DIGITAL FORENSICS INVESTIGATION FRAMEWORK FOR RASPBERRY Pi

SINA MANAVI

FSKTM 2015 26

DIGITAL FORENSICS INVESTIGATION FRAMEWORK FOR RASPBERRY Pi

By

SINA MANAVI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillments of the Requirements for the Degree of Master of Science

July 2015

DEDICATIONS

This thesis is dedicated to my parents for their love and endless support throughout my life.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the Degree of Master of Science

DIGITAL FORENSICS INVESTIGATION FRAMEWORK FOR RASPBERRY Pi

By

SINA MANAVI

July 2015

Chairman : Azizol Bin Hj Abdullah, PhD
Faculty : Computer Science and Information Technology

Raspberry Pi is a Linux based embedded computer device in a palm hand size, with 512MB of RAM, 700MHz of ARM CPU and GPU Integrated in a single chipset with HDMI output, providing USB ports and Network plugs. In addition, this tiny computer device has a low price in the market and easily accessible for public. Different Linux distribution has been developed for Raspberry Pi from Media Center OS, Penetration Testing OSes such as W3afi Pi ("w3af," 2013), ARM Kali Linux (Ofensive-Security, 2012) and PWNPI ("PwnPI," 2012) and web application security scanners such as Glasptopf Pi ("Honeypot Project," 2012) and Kippo Pi ("SSH Honeypot," 2009) as web application honeypot projects. Due to its open source characteristics, scientific industry people can easily develop application to use in robotics projects and smart home technologies.

Since Raspberry is new in the market, the unknown data structure and lack of digital forensics methods for Raspberry Pi put digital forensics examiner in difficulties for data acquisition and analysis. This study focuses on developing a digital forensics framework to bypass the security mechanism, collect stored data of the SD card and volatile memory and then analyze and extracted the evidence from the captured data.
This study has two main objectives. The first objective is to propose and develop a new method to bypass the security mechanism and gain privileged access for data acquisition. And the second objective is to propose and develop a tool to extract and analyze evidence from volatile memory. The scope of this research is bypassing the security mechanism of the Linux kernel, data collection of the volatile memory and SD card, and finally analyzing the dumped volatile memory.

To perform this research, available data collection and analysis methods of ARM Linux based embedded devices has been studied and applied on the Raspberry Pi to find the best approach. Raspberry Pi Digital Forensics Investigation Framework (RPiDFIF) is proposed and development framework that has two major components. Data collection component bypasses the Security mechanism of the Linux kernel, dumps the volatile memory and SD card with minimum interaction and changing the integrity of the live Raspberry Pi. Second component analyzes the SD card content and volatile memory of the RAM. While there are available tools to extract and analyze the SD card data, the developed component with interaction of the Volatility framework extract the running process, established network connections, log files, encryption keys and many more. Forensics investigator by using these two independent automated components of RPiDFIF can easily investigate remotely or by having physical access of the Raspberry Pi in the crime scene.

To evaluate RPiDFIF, three evaluations have been conducted. In the first evaluation experiment, data collection has been done separately to ensure if data collection works properly and independently and capture the whole data stored on the SD card and volatile memory. Then in the second evaluation, volatile memory investigation has been performed to extract evidence from captured volatile memory. Finally, in the last evaluation, we performed a real world attack case study based on one of the challenges of the Honeynet project has been selected. In this scenario, we compromised the Raspberry Pi as a Linux web server and using the RPiDFIF we bypassed the security mechanism and acquired data from both SD card and volatile memory, and using the Autopsy for SD card investigation and developed plugins and profile for Volatility framework.

Based on the developed RPiDFIF framework, digital forensics investigator can easily examine the Raspberry Pi remotely or by having physical access to the device automatically and without learning new commands.

Abstrak tesis yang dikemukakan kepada senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk Ijazah Master Sains

