

## **A NEW DIGITAL EVIDENCE RETRIEVAL MODEL FOR GAMBLING MACHINE FORENSIC INVESTIGATION**

PRITHEEGA MAGALINGAM<sup>1</sup>, AZIZAH ABDUL MANAF<sup>2</sup>, ZURAIMI YAHYA<sup>3</sup> & RABIAH AHMAD<sup>4</sup>

**Abstrak.** Analisis forensik perkakasan melibatkan proses menganalisa data yang di perolehi secara elektronik untuk menunjukkan bukti sama ada peralatan elektronik adalah digunakan untuk melakukan jenayah, mengandungi bukti jenayah atau ia adalah satu sasaran jenayah. Penyalahgunaan mesin permainan merupakan sumber utama permainan haram dijalankan. Kerja penyelidikan ini memperkenalkan kaedah mendapatkan maklumat dari satu mesin permainan yang telah dirampas oleh PDRM dan menganalisis data yang diterjemahkan untuk membuktikan bahawa mesin permainan tersebut digunakan secara haram. Prosedur mendapatkan bukti digital ini dibina untuk membantu pihak polis atau penyiasat dalam penganalisan maklumat digital dan ia boleh dijadikan sebagai satu garis panduan untuk mengenalpasti bukti yang relevan untuk menunjukkan aktiviti perjudian haram dijalankan.

*Kata kunci:* Forensik digital; analisis forensik; mesin judi; kaedah pengambilan informasi; penterjemahan; pencarian kata

**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 method; interpretation; string search

### **1.0 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

---

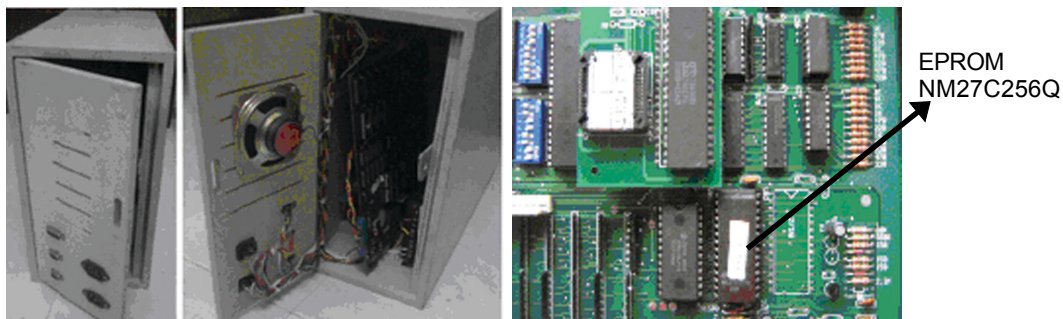
<sup>1,2,3&4</sup>Centre For Advanced Software Engineering, College of Science and Technology, Faculty of Electrical Engineering, Universiti Teknologi Malaysia, International Campus, Jalan Semarak, 54100 Kuala Lumpur  
Email: <sup>1</sup>[mprihee@gmail.com](mailto:mprihee@gmail.com), <sup>2</sup>[azizah07@citycampus.utm.my](mailto:azizah07@citycampus.utm.my), <sup>3</sup>[zuraimibinyahya@yahoo.com](mailto:zuraimibinyahya@yahoo.com), <sup>4</sup>[rabiah@citycampus.utm.my](mailto:rabiah@citycampus.utm.my)

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 cafe 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.

## 2.0 BACKGROUND

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.



**Figure 1** Gaming CPU and Z80 Microcontroller

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.

### 3.0 RELATED WORK IN COMPUTER FORENSIC

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 in order to obtain investigative information [3]. Memory acquisition procedures for microprocessor-based devices have been analyzed. Some previous research is discussed in Section 3.1-3.6.

#### 3.1 Forensic Data Recovery from Flash Memory

Marcel Breeuwsma *et al.* (2007) claims that most forensic tools in market today perform logical data extraction and are not capable of retrieving all possible information from storage medium. Three types of methods for low-level information acquisition from flash memories were introduced. These include flasher tools, the use of an access port for testing and debugging, and a semi-invasive method in which flash memory chips are physically removed from printed circuit board [4]. Further, it explains the steps necessary to translate the extracted data to file system level. Our exhibit falls under the third category where the seized wooden gaming box contains only the printed circuit board to be examined.

