THE PRACTICAL ANALYSIS TOWARDS DEVELOPING A GUIDELINE FOR THE XBOX 360 FORENSIC

HAIRUL AZNI BIN MOHD ISA

UNIVERSITI TEKNOLOGI MALAYSIA

THE PRACTICAL ANALYSIS TOWARDS DEVELOPING A GUIDELINE FOR THE XBOX 360 FORENSIC

HAIRUL AZNI BIN MOHD ISA

A project report submitted in fulfilment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Centre for Advanced Software Engineering
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

OCTOBER 2009

To my beloved wife, mother and father

ACKNOWLEDGEMENT

Praise and thanks to Allah first and foremost whose blessing enabled me to accomplish this project.

I wish to express my deepest appreciation to my supervisor Prof. Dr. Azizah Abdul Manaf who supervised and giving me a relentless guidance through the entire project. She was always there when I need her help. Thanks also to all my UTM lecturers for giving me helpful suggestion and moral encouragement to complete this task.

A special thank to my wife, parents and to all my teachers I have had. Thank you to my Information Security classmate for supporting me morally through the project.

My sincerely thanks to all those whom directly or indirectly help me to complete this project.

ABSTRACT

The advancement of the technology has built the Xbox 360 with the powerful hardware. It comes with a cheap price and affordable to everybody. Moreover, it's becoming a networked media platform to perform flexible connectivity through the internet. These features has made the Xbox 360 as an ideal tool to perform a cyber crime by utilizing it capabilities to the maximum. Since there is no proper guideline on conducting the investigation procedure on the Xbox 360 forensic, it is difficult to determine whether the Xbox 360 has been used as a crime tool. The immediate objective of this study is to investigate the physical modification of the Xbox 360 as well as to examine the best imaging technique for the Xbox 360 data storage. Then a new guideline was developed based on the result of the study. Several experiments had been conducted which involved several techniques and procedures for dismantling and imaging the Xbox 360's hard-disk. As the result, the best techniques and procedures for dismantling the Xbox 360's hard-disk had been determined. On the other hand, FTK Imager was chose after been compared with several imaging tools. Therefore, it had been used as an imaging tool for this purpose because it produced an image that's complies with the NIST standard for a forensic disk imaging tool. The guideline that was produced will give a great value and benefit to the forensic examiner community since there is no such research has been done before. Hence, this study can be a basis for the retrieving potential evidence techniques as well as developing a complete SOP for the Xbox 360 forensic in the future.