RANGKA KERJA PENYIASATAN DIGITAL FORENSIK UNTUK RASPBERRY Pi

Oleh

SINA MANAVI

Julai 2015

Pengerusi : Azizol Bin Hj Abdullah, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Raspberry Pi merupakan peranti komputer tertbenam sekecil tapak tangan, dengan 512MB RAM, 700MHz ARM CPU dan GPU bersepadu di dalam chipset yang tunggal dengan output HDMI, port USB dan palam mahupun penyumbat rangkaian. Tambahan pula, peranti komputer yang kecil ini merupakan peranti yang murah dan mudah dicapai orang ramai. Agihan Linux yang berbeza dibangunkan untuk Raspberry Pi dari pusat media OS, ujian penembusan OS seperti W3afi Pi ("w3af," 2013), Linux Kali ARM (Ofensive-Security, 2012) dan PWNPI ("PwnPI," 2012) dan pengimbas keselamatan aplikasi web seperti Glasptopf Pi ("Honeypot Project," 2012) dan Kippo Pi ("SSH Honeypot," 2009) sebagai projek komputer madu aplikasi web. Ciri-ciri sumber terbukanya membolehkan pihak industri saintifk membangunkan aplikasi yang boleh digunakan dalam projek robotik dan teknologi rumah pintar dengan lebih mudah.

Oleh kerana Raspberry adalah baru di pasaran, struktur data yang tidak diketahui dan kekurangan kaedah forensik digital untuk Raspberry Pi, ia menyebabkan pemeriksa forensik digital sukar untuk memperoleh dan menganalisis data. Kajian ini difokuskan untuk membangunkan rangka kerja forensik digital untuk memintas mekanisme keselamatan dan mengumpul data yang disimpan pada kad SD serta ingatan meruap, dan kemudian menganalisis dan mengekstrak bukti dari data yang dirakam.

Kajian ini mempunyai dua objektif utama. Objektif pertama adalah untuk mencadangkan dan membangunkan satu kaedah baru untuk memintas mekanisme keselamatan dan mendapat akses istimewa untuk pemerolehan data. Objektif kedua adalah untuk mencadangkan dan membangunkan alat untuk mengekstrak dan menganalisis bukti-bukti dari ingatan meruap. Skop kajian ini memintas keselamatan kernel Linux, koleksi data ingatan meruap dan kad SD, serta menganalisis ingatan meruap yang telah dipadatkan.

Untuk melaksanakan kajian ini, kaedah pengumpulan data dan analisis peranti terbenam berasaskan Linux ARM yang sedia ada telah dikaji dan digunakan pada Raspberry Pi untuk mencari pendekatan yang terbaik. Rangka kerja penyiasatan forensik digital Raspberry Pi (RPiDFIF) adalah rangka kerja yang dicadangkan dan dibangunkan yang mana ia mempunyai dua komponen utama. Komponen pengumpulan data memintas mekanisme keselamatan Linux kernel, memadatkan ingatan meruap dan kad SD dengan interaksi minimum dan menukar integriti Raspberry Pi hidup. Komponen kedua menganalisis kandungan kad SD dan ingatan meruap RAM. Walaupun terdapat alatan yang tersedai ada untuk mengekstrak dan menganalisis data kad SD, komponen yang dibangunkan dengan interaksi rangka kerja kemeruapan berkebolehan untuk mengekstrak proses berjalan, sambungan rangkaian mantap, fail log, kekunci penyulitan dan banyak lagi. Dengan

penggunaan kedua-dua komponen automatik bebas RPiDFIF, penyiasat forensik boleh menyiasat Raspberry Pi dari jauh atau dengan mempunyai akses fizikal di tempat kejadian dengan lebih mudah.

Untuk menilai RPiDFIF, tiga penilaian telah dilaksanakan. Dalam penilaian pertama, pengumpulan data telah dilakukan secara berasingan untuk memastikan jika pengumpulan data berfungsi dengan baik, secara bebas dan merakam kesemua data yang disimpan pada kad SD dan ingatan meruap. Dalam penilaian kedua, penyiasatan terhadap ingatan meruap telah dijalankan untuk mengekstrak bukti-bukti dari ingatan meruap yang telah dirakam. Akhir sekali, dalam penilaian terakhir, kami melakukan kajian kes serangan dunia sebenar berdasarkan salah satu cabaran projek rangkaian madu (Honeynet) yang telah dipilih. Dalam senario ini, kami telah mengkompromi Raspberry Pi sebagai pelayan web Linux dan dengan menggunakan RPiDFIF kami memintas mekanisme keselamatan dan data yang diperolehi daripada kedua-dua kad SD dan ingatan meruap, serta menggunakan Autopsy untuk siasatan kad SD dan plugin yang dibangunkan, dan profil untuk rangka kerja kemeruapan.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude and appreciation to my supervisor, Dr. Azizol Abdullah for his continuous support, advice and enthusiasm. His guidance has helped me throughout my research and writing of this thesis. I would also like to thank the rest of my thesis committee, Dr. Ali Dehghantanha and Dr. Mohamed Afendee Bin Mohamad, for their encouragement and insightful comments. My sincere thanks also go to my family, for their encouragement and support during the course of this study and all of my life.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CPS	Cyber Physical Systems
CPU	Computer Processing Unit
DOJ	Department Of Justice
GPS	Global Positioning System
GPU	Graphical Processing Unit
FTK	Forensics Toolkit
JTAG	Joint Test Action Group
LAM	Log Analyzer Module
LiME	Linux Memory Extractor
PAM	Process Analyzer Module
MITM	Man In The Middle
NAM	Network Analyzer Module
OS	Operating System
PS3	Play Station 3
RAM	Random Access Memory
RPiDFIF	Raspberry Pi Digital Forensic Investigation Framework
SD	Secure Digital
USB	Universal Serial Bus

