A New Digital Evidence Retrieval Model for Gambling Machine Forensic Investigation

Pritheega Magalingam(1), Azizah Abdul Manaf(2), Rabiah Ahmad(3), and Zuraimi Yahya(4)

(1) Centre For Advanced Software Engineering, mprithee@gmail.com
(2) College Science and Technology, azizah07@citycampus.utm.my
(3) Centre For Advanced Software Engineering, rabiah@citycampus.utm.my
(4) Faculty of Electrical Engineering, Universiti Teknologi Malaysia, International Campus, Jalan Semarak, 54100 Kuala Lumpur, zuraimibinyahya@yahoo.com

Abstract - Gambling machines serve as the principal means by which illegal games are conducted. This paper presents a method for retrieving information from seized gaming machines along with an analysis of the interpreted information to prove that the gaming machine was used illegally. The process is illustrated using a machine seized from a suspected illegal gambling operation. A detailed gambling machine forensic procedure provides important assistance to forensic investigators (e.g., police or private investigators) in gathering evidence relevant to illegal gambling.

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

1. Introduction

Any device used for calculation, computation, or information storage may be used for criminal activity, by serving as a convenient storage mechanism for evidence or in some cases as a target of attacks threatening the confidentiality, integrity, or availability of information and services. Computer forensic analysis focuses on the extraction, processing, and interpretation of digital evidence.

A major challenge for police forces is determining whether gaming machines in cyber cafes are being operated illegally. Modern gaming machines contain sophisticated computer software and hardware, and locating relevant digital evidence becomes a difficult task requiring the assistance of forensics experts. Presenting this evidence in court requires a detailed analysis of the gaming machine hardware used to store data and programs, a method of extracting data from non-volatile memory, and an examination of the data to obtain reliable evidence.

2. Background Problem

Technological evolution has enabled computers to serve as gambling machines in which all functions are electronically controlled. Some
gaming machines are constructed with a mother-
board programmed to provide a dual function, al-
lowing players to use the machine for amusement 
or for gambling. Switching the operating mode is 
a common method of preventing the police from 
discovering illegal gambling [1].

The major functions of the machine are con-
trolled via software encoded on a non-volatile EPROM 
(Erasable Programmable Read Only Memory) chip [1]. 
Older machines may be converted into amusement 
machines by inserting new EPROM chips. However, 
if the EPROM is programmed for gambling functions, 
the device may be operated illegally. A gambling 
machine serving as physical evidence in a court case 
represents a significant challenge in a computer 
crime investigation. Unfortunately, the current pro-
cedures for identifying CPUs containing games relat-
ed to gambling are inadequate because it is difficult 
to visually differentiate a normal operating system 
from a system running a gaming event.

This paper provides guidelines for determin-
ing whether confiscated computer devices con-
tain useful evidence and proposes evidence acquisition and examination procedures. The 
procedures were employed in a hardware forensic 
analysis conducted on a gaming machine manu-
ally assembled by the owner and seized by the 
Royal Malaysian Police Force. Figure 1 contains 
photographs of the seized gaming box and the 
EPROM installed in the printed circuit board.

3. Computer Forensic Research

This paper focuses on computer misuse and 
methods of acquiring digital evidence from elec-
tronic machines. Unlicensed gaming devices 
fall into the category of computer misuse when 
they are used to conduct illegal gambling [2]. The 
components of an electronic device should be 
traced in order to obtain investigative informa-
tion [3], and the memory should be analyzed. Several previously published memory acquisition 
procedures for microprocessor-based devices are 
described below.

3.1. Forensic Data Recovery from Flash 
Memory

Marcel Breeuwsma et al. (2007) claimed that 
most forensic tools currently on the market 
perform logical data extraction and are not 
capable of retrieving all possible information from 
the storage medium. Three methods for low-level 
information acquisition from flash memories 
were introduced, including flasher tools, the use 
of an access port for testing and debugging, and 
a semi-invasive method in which flash memory 
chips were physically removed from the printed 
circuit board [4]. The paper also described the 
steps necessary to translate the extracted data to 
the file system level. Our exhibit falls into the 
third category, since the seized wooden gaming 
box contained a printed circuit board with no 
means for external connections.