#### 3.2 Memory Acquisition Procedure for Digital Investigation

A hardware-based procedure for the retrieval of information from a volatile memory contents has been introduced. Brian D. Carrier and Joe Grand (2004) also claims that existing data acquisition method involve untrusted software because they write back to the memory and use only certain tools to obtain obvious data (thereby leaving behind the rest of the memory unanalyzed). The solution to these issues was a Peripheral Component Interconnect (PCI) expansion card, installed in a computer before a crime occurs. The back of the card has a switch to enable it; once enabled, the PCI controller on the card is activated and takes control of the PCI bus. It is able to access memory without relying on the operating system and does not use memory. Finally, it will copy the exact contents of volatile memory to an external, non-volatile storage medium [5].

#### 3.3 Xbox Forensics

Burke and Craiger [20] showed an easy and non-intrusive method of data extraction. Main aim of the paper is to identify whether an Xbox is compromised by the hackers to install non-approved software to run an operating system other than the one built in to the system by Microsoft. The author uses Linux to conduct the analysis of an Xbox and the output is examined line by line. The usage of strings utility and hex viewer in Linux provides a good starting point to determine evidence exist on the partition in ASCII form. This helped to describe the binary data of the evidence retrieved.

### **3.4 Forensic Investigation of the Nintendo Wii**

Nintendo Wii, a gaming console offering 256MB of flash-based memory that can be connected to the internet wirelessly. The aim of this gaming console investigation is to record all activity to make sure that there is no alterations in the system. One of the features found in this gaming console is its automated logging, which logs information of the game played as well as the length of time for which the machine has been played. The proposed method on this research involves the activation of an external logging mechanism or recording device, determination of the current unit time via checking the settings, identification of the messaging system and determination of the usage of the system (i.e., any other notes sent between individuals) for a particular date [7].

### **3.5 Preserving Computer Memory Using Expansion Card**

This is a method for preserving digital evidence of computer misconduct. The method involves the steps that are prior to the misconduct, installing an expansion card capable of retrieving and storing a memory image and register information from a digital electrical computer. A switch is connected to regulate the expansion card from a location other than the computer. At the time of the misconduct, the switch is used to trigger the retrieving and storing of the memory image and the register information into the expansion card [19].

### **3.6 A Methodology for Forensics Analysis of Embedded Systems**

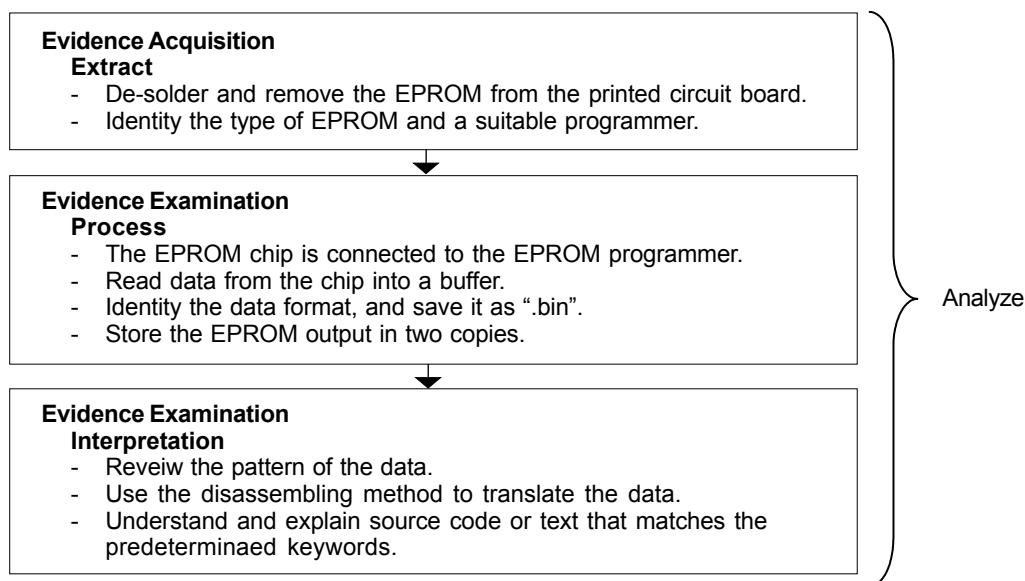
Kyung-Soo Lim and Sangjin Lee [21] have introduced analysis method which is divided into two phases, hardware and software analysis of embedded system which includes Microsoft Xbox, Sony Playstation 3, Nintendo Wii, GPS navigation and other devices. In both phases, the author compares the target system information with the manufacturer provided information to identify illegal activities. In our case, the seized gaming machine is not built by a specific manufacturer but an illegal owner in cyber cafe. (See Figure 1.) Thus, specific examination on the chips embedded in the existing microcontroller is essential.

