International Journal of Electronics and Communication Engineering.
ISSN 0974-2166 Volume 5, Number 3 (2012), pp. 311-318
© International Research Publication House
http://www.irphouse.com

Forensic Analysis of Electronic Systems: A Comprehensive Methodology

Prof. D.V.S. Reddy and K. Ayyanna

*Dept. of ECE, Brindavan Institute of Technology and Science,
Kurnool, India
E-mail: dvsreddy06@yahoo.com, ayyanna111@gmail.com*

Abstract

An embedded system is a special-purpose computer system designed to perform one or a few dedicated functions, for example, just portable devices such as MP3 players, cell phone, to telemetric system like car navigation system etc. The more embedded systems are diversifying various types, the more forensic community is concentrating on efforts of research correspond to all kinds of embedded systems. Forensic analysis of electronic systems will become an area of increasing significance in the near future. Clearly, the growing use of embedded systems and the ubiquitous age is required advanced digital forensic techniques for the future forensic computing. In this paper, we introduce new emerging embedded systems and show a comprehensive methodology for forensic analysis of electronic systems.

Introduction

Now, in the dawning age of ubiquitous computing, digital devices are everywhere and everything is connected to networks: not only computers but also various devices including cell phones, video game consoles, home appliances, and GPS Navigation systems. As we know, an embedded system is a special-purpose computer system designed to perform one or a few dedicated functions, for example, just portable devices such as MP3 players, cell phone, to telemetric system like EDRs (Event Data Recorders), GPS Navigation system etc.

The more embedded systems are diversifying various types of devices, the more forensic community is concentrating on research effort about all kinds of embedded systems. So, embedded system forensics has recently gained great attention in cyber forensics community.

In fourth annual IFIP WG 11.9 international conference on digital Forensics, Nathan’s paper [1] shows new forensic analysis about EDRs. His paper shows automobile event data recorders provide vital information for reconstructing traffic crashes. And examines the primary issues related to evidence recovery from EDRs and its use in crash reconstruction.

Burke and Craiger [2] show forensic analysis methodology about an Xbox game console and Vaughan [3] suggests security issues and forensic recovery methodology about Xbox. These papers are concerned with forensic analysis of embedded system and show great solution about each system. But we need a general-purpose methodology for forensic analysis. The aim of this paper is to provide an analysis methodology of the recent embedded systems for future forensic computing.

The remainder of this paper is organized as follows. Section 2 describes current issues of new emerging embedded systems. Section 3 presents proposed methodology for forensic analysis of embedded systems.

Present Issues of New Emerging Embedded Systems

A famous video game console, like Microsoft Xbox console is little more than a low-end personal computer. (The performance of Xbox 360's CPU, latest version of Xbox console, jumps ordinary personal computer performance over.) A current issue of Xbox is the fact that it could be modified several purpose, for example, for running other operating system, storing hundreds of gigabytes, operating various computer services, etc. In Vaughan's paper shows that Xbox will be changed into hacking system applying to Linux machine. And these techniques enlarged to various game consoles, such as Sony Playstation 3, Nintedo Wii, etc.

On focus of anti-forensics, it is used to perform hiding data in data storage device in the console. If a suspect, who tries to hide illegal files in game console, has basic knowledge of computer hardware, he can disassembly it and remove hard disk drive from it. And he will connect removed hard disk other USB external disk device and change partition configuration on operating system. Finally, he can move any confidential or illegal files in removed storage device, he wishes to hide. But, a forensic investigator, who didn't know this hiding technique, seems to recognize just a video game console.