3.2. Memory Acquisition Procedure for 
Digital Investigation

A hardware-based procedure for information 
retrieval from volatile memory was described by 
Brian D. Carrier and Joe Grand (2004), who also 
claimed that existing data acquisition methods are 
unreliable because they write back to the memory 
and use only certain tools to obtain obvious data
(leaving the rest of the memory unanalyzed). Their solution was to install a Peripheral Component Interconnect (PCI) expansion card before the crime occurs. The back of the card is equipped with a switch to activate the PCI controller on the card. Once activated, the card takes control of the PCI bus and is able to access memory without relying on the operating system or system memory for storage. It will copy the exact contents of the volatile memory to an external non-volatile storage medium [5].

3.3. Xbox Forensics

Burke and Craiger [20] reported an easy and non-intrusive method of data extraction to identify whether hackers have compromised an Xbox by installing non-approved software to run an operating system other than the one originally installed. The author used Linux to conduct the Xbox analysis, and the output was examined line by line. The use of the string utilities and hex viewer in Linux provided a good starting point to determine if evidence existed on the partition in ASCII form and helped to describe the binary data in the retrieved evidence.

3.4. Forensic Investigation of Nintendo Wii

The Nintendo Wii is a gaming console offering 256MB of flash-based memory that can be wirelessly connected to the internet. Dr. Benjamin Turnbull [7] aimed of this investigation was to record all activity to ensure the system was unaltered. This gaming console features automated logging, which records information including the game being played and the duration of play. The investigation method involved activation of an external logging mechanism or recording device, determination of the current unit time in the system settings, and identification of the messaging system and the extent of system use, i.e. notes sent between individuals on a particular date [7].

3.5. A Methodology for Forensics Analysis of Embedded Systems

Kyung-Soo Lim and Sangjin Lee [21] introduced a two-phase analysis method for embedded systems such as Microsoft Xbox, Sony Playstation 3, Nintedo Wii, and GPS navigation units. In both phases, the authors compare the target system information with information provided by the manufacturer to identify illegal activities. In our case, the seized gaming machine was not built by a specific manufacturer but by the owner of a cyber café, and specific examination of the chips connected to the existing microcontroller was essential.

4. Forensic Analysis Design

In order for a gaming machine to be classified as an illegal gambling machine, the evidence must support certain facts, and the following three relevant pieces of information must be present [10]:

(a) A betting mechanism that allows the raising of various sums of money depending on the outcome of the game,
(b) A random number generation process to establish the game results, and
(c) A payout value displayed to winning players.

The information may be extracted from the EPROM program memory embedded in the gaming machine microcontroller[11]. Relevant information concerning this process was gathered from optimal practices as well as standard operating procedures. A proposed evidence retrieval method is diagrammed in Figure 2.

5. Implementation and Results

5.1. Evidence Acquisition

Fortunately, in our case the EPROM was inserted into a chip socket and could be gently removed from the microcontroller board using forceps. This is a better method than de-soldering, since the heat required for de-soldering may damage the memory chip. The test may only be performed on non-encrypted EPROMs. The type of EPROM being examined was the NM27C256Q, and the ChipMax reader was selected for program extraction [13].
5.2. Evidence Examination Procedure

5.2.1. Process

The ChipMax reader depicted in Figure 3 was used to read the EPROM memory. The EPROM was placed in the reader socket and two copies of the EPROM contents were saved in binary (".bin") form. One copy was kept as original evidence and the other was used during the forensic examination. A hash value generated from both copies was used to demonstrate that the evidence had not been modified.

5.2.2. Interpretation

Reverse engineering is the process of translating the object code into understandable source code [12]. Several software tools were identified and tested for use in disassembly and conversion to source code, including the Barleywood Z80 Simulator, Z80 Simulator IDE 8080, and Z80 Assembler Disassembler Suite. The most suitable tool in this case was the Z80 Simulator IDE. Representative output of the disassembly process appears in Figure 4.

6. Output Analysis

The output following the disassembly process is an assembly language program, which in our

Fig. 2. Gambling Machine Forensic Analysis Guidelines

Figure 2 lists the steps involved in digital forensic investigation, emphasizing the evidence analysis phase. This phase is divided into evidence acquisition and examination activities, and appropriate guidelines are mapped onto each main step.

