|  |  |
| --- | --- |
| **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?

Q2. How is the duplication of evidence carried out?

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

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

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

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.
2. Evidence Acquisition

1. Investigation and Analysis

1. Documentation and Reporting

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

- End -