

Lab 1 : Introduction To Digital Forensic

Group Members:

|  |  |
| --- | --- |
| Name | Matric No |
| MUHAMMAD RIFQI BIN RAMLAN | B032020028 |
| MUHAMMAD IKMAL BIN MAZLAN | B032020002 |
| NUR AFIQAH BINTI SHAHRULNIZAM | B032020023 |



**Lab 1.1: Digital Forensic Investigation Process**

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



Explain the Digital Forensic Investigation process

Respond to a case using the Digital Forensic Investigation process

This lab will cover topics on Digital Forensic Investigation process.

# 1.1.1 Introduction

Digital Forensic is an area in forensic science that focuses on the recovery and investigation of evidence found in a digital devices, normally related to computer crime. Digital forensic define the process of searching and uncovering electronic data. The objective of digital forensic is to define a structured investigation process on digital medium by performing collecting, identifying and validating the digital information for the purpose of reconstructing past events. The structured investigation is perform in order to make sure all the evidence found can be use and accepted in a court of law, though digital forensics can also be used in other instances.

There are 7 Stages of Digital Forensic Investigation in tracking computer crime, the stages are

1. Identifying the crime
2. Gathering the evidence
3. Building a chain of custody
4. Analysing the evidence – use duplicate one
5. Presenting the evidence
6. Testifying
7. Prosecution

## 1.1.2 Case Study 1 on a Computer Crime

**Case Study 1:**

Azcam Sdn Bhd is a renowned Software house company and has 35 employers which 8 of them are involving in a new mobile operating system project that will revolutionize the mobile industry. Unfortunately, 2 months before the launching a similar source code of the Azcam new OS’s kernel is publicly available on the GitHub page, uploaded by a user known as Julias Maxim. An internal investigation found that there is no external security breach indicator on the main server that stored all the project source code. Azcam’s Chief Technical Officer has lodged a police report on the incidents and as the investigator assigned to this case you are responsible to execute the investigation.

## Tasks

1. Identify the crime that has been taken place in case study.

The crime would likely to be a copyright infringement. The attacker which known as Julias Maxim uploaded the project source code into GitHub 2 months before the launching for his own fame and benefit. The suspected may come from one of the 8 people that are involved in the new mobile operating system project.This is said because the 8 of them have access to the project source code.

1. Once the crime is identified, planned your strategy to solve the case.

First, collect all evidence as much as we can. The digital and physical evidence would be the project source code itself and the computer that they are using. Before proceed to the analysis phase, perform an imaging for the project source code would be the right thing to do. Analyse the evidence and information thoroughly that are gathered from the investigation. Present the evidence to the court and elaborate the conclusion that have been made based on the investigation.

1. By applying the digital forensic investigation process, write a short report on how the study case will be handled.

The attacker(Julias Maxim) uploaded the project source code into GitHub 2 month before the launch of a new mobile operating system project. This crime can be identified as copyright infringement. 8 from 35 employees worked at Azcam Sdn Bhd are responsible for the project. The impostor may come from the eight employees as stated. Before gathering the evidence and information, permission need to be ask from Azcam Sdn Bhd first. Next, collaborate with GitHub company to get more details about an account named “Julias Maxim”. The digital and physical evidence would be the project source code itself and the computer that they are using. After that, build a chain of custody for the evidence that have been gathered so that the originality will be preserved. Analyse the evidence using the duplicate one and important information that have been collected. Based on the evidence and information, make the best conclusion throughout the investigation. Then, present the evidence to the court and an explanation about the concluded conclusion during the testifying and prosecution phase.

## 1.1.3 Case Study 2 on a Computer Crime

**Case Study 2:**

Ahmad Faizul just logged in to his CMBT online banking site and found that his account balance is RM 0.00. On checking the online banking statement, Faizul found out that his money from the account has been used to purchase a few items from Lazada.com.my and he is not aware of purchasing those item. Another information that has caught Faizul intention is that the last access to his account is a day before and found to be from an IP address of his office. Prior to the event Faizul has access his account from an email send by the CMBT bank which requires him to check his account security from the link given in the email.

Hence, Faizul believe his account has been hacked through the email. In order to get his money back Faizul has lodged a complaint to the CMBT Bank and lodge a police report on the loss of his money. As the Forensic team of the CMBT you need to work together with the police investigator to investigate the case.

## Tasks

1. Identify the crime that has been taken place in case study.

The crime is most likely to be a form of email phishing. A hacker might pretend to be the CMBT Bank and sent malicious link along with the email.

1. Once the crime is identified, planned your strategy to solve the case.

First investigate Faizul’s computer in his office and find out whether Faizul’s computer was accessed without his knowledge. Next, investigate the content of the email sent to Faizul and the sender’s email address. Analyze and gather information on the site directed by the link and contact the CMBT Bank for further information.

1. By applying the digital forensic investigation process, write a short report on how the study case will be handled.

First, we identify the crime that has taken place which is email phishing. Next, gather the analyze Faizul’s computer and the content of the email. Preserve a copy of the email and Faizul’s computer for to ensure untampered evidence. Duplicate Faizul’s interaction with the email’s link in a secure environment. Present the information gathered to the CMBT Bank and police. From the evidence, make conclusion on who’s responsible for the phishing attack. Once the hacker has been found, the prosecution process will then be executed.

# 1.1.4 Self-Review Questions

1. List the number of personal and responsibility of each personal in a digital forensic investigation team?
2. Forensic Leader

The person in charge who is responsible for coordinating between the three teams and responsible of achieving some other responsibilities

1. Physical Crime Scene Team

Responsible for recognition, collection of physical evidence, preservation, transportation and storage of electronic evidence from the physical crime scene.

1. Laboratory Examination Team

Responsible for the digital crime scene or secondary scene.

1. Courtroom Team

Responsible of reporting and presenting the case, experienced expert witness testimony provided in courts, ensure the chain of custody during all the previous phases and also responsible for the closure phase.

1. Define what is a public and private case?

Public cases involve government agencies responsible for criminal investigations and prosecution and organizations must observe legal guidelines. Private cases deal with private companies, non-law-enforcement government agencies, and lawyers and aren’t governed directly by criminal law or Fourth Amendment issues.

1. State the Malaysian Cyberlaw ACT that related to the two case study above?

I. COPYRIGHT ACT (AMENDMENT) 1997

II. COMPUTER CRIME ACT 1997