Digital Forensics Investigation: Discovering Digital Evidence

5

By the end of the practical session, the students should be able to:

- Identify the potential digital evidence based on the incident case
- Implement the investigation processes in identifying Who, What, When, Where and How for an incident case
- Present the investigation findings

This lab will cover topics on understanding how to execute the investigation process in order to discover the evidence of the incident cases.

5.0 Introduction

Digital forensic investigation is defined as the process of identifying, collecting, tracing, mapping, documenting and presenting the incident traces as digital evidence which may be used in the court of law. Hence, the aim of this lab is to test the student's capability on the investigation skills (including on using the forensics tool), interpretation skills on analysing the incident or crime and presentation skills on describing and presenting the findings from the analysis (evidence).

Lab 5.1: Investigating Incident Case

5.1.1 Requirements

In this task activities, use suitable forensics tool (choose one) to extract and analyze an image file. The requirements of this task is shown in Table 1.

Table 1: Requirements

Tool (e.g.)	**Image**
FTK Toolkit	Thumbdrive.E01
OSForensic	Washer.E01

Notes: Please download the tools and images from your lecturer's PC.

5.1.2 Task

1. Do investigation in Group (5/6 members). Refer to group for Assignment 1.

2. Do investigation based on the image provided. Your team should identify and explain the following:
    a. What is the case (nature of case)?
    b. What is evidence that support the case?
    c. How you investigate?
    d. How the crime is happened?
    e. Discuss the scenario
    f. Is there any relationship between both images provided? If yes, discuss.

3. You team need to provide the presentation slide and present the findings from the investigation process.