The Stage Model of Intelligent System Forensics

Ziyu Zhao¹, Yongquan Wang¹,²,* and Genwei Liao¹

¹ School of Criminal Justice, East China University of Political Science and Law, Shangjie Building, 555 Longyuan Road, Songjiang District, Shanghai 201620, China.
² Department of Information Science and Technology, East China University of Political Science and Law, Room 317, Shangjie Building, 555 Longyuan Road, Shanghai 201620, China.
* Corresponding author, Email: wangyongquan@ecupl.edu.cn

Abstract. With the rapid development of Internet, mobile communication is moving towards the 5G era, and the application of intelligent systems is in the ascendant. The corresponding intelligent system forensics has become one of the research highlights. By comparing the differences between intelligent system forensics and traditional electronic data forensics, this paper studies the specific content of intelligent system forensics, and proposes a stage model of forensics, which mainly included seven stages: formulation of forensics strategy, safe collection of media/equipment, equipment protection before laboratory forensics, preparation before laboratory forensics, development of laboratory forensics, reconstruction of the case process, and preservation of evidence. The model will be conductive to a more normalization process to improve the reliability, integrity and avoid misoperation of intelligent system forensics.

1. Introduction

Recent years, we have witnessed the boom of multi-functional intelligent system. However, intelligent system has provided convenient services to human beings, which has caused a lot of crime as well. Therefore, it is crucial to study the intelligent system forensics. The research of intelligent system forensics should be different from the traditional electronic data forensics. Traditional electronic data forensics refers to the process of fixing, extracting, analysing, testing and displaying the data stored in electronic equipment. According to the procedures, it finds out the connection with the case, and provides expert opinions [1]. To be specific, intelligent system forensics refers to a process that comprehensive use of computer technology, Internet of things technology and other forensic technologies. In accordance with the way of laws and regulations, it extracts the involved data of intelligent system. Then it carries out intelligent analysis to make judgments on crime, and make it as legal evidence.

There has been established a hierarchical model on electronic data forensics at home. At the same time, the challenge of intelligent system forensics includes not only the technical level but also the evidential level. At the technical level, the diversity of forensic platforms, the exclusivity of applications (such as patents and trade secrets), and extensive security measures (such as encryption algorithms) added the difficulty of obtaining electronic evidence. At the evidential level, it is very difficult to ensure that equipment state is not changed before obtain evidence. You need higher permissions to get data, which will inevitably destroy the original state. On the other hand, if the evidence is not in compliance with the program specification, the data will easily loss or damage.
2. The Difference between Intelligent System Forensics and Traditional Electronic Data Forensics

This paper combines a large number original mirror images of intelligent systems and traditional systems, as well as kinds of domestic and foreign literature, web page information, Chinese and English materials, and industry development information to analyze the details of intelligent system forensics. By combining the theoretical and experimental analysis method, we have concluded the differences between intelligent system forensics and traditional electronic data forensics are mainly included hardware platform, operating system platform, application and network.

In traditional electronic data forensics, professionals can impound the disk to obtain evidence. And they can completely record the deleted files, unallocated space and other contents by copying the image [4], and search relevant contents of the case. For intelligent systems, the traditional offline forensics method has failed in the large-scale distributed storage environment [4]. A complete file is divided into several data blocks and stored on different nodes [5].

2.1. The Difference among Hardware Platform, Operating System Platform and Application is Shown in Table 1

| Table 1. The difference among hardware platform, operating system platform and application. |
|-----------------------------------------------|-----------------|
| Platform                                      | Traditional electronic data forensics | Intelligent system forensics |
| Hardware platform                             | USB, CD, hard disk                     | Intel Edison boards, ARM mbed boards, Arduino boards |
| Operating system platform                     | Computer: Windows, Linux, Mac OS, Unix | mbed OS, Embed Linux, Tiny OS, VxWorks, Brillo |
|                                              | Mobilephone: Android, IOS, Windows Phone, Symbian | Including some traditional applications (Such as: GPS, file storage related applications, etc.) |
|                                              | Office software: WPS, Microsoft Office, notepad | ②New applications: AWS IoT, Sales force, Micrium (Real Time Operating System), Postscapes, etc. |
| Application                                   | ①Chatting software: WeChat, QQ, YY, Aliwangwang | |
|                                              | ②Internet software: Various types of Browsers | |
|                                              | ③File download software: Thunder, Baidu Netdisk, Express, EMule Download | |
|                                              | ④Email software: NetEase Mail, QQ Mail, Firefox Mail | |