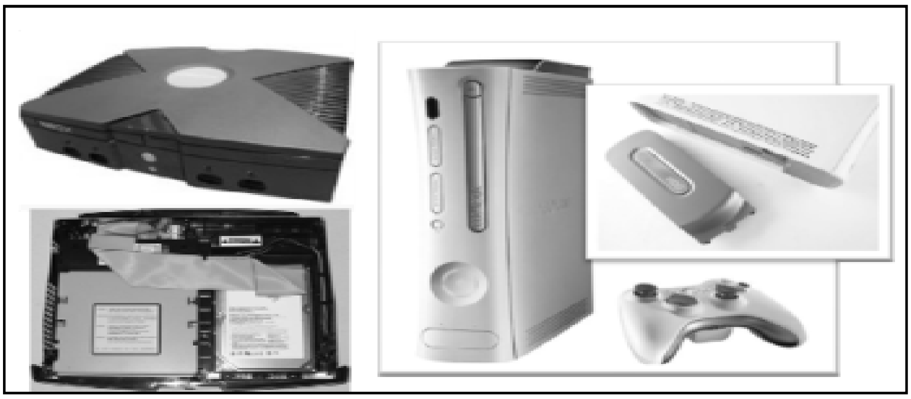


Figure 1: Microsoft S Xbox and Xbox 360

An IPTV set-top boxes are similar to game console about forensic issues. (See Figure 2) Because most of IPTV set-top have their own operating system and hard disk storage device, it is possible to hide a suspect's private information into storage media. Other issue is that it used to establish his alibi on some crime cases, which is insisted by the suspect watched IPTV contents for crime time of occurrence. So a forensic investigator should seizure set-top box and examine his alibi.

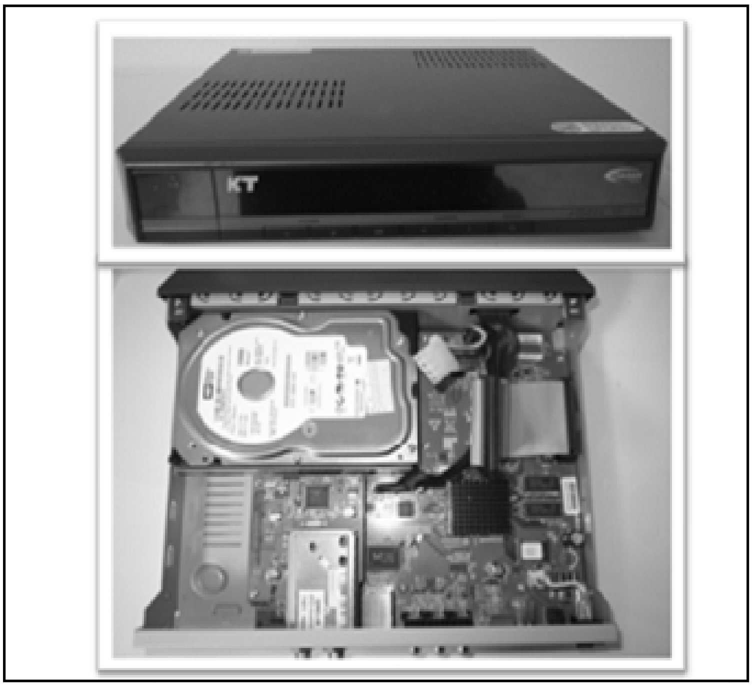


Figure 2: An example of IPTV console box

GPS navigation devices are one of the most popular kinds of satellite navigation devices in the world wide, and are increasingly being examined in criminal cases to identify data of evidential value. [5] The navigation functionality of ordinary GPS navigation devices allows the user to plan routes, save favorite destinations, and look up points of interest. The devices can also, act as a USB Mass Storage device, when it connected to a computer.

This information, where hundreds or even thousands of location entries are recovered from a navigation device, used in a number of different investigations including cases of kidnap and murder through tracking suspect's behavioral radius of action.