#### 4.0 DISASSEMBLING DESIGN

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

- (a) A betting mechanism, which will allow the raising of various sums of money depending on the outcome of the game.
- (b) A random number generation process which establishes the game results
- (c) A payout value displayed to players winning a game

The pieces of information can be extracted from EPROM, a program memory which is embedded in the gaming machine microcontroller [11]. Relevant information has been gathered from the optimal practices as well as standard operating procedures. Finally the proper methods for both the retrieval of information from gaming machine memory and evidence examination have been introduced. The proposed method is as shown in Figure 2.



**Figure 2** Gambling Machine Forensic Analysis Model

The Figure 2 above shows the steps involved in digital forensic investigation that emphasize on the evidence analysis phase. This phase has been divided into two major activities. These major activities are evidence acquisition and examination method where appropriate guidelines are mapped into each main step that is relevant to gambling machine forensic analysis.

## 5.0 IMPLEMENTATION OF FORENSIC ANALYSIS AND RESULTS

### 5.1 Evidence Acquisition

The EPROM is physically removed gently from the microcontroller board using forceps. The EPROM is separated from the printed circuit board. This is a better method than de-soldering which through heat may destroy the memory chip. This work effort will address certain limitations. First, the test is performed on the non-encrypted EPROM; second, the chip extracting method is applied to non-soldered chip on the microcontroller board. The type of EPROM under consideration during the implementation phase is the NM27C256Q, EPROM type and relevant memory chip reader are identified. For the EPROM NM27C256Q, the suitable program reader identified is the ChipMax [13].

### 5.2 Evidence Examination Procedure

#### 5.2.1 Process

The device shown in Figure 3 is used to read program stored in the EPROM. The EPROM is placed on the ChipMax reader socket. It is important to ensure that the EPROM chip is correctly inserted into the socket slot to permit accurate reading of the data. The output file is saved in binary (".bin") form and it is stored in two copies. One is kept as original evidence and the other is used to work on the forensic examination. Generate a hash value of both the copies and it is used to demonstrate that the evidence is not modified. If the reading process is successful, the results are as shown in Figure 4.



**Figure 3** EPROM in ChipMax Reader Socket [15]

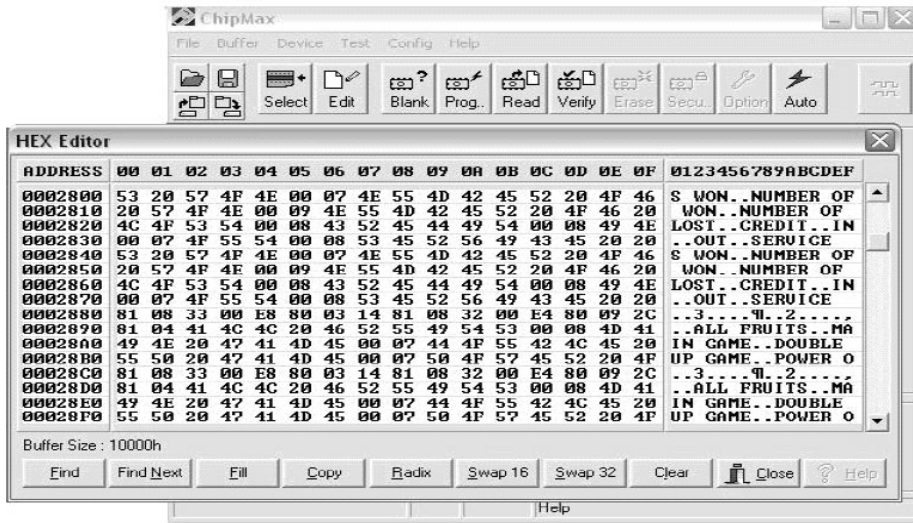


Figure 4 Data View

5.2.2 Interpretation

Reverse engineering is the process of translating the object code into source code that can be understood [12]. In order to conduct the disassembly process for interpretation of the machine code, several software tools have been identified and tested. These tools include Barleywood Z80 Simulator, Z80 Simulator IDE 8080 and Z80 Assembler Disassembler Suite. The most suitable tool found for this case is Z80 Simulator IDE.