Fig. 3. EPROM in ChipMax Reader Socket[13]

Fig. 4. Output of disassembly process
case study was written using the Z80 instruction set. Each command in the program was analyzed to facilitate understanding of the program function [8]. In particular, the program analysis sought to identify common gambling functions such as a random number generator, betting function, and payout mode. Several factors hampered the identification of subroutines involved in the gaming operation, including frequent repetition of the Z80 instruction pattern and an inability to determine the starting instruction point in the absence of inputs from the actual gaming hardware. For this reason the assembly program was trapped in a loop for almost 12 hours.

In order to circumvent these problems, we developed an alternative analysis method. Data related to the current game or to the last game played could provide the game sequence and output [14]. The machine code retrieved from the EPROM was therefore converted into readable plain text to enable string searching using a hex editor.

During the machine code analysis, a group of symbols, numbers, and letters related to gambling operation were identified. These lines were collected to determine their actual meaning, leading to the discovery of additional gambling terms:

(a) **ALL *2..A900 W198..GAME PLAYED**

“ALL” in the statement shows that the player chose to play all games. This means that the machine will rapidly display all of the games available based on the player’s purchased ticket [15].

(b) **DOUBLE UP GAME**

The term “double-up game” indicates that the player chose to play [16] a second time using a wager amount equal to the value played in the first round. “Wager” indicates the amount the player paid to play the game. Wagers typically take the form of a token, coin, or currency note.

(c) **POINTS WON..NUMBER OF WON..NUMBER OF LOST..CREDIT..IN..OUT..SERVICE S WON..NUMBER OF LOST..CREDIT..IN..OUT..SERVICE**

This information pattern stored in the EPROM indicates that the player activated services within the machine to view the number of points won, number of points lost, value of money credited, and credits won.

(d) **ALL FRUITS**

This is the combination of composite symbols on the gaming machine monitor that represents a winning combination [15].

(e) **MAIN GAME..DOUBLE UP GAME..POWER ON..60..70..80..90..60..70..80..90**

This indicates that the player returned to the main game and doubled up the betting amount.
(i.e., he increases the money to play another set of games). The numbers “60..70..80..90..” could represent the winnings during play.

(f) HOPPER EMPTY..CALL ATTENDANT
This string is used to report a fault condition in the coin output (hopper) system when the player attempted to redeem the money won through the game. The message is displayed if the payout coins did not pass a hopper output sensor within a specified time [14], and instructs the player to receive payment from the attendant.

(g) SPECIAL ODDS FOR TOTAL BET
According to Casino Gambling Terms and Definitions, the “odds” describe the ratio of probabilities or the amount a bet pays [17]. The pay-out table holds the combinations of game elements that will appear in the video cells and the pay value is associated with a winning combination of game elements [18]. The probability table or pay-out table is stored in the EPROM and is accessed by the odds routines to calculate the points won by the player [9].

7. Contribution

![Fig. 6. Information Retrieval and Evidence Analysis Model](image)

This study has contributed to the development of a gambling machine forensic analysis model. Figure 6 diagrams the information retrieval and evidence analysis process. Each arrow in the diagram is numbered and represents a certain function involved in the forensic analysis process.

1: The EPROM chip is removed from the Z80 microcontroller.
2: Information stored in the EPROM chip is retrieved using ChipMax.
3: The output from the chip reading process is identified as machine code.
4: The Z80 Simulator IDE is used to disassemble the machine code.
5: The output from the disassembly process is examined.
6: The assembly program is translated manually into Z80 instruction synonyms.
7: The machine code is read using Hex Editor tool.
8: The output from step 7 is a group of symbols, numbers, text and letters.
9: A string search process is conducted and gambling terms found.

8. Conclusion

A gaming machine is considered a gambling machine when it involves an actual monetary transaction and a bet to win the game. In order to choose the winning combination, a random number generating process is called and the payout value is selected from the payout table stored in memory. The following routines are commonly identified in gambling programs, and were present in our case study:

(a) A betting mechanism

The “double up game” string identifies a gambling mode which is used by the player to place another bet or to play the game a second time using the same amount of money. Based on this string, we proved that the machine allows doubling up in a game that can be played only by betting a certain number of credits.