CHAPTER 1

INTRODUCTION

1.1. Research Background

Computer crimes include any traditional crimes, plus a new class of crime, which has been coined since computers have become more popular with lower prices. Computer crimes are defined by U.S Department of Justice (DOJ), as any violation and activity that are involved with computer technology that compromise the law of the country is considered as computer crime (Nugent, 1995).

In this context, computer crimes can be divided into three types: object of the crime, subject of the crime and assistant of the crime. When the target of the malicious user is the computer, the computer is considered as the object of the crime. The next category is known as the subject of the crime that deals with any infection and computer attack, data loss or damage by the malicious user. Assistant of the crime is the last category in the law enforcement looking after them. It is involved with traditional crimes such as drug dealing, child abuse, and fraud and etc.

Digital forensics is the combination of computer science and law. The digital forensic investigator is an expert with experience in computer hacking, network and web security who may work privately or publicly in law enforcements. They deal with multiple devices with a variety of operating systems and applications. Different devices demand specific tools and methodologies. Every device demands different types of evidence depending on their application, user and criminal case.

1.2. Motivation

Digital forensics science deals with different types of popular devices such as PC and laptops, cell phones and smart phones, and embedded devices. Raspberry Pi has an operating system and powerful resources such as Random Access Memory (RAM), Graphical Processing Unit (GPU) and Computer Processing Unit (CPU) and network connection, low in price, easily accessible and has programming features which makes it's a demanding embedded device in the industry such as smart home projects, robotics, educations, and commercial projects and many computer security projects such as Glasptopf Pi and Kippo Pi as web application honeypot projects, Kippo Pi and W3af Pi as an open source web application security project ("w3af," 2013). Many Linux distributions have been prepared by hacking communities such as ARM Kali Linux (Ofensive-Security, 2012), PWNPI ("PwnPI," 2012), Pwnberry Pi ("PwnBerryPi," 2012) for penetration testing.

Due to the small size of Raspberry Pi, it can be hidden easily and may be used for hackers in cyber physical systems. By using wireless dongle and battery, malicious users may hide it in the cyber physical environment for eavesdropping and terrorist attack. The information stored on SD card contains: programs and files, open files and directory, zip files, music and videos, photos, hidden files, spreadsheets and

word-processor files log files and history, saved pages and histories. The physical memory contains many footprints such as: users, process information, kernel objects, dump conversion, latest commands and histories and passwords. If all the above, mentioned information is examined forensically, undeniable evidence will be obtained to present in the court as a chain of custody. Raspberry pi forensic investigators need to identify where the evidence may be stored and hidden. So, this device has great potentials to be used for criminal purposes. As a result, it's worthwhile studying from digital forensic perspectives.