ABSTRAK

Kepesatan teknologi pada masa kini telah berjaya menghasilkan “Xbox 360” yang dilengkapi dengan perkakasan yang berkuasa tinggi dan ditawarkan pada harga yang murah serta mampu dimiliki oleh sesiapa sahaja. Tambahan pula, ianya kini menjadi landasan media berangkai yang bertindak untuk menghasilkan hubungan secara fleksibel menerusi internet. Ciri-ciri sebegini telah membuatkan “Xbox 360” sangat sesuai untuk dijadikan alat melakukan jenayah dengan mengubahsuai keupayaannya ke tahap maksimum. Pada masa kini, sukar untuk menentukan sekiranya sesebuah “Xbox 360” itu digunakan sebagai alat untuk melakukan jenayah kerana tiadanya panduan yang sesuai untuk digunakan dalam proses siasatan forensik. Maka, objektif bagi kajian ini adalah untuk menyiasat pengubahsuaian dari segi fizikal “Xbox 360” dan dalam masa yang sama menyelidik teknik salinan yang terbaik untuk cakera keras “Xbox 360”. Kemudian satu panduan baru untuk forensik “Xbox 360” akan dihasilkan berdasarkan keputusan kajian yang telah dijalankan. Beberapa ujikaji telah dijalankan yang mana ianya melibatkan beberapa teknik dan prosedur untuk membuka dan menyalin cakera keras “Xbox 360”. Teknik-teknik yang terbaik bagi membuka cakera keras “Xbox 360” telah dipilih berdasarkan ujian-ujian yang telah dilakukan. Dalam pada masa itu, “FTK Imager” telah berjaya melepasi ujian saringan untuk dipilih sebagai alat bagi menyalin cakera keras “Xbox 360” kerana ia telah berjaya melepasi piawaian yang telah ditetapkan oleh NIST sebagai alat penyalinan forensik. Panduan yang telah dihasilkan ini diharap dapat memberikan manfaat secara menyeluruh kepada komuniti pemeriksa forensik kerana belum pernah lagi kajian seumpama ini dilakukan sebelum ini. Dengan itu, kajian ini dapat dilihat sebagai asas untuk kajian selanjutnya terhadap teknik perolehan kembali bahan-bahan yang berpotensi untuk dijadikan bukti digital pada masa akan datang. Apabilanya semuanya telah lengkap, ianya boleh dijadikan sebagai Prosedur Operasi Piawaian (Standard Operating Procedure) untuk forensik “Xbox 360”.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENTS	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	x
	LIST OF FIGURES	xi
	LIST OF ABBREVIATIONS	xiv
1	**PROJECT INTRODUCTION**	1
	1.1 Introduction	1
	1.2 Background of The Problem	2
	1.3 Problem Statement	3
	1.4 Project Objectives	3
	1.5 Project Aim	4
	1.6 Project Scope	4
	1.7 Summary	4
2	**LITERATURE REVIEW**	5
	2.1 Introduction	5
	2.2 Computer Forensic	7
	2.2.1 Computer Forensic	7

2.2.2 Digital Evidence 8

2.2.3 Investigation Tools 9

2.2.4 Legal Aspects 10

2.2.4.1 Chain of Custody 10

2.2.4.2 Admissibility of Evidence 10

2.2.4.3 Evidential Value of Evidence 10

2.3 The Xbox 360 Forensic Techniques Procedure 11

2.4 Summary 13

3 RESEARCH METHODOLOGY 14

3.1 Introduction 14

3.2 Forensic Tools 19

3.3 Forensic Laboratory 21

3.4 Summary 22

4 FORENSIC TECHNIQUES AND EXPERIMENTS 23

4.1 Introduction 23

4.2 The Xbox 360 Surrounding Environment and Physical Modification 23

4.2.1 The Xbox 360 Surrounding Environment 23

4.2.2 The Xbox 360 Physical Modification 25

4.3 The Xbox 360 Data Storage Imaging 29

4.3.1 The Xbox 360 Data Storage Dismantle 29

4.3.2 The Xbox 360 Data Storage Connected to PC Through SATA Port 33

4.3.3 The Xbox 360 Data Storage Imaging and Accessing 34

4.3.3.1 Imaging the Xbox 360 Data Storage 34

4.3.3.2 Accessing Image of the Xbox 360 45

4.4 Summary 50

5 **THE XBOX 360 FORENSIC'S GUIDELINES** 51

5.1 Introduction 51

5.2 Purpose 53

5.3 General Guidelines 53

5.3.1 Audit Trails 53

5.3.2 Technical Preparation 54

5.3.3 Performing the Forensics Process 54

5.3.4 Data Collection 55

5.3.5 Examination and Analysis 56

5.3.6 Reporting 57

5.4 Investigation Tools 57

5.5 Forensic Laboratory 58

5.6 Forensic Tools 59

5.7 The Xbox 360 Surrounding Environment 60

5.8 The Xbox 360 Physical Modification 61

5.9 The Xbox 360 Data Storage Dismantle Procedures 61

5.10 The Xbox 360 Data Storage Connected to PC Through SATA Port 63

5.11 The Xbox 360 Data Storage Imaging and Accessing 64

5.11.1 Data Storage Imaging 64

5.11.2 Data Storage Accessing 66

6 **DISCUSSION AND CONCLUSION** 67

6.1 Introduction 67

6.2 Overview and Conclusion 67

6.3 Differences of The Research 69

6.4 Contribution 69

6.5 Future Work 70

REFERENCES 72

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENTS	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	x
	LIST OF FIGURES	xi
	LIST OF ABBREVIATIONS	xiv
1	**PROJECT INTRODUCTION**	1
	1.1 Introduction	1
	1.2 Background of The Problem	2
	1.3 Problem Statement	3
	1.4 Project Objectives	3
	1.5 Project Aim	4
	1.6 Project Scope	4
	1.7 Summary	4
2	**LITERATURE REVIEW**	5
	2.1 Introduction	5
	2.2 Computer Forensic	7
	2.2.1 Computer Forensic	7

