|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2022/23) Semester 4/6 | Week 1 |
| Tutorial 1 |
| **Computer Forensics & Digital Evidences** | |

**OBJECTIVES**

After completing this topic, you should be able to

1. Explain the need for duplicating the evidence before investigation.
2. Briefly describe the 3 stages involved in a computer forensic investigation

**ACTIVITIES**

Q1. In computer forensics, why is it important that the acquired evidence be duplicated before investigation can take place?

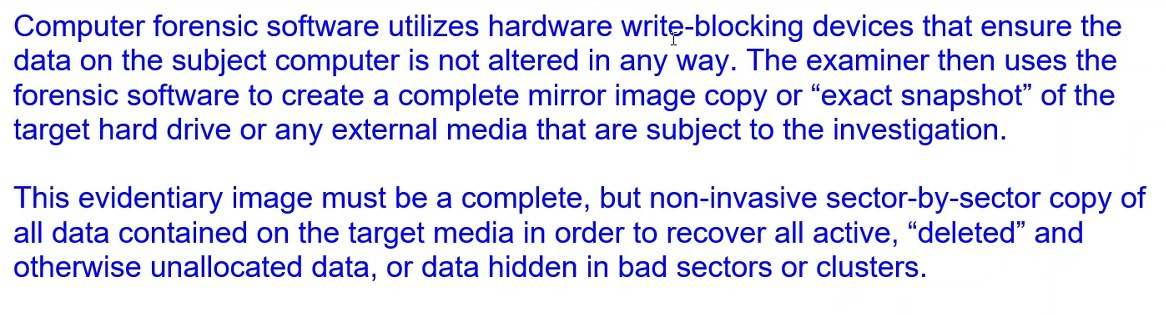
The evidence must be duplicated to preserve the integrity of the original evidence. Should the forensic investigator (FI) analyze and modify the original evidence, it compromises the integrity of the evidence as the FI might make changes to the original evidence unknowingly. This would cause the evidence to become inaccurate and unsuitable for use in court.

Q2. How is the duplication of evidence carried out?

Duplication of evidence is carried out using the forensic image of the suspect computer system. A forensic image is a copy of original evidence generally collected by a tool that performs bit-level copying from one location to another. Generally, there will be 2 duplicates of the original evidence and there are multiple ways to duplicate the evidence. The 3 ways are, complete disk, partition, and logical.

To perform the duplication, ensure that the computer system has been turned off and booteed to a forensic imaging environment, or that the disk has been plugged into an imager or examination workstation. A write blocked must also be used to ensures data integrity as it prevents the evidence from getting corrupted should the workstation have any viruses.

Ans:



Q3. Briefly describe the 3 stages involved in a computer forensics.

1. Evidence Acquisition

This is the stage where the FI starts to investigate by identifying the evidence and its location.

1. Investigation and Analysis

This is the stage where the FI extracts (duplicates) the evidence found and analyzes the evidence as well as interpret his findings.

1. Report Findings

This is the stage where the FI documents his findings from his investigation from the beginning to the end.

Ans:

Text, timeline

Description automatically generated

Q4. What are the common evidences a Forensic Investigator should look for when investigating a computer crime?

Digital evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.

Examples of these evidence include:

* Email
* Digital Photographs
* Word processing documents
* Instant message histories
* Internet browser histories
* Content of Memory (RAM)

Ans:

Graphical user interface, text, application

Description automatically generated

Q5. What are the main differences between active and latent files?

Active data is data that can be seen and used by the OS, while latent data is data that exists despite being deleted. It also requires a specialized tool to be used to recover it.

Ans:

Text

Description automatically generated

Q6. Your client has engaged your service to perform a forensic investigation on a case that involves one of its employees suspected of misusing company data for personal gain. The suspect was alleged to have been sending company Excel worksheets that contain confidential customer quotation information to his personal email address.

Your colleague, John, has identified and seized the suspect’s hard disk from the client’s office. He took a picture of the scene and recorded the specifications of the hard disk. He transported the seized evidence to the office and stored it in Cabinet 1 of Lab Alpha. John has also performed imaging/acquisition using forensic workstation and stored the evidence file on the server located in the lab. You retrieved the evidence file from the server to perform your investigation using EnCase.

Answer the following questions based on the above scenario.

1. The forensic investigation process follows the 3 stages below. For each of the following stages, highlight ONE relevant step that was performed in the above case.

Graphical user interface, text, application

Description automatically generated

1. Evidence Acquisition

John identifying and seizing the suspect’s hard disk.

1. Investigation and Analysis

John performing imaging using the forensic workstation to duplicate the evidence.

1. Documentation and Reporting

John taking a picture of the scene and recording the specifications of the hard disk.

1. John connected the suspect’s hard disk to the forensic workstation directly using a cable to perform imaging/acquisition. Identify ONE mistake he has made and explain how this mistake could affect the investigation. With the aid of a well-labeled diagram, illustrate the correct setup for performing imaging/acquisition.

|  |  |  |
| --- | --- | --- |
| [http://t1.gstatic.com/images?q=tbn:ANd9GcQZRlLuzuXLonnVoMUszY0Mj6dYF8-Dgjni2FCgfu6zBJerfWg0Nw](http://www.google.com.sg/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=0CAgQjRw&url=http://en.wikipedia.org/wiki/Western_Digital&ei=KyZ4VI-WH5HjuQSVh4CADQ&psig=AFQjCNGMoWU3icc390ZSxmniu6LPXdLQjg&ust=1417246635600301) | Cable | [Arbeitsplatz](http://thumbs.dreamstime.com/z/arbeitsplatz-14284156.jpg) |

Suspect’s Hard Disk

Forensic Workstation

The mistake John made was not using a write blocker. A write blocker is used to prevent source media from being modified. Sitting in the connection between a computer and a storage unit, it monitors the commands that are being issued and prevents the computer from writing data to the storage device. Without a write blocker, should the forensic workstation have any viruses or software that can modify the suspect’s hard disk, it could corrupt the data in the hard disk. This is a compromise of the integrity of the evidence.

Text, letter

Description automatically generated

Diagram

Description automatically generated with medium confidence

- End -