- (i) Disassembler tool from the Z80 Simulator IDE software.

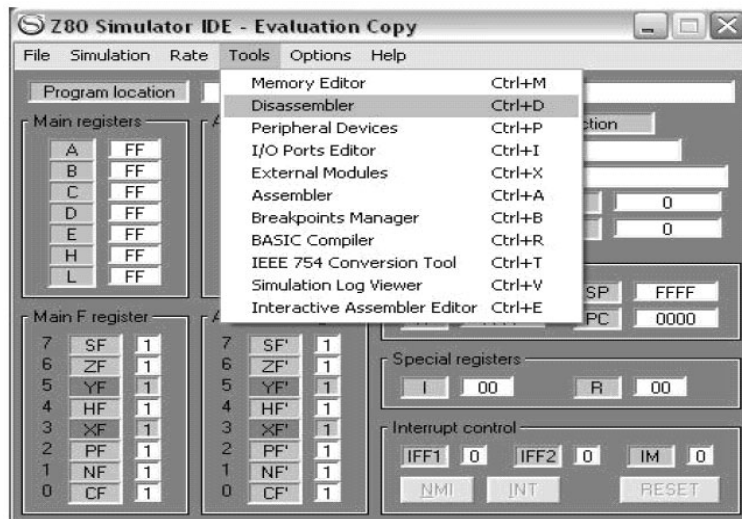


Figure 5 Z80 Simulator IDE Software

(ii) Output of the disassembly process.

```

Disassembler
File Tools Options
Loaded program C:\Documents and Settings\user\Desktop\Project 2\Testing\NM27C256Q

Z80 DISASSEMBLER LISTING
-----
Line  Addr  OpCodes      Label  Instruction
-----
0001  0000  C3 97 00          JP L0001
0002  0003  04              INC B
0003  0004  43              LD B, E
0004  0005  4F              LD C, A
0005  0006  44              LD E, H
0006  0007  45              LD E, L
0007  0008  20 45          JR NZ, L0002
0008  000A  52              LD D, D
0009  000B  52              LD D, D
0010  000C  4F              LD C, A
0011  000D  52              LD D, D
0012  000E  00              NOP
0013  000F  00              NOP
0014  0010  21 46 63      L0003: LD HL, 8346H
0015  0013  CB 3E          SRL (HL)
0016  0015  30 F9          JR NC, L0003
0017  0017  C9              RET
0018  0018  21 04 80      LD HL, 8004H
0019  001B  7E              LD A, (HL)
0020  001C  B7              OR A
0021  001D  20 08          JR NZ, L0004
0022  001F  3A 01 B8      LD A, (0B801H)
0023  0022  2F              CPL
0024  0023  B7              OR A
0025  0024  28 01          JR Z, L0004
0026  0026  77              LD (HL), A
0027  0027  3A 10 B8      L0004: LD A, (0B810H)
0028  002A  E6 01          AND 01H

```

Figure 6 Output

## 6.0 OUTPUT ANALYSIS

The output of the machine code after the execution of the disassembly process is in assembly language. The output as shown in Figure 6 is analyzed, and the assembly language source code is found to be Z80 instruction code. The assembly program further translated in a detailed manner into a set of Z80 instructions to facilitate the identification and understanding of functions involved in the assembly program [8].

Assembly program analysis is performed to find a random number generator, betting function, and payout mode. After the translation of the whole program, some factors caused difficulty in finding the routines involved in the gaming operation. The factors are described below.

- (1) Z80 instruction pattern was repeated consistently.
- (2) The program was test run using peripheral devices interface in the Z80 simulator IDE, but the assembly program loops for almost twelve hours. This occurred because the running program needs input from the actual machine, thus the exact instruction which will be executed first in order to start the gaming operation was unable to be determined.