2.2.2 Digital Evidence 8

2.2.3 Investigation Tools 9

2.2.4 Legal Aspects 10

2.2.4.1 Chain of Custody 10

2.2.4.2 Admissibility of Evidence 10

2.2.4.3 Evidential Value of Evidence 10

2.3 The Xbox 360 Forensic Techniques Procedure 11

2.4 Summary 13

3 RESEARCH METHODOLOGY 14

3.1 Introduction 14

3.2 Forensic Tools 19

3.3 Forensic Laboratory 21

3.4 Summary 22

4 FORENSIC TECHNIQUES AND EXPERIMENTS 23

4.1 Introduction 23

4.2 The Xbox 360 Surrounding Environment and Physical Modification 23

4.2.1 The Xbox 360 Surrounding Environment 23

4.2.2 The Xbox 360 Physical Modification 25

4.3 The Xbox 360 Data Storage Imaging 29

4.3.1 The Xbox 360 Data Storage Dismantle 29

4.3.2 The Xbox 360 Data Storage Connected to PC Through SATA Port 33

4.3.3 The Xbox 360 Data Storage Imaging and Accessing 34

4.3.3.1 Imaging the Xbox 360 Data Storage 34

4.3.3.2 Accessing Image of the Xbox 360 45

4.4 Summary 50

5 THE XBOX 360 FORENSIC'S GUIDELINES 51

5.1 Introduction 51

5.2 Purpose 53

5.3 General Guidelines 53

5.3.1 Audit Trails 53

5.3.2 Technical Preparation 54

5.3.3 Performing the Forensics Process 54

5.3.4 Data Collection 55

5.3.5 Examination and Analysis 56

5.3.6 Reporting 57

5.4 Investigation Tools 57

5.5 Forensic Laboratory 58

5.6 Forensic Tools 59

5.7 The Xbox 360 Surrounding Environment 60

5.8 The Xbox 360 Physical Modification 61

5.9 The Xbox 360 Data Storage Dismantle Procedures 61

5.10 The Xbox 360 Data Storage Connected to PC Through SATA Port 63

5.11 The Xbox 360 Data Storage Imaging and Accessing 64

5.11.1 Data Storage Imaging 64

5.11.2 Data Storage Accessing 66

6 DISCUSSION AND CONCLUSION 67

6.1 Introduction 67

6.2 Overview and Conclusion 67

6.3 Differences of The Research 69

6.4 Contribution 69

6.5 Future Work 70

REFERENCES 72

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	Comparison between the Xbox 360 and the Xbox hardware features	6
2.2	Various gaming console forensic techniques procedure	12
3.1	The Xbox forensic tools	19
4.1	Comparison between various imaging tools	35
5.1	Guideline's compliance	51

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
2.1	The Xbox 360 (left) and the Xbox (right)	6
3.1	Research methodology flowchart	16
3.2	Disk storage dismantle flowchart	17
3.3	Disk imaging experiment flowchart	18
4.1	The Xbox 360 as a server	24
4.2	The Xbox 360 attached together with USB-to-Box, keyboard and mouse	25
4.3	The old warranty seal for Microsoft Xbox 360	26
4.4	The latest warranty seal for Microsoft Xbox 360	27
4.5	The 7 tabs of Microsoft Xbox 360 side cover	27
4.6	The 23 pieces screw of Microsoft Xbox 360 bottom side	28

