Digital Evidence Retrieval and Forensic Analysis on Gambling Machine

Pritheega Magalingam[1], Azizah Abdul Manaf[2],
Rabiah Ahmad[1], and Zuraimi Yahya[3]

[1] Centre For Advanced Software Engineering, [2] College Science and Technology,
[3] Electrical 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.

S. Goel (Ed.): ICDF2C 2009, LNICST 31, pp. 111–121, 2010.

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.

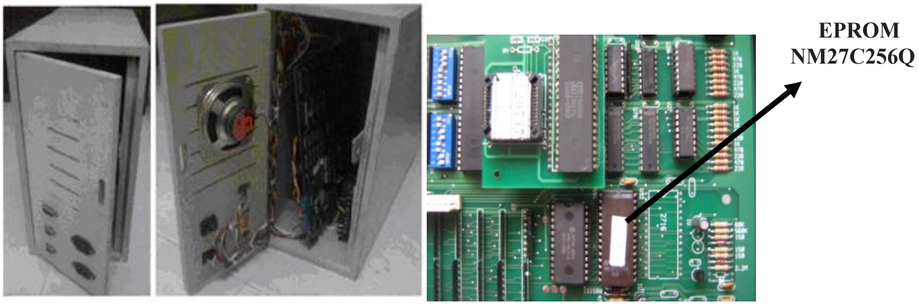


Fig. 1. Gaming CPU and Z80 microcontroller

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

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

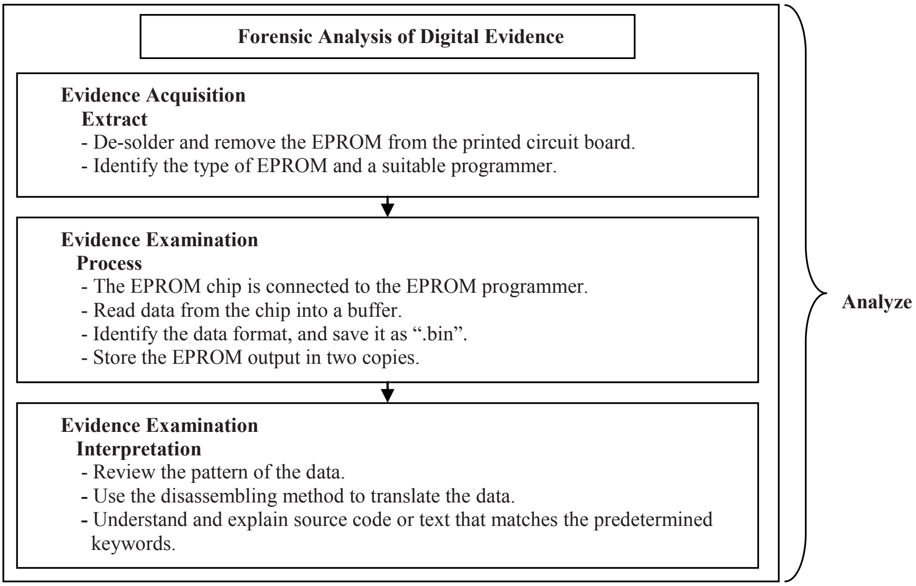
Kyung-Soo Lim and Sangjin Lee [21] have introduced analysis method which is divided into two phases, hardware and software analysis of embedded system which includes Microsoft Xbox, Sony Playstation 3, Nintedo Wii, GPS navigation and other devices. In both phases, the author compares the target system 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 Forensic Analysis 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 shown 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.



Forensic Analysis of Digital Evidence

Evidence Acquisition
Extract
- De-solder and remove the EPROM from the printed circuit board.
- Identify the type of EPROM and a suitable programmer.

Evidence Examination
Process
- The EPROM chip is connected to the EPROM programmer.
- Read data from the chip into a buffer.
- Identify the data format, and save it as ".bin".
- Store the EPROM output in two copies.

Evidence Examination
Interpretation
- Review the pattern of the data.
- Use the disassembling method to translate the data.
- Understand and explain source code or text that matches the predetermined keywords.