### 7.0 SOLUTION TO THE PROBLEM

In order to circumvent these problems, alternative method has been identified. Data related to the last or the current game could provide the game sequence and output of the play [14]. Thus, the machine code retrieved from the EPROM is converted into readable plain text to permit searching of its strings. One of the methods used involves viewing the file using a Hex Editor.

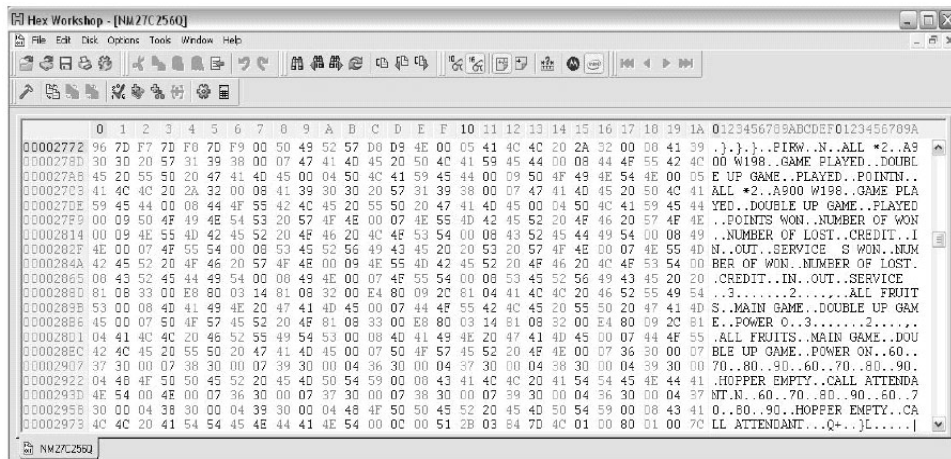


Figure 7 Machine Code Shows Game Played

**.}.}.}.PIRW..N..ALL \*2..A900 W198..GAME PLAYED..DOUBLE UP  
 GAME..PLAYED..POINTN..ALL \*2..A900 W198..GAME PLAYED..DOUBLE  
 UP GAME..PLAYED..POINTS WON..NUMBER OF WON..NUMBER OF  
 LOST..CREDIT..IN..OUT..SERVICE S WON..NUMBER OF WON..NUMBER OF  
 LOST..CREDIT..IN..OUT..SERVICE .3.....2.....,ALL FRUITS..MAIN  
 GAME..DOUBLE UP GAME..POWER O..3.....2....., ALL FRUITS..MAIN  
 GAME..DOUBLE UP GAME..POWER ON..60..70..80..90..60..70..80..90..HOPPER  
 EMPTY..CALL ATTENDANT. N..60..70..80..90..60..70..80..90..HOPPER  
 EMPTY..CALL ATTENDANT...**

During the machine code analysis, a group of symbols, numbers and letters are found. Information related to the gambling operation has been identified. These lines are gathered together to determine their actual meaning and it is found that these lines contain gambling terms. The following description further describes the relationship of the printable character content to the gambling operation executed.

- (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 or gamble [16] a second time by using a wager amount equal to the same value played in the first round. “Wager” also indicates the amount the player paid to play the game and 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 WON..NUMBER OF LOST..CREDIT..IN..OUT..SERVICE

This information pattern stored in the EPROM shows that the player activated services from the machine to view the number of points won, number of points lost, value of money credited in 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

The player returns to the main game, and he doubles up the game (i.e., he increases the money to play another set of games). The number “60..70..80..90..” could be the winnings during play, which represent the winnings generated from a particular play.