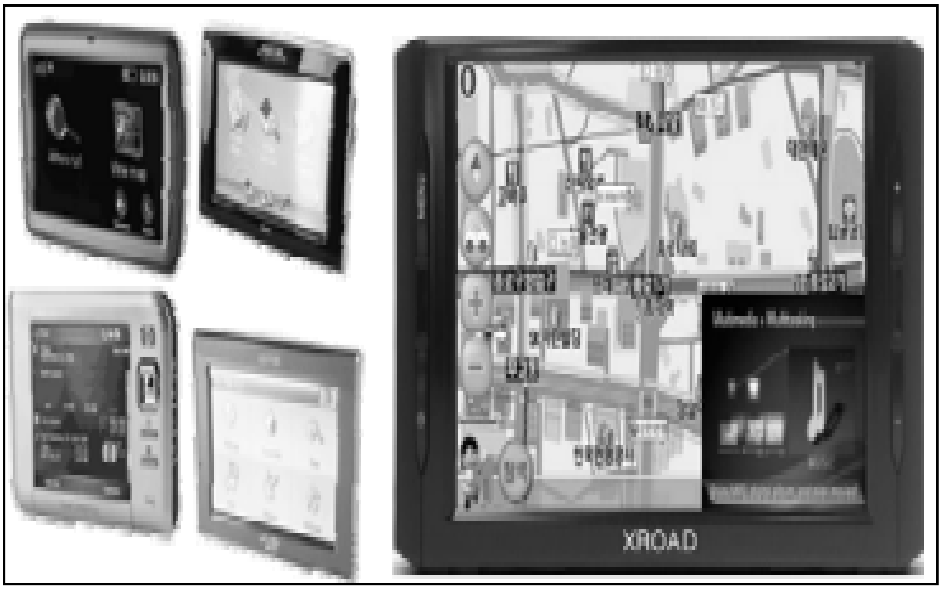


Figure 3: GPS navigation systems

A Methodology for Forensic Analysis

In this paper, I introduce a methodology for forensic analysis of embedded systems. The purpose of our methodology provides comprehensive analysis techniques, because, there are various, or even a hundred, types of embedded systems in our environment. So, we can come up with each methodology responding to every digital device. So we focus on current issues about new emerging embedded systems. Our analysis methodology separates two analysis phases, hardware analysis and software analysis. The hardware analysis focuses on hardware modification, through which a suspect has reconstructed embedded system for special purpose, like examples of the video game console. The software analysis is based on installed software or firmware on an embedded system, such as operating systems, utilities, applications. The necessity of software analysis is connected with GPS navigation system analysis. Each GPS navigation system has its own particular file formats for saving plan routes, favorite destination, etc. So we need to analysis each file format and operation workflow to get vital information.

Hardware Analysis Phase

First of all, it is essential to investigate hardware specifications and characteristics of each embedded system on the focus of forensic analysis. Each embedded system has standard hardware specification on their product name and version. Moreover, the manufacturer, through serial number or unique identification number of target system, could provide us detailed hardware information. Comparing manufacturer provided information with target system information is used for confirming system usage for malicious purpose using H/W Modification, cracking hardware for illegal software copies, other storage space for data hiding. For an instance, Microsoft's Xbox console can change new hard disk storage through removing an original hard disk drive and it is possible to change partition configuration and hide particular files.

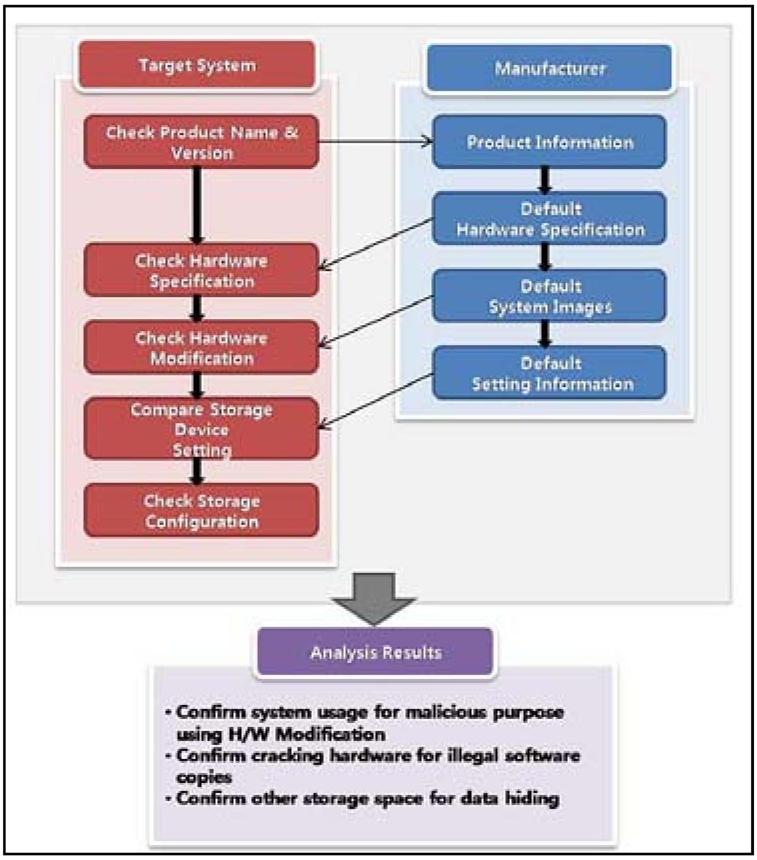

Target System
Check Product Name & Version
Check Hardware Specification
Check Hardware Modification
Compare Storage Device Setting
Check Storage Configuration
Manufacturer
Product Information
Default Hardware Specification
Default System Images
Default Setting Information
Analysis Results
• Confirm system usage for malicious purpose using H/W Modification
• Confirm cracking hardware for illegal software copies
• Confirm other storage space for data hiding

