UNDERSTANDING COMPUTER FORENSICS REQUIREMENTS IN CHINA VIA THE "PANDA BURNING INCENSE" VIRUS CASE

Frank Law, K P Chow
University of Hong Kong
Department of Computer Science
Hong Kong
{ywlaw, chow}@cs.hku.hk

Y H Mai
Wuhan University
Hubei University of Police
Hubei, China
myh9999@163.com

ABSTRACT

In March 2012, Mainland China has amended its Criminal Procedure Law, which includes the introduction of a new type of evidence, i.e., digital evidence, to the court of law. To better understand the development of computer forensics and digital evidence in Mainland China, this paper discusses the Chinese legal system in relation to digital investigation and how the current legal requirements affect the existing legal and technical usage of digital evidence at legal proceedings. Through studying the famous "Panda Burning Incense (Worm.WhBoy.cw)" virus case that happened in 2007, this paper aims to provide a better understanding of how to properly conduct computer forensics examination and present digital evidence at court of law in Mainland China.

Keywords: computer forensics, Panda burning incense virus, Chinese legal system, digital evidence, Worm.WhBoy.cw

1. INTRODUCTION

With the proliferation of digital evidences, computer forensics is becoming a key component in criminal or civil proceedings, and is evolving as an integral part of information security. The trend is no difference in Mainland China and many criminal trials or civil proceedings have involved the use of digital evidences at court of law. The demand of computer forensics in Mainland China has increased in recent years, resulting in a number of reviews by the Chinese government on the existing legal system to ensure that digital evidences retrieved by such means is forensically sound, accurate, and supported by legal basis.

Very often, digital evidence obtained in the context of computer forensics process will be presented within a defined legal framework (Brown, 2010; Casey, 2011) such that the evidence itself could be accepted by the court as legitimate and accurate evidence. In this regard, digital investigators often must be familiar with the legal requirements and have a strong knowledge foundation of the information technologies to maintain the objectivity, legality and relevancy of digital

evidence used in legal proceedings. For digital investigators who are working or wish to start their computer forensic careers in Mainland China, the requirements of legal foundation knowledge is even higher since the Chinese court has strict regulations in relation to the presentation of digital evidence.

The legal system in Mainland China (Zhai, 2002) is very unique and different from the western countries. Although the development of computer forensics had started since 2000, the legal system only started to consider the legitimacy of digital evidence and formally accepted it as a type of legal evidence on 1st of March 2013 (Rosenzweig et al., 2102). In order to successfully present digital evidence at court of law, it requires a specialized procedure that is different from the western legal system. To better understand the development of computer forensics and the legal requirements of Mainland China in relation to the use of digital evidence, this paper discusses the current legal situation and outlines the existing practices in conducting computer forensics and presenting digital evidences at court of law. In Section 2, we summarize the history of computer forensics development in Mainland China, and then discuss the computer forensics model adopted by Chinese practitioners in Section 3. In Section 4 and Section 5, we outline the current legal requirements on digital evidence and illustrate how we could utilize computer forensics techniques in presenting digital evidence at Chinese court through the study of the "Panda Burning Incense" virus case. Section 6 concludes the paper.

2. HISTORY OF COMPUTER FORENSICS DEVELOPMENT IN MAINLAND CHINA

The Ministry of Public Security (MPS) of Chinese government first established a technical research project against cybercriminals and digital evidence in May 2000. At the same year, the MPS established the Public Information Network Security Supervision Bureau to deal with cybercrime investigation, during which a department responsible for computer forensic examination was established in the college of MPS (Xu, 2011).

In April 2005, the Committee of Experts on Computer Forensics was established under the Chinese Institute of Electronics to define the basic principles as well as standards of digital evidence. Members of the committee were from the Ministry of Information Industry, the Chinese Academy of Sciences, universities and private sectors. At that time, the Committee of Experts initiated a project to study overseas and Chinese legislations in relation to digital evidence and computer forensics. In November 2005, the first computer forensics research seminar was held in Beijing. Experts from the Chinese Academy of Sciences, the Law School of Renmin University of China, domestic enterprises, and MPS reviewed a couple of conventional computer forensics models to formulate the prototype of Chinese computer forensics model (Xu, 2011). The experts also started to provide computer forensics training and discuss the importance of capacity building.

From 2005 to 2012, the China Computer Forensics Conference (2012) was held yearly to promote standards and facilitate the exchange of information among various stakeholders in this field. From 2007 to 2012, a series of international anti-terrorism police equipment exhibitions were held in Beijing, during which the coverage of computer forensics tools were increased. From 2009 to 2012, the China national prosecutors' college conducted several digital evidence identification courses to certify a group of prosecutors who were capable of understanding and presenting digital evidence at court.