4.7 The Xbox 360 laptop 28

4.8 The Xbox 360 hard-disk casing, a flathead screw driver, a T-6 and a T-10 TORX screw driver 29

4.9 Four inner T-10 TORX crews (marked in red) 30

4.10 Metallic cover and the Xbox 360 hard-disk 31

4.11 Slide out the hard-disk 31

4.12 The Xbox 360 SATA 2.5" hard-disk and adapter 32

4.13 The Xbox 360 spring for hard-disk casing 32

4.14 The Serial ATA (SATA) 33

4.15 The Xbox 360 hard-disk connection to PC 34

4.16 FTK Imager application 38

4.17 Source evidence type selection 38

4.18 Source drive selection 39

4.19 Button for creating disk image 39

4.20 Source evidence type selection for disk imaging 40

4.21 Source drive selection for disk imaging 40

4.22 Add image destination 41

4.23 Selection for destination image type 41

4.24 Evidence item information 42

4.25 Selection for image destination 42

4.26 Start button to create image 43

4.27 Creating image in progress 43

4.28 Image successfully created 44

4.29 Verifying results for drive image 44

4.30 The Xplorer360 interface 46

4.31 Open the Xbox 360 hard-disk 47

4.32 The Xbox 360 hard-disk's partition 48

4.33 The Xbox 360 hard-disk's cache folder 49

LIST OF ABBREVIATIONS

ABBREVIATIONS		DESCRIPTION
BIOS	-	Basic Input/Output System
CD	-	Compact Disc
COFEE	-	Computer Online Forensic Evidence Extractor
CPU	-	Central Processing Unit
DVD	-	Digital Versatile Disc
FAT	-	File Allocation Table
FTK	-	Forensic Toolkit
GASSP	-	Generally Accepted System Security Principles
GB	-	Gigabyte
HDD	-	High Definition Display
HD DVD	-	High-Definition/Density DVD
HTML	-	HyperText Markup Language
IDE	-	Integrated Drive Electronics
I/O	-	Input/Output
ISO	-	International Organization for Standardization
LCD	-	Liquid Crystal Display
MB	-	Megabyte
MD5	-	Message-Digest algorithm 5
MHz	-	Mega Hertz
NIST	-	National Institute of Standards and Technology
NTFS	-	NT File System
OS	-	Operating System
PATA	-	Parallel (ATA) Advanced Technology Attachment
PC	-	Personal Computer

RAM	-	Random Access Memory
SATA	-	Serial (ATA) Advanced Technology Attachment
SCSI	-	Small Computer System Interface
SD	-	Secure Digital
SHA1	-	Secure Hash Algorithm 1
SIM	-	Subscriber Identity Module
SOP	-	Standard Operating Procedure
USB	-	Universal Serial Bus

CHAPTER 1

PROJECT INTRODUCTION

1.1 Introduction

In the era of current technological civilization, information security has appears as an evolving and a challenging field of knowledge, which assimilates in it many forces of technology. Development of technology in many ways is related to, perhaps even dependent on, information security. The emergence of technology not only followed by the way to strengthen it, but at the same time there are people who are committed in defeating the security of the technology. Technology has been used as a crime tools in order to defeat all kind of security mechanisms. Some of the crime tools are quite new and advanced like using clustered central processing unit (CPU) to gain massive capabilities of data processing (brute force). Some of the crime tools are obsolete but still manage to defeat some of the security applications like using ordinary computer system. The Xbox 360 gaming console is one of the possible devices to use as a crime tool and it will be discussed further in this research.

Gaming console is game device and purposely created for playing video games by connecting it to the television. There are many types of gaming console that had been produced before. The current technology has made the new generation of gaming console having the similarity as a personal computer. It has become networked media platform that can replace traditional personal computer to perform flexible connectivity, reading email, browsing internet, and chatting (Turnbull, 2008).