2.2. The Network Differences is Shown in Table

| Table 2. The network difference |
|--------------------------------|
| System types                  | TCP/IP Protocol Stack | Z-wave | ZigBee | 6LoWPAN |
| Network Type Protocol         | Legacy system         | Intelligent system | |
| Application Layer             | HTTP, RTP, FTP        | Device & Command Classes | Application Profile(s) | HTTP |
| Transmission Layer            | TCP, UDP, ICMP        | Routing Layer | Application Support SL | UDP, ICMP |
| Network Layer                 | IP                    | Transport Layer | NWK Layer | IPv6 with 6LoWPAN |
| Data Link Layer               | Ethernet MAC          | Proprietary MAC | IEEE802.15.4 MAC | IEEE802.15.4 MAC |
| Physical Layer                | Ethernet PHY          | Proprietary PHY | IEEE802.15.4 PHY | IEEE802.15.4 PHY |

3. The Stage Model of Intelligent System Forensics

Most data extracted from intelligent systems is fragmented, which has no file identity and may have two or more locations to store the same file. Fragmented data is meaningless. It must be analyzed before cases can be reconstructed. In order to maximum obtain electronic data; this paper proposes a stage model of intelligent system forensics. The model is mainly divided into seven stages: formulation of forensics strategy, safe collection of media/equipment, equipment protection before laboratory forensics, preparation before laboratory forensics, development of laboratory forensics...
(client forensics, server forensics, and mounted load forensics), reconstruction of the case process, and preservation of evidence. This model provides the clarity for intelligent system forensics. It is benefit to the orderly process of forensics.

3.1. Formulation of Forensics Strategy
Intelligent system forensics can be used for case investigation, developing forensics software, or practical teaching. It can reduce unnecessary work to formulate forensic strategy before obtaining evidence. For example, some cases only analyzed the user and log information to prove the relationship between equipment and suspects.

3.2. Safe Collection of Media/Equipment
Taking photos or videos of intelligent system devices, recording information such as characteristics and device models, as well as the system time and its difference from the standard time. According to the type of different intelligent system devices, we should shut down the devices correctly and record the operation steps. (Note: If the UAV is in flight, it should land firstly). What’s more, if the record storage device can be dismantled, it shall be dismantled for preservation. If it cannot be disassembled, the characteristics should be photographed and recorded. If the intelligent system device has a data interface, it should be recorded; for intelligent system devices with other mounted loads, the mounted device should be removed first.

3.3. Equipment Protection before Laboratory Forensics
The following requirements shall be met for the packaging and transportation of intelligent system equipment, related control equipment, storage equipment, and mounted load. To smaller devices such as UAV, it should be removed the power device, and packaged specially. And to larger devises such as smart home and intelligent vehicle, the data should be extracted on scene in accordance with certain requirements. It should be shut down the power firstly for the control equipment of intelligent system. At the same time, the anti-static bag packaging should be marked and the wireless signal should be isolated. The mounted load on the intelligent system equipment can be disassembled and packaged independently. If removable storage medium is available, remove it from the package.

3.4. Preparation before Laboratory Forensics
Intelligent system forensics requires a dust-free, anti-static laboratory environment. Investigators should prepare the workstation and other forensic tools needed in the laboratory. And then, they should copy or make evidence image of the intelligent system equipment, calculate hash value, and specify the technology used for forensics.