In 2009, the National Accreditation Committee and the Ministry of Justice established an international standard computer forensics laboratory, and formalized the certification and accreditation of computer forensics examiners. In January 2012, the Ministry of Justice published digital evidence training materials and started to conduct

respective training through the national computer forensics seminar held in Wuhan. The above are the salient milestones of computer forensics development in Mainland China. Currently, the domestic activities in relation to computer forensics have been very active and evolved from year to year.

3. COMPUTER FORENSICS MODEL IN MAINLAND CHINA

The usage rate of information technology in Mainland China has grown explosively in the past ten years (Internet Usage Rate, 2013). To address the needs of obtaining digital evidence to facilitate criminal or civil investigations, the advancement of computer forensics has been in parallel with the technological development. Albeit the term "computer forensics" has a variety of interpretations by various judiciary and enforcement entities because of different cultural and jurisdictional factors, the terminology of "computer forensics" embraced a wider scope of elements, which may include "electronic forensics", "network forensics", and "mobile forensics". In addition, the Chinese law enforcements consider computer forensics as a technique for recovering evidence from digital exhibits, thereby defining it as a type of exhibit handling method.

In Mainland China, it is observed that computer forensics is an interdisciplinary subject which incorporates the utilization of both legal and scientific knowledge for digital evidence retrieval, and could be applied to a couple of related subjects depending on different situations (Sun, 2004). In order to better utilize and define the scope and functionalities of computer forensics, the Chinese law enforcement developed a model to break down the subject into multiple levels according to the nature of application, goals of examination, requirements of technical know-how, and legal knowledge. In this regard, computer forensics has been categorized into the following four independent levels:

1. Evidence level – The process of examining and retrieving digital evidence so as to support criminal, civil and administrative proceedings.
2. Application level – The understanding of user activities through analyzing software applications or specific devices.
3. Technical level – The scope of examinations against various activities and devices involving in the commission of acts.
4. Fundamental level – The basic principles and standards defined for computer forensics examination.

The four levels closely correlated and formulated the overall responsibilities and framework of computer forensics examination. Figure 1 shows a hierarchy diagram illustrating the computer forensics model adopted by the Chinese law enforcement.

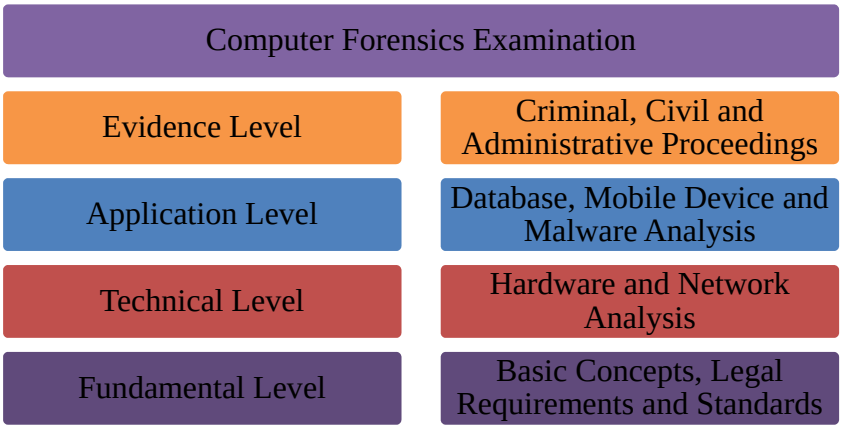

Figure 1 Computer Forensics Model defined by Chinese Law Enforcement

Digital investigators of Chinese law enforcement basically follows the above four levels when conducting computer forensics examination. Such practice has been testified and verified at Chinese court, and could be considered as the basic standard that would be followed by private practitioners in the same field.

4. LEGAL REQUIREMENTS OF COMPUTER FORENSICS IN MAINLAND CHINA

Though a model of examination has been set up by the law enforcement, digital evidence retrieved by computer forensics examination still require legal basis in order to be used during legal proceedings. In March 2012, the National People's Congress of Chinese government examined and adopted a new Criminal Procedure Law (National People's Congress, 2014) to accommodate the emerging need of digital evidence being used at criminal proceedings. The Article 48 of the Criminal Procedure Law stated that "Anything can be used to prove the material facts of case are evidences, which included: physical evidence; documentary evidence; witness testimony; victims statements; suspects confession of the accused and defense; expert opinions; inspection, inspection, identification, detection experiments transcripts; visual materials, electronic data." Article 52 under the same ordinance also stipulated that "the administration or collection of documentary evidence, audio-visual materials, electronic data and other evidence by law enforcement during investigation to support criminal proceedings may be used as evidence."

