|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2022/23) Semester 4/6 | Week 2 |
| Tutorial 2 |
| **Investigative Process** | |

**OBJECTIVES**

After completing this topic, you should be able to

1. Briefly describe the forensic investigative process
2. Explain the guidelines involve when performing first response at crime scene
3. Explain the purpose of maintaining “chain-of-custody” of evidences.

Q1. List any 5 items that a First Responder needs at the crime scene. Briefly describe their usage.

Forensic software - e.g. Encase to acquire/collect evidence

Live response tools - To acquire volatile content

Large capacity drive - to store image files

Write-blockers - to prevent contaminating original evidence while imaging

Camera - to capture the investigation scene

Or any correct answers

Q2. Explain the reasons for recording and photographing the scene. How can this be done appropriately?

It is important to know the initial state of the scene before anything is done. This is to protect the first responder against any accusation of contaminating the evidence

Before anything is touched or removed, the scene is recorded through a combination of field notes, sketches, video, or still images. Once the scene is recorded to show how things were initially found, the team begin their search-and seizure process.

Q3. During the acquisition of lower-end computer (such as desktop, laptop etc.), if the computer is running, why is it sometime advisable to pull the power cable from the computer rather than shutting it down?

The reasons for pulling the power cable include:

﻿

* Any script the suspect has written that should execute upon shut-down doesn't get a chance to run.
* Temporary word-processing and other interim files remain on the hard drive, whereas they might get deleted if the software applications shut down more gracefully.

Q4. When shutting down a computer, what information is typically lost?

A. Data in RAM

B. Running processes

C. Current network connections

D. Current logged-in users

E. All of the above

Q5. During evidence acquisition, explain why is it important to ensure that the examiner’s storage device is forensically clean.

If the examiner’s storage device is not forensically clean, there might be traces of previous content and resulting in evidence file being contaminated.

Q6. Explain the purpose of maintaining “chain of custody” in any forensic investigation.

The term “chain of custody” refers to documentation that identifies all changes in the control, handling, possession, ownership, or custody of a piece of evidence. You need to be able to trace the route that evidence takes from the moment you collect it until the time it is presented in court or at a corporate briefing.

This document contains the basic information about the parties involved, details about the media such as brand, type, serial number, and other basic information. A fully detailed chain of custody report is necessary to prove the physical custody of the piece of evidence and show all parties that had access to said evidence at any given time.

Q7. Explain the purpose of bagging and tagging of evidence.

Bagging - protects against contamination and tampering

Tagging – provides a means of associating the attached and bagged evidence with a particular location, time, date, case, event, and seizure agent. It provides a first link in the chain of custody of the evidence.

Q8. Private data for more than 90,000 customers of CT bank’s credit-cards subsidiary has been stolen and unlawfully resold. *“The theft of the customers' data was not carried out by hackers, but rather by parties who had been given access to the data legitimately and abused their trust”*, a source familiar with the situation told the reporters.

As a private forensic investigator, you have been contracted by CT bank to investigate the case. You have been given permission to perform search and seizure at CT bank’s staff office.

1. You have identified the suspect and wished to perform search and seizure at the suspect’s house without prior notice. Which important document should you obtain before entering the crime scene?

Search warrant to be issued.

1. Suggest a reason for performing search and seizure at the suspect’s house without prior notice.

To prevent the suspect from damaging the evidence and rendering it useless if the suspect knows of the investigation.

- End -