(b) A random number generation process

The string “special odds for total bet” indicates that a special odds payout table was called to determine the total points won by the player.
The winning combination of “all fruits” is related to random number generation, because the game element displayed in the video display cells is selected randomly from an associated random table containing the numbers and game elements [18]. The game elements described are actually typical slot machine objects (e.g., “bars”, “oranges”, “cherries”). When a game is played, the entire array of cells is examined. The payout table holding the “all fruits” combination of game elements is called to determine the winning combination and its associated payout value.

(c) Presence of a payout value

The presence of the “hopper empty...call attendant” string demonstrates that a player has requested a payout. At the end of play, the player decided to redeem his winnings; however a coin output error occurred. This statement was stored in memory as information related to the game played [14]. This string proves that the machine is able to redeem credits won by a player.

Our findings prove that the gaming machine described in this paper is a gambling machine. If the establishment where the machine was confiscated was unlicensed, this would constitute an illegal gambling operation.

9. Future Work

The search process could be improved by the development of software tools containing intelligent agents to perform keyword or subroutine searches and identify gambling-related terms or mechanisms within the machine memory. Current gambling machines exploit advances in system development to avoid dependence on hardware components. Advanced extraction and analysis techniques are necessary to identify gaming machines which are capable of conducting gambling activities.

Acknowledgments

Special thanks to UTM for supporting us with the facilities necessary for this research. Great thanks to the Royal Malaysian Police Force for providing us with the forensic exhibit (gambling machine). Their full cooperation assisted us in the completion of our research and is highly appreciated.

References

Pritheega Magalingam
Centre for Advanced Software Engineering, University Technology Malaysia

Pritheega Magalingam is a MSc.(Information Security) graduate (2009) from University Technology Malaysia. Currently, she is a research and teaching assistant in Centre for Advance Software Engineering, University Technology Malaysia. Her MSc. thesis comprises Digital Evidence Retrieval and Forensic Analysis Guideline for an Illegal Gambling Machine and she has published few papers on how to extract evidence from gambling machine and data analysis using keyword search techniques. Her current research focuses on forensic analysis tool development for evidence retrieved from electronic gaming machine. Applying artificial intelligence techniques through the development of a multiagent system that acts based on expert’s knowledge of the technical domain would be her great interest.

Azizah Abdul Manaf
College Science and Technology, University Technology Malaysia

Azizah Abdul Manaf (PhD) is a Professor of Image Processing and Pattern Recognition from University Technology Malaysia (UTM). She graduated with B. Eng. (Electrical) 1980, MSc. Computer Science (1985) and PhD (Image Processing) in 1995 from UTM. Her current areas of interest and research are image processing, watermarking, steganography and computer forensics and have postgraduate students at the Masters and PhD level to assist her in these research areas. She has written numerous articles in journals and presented an extensive amount of papers at national and international conferences on her research areas. Prof. Dr. Azizah has also held management positions at the University and Faculty level such as Head of Department, Deputy Dean, Deputy Director and Academic Director pertaining to academic development as well as on training for teaching and learning methodologies at the University.

Rabiah Ahmad
Centre for Advanced Software Engineering, University Technology Malaysia

Rabiah Ahmad, Ph.D. is a senior lecturer for Information Security at Centre for Advanced Software Engineering, University Technology Malaysia (UTM). She graduated with BSc. Computer Science (UTM) in 1997, MSc. Information Security (Royal Holloway University of London, UK) 1998 and Ph.D. Information Studies (University of Sheffield, UK) 2006. Her current areas of interest and research are Threat Identification Tools for Medical Online System Using Combination Technique Genetic Algorithm and Coz Regression, Virus and Worm Analysis Using Bayesian Network and Regression Model for Healthcare System, Privacy issue in data mining and Security Architecture and Access Control. She is the author of numerous journal publications and article in the field of digital forensics, watermarking, steganography and health information management research. She presented an extensive amount of papers at national and international conferences on her research areas. Rabiah Ahmad has also held management position at the Faculty level such as Program Coordinator Master Computer Science Information Security (2004-2009), Assistant Treasurer for Malaysia Society of Cryptology Research (2009 – Present) and Academic Adviser at German Malaysian Institute (2005 – Present).