The Civil Procedure Code in China also clearly defined electronic data as legal evidence (Civil Procedure Law of the People's Republic of China, 2014). The Notice of the Supreme People's Court, the Supreme People's Procuratorates, the Ministry of Public Security, the Ministry of State Security and the Ministry of Justice concerning the examination and judgment of evidence in death sentence cases and the provisions on several issues concerning the exclusion of illegal evidence in criminal cases effective on 1st of July 2010 (Notice of the Supreme People's Court, 2014) also defined that the examinations of e-mail, electronic data interchange, online chats, online blog, mobile phone text messages, electronic signatures, domain names, and other electronic evidence should be combined and presented with other evidence, such as time, place, object, witness, producer, production process, equipment, etc., to review its authenticity and relevancy. The above had established a strong legal basis for the use of digital evidence at court proceedings in Mainland China.

Nevertheless, in order to allow digital evidence to be used and accepted at the court of law, the Decision of the Standing Committee of the National People's Congress on the Administration of Judicial Authentication defined in its statue that digital evidence used in any lawsuit by the judicial authority should be approved by authenticators or authentication institutions that are registered and authorized by the judicial administrative department of the State Council, the Supreme People's Court or Supreme Peoples' Procuratorate. In other words, digital evidence could not be simply accepted by the Chinese court but need to go through the aforementioned authentication process before it could be submitted and accepted as legal evidence at court.

However, the above requirement was evolved upon the adoption of the Criminal Procedure Law amendments on 1st January 2013. Under the new law, electronic data could be directly presented and accepted at court of law as digital evidence. Digital investigators, who had been accredited by appropriate authentication authority, could simply present the forensic findings in a report and submit it to the court for consideration. Unless there is a critical problem, such as the examination of a wrong

media or the damage of data integrity that occurred in the context of evidence retrieval, the findings could not be challenged by a third party. As the requirements are new to the society, there still exits a lot of debate on the best method in presenting digital evidence at courts of laws.

5. USAGE OF COMPUTER FORENSICS IN CHINA

Indeed, the computer forensics process in Mainland China is no difference with the existing practice adopted by the western countries. It encompasses various domains of computer science and legal concepts as well as the steps of identification, collection, preservation, examination, analysis and report. The ultimate goal is to harvest and produce digital evidence that could be used at the court of laws. Unlike traditional evidence that is scattered around in the physical environment, electronic data is often stored within a digital storage medium and the entire medium will be seized for examination. The actual search of data that has probative value is typically performed in a specialized computer forensic laboratory (National People's Congress, 2005).

The most important step in conventional computer forensics is the creation of a forensically sound duplicate of the evidentiary medium (Brown 2010). In China, this is also the basic requirement to ensure that the original evidence is not compromised by any means. An exact bit-by-bit image of the data stored at the evidentiary medium is obtained, and the forensic examinations as well as data analysis are performed on such copy (Ieong, 2006). For the imaging process to be admissible by the court as authentic procedure, the process must be repeatable and reproducible (Casey, 2011) and the whole process can be verified by hashing algorithm.

5.1 The Panda Burning Incense (Worm.WhBoy.cw) Virus Case

The "Panda Burning Incense (Worm.WhBoy.cw)" virus case happened in China between 2006 and 2007. The virus infected about 300,000 computers daily; with a total of more than 10 million infected. Using the virus, the creator earned CNY 3,000 to 5,000 a day, with the highest one-day income of CNY 10,000 (Report: Chinese Police, 2007). The case was very well-known in China and we will use it to illustrate the computer forensics process adopted by the Chinese law enforcement.

The creator of the virus was identified through the re-engineering of the virus' binary file. He was arrested by the Hubei Police and a number of digital media was seized from his residence. Prior to the examination, the digital investigator needed to confirm whether the case fall within the legal requirements. According to section 286 of the Chinese Criminal Law, which stipulates that "the intentional spread of computer viruses and other destructive programs affecting normal operation of computer system is a serious offence, and shall be punished in accordance with the first section of the Ordinance", it was observed that the case had legal basis to support the examination.