Figure 4: Hardware analysis

Following previous research, it is necessary to detect data hiding from the storage devices in particular embedded system. In anti-forensic point of view, suspects try to conceal crucial evidence in hiding place, as unrevealed storage device. It is suitable for data hiding in the storage o embedded system. So, an investigator analyzes differences between default file system settings, such as directory structures and files, and file system information of existing suspect’s embedded system.

Software Analysis Phase

In software analysis phase, we examine directory configuration and system files comparing with manufacturer information. Because, the suspect might be modified application default setting and changed or added a particular files on his intend. To obtain correct results, we need to get substantial data from corresponding to manufacturer. Therefore, it must be studied most kinds of embedded systems and establish the reference data set (RDS) by analyzing unique properties of hardware and software specification of them.

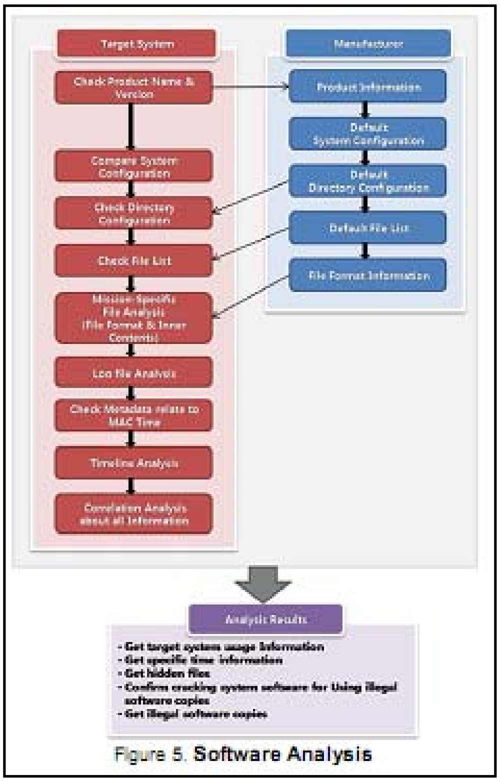
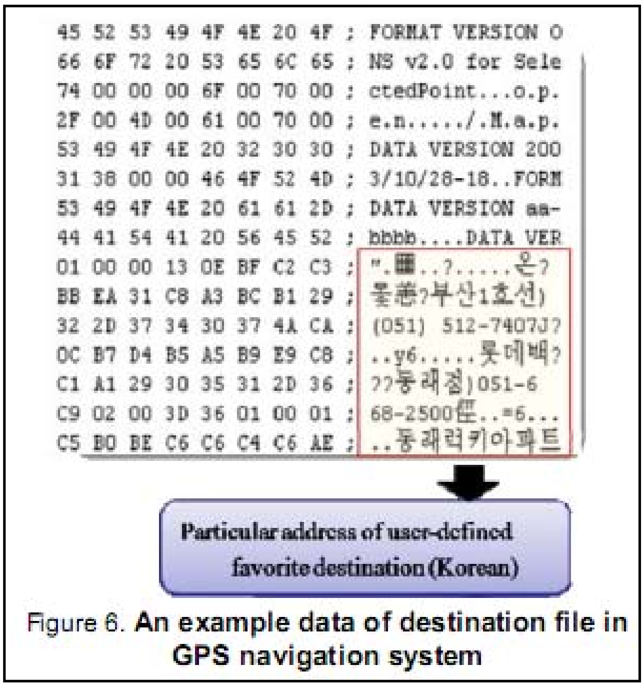

Target System
Manufacturer
Check Product Name & Version
Product Information
Default System Configuration
Compare System Configuration
Default Directory Configuration
Check Directory Configuration
Default File List
Check File List
File Format Information
Mission-Specific File Analysis (File Format & Inner Contents)
Log file Analysis
Check Metadata relate to MAC Time
Timeline Analysis
Correlation Analysis about all Information
Analytic Results
- Get target system usage Information
- Get specific time information
- Get hidden files
- Confirm cracking system software for Using illegal software copies
- Get illegal software copies
Figure 5. Software Analysis

Figure 5: Software analysis

Using overall steps, related comparing target system and default system configuration, we could conclude difference system settings or abnormal file list. So we can extract user-added or user-changed data from largest system. And we can recognize hidden files, which a suspect moved, such as any confidential or illegal files.