Fig. 2. Gambling machine forensic analysis guidelines

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 Implementation 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

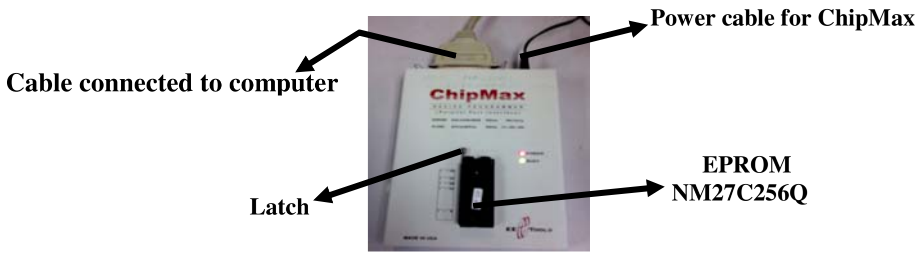


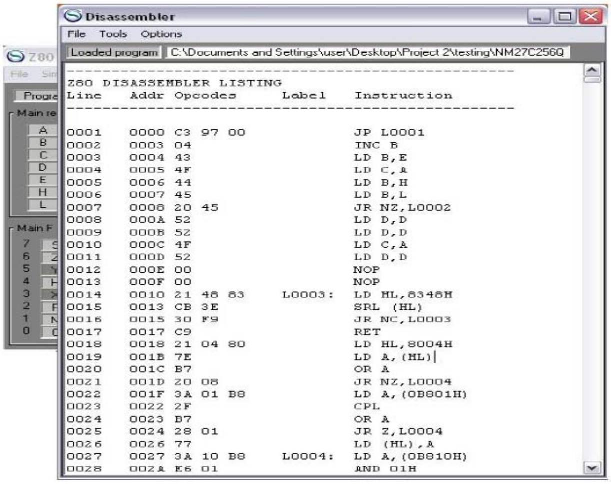
Fig. 3. EPROM in ChipMax Reader Socket [13]

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.

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. Output of the disassembly process is shown in Figure 4.