5.1.1 Evidence Level Analysis

After confirming the legal basis, the next procedure was to acquire a forensically sound image from the criminal's hard drive to facilitate evidence level analysis. Upon data searching on the drive image, the investigator detected a volume containing the source code files, a couple of complied virus programs and the writer's notes under the path "\Source Code\Delphi\My_Work\infect". Those electronic data were considered critical evidence for the criminal charge because they were able to prove the production as well as the knowledge of the writer about the virus. Figure 2 is the screenshot of the relevant electronic data recovered from the hard drive image.

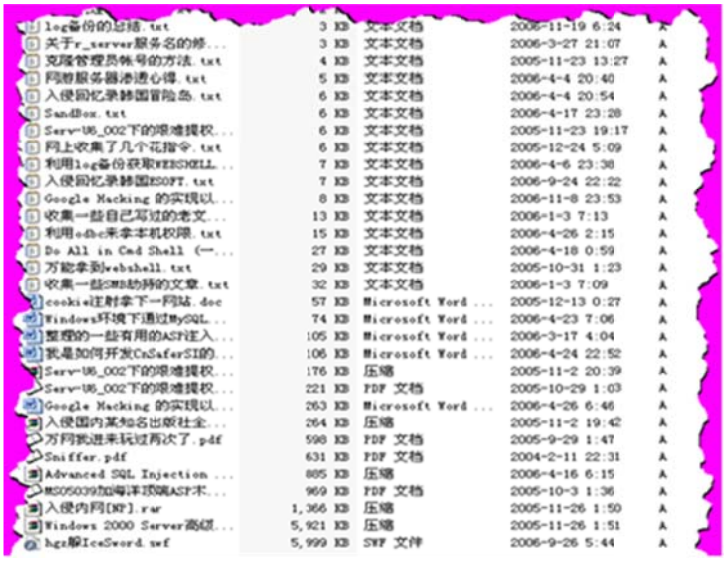

Figure 2 Source Code Files and Virus Programs Recovered from Criminal's Computer

5.1.2 Application Level Analysis

Following the evidence analysis, the investigator then looked for other information that could assist in the understanding of the computer users' activities. Through analyzing the traces of virus compiler programs, a couple of files containing large number of IP addresses, computer names and network games' login credentials, including the game "hangame", "itembay", "journey", "Adventure Island", etc., were recovered from another folder within the same hard drive image. When correlating the data with the "readme.txt" file from the "\Source Code\Delphi\My_Work\infect" folder, it showed that the virus was able to spread across the Internet as well as to steal network game credentials. Some instant message chat records were also recovered and proved that the virus writer wished to resell the stolen credentials for monetary gain, inferring that the writer created the virus intentionally.

In addition, there were documents recovered from the hard drive proving that the virus writer had rented a computer server for hosting a malicious website with an intent to spread the virus in a faster manner. The writer also rented out part of the infected computers to others for malicious use. Figure 3 is a screenshot of advertisement posted by the writer to rent out the infected host. The advertisement listed the prices of the virus (CNY 1000 per set) and the compiler program of the virus (CNY 5000 per set). In the "MyHacker\often read articles\bill" folder, account information of the virus writer were recovered, indicating that he had earned approximately CNY 40 million from advertising companies between the period of January 2005 to July 2006. This corroborated the fact that the virus writer willfully created the virus.

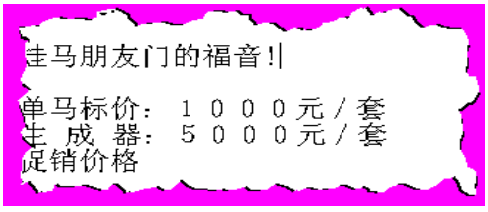

Figure 3 Advertisement of "Panda" virus

5.1.3 Technical Level Analysis

For the technical level analysis, it was observed that the computer devices infected with the virus would be slowed down, restarted frequently, and controlled remotely by the virus writer. In accordance with the commands issued by the writer, the infected computer would visit advertising websites and regularly download files, which assisted the writer in earning cash reward periodically. Through the correlation of the information recovered from the bank account of the writer's handling of the proceeds, the digital traces recovered from the computer devices and virus program, the signatures of the writer embedded within the virus program, as well as the intelligence obtained by Hubei Police from historical cases, it was able to pin down the true identity of the writer.

In brief, the virus writer acted in full compliance with the purpose of destructing computer systems and fulfilling the elements of crime stipulated under section 286 of the Chinese criminal law. Following the different levels of examination, the recovered digital evidences were presented to the Chinese court and were accepted as legitimate evidence. The virus writer was finally convicted and sentenced to 4 years of imprisonment.