On the other hand, we confront unpredictable situation to collect information on target embedded system in crime scene. To perform software analysis, we should collect proper digital evidences on forensic oundness. But, some kinds of storage device in the embedded system prohibit reading operation to protect heir trade secret or privacy protection. So we must research bypass techniques for duplicating forensic images to collect and examine digital evidence. If we can access or collect files in file system of target system, we should analyze mission-based files according to each embedded system. In GPS navigation system, most of operating system or firmware in navigation system manages destination information, like recent destination and favorite destination or most visited places, which a suspect visited repeatedly, and store these data in particular files. But most of navigation systems use their own files. So, to prove the suspect's alibi and analyze his traces tracking his radius of action, we should analyze and extract vital information to solve the case. Following capture image figure 6, we can see address information which user defined favorite destination in Korean.



```
45 52 53 49 4F 4E 20 4F ; FORMAT VERSION O
66 6F 72 20 53 65 6C 65 ; NS v2.0 for Sele
74 00 00 00 6F 00 70 00 ; ctedPoint...o.p.
2F 00 4D 00 61 00 70 00 ; e.n...../.M.a.p.
53 49 4F 4E 20 32 30 30 ; DATA VERSION 200
31 38 00 00 46 4F 52 4D ; 3/10/28-18..FORM
53 49 4F 4E 20 61 61 2D ; DATA VERSION aa-
44 41 54 41 20 56 45 52 ; bbbb....DATA VER
01 00 00 13 0E BF C2 C3 ; ".▦..?.....온?
BB EA 31 C8 A3 BC B1 29 ; 롯淞?부산1호선)
32 2D 37 34 30 37 4A CA ; (051) 512-7407J?
0C B7 D4 B5 A5 B9 E9 C8 ; ..y6.....롯데백?
C1 A1 29 30 35 31 2D 36 ; ??동래점)051-6
C9 02 00 3D 36 01 00 01 ; 68-2500匡..=6...
C5 B0 BE C6 C6 C4 C6 AE ; ..동래럭키아파트
```

Particular address of user-defined favorite destination (Korean)

Figure 6. An example data of destination file in GPS navigation system

Figure 6: An example data of destination file in GPS navigation System

Conclusion and Future works

In this paper, we introduce new emerging embedded systems and show a comprehensive methodology for forensic analysis of electronic systems. The more embedded systems are diversifying various types, the more forensic community is concentrating on efforts of research correspond to all kinds of embedded systems. Forensic analysis of electronic systems will become an area of increasing significance in the near future. Clearly, the growing use of embedded systems and the ubiquitous age is required for advanced digital forensic techniques for the future forensic computing.

References

[1] Cryptographic Protection and Recovery of Railroad Event Recorder Data, Mark Hartong, Rajni Goel and Duminda Wijesekera, Fourth Annual IFIP WG 11.9 International Conference on Digital Forensics, 2008

[2] Automobile Event Data Recorder Forensics, Jeremy Daily, Nathan Singleton and Gavin Manes, Fourth Annual IFIP WG 11.9 International Conference on Digital Forensics, 2008

[3] Forensic Analysis of XBOX Console, Paul K. Burke, Philip Craiger, Journal of Digital Forensic Practice, 2006. 12. 01.

[4] Xbox security issues and forensic recovery methodology (utilizing Linux), Chris Vaughan, Journal of Digital Investigation, 2004

[5] Pinpointing TomTom location records: A forensic analysis, Beverley Nutter, Journal Digital Investigation, VOL 1, NO. 9, 2008

[6] Mobile Device Analysis, Shafik G. Punja & Richard P. Mislan, Small Scale Digital Forensic Journal, VOL 2, NO. 1, JUNE 2008

[7] Forensic Investigation of the Nintendo Wii: A First Glance, Dr Benjamin Turnbull, Small Scale Digital Forensic Journal, VOL 2, NO. 1, JUNE 2008

[8] A Small Scale Digital Device Forensics ontology David Christopher Harrill and Richard P. Mislan Small Scale Digital Forensic Journal, VOL 1, NO. 1 JUNE 2007