The Xbox 360 is the second gaming console developed by Microsoft. It has been categorized as a seventh generation of video game consoles along with Sony's Playstation 3 and Nintendo's Wii. According to Microsoft 28 millions unit of Xbox 360 has been sold worldwide through 2008 since its launched in November 2005 (Graft, 2009). The resemblance of the Xbox 360 itself make it similar to a personal computer and easy to use it as a crime tools. The Xbox 360 can be used to run Linux operating system once it's exploited. Then it can be used to store indecent image, illegal software, fraudulent documents, as a hacking platform, and other thing that a standard personal computer might do (Vaughan, 2004).

1.2 Background of The Problem

The cases of cyber crime had steadily increased for year over year along with the increasing of security applications and technologies. A lot of tools has been used to encounter the application security barrier that been set by the technology developer. Normally a typical hacker will try as many as possible ways or methods to break the security barrier. Their effort has been supported by a networked community groups of underground hacker. They always communicating each other, sharing knowledge among them, even trying something that we as a normal people can not even think that it is possible to be done. These things turned forensic analysts job much more difficult than before when performing the forensic investigation on a digital evidence since there are lot of things have not been discovered by them before.

The Xbox 360 is one of the things that has been successfully exploited to perform other function rather than just playing video games. Normally it will be used to perform a similar function as a lower end personal computer system when some modification been done. Some people use it for a good purpose and some people use it otherwise. Then it can be described as a crime tool when it is found at the crime scene. Beforehand, one has to make sure that the Xbox 360 has really being used as a crime tool such as the things that can physically relate the Xbox 360 as a crime tool.

For example, these are among the questions rose during seizing the crime scene. Is the Xbox 360 being used to perform crimes? Is the Xbox 360 is connecting to the internet during seized? Is it a keyboard attached with the Xbox 360? Are there any other suspicious thing surrounding the Xbox 360 that can possibly related as a part of the Xbox 360 modification? (Burke and Craiger, 2007).

1.3 Problem Statement

Several forensic studies analysis had been done on the Xbox but very few on the Xbox 360. Even though a lot of information can be found in the internet regarding this matter, most of them are not in the organized form and scatter every where. Some of the information focusing more about data retrieval and extraction, some of them discussing about the modification of the external part (hardware) and internal part (software and application) of the Xbox 360, and some of them giving information about it's architecture. Hence, it is very important to conduct a study for having a proper practical analysis and guidelines procedures since there is no formal forensic analysis when dealing with the Xbox 360 as a crime tool.

1.4 Project Objectives

The objectives of this project will be as follows:

i. To investigate the physical modification on Xbox 360.

ii. To investigate the surrounding environment of the Xbox 360 – Determination of other computer peripherals that can possibly be used on Xbox 360 to perform crimes such as computer keyboard and mouse.

iii. To examine the dismantling techniques and guidelines for Xbox 360 data storage.

iv. To examine the imaging techniques and guidelines for Xbox 360 data storage.

v. To integrate all the objectives above to become a new guideline for Xbox 360 forensic.

1.5 Project Aim

The aim of this research is to explore the existing forensic analysis techniques and guidelines from the other video game consoles platform especially the Xbox 360 and the other forensic related information from the internet. Therefore, the expected outcome from the study will be a new practical analysis that containing the first and second phase of the Xbox 360 forensic procedures.

1.6 Project Scope

This research will focus on the identification for the Xbox 360 modification. It will be based on the surrounding environment of the crime scene and the condition of the Xbox itself. This research will focus more on finding a technique to create an image of the storage media attached within the Xbox 360 as well as browsing files and folder from the created storage image.

1.7 Summary

From the recent announcement made by the Microsoft regarding a total sale of 28 million units of the Xbox 360, it was known that many people are using Xbox 360 as a video game console. From the figure, it is not impossible that someone will modify the Xbox 360 and use it as a tool to perform a cyber crime since most of the Xbox 360 hardware are very similar like a personal computer and very easy to modify and use. It should be considered to be an evidential item when found at the crime scene due to it's capability. Therefore, there is a strong needs for developing a new guideline when conducting the Xbox 360 forensic analysis. Furthermore it will make the job of forensic analyst more easier in the future when dealing with this kind of situation.