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 B,H
0006    0007 45                    LD B,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 48 83     L0003:   LD HL,8348H
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
```

Fig. 4. Output

6 Output Analysis

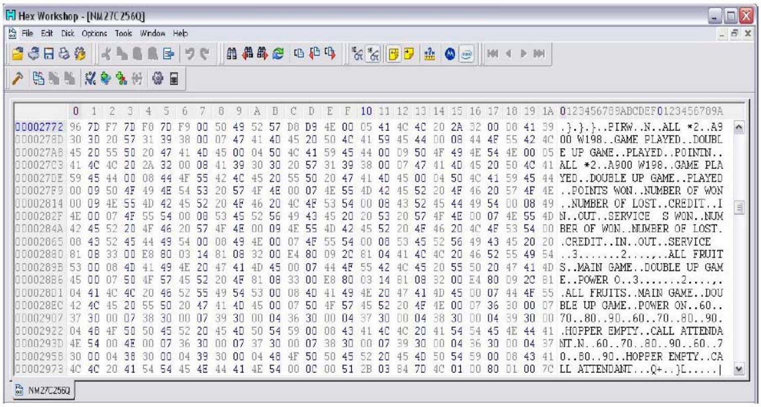
The output of the machine code after the execution of the disassembly process is in assembly language. The output as shown in Figure 4 is analyzed, and the assembly language source code is found to be Z80 instruction code. The assembly program further translated in a detailed manner into a set of Z80 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 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 opening the file using a Hex Editor.


Hex Workshop - [NM27C256Q]
File Edit Disk Options Tools Window Help
NM27C256Q

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13 14 15 16 17 18 19 1A 0123456789ABCDEF0123456789A
00002772 96 7D F7 7D F8 7D F9 00 50 49 52 57 D8 D9 4E 00 05 41 4C 4C 20 2A 32 00 08 41 39 .}.}.}..PIRW..N..ALL *2..A9
0000278D 30 30 20 57 31 39 38 00 07 47 41 4D 45 20 50 4C 41 59 45 44 00 08 44 4F 55 42 4C 00 W198..GAME PLAYED..DOUBL
000027A8 45 20 55 50 20 47 41 4D 45 00 04 50 4C 41 59 45 44 00 09 50 4F 49 4E 54 4E 00 05 E UP GAME..PLAYED..POINTN..
000027C3 41 4C 4C 20 2A 32 00 08 41 39 30 30 20 57 31 39 38 00 07 47 41 4D 45 20 50 4C 41 ALL *2..A900 W198..GAME PLA
000027DE 59 45 44 00 08 44 4F 55 42 4C 45 20 55 50 20 47 41 4D 45 00 04 50 4C 41 59 45 44 YED..DOUBLE UP GAME..PLAYED
000027F9 00 09 50 4F 49 4E 54 53 20 57 4F 4E 00 07 4E 55 4D 42 45 52 20 4F 46 20 57 4F 4E ..POINTS WON..NUMBER OF WON
00002814 00 09 4E 55 4D 42 45 52 20 4F 46 20 4C 4F 53 54 00 08 43 52 45 44 49 54 00 08 49 ..NUMBER OF LOST..CREDIT..I
0000282F 4E 00 07 4F 55 54 00 08 53 45 52 56 49 43 45 20 20 53 20 57 4F 4E 00 07 4E 55 4D N..OUT..SERVICE  S WON..NUM
0000284A 42 45 52 20 4F 46 20 57 4F 4E 00 09 4E 55 4D 42 45 52 20 4F 46 20 4C 4F 53 54 00 BER OF WON..NUMBER OF LOST.
00002865 08 43 52 45 44 49 54 00 08 49 4E 00 07 4F 55 54 00 08 53 45 52 56 49 43 45 20 20 .CREDIT..IN..OUT..SERVICE  
00002880 81 08 33 00 E8 80 03 14 81 08 32 00 E4 80 09 2C 81 04 41 4C 4C 20 46 52 55 49 54 ..3.......2....,..ALL FRUIT
0000289B 53 00 08 4D 41 49 4E 20 47 41 4D 45 00 07 44 4F 55 42 4C 45 20 55 50 20 47 41 4D S..MAIN GAME..DOUBLE UP GAM
000028B6 45 00 07 50 4F 57 45 52 20 4F 81 08 33 00 E8 80 03 14 81 08 32 00 E4 80 09 2C 81 E..POWER O..3.......2....,.
000028D1 04 41 4C 4C 20 46 52 55 49 54 53 00 08 4D 41 49 4E 20 47 41 4D 45 00 07 44 4F 55 .ALL FRUITS..MAIN GAME..DOU
000028EC 42 4C 45 20 55 50 20 47 41 4D 45 00 07 50 4F 57 45 52 20 4F 4E 00 07 36 30 00 07 BLE UP GAME..POWER ON..60..
00002907 37 30 00 07 38 30 00 07 39 30 00 04 36 30 00 04 37 30 00 04 38 30 00 04 39 30 00 70..80..90..60..70..80..90.
00002922 04 48 4F 50 50 45 52 20 45 4D 50 54 59 00 08 43 41 4C 4C 20 41 54 54 45 4E 44 41 .HOPPER EMPTY..CALL ATTENDA
0000293D 4E 54 00 4E 00 07 36 30 00 07 37 30 00 07 38 30 00 07 39 30 00 04 36 30 00 04 37 NT.N..60..70..80..90..60..7
00002958 30 00 04 38 30 00 04 39 30 00 04 48 4F 50 50 45 52 20 45 4D 50 54 59 00 08 43 41 0..80..90..HOPPER EMPTY..CA
00002973 4C 4C 20 41 54 54 45 4E 44 41 4E 54 00 0C 00 51 2B 03 84 7D 4C 01 00 80 01 00 7C LL ATTENDANT...Q+..}L.....|
```

Fig. 5. Gambling terms found in machine code

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.

(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 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 Contribution

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

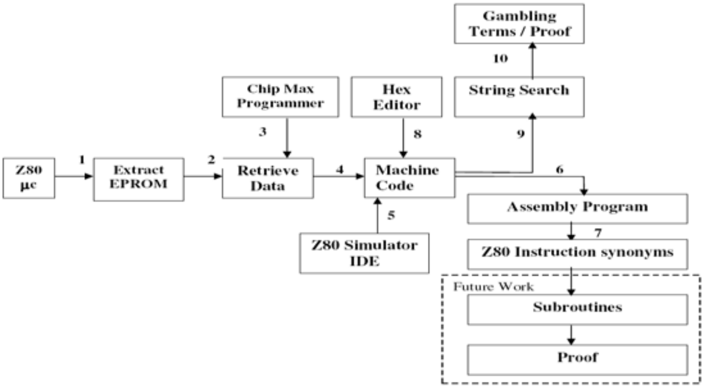


Fig. 6. Information retrieval and evidence analysis model

9 Conclusion

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.