CONCLUSION

In China, apart from criminal investigation, electronic data often plays an important role in resolving civil disputes. Electronic discovery is becoming a routine part of civil investigation to uncover and assemble the information needed for a civil trial. Computer forensics has undoubtedly become one of the major challenges to law enforcement agencies and private sectors in Mainland China. On one hand, it requires very specialized knowledge in information technology and computer forensics which are not normally possessed by traditional investigators (Casey, 2011). Such knowledge is relied not only on education and training but also on personal experiences (Cohen, 2008). On the other hand, the global reach of the Internet allows offenders to perform their illegal acts in any place they choose.

Digital evidence may be created at different places across multiple provinces or jurisdictions (National Institute of Justice, 2007). However, knowledge and expertise of investigators varies from different provinces within Mainland China. Some of them have advanced techniques while others do not know what information they should look for. This requires the harmonization of competencies borne by digital investigators to maintain the efficacy of investigation (Chow, et al., 2009). Generally speaking, the computer forensics standards in China are still not in uniformity and this requires a lot of training as well as guidance from the government before it could develop a hefty, mature and robust system.

REFERENCES

APA Citation Style. (2014). Retrieved from http://www.apastyle.org/

Brown, C.L.T. (2010). Computer Evidence: Collection and Preservation, 2nd edition. Boston, MA: Course Technology.

Casey, E. (2011). Digital Evidence and Computer Crime: Forensics Science, Computers and the Internet, 3rd edition. Elsevier Academic Press.

Civil Procedure Law of the People's Republic of China. (2014). Retrieved from http://www.china.org.cn/english/government/207343.htm

8th Annual China Computer Forensics Conference & Exhibition (CCFC). (2012). Retrieved from http://www.fulldata.cn/news1info-0-345.html

Farmer, Dan, & Venema, Wietse. (1999). Forensic Discovery, Computer Forensics Analysis Class Handouts. Retrieved from http://www.porcupine.org/forensics/handouts.html

Ieong, Ricci S. C. (2006). FORZA – Digital forensics investigation framework that

incorporate legal issues, Digital Forensics Research Workshop (DFRWS).

Internet Usage Rate in China, Statistics and Trends. (March 2013). Retrieved from http://www.go-globe.com/blog/internet-usage-china/

Institute of Forensic Science, Ministry of Justice. (2009). Retrieved from http://www.ssfjd.com/WebEN/WebInfo/WebInfoList02_1.aspx?ID=19

Ieong, Ricci S. C. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues, Digital Forensics Research Workshop (DFRWS).

National Institute of Justice. (2007). Digital evidence in the courtroom: A guide for law enforcement and prosecutors, U.S. Department of Justice. Retrieved from http://www.ncjrs.gov/pdffiles1/nij/211314.pdf

National People's Congress, Criminal Procedure Law. (2014).

National People's Congress Standing Committee. (February 28, 2005). "National People's Congress Standing Committee on the forensic management issues".

Notice of the Supreme People's Court, the Supreme People's Procuratorates, the Ministry of Public Security, the Ministry of State Security and the Ministry of Justice on Issuing the Provisions on Several Issues Concerning the Examination and Judgment of Evidence in Death Sentence Cases and the Provisions on Several Issues Concerning the Exclusion of Illegal Evidence in Criminal Cases. (2014). Retrieved from http://www.lawinfochina.com/display.aspx?lib=law&id=8205&CGid=

Report: Chinese Police Arrest Eight for Computer Virus. (February 13th, 2007). Retrieved from http://www.infoworld.com/d/security-central/report-chinese-police-arrest-eight-computer-virus-496

Rosenzweig, Joshua, et al (2102). The 2012 Revision of the Chinese Criminal Procedure Law: (Mostly) Old Wine in New Bottles.

Sun, Bo. (2004). Research on Key Aspects of Computer Forensic Methods. Beijing: Chinese Academy of Sciences, p.1.

Xu, Rongsheng. (2011). Digital Forensic in Mainland China, Dec 5th 2011. Retrieved from http://www.lawtech.hk/wp-content/uploads/2011/12/ChinaDF2011-HK-5.pdf

Zhai, Jianxiong (2002). Features – Judicial Information of the People's Republic of China: A Survey.

Cohen, F. (2008). Challenges to Digital Forensics Evidence. CA: Fred Cohen & Associates.

Law, F., Chow, KP, Lai, P., and Tse, H. (2009). A Host-Based Approach to BotNet Investigation, First International ICST Conference (ICDF2C). (2009). Retrieved from http://www.cs.hku.hk/cisc/forensics/papers/09_05.pdf