1.3. Problem Statement

Raspberry Pi is attracting different communities from educational and scientific to industry and hackers and geeks which increases risk of cybercrime in the future (Paganini, 2013). We studied the latest digital forensics investigation literature review with the scope of data collection and analysis of Linux based embedded devices such as GPS (Colombini & Colella, 2012; Nutter, 2008; van Eijk, 2010), Gaming Consoles (Conrad & Craiger, 2010; Stewart, 2010; Vaughan, 2004), and Android devices (Case, 2012; Leithner & Weippl, 2012). Based on the literature review study, we gathered the latest tools and techniques to examine if they can be applicable in Raspberry Pi forensics. Raspberry Pi stores OS and personal data on the SDcard and the current activity such as running processes, established network connection, latest executed bash commands and open files, demsg logs, encryption keys and many more are in the RAM, which will disappear once the device turned off. There are number of tools such as Autopsy, FTK Imager from AccessData and Encase for SDcard analysis to assist digital forensics investigator. We need to find a method for data collection and analysis method for Raspberry Pi's volatile memory. In an experimental study by examining every data collection and analysis techniques and tools we learned that none of them are applicable for forensic investigation of Raspberry. Linux kernel 2.6 has restricted access to the physical memory stored data in */dev/mem* file to protect from any malicious activity which drive the significant problem. The first problem is that to the best of my knowledge at moment of writing this research there is no public method or technique to be able bypass restriction access to the */dev/mem* file with minimum interaction on the current state of the Raspberry Pi in the crime scene. Raspberry Pi hardware architecture, are integrated GPU, CPU and RAM into a single chipset, which drive the second difficulty for data collection and extracting of RAM's data among other GPU and CPU registers. The second problem is that there is no available technique and research to guide how to extract and analyze evidence from unknown data structure of Raspberry Pi's RAM. By conducting several experimental tests using related tools in embedded device forensics, none of them could successfully perform effectively data collection and analysis from Raspberry Pi in a forensics sound.

1.4. Research Objective

The objective of this study is to propose and develop a new framework for forensics investigating of the Raspberry Pi device in cybercrime cases. In order to achieve this objective two goals must be achieved:

1. To propose and develop a new method for data collection.
2. To propose and develop a method for data analysis.

1.5. Research Scope

The scope of this research is to propose and develop a live forensics investigation framework for the Raspberry Pi. The proposed framework can be divided in two different phases. Data collection deals with bypassing the restricted access for data collection as well as capturing the SDcard data and dumping volatile memory remotely or with physical access automatically. In addition, for data analysis, deals with evidence extraction and analysis the volatile memory and SD card independently.

1.6. Research Contribution

The main contribution of this research is a novel framework named Raspberry Pi Digital Forensic Investigation Framework (RPiDFIF) to gain privileged access, data collection and data analysis for the Raspberry Pi.

1- The proposed data acquisition method is forensics sound which has the minimum interaction with the user land and the minimum changes in the state of the Raspberry Pi.
2- The proposed data analysis module for Raspberry Pi produces an accurate, easy to understand output for law enforcement and court. In addition, using this method the digital forensic investigators can re-experiment, which means that if law enforcement wants to produce the same analysis of the same image, it is feasible, and using this framework will produce the same result.

1.7. Organization of the Thesis

The Thesis is written based on the standard structure of University Putra Malaysia to cover how the research is accomplished and the remainder of the thesis is organized as follows:

In **Chapter 2** a literature review of forensic investigation of Linux based embedded devices in cyber physical systems have been presented. To enrich this Chapter, journals, conference proceedings, seminars, thesis, books, and online resources have been used as the main references.

In **Chapter 3** the design of a framework for investigating the Raspberry Pi embedded device has been introduced. The methodology follows standard digital forensics investigation steps from data collection to data analysis.

In **Chapter 4**, Raspberry Pi Digital Forensics Investigation Framework (RPiDFIF), and the implementation of the proposed framework has been discussed.

In **Chapter 5**, RPiDFIF framework has been evaluated and the generated results are discussed. Also, the findings along with the analysis of Raspberry Pi are presented. In **Chapter 6**, the conclusion of the overall research, the limitations of the proposed framework and future works has been presented.

1.8 Summary

In this Chapter, we introduced Raspberry Pi as an embedded device that is growing fast in the market and attracting a lot of users. Similar to any other digital device, it can be used as cybercrime as well. As a result, since the device is new, there is no study on this device with digital forensics investigation perspective. In this Chapter, we clarified the need of digital forensics investigation on the Raspberry Pi based one defined scope and contribution.

REFERENCES

Adelstein, F. (2006). Live forensics: diagnosing your system without killing it first. *Communications of the ACM*. ACM.

Anglano, C. (2014). *Forensic analysis of WhatsApp Messenger on Android smartphones*. *Digital Investigation*. University Of New Orleans.

Arthur, K. K., & Venter, H. S. (2004). An Investigation Into Computer Forensic Tools. In *Imformation And Computer Ssecurity Architecture I C S A* (pp. 1–11).

Ayers, D. (2009). A second generation computer forensic analysis system. *Digital Investigation*, *6*, S34–S42.

Blais, C. (2001). *Naval Postgraduate School Modeling, Virtual Environments, and Simulation Academic Group. Simulation.*

Breeuwsma, M. F. (2006). Forensic imaging of embedded systems using JTAG (boundary-scan). *Digital Investigation*, *3*(1), 32–42.