3.5. Development of Laboratory Forensics
Intelligent system forensics should collect all relevant data according to the nature of the case. Forensics of the intelligent system device generally uses static forensic technology. We need to preserve and analyze the original data of intelligent system equipment, and then find out the electronic evidence related to the case [9]. For server-side forensics of intelligent systems, it’s usually use dynamic forensics technology. To conduct real-time monitoring, analysis, and preservation of memory data, network activity data, and system running of intelligent system devices in the state of start-up or networking, and find relevant evidence of crime [9]. We divided the evidence source into three categories: client, server and mount load.

3.5.1. Client forensics. For client forensics, the following contents are mainly extracted, as shown in figure 1.
Figure 1. Data source for client forensics.

3.5.2. Server-side forensics. It is more difficult to extract evidence at server-side, so we divide the server-side data source into three types: physical resources, virtual resources and application service resources, as shown in figure 2.

Figure 2. Data source for server-side forensics

3.5.3. Forensics of mounted load. The commonly intelligent system device with mounted load is a UAV. Most people are attracted by UAV aerial photography function, the civilian UAV will be mounted with motion cameras to take pictures or videos, and some people will put infrared sensors on it. Therefore, the forensics of mounted load is mainly targeted to UAV, as shown in figure 3.

Figure 3. Data source for mounted load forensics

3.6. Reconstruction of the Case Process
Save screenshots or videos of the forensics process to clearly present the evidence obtained. The electronic data obtained will be sorted out to analyze whether there is any contradiction between the electronic data. To analyze the correlation between the electronic data and the evidence obtained by the public security organs. If the evidence is lacking, it should be back to re-enact the forensic strategy and continue to collect evidence.

3.7. Preservation of Evidence
We write the detected data on a blank disk or in special storage medium by means of sealing and burning, and calculate the integrity check value of it. It has a new seal of the equipment that still have
storage condition, and we will record the process. The photographs shall reflect the conditions from multiple angles before and after the sealing of the materials, and clearly reflect the conditions at the sealing or barbed edges. When the data is sealed, it should be placed in a dry and anti-interference area to ensure the accuracy and integrity of the data.

Taking all respects into consideration, we proposed the stage model of intelligent system forensics is shown in figure 4.

![Stage Model of Intelligent System Forensics](image)

**Figure 4. The stage model of intelligent system forensics.**

4. **Conclusion**
It is not only necessary but also practically significant for intelligent system forensics. Through the combination of theory and practice, we make an in-depth study and compare the differences between the intelligent system forensics and traditional electronic data forensics. On this basis, we propose a stage model of intelligent system forensics, and analyze each phase of the model concretely. To some degree, it not only enriches the theory of electronic data forensics on intelligent systems, but also has important theoretical significance and practical value to study the intelligent system forensics more deeply and comprehensively.

5. **Acknowledgments**
This article is supported by the 2014 National Social Science Fund Major Project (second batch) "Research on Legal Regulations of Information Network Crimes" (14ZDB147), the second batch of
2017 Education Ministry “Cloud Number Integration and Education Innovation” Fund Project “the Law Big Data Application Research” (2017B06106), and the East China University of Political Science and Law “Introduction to Artificial Intelligence” general education key project construction project.

6. References
[1] Malin Z, Xiwu L and Ying Z 2014 Southeast of the Law pp 23-32
[2] Zhenxing Z and Shihai Y 2017 Net. Security Tech. & Appl. pp 141-142
[3] Fangju Y 2016 Net. Security tech. & Appl. pp 110-112
[4] Chao W and Shuang Y 2018 Ind. and Tech. pp 78-79
[5] Xiaonan W and Yi M 2017 J. of Info. Security and Appl. p 34
[6] Yongquan W, Ling T and Sanman L 2018 E-Crime and Comput. Forensics (CN: Posts and Telecom Press) pp 178-180
[7] Qiqian Z and Junsheng Y 2017 Info. Security Research pp 795-802
[8] Martin K 2013 Digit. Invest. p10
[9] Josep D and Katherine A 2017 Sci. & Justice p 57