## (f) HOPPER EMPTY..CALL ATTENDANT

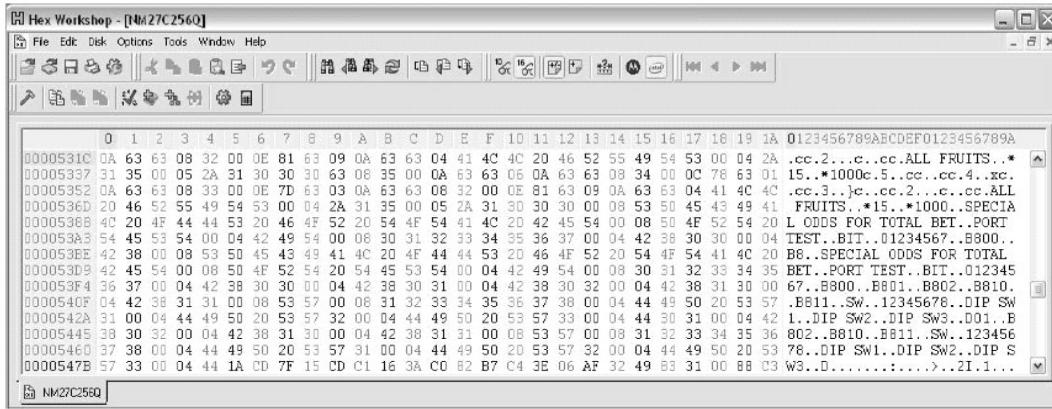
This is a fault condition in the coin output (hopper) system. “HOPPER EMPTY” indicates that a coin output error. Here, the player tried to redeem the money won through the game; however, the machine showed “ERROR: HOPPER EMPTY”. This message indicates that the coins did not pass a hopper output sensor within a specified time. Therefore, the machine automatically showed a message “CALL ATTENDANT” [14] to direct the player to call the counter attendant for hand pay. Hand pay indicates a monetary award paid by the attendant rather than being dispensed by the machine.

Figure 8 exhibits the second part of the machine code and these lines form another set of gaming terms.

Descriptions for the terms as well as their relationship to the gambling operation are identified.

## (g) SPECIAL ODDS FOR TOTAL BET

According to Casino Gambling Terms and Definitions, odds” describes a ratio of probabilities or the amount a bet pays [17]. The pay-out table holds the combinations



**Figure 8** The Second Part of the Machine Code

```
.cc.2...c..cc.ALL FRUITS..* 15..*1000c.5..cc..cc.4..xc. .cc.3..}c..cc.2...c..cc.ALL
FRUITS..*15..*1000..SPECIAL ODDS FOR TOTAL BET..PORT
TEST..BIT..01234567..B800.. B8..SPECIAL ODDS FOR TOTAL BET..PORT
TEST..BIT..01234567..B800..B801..B802..B810..B811..SW..12345678..DI###P SW1..DI###P
SW2..DI###P SW3..D01..B1..DI###P SW2..DI###P SW3..D01..B
802..B810..B811..SW..12345678..DI###P SW1..DI###P SW2..DI###P SW3..D.....>..2I1...
```

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 which will be accessed by the odds routines to calculate the points won by the player [9].

**8.0 MAIN FACTORS TO BE PRESENTED AS PROOF**

A gaming machine is considered a gambling machine when it involves money and a bet to win the game installed in the machine. In order to choose the winning combination, a random number generating process will be called and the payout value will be selected from the payout table stored. Each factor is discussed further.

(a) A betting mechanism

The string “double up game” demonstrates a gambling feature in the machine. This feature is used by the player to bet another time or play the game a second time using some amount of money. Based on this string, we prove 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 the special odds payout table is 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 string to determine that a player has redeemed credits won is the “hopper empty...call attendant” string. At the end of play, the player decided to redeem his money won in the game; however a coin output error occurred. This statement was stored in the memory as part of information related to the game played [14]. This string proves that the machine is able to pay credits won by a player. A “coin hopper” is related to a device in gambling machines that is able to dispense a designated number of coins.