10 Future Work

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 indentify 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 assisted towards the achievement of this research and it is highly appreciated.

References

1. Lemay, S.G., Rodges, A.M., Breckner, R.E., Chen, X.: EPROM file system in gaming apparatus, structure of a gaming system. United States Patent No.7108605 (2006), `http://www.freepatentsonline.com/7108605.html`

2. John, D., McMullan, L., David, D., Perrier, C.: Cheats At Play: The Social Organization Video Lottery Terminal Fraud. In: Gambling, Law Enforcement and Justice System Conference, Alberta Gaming Institute and University of Alberta, Edmonton, Alberta (2002)
3. Catsoulis, J.: Designing Embedded Hardware. O'Reilly, USA (2005)
4. Breeuwsma, M., De Jongh, M., Klaver, C., van der Knijff, R., Roeloffs, M.: Forensic Data Recovery from Flash Memory. SSDDFJ 1(1) (2007)
5. Brian, D., Carrier, J.G.: A Hardware-Based Memory Acquisition Procedure for Digital Investigations. IDJE 1(1) (2004)
6. Nick, L., Petroni Jr., Walters, A., Fraser, T., Arbaugh, W.A.: FATKit: A Framework for the Extraction and Analysis of Digital Forensic Data from Volatile System Memory. Digital Investigation Journal 3(4) (2006)
7. Benjamin Turnbull, D.: Forensic Investigation of the Nintendo Wii: A First Glance. ISSN 2(1) (2008)
8. Brey, B.B.: The Z80 Microprocessor Hardware, Software, Programming, an Interfacing. Prentice-Hall, Inc., Englewood Cliffs (1988)
9. Siekiersi, W.R., Sterling, M.: Random Number Generating Techniques and Gaming Equipment Employing such Techniques. United States Patent No. 4527798 (1985), http://www.freepatentsonline.com/4527798.html
10. 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
11. SCI Counsel James F. Villere. Illegal Gambling. Unpublished Report, Division of Criminal Justice in the Attorney General's Department of Law and Public Safety (1991)
12. Asim, M.: Reverse Engineering. Unpublished note, Blekinge Institute of Technology
13. SCI Counsel eeTools, EPROM Programmer, http://www.eetools.com/index.cfm?fuseaction=devices.do_search
14. The National Standard Working Party.: Revision 9.0. Australian/New Zealand Gaming Machine National Standard. New Zealand: Australian and New Zealand gaming regulators (2007)
15. Dietz II, M. J., Morris, E.D., Miller, R.A.: Instant, Multiple Play Gaming Ticket And Validation System. United States Patent No. 5949042, http://www.freepatentsonline.com/5949042.html
16. Gaming Labs Certified. Standard Series. Version 2.0. Client-Server Systems. Gaming Laboratories International, Inc. (2007)
17. Casino Gambling Terms and Definitions, http://www.bestukcasinos.co.uk/casino-terms.html
18. Manship, J., Vinneau, M., Ross, D., Hache, N., Maillet, C.: Video Gaming Machine. United States Patent No. 5393061 (1995), http://www.freepatentsonline.com/5393061.html
19. Grand, J., Carrier, B.: Method and Apparatus For Preserving Computer Memory Using Expansion Card. United States Patent No. 7181560 (2007), http://www.freepatentsonline.com/7181560.pdf
20. Burke, P.K., Craiger, P.: Xbox Forensics. Journal of Digital Forensic Practice 1(4), 252–282 (2006)
21. Lim, K.-S., Lee, S.: A Methodology for Forensic Analysis of Embedded Systems. In: Second International Conference on Future Generation Communication and Networking, pp. 283–286. IEEE Computer Society, Los Alamitos (2008)