Introduction to Digital Forensic 1

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.
2. Once the crime is identified, planned your strategy to solve the case.
3. By applying the digital forensic investigation process, write a short report on how the study case will be handled.

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.
2. Once the crime is identified, planned your strategy to solve the case.
3. By applying the digital forensic investigation process, write a short report on how the study case will be handled.

1.1.4 Self-Review Questions

1. List the number of personal and responsibility of each personal in a digital forensic investigation team?
2. Define what is a public and private case?
3. State the Malaysian Cyberlaw ACT that related to the two case study above?