Digital Evidence Retrieval and Forensic Analysis on Gambling Machine

Pritheega Magalingam¹, Azizah Abdul Manaf², Rabiah Ahmad¹, and Zuraimi Yahya³

¹Centre For Advanced Software Engineering, ²College Science and Technology, ³Electrical Engineering, Universiti Teknologi Malaysia, Int’l Campus, Jalan Semarak, Kuala Lumpur
mprithee@gmail.com, {azizah07, rabiah}@citycampus.utm.my, zuraimibinyahya@yahoo.com

Abstract. Hardware forensic analysis involves the process of analyzing digital evidence derived from digital sources. The analysis is done to facilitate and prove either the device is used to commit crime, whether it contains evidence of a crime or is the target of a crime. Gambling machines serve as the main source by which illegal games are conducted. This paper presents a method for retrieving information from a seized gaming machine, along with an analysis of the interpreted information to prove that the gaming machine was used illegally. The proposed procedures for the gambling machine forensic process will be important for forensic investigators (e.g., the police or private investigators), as they will assist these individuals in the digital forensic evidence analysis necessary to produce evidence relevant to illegal gambling.

Keywords: digital forensic, forensic analysis, gambling machine, information retrieval, digital evidence, interpretation, string search.

1 Introduction

Any device that is used to store, calculate or compute programs can provide different ways for criminals to commit crimes. Such a device can serve as a convenient storage mechanism for evidence and, in certain cases, can be the target of damage threatening the confidentiality, integrity and availability of information and services. Computer forensic analysis focuses on the extraction, processing and interpretation of digital evidence.

The major challenge for the police force in Malaysia is to prove that the gaming machine operated in cyber cafes is illegal. The current gaming machines contain sophisticated computer software and hardware. Locating relevant digital evidence to serve as technical proof becomes a difficult task, and the police require the expertise of forensics. Producing this evidence in court requires a detailed analysis of the parts of the gaming machine hardware that store data and programs, a method for extracting data from non-volatile memory, and an examination of the data to find reliable evidence.
2 Background Problem

Evolving technology has allowed independent computers to serve as gambling machines, in which where the highly sophisticated, computer-controlled machine controls all functions from accepting coins to initiating play to determining game-winning combinations. Some gaming machines are built with a motherboard programmed to provide dual functions thereby allowing players to use for amusement or gambling games. Switching machine mode is common among players in order to prevent police from discovering illegal gambling [1].

A non-volatile EPROM (Erasable Programmable Read Only Memory) chip is the core of a machine which controls the major activities [1]. Old machines are turned into amusement machines with new EPROM chips. If the EPROM used is programmed for gambling, then the device operates illegally. A gambling machine exhibit, serving as evidence in physical form brought before the court, can provide a vast challenge in a computer crime investigation. Unfortunately, there are currently insufficient procedures for the identification of CPUs containing games related to gambling because it is difficult to visually differentiate a normal operating system from a windows system running a gaming event.

This paper analyzes the problem and provides guidelines to determine whether an exhibit contains evidence. It also proposes evidence acquisition and evidence examination procedures through hardware forensic analysis conducted on gaming machine manually assembled by an illegal owner and seized by the Royal Malaysian Police Force. Figure 1 shows a seized wooden gaming box that resembles a CPU and the identified EPROM embedded in the printed circuit board.

3 Computer Forensic Research

This paper focuses on computer misuse and the method of examining an electronic machine to acquire digital evidence. Unlicensed gaming devices also fall into the category of computer misuse when they are illegally used to conduct gambling [2]. Research has found that potential components of an electronic device should be traced