Brief History of the FBI. (2001). *The FBI Federal Bureau of Investigation*. Retrieved July 13, 2014, from http://www.fbi.gov/about-us/history/brief-history

Burke, P. K., & Craiger, P. (2007). Xbox Forensics. *Journal of Digital Forensic Practice*. Springer.

Case, A. (2012). Acquisition and analysis of volatile memory from android devices. *Digital Investigation*, *8*(3-4), 175–184.

Chu, H. C., Lo, C. H., & Chao, H. C. (2013). The disclosure of an Android smartphone's digital footprint respecting the InstantMessaging utilizing Skype and MSN. *Electronic Commerce Research*, *13*(1), 399–410.

Chu, H.-C., Yang, S.-W., Wang, S.-J., & Park, J. H. (2012). The Partial Digital Evidence Disclosure in Respect to the Instant Messaging Embedded in Viber Application Regarding an Android Smart Phone. In *Lecture Notes in Electrical Engineering* (Vol. 180 LNEE, pp. 171–178).

Cohen, M. (2012). The Pmem Memory Acquisition Suite. Retrieved from https://code.google.com/p/pmem/

Collins, D. (2009). XFT: A Forensic Toolkit For The Original Xbox Game Console. *International Journal of Electronic Security and Digital Forensics*.

Colombini, C. M., & Colella, A. (2012). The Digital Profiling Techniques Applied to the Analysis of a GPS Navigation Device. In *6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing* (pp. 591–596). Ieee.

Conrad, S., & Craiger, P. (2010). Forensic Analysis of a PlayStation 3 Console. In *IFIP Advances in Information and Communication Technology* (Vol. 337 AICT, pp. 65–76). Springer.

Dalvik Debug Monitor Server (DDMS). (2012). Retrieved from http://developer.android.com/tools/debugging/ddms.html

Daniel, L., & Daniel, L. (2012). *Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom* (First.). Syngress.

Desnos, A. (2009). Draugr-Live memory forensics on Linux. Retrieved from https://code.google.com/p/draugr/

Digital Forensic Research Workshop Challenge. (2011). In *Digital Forensic Research Conference*. Retrieved from http://www.dfrws.org

Farmer, D., & Venema, W. (2009). The Coroner's Toolkit (TCT). Retrieved from http://www.porcupine.org/forensics/tct.html

Girault, E. (2010). Volatilitux: Physical memory analysis of linux systems. December. Retrieved from https://code.google.com/p/volatilitux/

Haggerty, J., & Taylor, M. (2006). Managing corporate computer forensics. *Computer Fraud and Security*, *2006*(6), 14–16.

Hannay, P. (2009). Satellite Navigation Forensics Techniques. *Proceedings of the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia*.

Heckendorn, B. (2013). Raspberry Pi turned into a portable gaming console. *Digital Trends*. Retrieved from http://www.digitaltrends.com/computing/the-ben-heck-show-turns-the-raspberry-pi-into-a-handheld-gaming-console-part-1-is-online/

Honeypot Project. (2012). Retrieved from http://glastopf.org/

Jones, D., & Sutherland, I. (2008). Global positioning systems: Analysis principles and sources of evidence in user devices. In *3rd International Annual Workshop on Digital Forensics and Incident Analysis* (pp. 30–39). Ieee.

Leithner, M., & Weippl, E. (2012). Android forensics. *Computers & Security*, *31*(1), 3. Retrieved from http://linkinghub.elsevier.com/retrieve/pii/S0167404811001301

Leppert, S. (2013, July). *Android Memory Dump Analysis*. Friedrich-Alexander-University Erlangen-Nuremberg.

Luttgens, J. T., & Pepe, M. (2014). *Incident Response & ComputerForensics, Third Edition. McGrawHill Education*. McGraw-Hill/Osborne.

Magkopian. (2014). Cloud IP Camera with POE. Retrieved September 8, 2014, from http://www.instructables.com/id/Raspberry-Pi-Cloud-IP-Camera-with-POE/

Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and examining computer forensic evidence. *Forensic Science Communications*, *2*(4), 1–13.

Nugent, H. (1995). Prosecuting computer criminals using state computer crime statutes. *International Review of Law, Computers & Technology*, *9*(1), 159–182.

