|  |  |
| --- | --- |
| **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 involved when performing first response at crime scene
3. Explain the purpose of maintaining “chain-of-custody” of evidence.

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

Latex Gloves – Avoid leaving fingerprints, hairs, fibers, and body tissues on the computer evidence

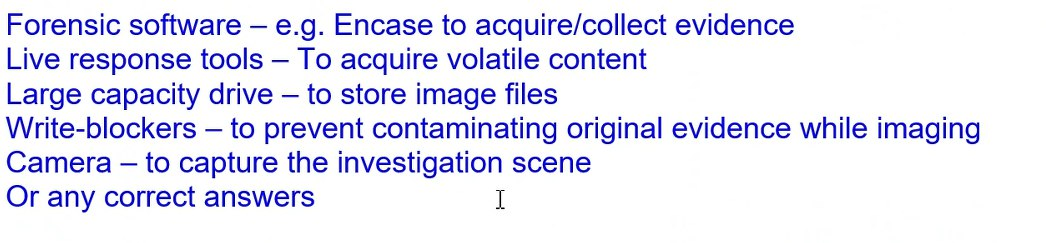
Camera – To doument the evidence and its surroundings to ensure integrity of evidence

Anti-static wrist straps – Prevents static from the FI to damage the computer evidence when handling evidence.

Write-blockers – Allows the FI to create a forensic image of the computer evidence while preserving the integrity of the evidence

Magnifying glass – To read words related to the crime that are in small font

Ans:



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

Reason being to ensure chain of custody which beings when evidence is collectedBy documenting the initial state and condition of the evidence at the scene, it can be proven in court that the evidence used are in pristine condition, thereby making it credible and accepted by the court as the integrity of the evidence is shown.

This can be done by recording the condition of computer system, storage media, electronic devices etc, any potential evidence. Photos of the evidence from different angles and photos of the entire site are good ways to document the scene.

Ans:

Text

Description automatically generated

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 shutdown process itself writes many entries to activity log files and changes the state of the evidence. This might render the evidence inadmissible in court. Furthermore, the suspect computer could run procedures that cleanses log files on shutdown, resulting in loss of crucial evidence.

Graphical user interface, text, application

Description automatically generated

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

Ans: E (B,C,D are all data that is stored in RAM)

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, it might modify the original evidence which would break the chain of custody as the integrity of the evidence is lost

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

Maintaining chain of custody is important as it ensures that the integrity of evidence is not compromised. By having a complete chain of custody, it ensures that the evidence is in pristine condition allowing it to be used in court.

Text

Description automatically generated

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

Bagging protects the evidence against contamination and tampering.

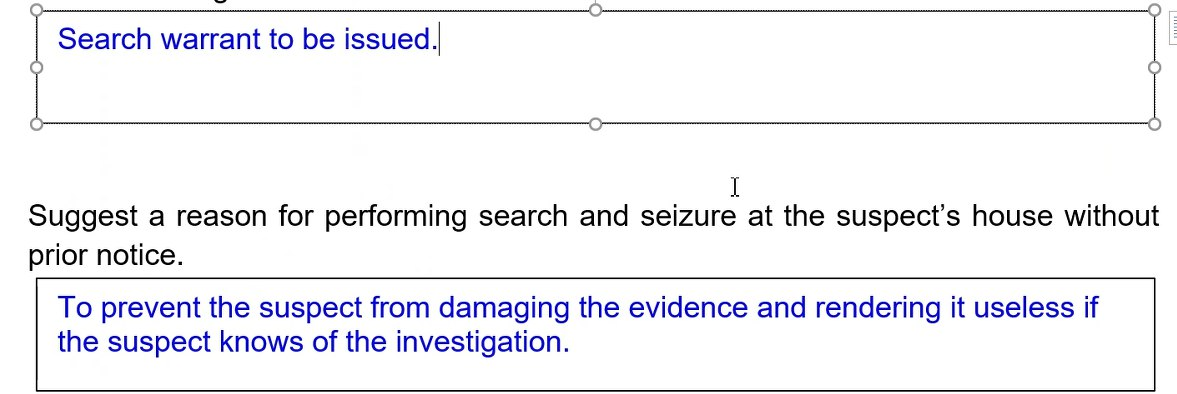
Tagging provides a mean of associate the attached and bagged evidence with a particular location, date, time, case, event, and seizure agent. It provies a first link in the chain of custody of the evidence.

Graphical user interface, text, application

Description automatically generated

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?

A search warrant to the suspect’s house.

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

Allows us to acquire evidence from a suspect’s machine without giving the suspect prior notice. With prior notice, the suspect might damage the evidence and render it useless is the suspects knows of the investigation.

- End -