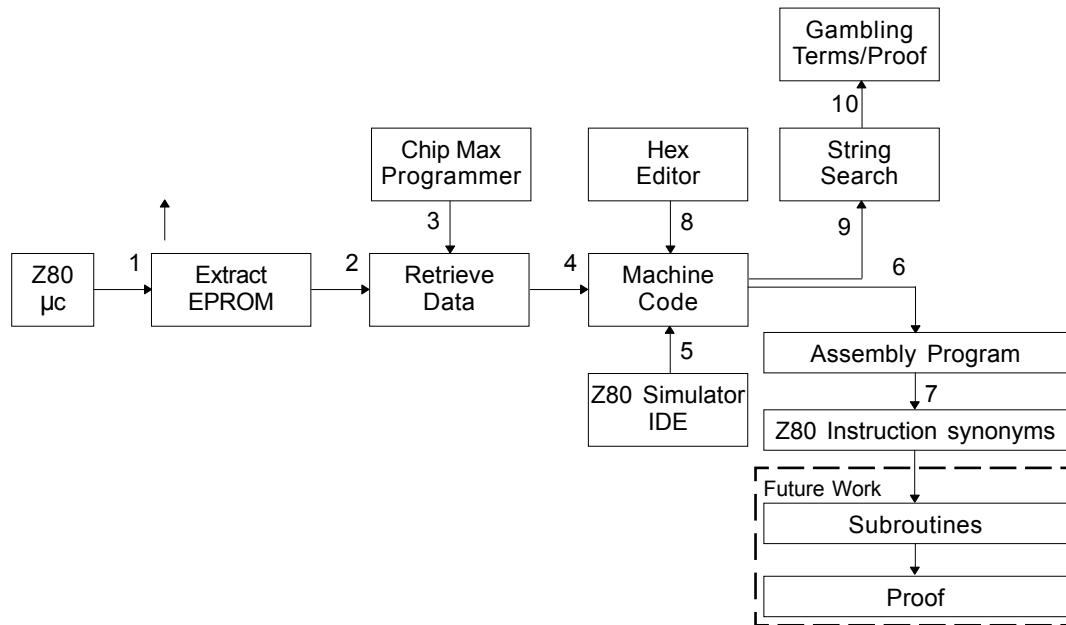
Findings and description of the evidence analysis process prove that the gaming machine seized by law enforcement officials is a gambling machine. If a location did not have a license to own this type of machine, an illegal gambling operation would exist on the premises.

## 9.0 CONTRIBUTION

This study has contributed to the gambling machine forensic analysis model as shown in Figure 2 and the information retrieval and evidence analysis work flow in Figure 9. Each arrow in the diagram is numbered and represents a certain function involved in the forensic analysis process.

## 10.0 CONCLUSION

The adaptability level of the existing evidence acquisition and electronic crime scene investigation guides to the current technology is very low [24]. Current game consoles have developed rapidly and contains wireless networking, image or video viewing capability, internet connectivity and messaging facilities. With these new facilities, game consoles can become a great source of evidence. An example of crime case which involves game consoles is console modding where changes being made to a device with protected intellectual property by installing realistic and interactive violent and sexual content to attract customers. This allows the console to be able to play pirated games. In another case, the criminal hides and possess illegal information from the game console chips which is a removable media. Besides, chat availability leads to drug dealing. In this paper we focus more on illegally assembled gaming machine which is abused as gambling machine. The method proposed in this research



**Figure 9** Information Retrieval and Evidence Analysis Flow Diagram

Each action is described below:

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

is more forensically sound in the traditional sense as the data obtained is accessible in its most raw form that is the machine code.

In future, a software tool can be developed with specialized intelligent agent for an example KeywordAgent or SubroutineAgent to assist in the findings for subroutine and gambling terms related to random number generating process or a betting mechanism. Current gambling machines use the system development to avoid dependency towards hardware components by taking advantage of the improvements in PC technology. Advanced extraction and analysis techniques should be introduced to identify different types of gaming machine which conducts gambling activity.

## ACKNOWLEDGMENTS

Special thanks to UTM which supported us with all the facilities needed for the research. Great thanks to Royal Malaysian Police Force which provided the forensic exhibit (gambling machine) for the experiment. Their full cooperation has assisted towards the achievement of this research and it is highly appreciated.

