinions in accordance with reliable scientific methods and principles. Steer clear of endorsing a specific result and concentrate on offering trustworthy professional analysis.