Nutter, B. (2008). Pinpointing TomTom location records: A forensic analysis. *Digital Investigation*, *5*(1-2), 10–18.

Ofensive-Security. (2012). Kali ARM on a Raspberry Pi. Retrieved from http://docs.kali.org/armel-armhf/install-kali-linux-arm-raspberry-pi

Paganini, P. (2013). Raspberry Pi as physical backdoor to office networks. *Security Affairs*. Retrieved September 6, 2015, from http://securityaffairs.co/wordpress/15471/hacking/raspberry-pi-as-physical-backdoor.html

Papanikolaou, A. (2013). A framework for teaching network security in academic environments. *Information Management & Computer Security*, *21*(4), 315–338. doi:10.1108/IMCS-11-2011-0056

Petroni, N. L., Walters, Aa., Fraser, T., & Arbaugh, W. A. (2006). FATKit: A framework for the extraction and analysis of digital forensic data from volatile system memory. *Digital Investigation*, *3*(4), 197–210.

PrivateEyePi Project. (2013). Retrieved from http://www.projects.privateeyepi.com/

Proven, L. (2012). Raspberry Pi IN THE SKY: Wallet-sized PC is disaster drone brain • The Register. Retrieved September 8, 2014, from http://www.theregister.co.uk/2012/06/12/raspberry_pi_drone/

PS3 Hacked via USB Dongle. (2010). Retrieved July 22, 2014, from http://beta.slashdot.org/story/139988

PwnBerryPi. (2012). Retrieved from https://github.com/g13net/PwnBerryPi

PwnPI. (2012). Retrieved from http://pwnpi.sourceforge.net/

Raytheon Pikewerks. (2009). Linux Intrusion Detection and Incident Response. Retrieved from http://secondlookforensics.com/

Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: A needs analysis survey. *Computers and Security*, *23*(1), 12–16.

Simon, M., & Slay, J. (2010). Recovery of Skype application activity data from physical memory. In *ARES 2010 - 5th International Conference on Availability, Reliability, and Security* (pp. 283–288). Ieee.

SSH Honeypot. (2009). Retrieved from https://github.com/desaster/kippo

Stewart, P. (2010, September). *Forensic Analysis of the Nintendo Wii Game Console*. *university of Strathclyde Glasgow*. university of Strathclyde Glasgow.

Strawn, C. (2009). Expanding the potential for GPS evidence acquisition. *Small Scale Digital Device Forensics Journal*, *3*(1), 1–12.

Sylve, J. (2013). LiME – Linux Memory Extractor. Retrieved from https://github.com/504ensicsLabs/LiME

Thing, V. L. L., Ng, K. Y., & Chang, E. C. (2010). Live memory forensics of mobile phones. *Digital Investigation*, *7*, S74–S82.

Turnbull, B. (2008). Forensic Investigation of the Nintendo Wii : A First. In *Small Scale Digital Device Forensics Journal* (Vol. 2, pp. 1–7).

University of Cambridge. (2008). Raspberry Pi. Retrieved from http://www.raspberrypi.org/about/

van Eijk, O. (2010). Forensic acquisition and analysis of the Random Access Memory of TomTom GPS navigation systems. *Digital Investigation*, *6*(3-4), 179–188.

Vaughan, C. (2004). Xbox security issues and forensic recovery methodology (utilising linux). *Digital Investigation*, *1*(3), 165–172.

w3af. (2013). Retrieved from http://sourceforge.net/projects/w3af/

Whitcomb, C. M. (2002). An historical perspective of digital evidence: A forensic scientist's view. *International Journal of Digital Evidence, 1*(1), 7–15.

Whitehouse, O. (2013). memgrep. Retrieved from https://github.com/nccgroup/memgrep

Wicker, N. (2014). The eNcade: A Portable Raspberry Pi Gaming Console. Retrieved September 8, 2014, from https://www.kickstarter.com/projects/2032055368/the-encade-a-portable-raspberry-pi-gaming-console

Wiles, J., & Reyes, A. (2007). *The Best Damn Cybercrime and Digital Forensics Book Period. The Best Damn Cybercrime and Digital Forensics Book Period.* Elsevier.

William, J. (2009). *Practice Guide for Managers of e-Crime Investigation.*

Xynos, K., & Harries, S. (2010). Xbox 360: A digital forensic investigation of the hard disk drive. *Digital Investigation, 6*(3-4), 104–111.

Zalewski, M. (2003). memfetch. Retrieved from http://freecode.com/projects/memfetch