## REFERENCES

- [1] Kanellis, Kiountouzis, Kolokotronis, Martakos. *Digital Crime and Forensic Science*. Hershey, PA, USA. : Idea Group Inc. 2006.
- [2] Steven G.Lemay, Andrew M.Rodges, Robert E.Breckner, Xuedong Chen. 2006. EPROM file system in gaming apparatus, structure of a gaming system. *United States Patent No. 7108605*. Retrieved on January 25 2008, from <http://www.freepatentsonline.com/7108605.html>.
- [3] Dr. John L. McMullan, Dr. David C. Perrier. Cheats At Play: The Social Organization Video Lottery Terminal Fraud. *Paper presented at the Gambling, Law Enforcement and Justice System Conference*, March Alberta Gaming Institute and University of Alberta: Edmonton, Alberta. 2002.
- [4] John Catsoulis. 2005. *Designing Embedded Hardware*. (2nd ed.) USA: O'Reilly.
- [5] Marcel Breeuwsma, Martin De Jongh, Coert Klaver, Ronald van der Knijff and Mark Roeloffs. 2007. Forensic Data Recovery from Flash Memory. *Small Scale Device Forensic Journal*. Vol.1,(1).SSDDFJ.
- [6] Brian D. Carrier, Joe Grand. 2004. A Hardware-Based Memory Acquisition Procedure for Digital Investigations. *Digital Investigation Journal*. Vol.1, (1). IDJE.
- [7] Nick L. Petroni, Jr. , Aaron Walters, Timothy Fraser, William A. Arbaugh. 2006. FATKit: A Framework for the Extraction and Analysis of Digital Forensic Data from Volatile System Memory. *Digital Investigation Journal*. Vol. 3(4).
- [8] Dr Benjamin Turnbull. 2008. Forensic Investigation of the Nintendo Wii: A First Glance. *Small Scale Digital Device Forensics Journal*, Vol. 2(1). ISSN.
- [9] Barry B. Brey. *The Z80 Microprocessor Hardware, Software, Programming, an Interfacing*. Englewood Cliffs, N.J.: Prentice-Hall, Inc. 1988.
- [10] Z8400, SGS. Z80 CPU Central Processing Unit, Product Specification. Retrieved on August 15 2008, from <http://www.z80.info/>.
- [11] Walter R. Siekiersi, Michael Sterling. 1985. Random Number Generating Techniques and Gaming Equipment Employing such Techniques. United States Patent No. 4527798. Retrieved on July 11 2008, from <http://www.freepatentsonline.com/4527798.html>.
- [12] Dr.Elazar (Azi) Zadok, Brig. Gen. Director, D.I.F.S. Gambling Machines Laboratory, Division of Identification and Forensic Science. Unpublished note, Investigation Department/Israel Police Headquarters.
- [13] SCI Counsel James F. Villere. 1991. Illegal Gambling. Unpublished Report, Division of Criminal Justice in the Attorney General's Department of Law and Public Safety.
- [14] Memon Asim. Reverse Engineering. Unpublished note, Blekinge Institute of Technology.
- [15] eeTools, EPROM Programmer. Retrieved on March 20 2008, from [http://www.eetools.com/index.cfm?fuseaction=devices.do\\_search](http://www.eetools.com/index.cfm?fuseaction=devices.do_search).
- [16] The National Standard Working Party. 2007. Revision 9.0. Australian /New Zealand Gaming Machine National Standard. New Zealand: Australian and New Zealand gaming regulators.
- [17] Michael J. Dietz, II, Earl D. Morris, Rolan A. Miller. 1999. Instant, Multiple Play Gaming Ticket And Validation System. United States Patent No. 5949042. Retrieved on August 25 2008, from <http://www.freepatentsonline.com/5949042.html>.
- [18] Gaming Labs Certified. 2007. Standard Series. Version 2.0. Client-Server Systems. Gaming Laboratories International, Inc.
- [19] Casino Gambling Terms and Definitions. Retrieved on September 4 2008, from <http://www.bestucasinos.co.uk/casino-terms.html>.

- [20] John Manship, Michael Vinneau, David Ross, Nathalie Hache, Charles Maillet. 1995. Video Gaming Machine. United States Patent No. 5393061. Retrieved on September 11 2008, from <http://www.freepatentsonline.com/5393061.html>.
- [21] Kazuyoshi Ishibashi. 1996. Display Apparatus For Gaming Machine. United States Patent No. 5547192. Retrieved on September 11 2008, from <http://www.freepatentsonline.com/5547192.html>.
- [22] Bingo 8 Line. Retrieved on September 11 2008, from [http://www.starlitegaming.com/files/NEW\\_BINGO\\_8\\_LINE.pdf](http://www.starlitegaming.com/files/NEW_BINGO_8_LINE.pdf).
- [23] Joseph Grand, Brian Carrier. 2007. Method and Apparatus For Preserving Computer Memory Using Expansion Card. United States Patent No. 7181560. Retrieved on May 13 2009, from <http://www.freepatentsonline.com/7181560.pdf>.
- [24] Benjamin.Turnbull. 2008. The adaptability of Electronic Evidence Acquisition Guides for New Technologies. e-Fornics 2008: Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop.

