Research and Review on Computer Forensics*

Hong Guo, Bo Jin, and Daoli Huang

Key Laboratory of Information Network Security, Ministry of Public Security, People's Republic of China (The 3rd Research Institute of Ministry of Public Security)
Room 304, BiSheng Road 339, Shanghai 201204, China
{guohong,jinbo,huangdaoli}@stars.org.cn

Abstract. With the development of Internet and information technology, the digital crimes are also on the rise. Computer forensics is an emerging research area that applies computer investigation and analysis techniques to help detection of these crimes and gathering of digital evidence suitable for presentation in courts. This paper provides foundational concept of computer forensics, outlines various principles of computer forensics, discusses the model of computer forensics and presents a proposed model.

Keywords: Computer forensics, computer crime, digital evidence.

1 Introduction

The use of Internet and information technology has grown rapidly all over the world in the 21st century. Directly correlated to this growth is the increased amount of criminal activities that involve digital crimes or e-crimes worldwide. These digital crimes impose new challenges on prevention, detection, investigation, and prosecution of the corresponding offences.

The emergence of highly technical nature of digital crimes was created a new branch of forensic science known as computer forensics. Computer forensics is an emerging research area that applies computer investigation and analysis techniques to help detection of these crimes and gathering of digital evidence suitable for presentation in courts. This new area combines the knowledge of information technology, forensics science, and law and gives rise to a number of interesting and challenging problems related to computer security and cryptography that are yet to be solved [1].

Computer forensics has recently gained significant popularity with many local law enforcement agencies. It is currently employed for judicial expertise in almost every enforcement activity. However, it is still behind other methods such as fingerprint analysis, because there have been fewer efforts to improve its accuracy. Therefore, the legal system is often in the dark as to the validity, or even the significance, of digital evidence [2].

* This paper is supported by the Special Basic Research, Ministry of Science and Technology of the People's Republic of China, project number: 2008FY240200.

X. Lai et al. (Eds.): E-Forensics 2010, LNICST 56, pp. 224–233, 2011.

This paper provides foundational concept of computer forensics, outlines various principles of computer forensics, discusses the model of computer forensics and presents a proposed model.

2 Definition of Computer Forensics

Those involved in computer forensics often do not understand the exact definition of computer forensics. In fact, computer forensics is a branch of forensic science pertaining to legal evidence found in computers and digital storage media.

2.1 Definition of Forensics and Forensic Science

The term forensics derives from the Latin "forensis", which means "in open court or public", which itself comes from the Latin "of the forum", referring to an actual location—a "public squarer marketplace used for judicial and other business". [3] In dictionaries forensics is defined as the process of using scientific knowledge for collecting, analyzing, and presenting evidence to the courts.

The term forensic science is "the application of scientific techniques and principles to provide evidence to legal or related investigations and determinations". [4] It aims to determining the evidential value of crime scene and related evidence.

2.2 Definition of Computer Forensics

Computer forensics is a branch of forensic science. The term computer forensics originated in the late 1980s with early law enforcement practitioners who used it to refer to examining standalone computers for digital evidence of crime.

Indeed, the language used to describe computer forensics and even the definition of the term itself varies considerably among those who study and practice it. [5] Legal specialists commonly refer only to the analysis, rather than the collection, of enhanced data. By way of contrast, computer scientists have defined it as valid tools and techniques applied against computer networks, systems, peripherals, software, data, and/or users -to identify actors, actions, and/or states of interest [6].

According to Steve Hailey, Cyber security Institute, computer forensics is "The preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found." [7].

In Digital Forensics Research Workshop held in 2001, computer forensics is defined as "the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital source for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. "

However, many experts feel that a precise definition is not yet possible because digital evidence is recovered from devices that are not traditionally considered to be computers. Some researchers prefer to expand the definition such as definition by Palmer to include the collection and examination of all forms of digital data, including that found in cell phones, PDAs, iPods and other electronic devices [8].

From a technical standpoint, Computer Forensics is formulated as an established set of disciplines and the very high standards in place for uncovering digital evidence extracted from personal computers and electronic devices (including those from large corporate systems and networks, across the Internet and the emerging families of cell phones, PDAs, iPods and other electronic devices) for court proceedings.

3 Principles of Computer Forensics

When dealing with computer forensics, the term "evidence" has the following meaning: "Any information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired in physical or binary (digital) form that may be used to support or prove the facts of an incident.

According to NIJ, the properties of digital evidence as follows: [9]

- Is latent, like fingerprints or DNA evidence.
- Crosses jurisdictional borders quickly and easily.
- Is easily altered, damaged, or destroyed.
- Can be time sensitive.

3.1 Rules of Evidence

Dye to the properties of digital evidence, the rules of evidence are very precise and exist to ensure that evidence is properly acquired, stored and unaltered when it is presented in the courtroom. RFC 3227 describes legal considerations related to gathering evidence. The rules require digital evidence to be:

- Admissible: It must conform to certain legal rules before it can be put before a court.
- Authentic: The integrity and chain of custody of the evidence must be intact.[10]
- Complete: All evidence supporting or contradicting any evidence that incriminates a suspect must be considered and evaluated. It is also necessary to collect evidence that eliminates other suspects.
- Reliable: Evidence collection, examination, analysis, preservation and reporting procedures and tools must be able to replicate the same results over time. The procedures must not cast doubt on the evidence's authenticity and/or on conclusions drawn after analysis.
- Believable: Evidence should be clear, easy to understand and believable. The version of evidence presented in court must be linked back to the original binary evidence otherwise there is no way to know if the evidence has been fabricated.

3.2 Guidelines for Evidence Handling

It is s important to follow the rules of evidence in computer forensics investigations. There are a number of guidelines for handling digital evidence throughout the process of computer forensics, published by various groups, for example, Best Practices for Computer Forensics by SWGDE, Guidelines for Best Practice in the Forensic Examination of Digital Technology by IOCE, Electronic Crime Scene Investigation:

A Guide for First Responders by NIJ and Guide to Integrating Forensic Techniques into Incident Response by NIST. Of all the guidelines referred to above, the G8 principles proposed by IOCE is considered the most authoritative one.

In March 2000, the G8 put forward a set of proposed principles for procedures relating to digital evidence. These principles provide a solid base from which to work during any examination done before law enforcement attends.

G8 Principles – Procedures Relating to Digital Evidence [11]

1. When dealing with digital evidence, all general forensic and procedural principles must be applied.
2. Upon seizing digital evidence, actions taken should not change that evidence.
3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved, and available for review.
5. An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.
6. Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

This set of principles can act as a solid foundation. However, as one principle states, if someone must touch evidence they should be properly trained. Training helps reduce the likelihood of unintended alteration of evidence. It also increases one's credibility in a court of law if called to testify about actions taken before the arrival and/or involvement of the police.

3.3 Proposed Principles

According to the properties of digital evidences, we summarized the principles of computer forensics as follows:

- Practice in a timely manner
- Practice in a legal way
- Chain of custody
- Obey rules of evidence
- Minimize handling of the original evidence
- Document any changes in evidence
- Audit throughout the process

4 Models of Computer Forensics

Forensic practitioners and computer scientists both agree that "forensic models" are important for guiding the development in the computer forensics field. Models enable people to understand what that process does, and does not do.

There are many models for the forensic process, such as Kruse and Heiser Model (2002), Forensics Process Model (NIJ, 2001), Yale University Model (Eoghan Casey, 2000), KPMG Model (McKemmish, 1999), Dittrich and Brezinski Model (2000),

Mitre Model (Gary L. Palmer, 2002). Although the exact phases of the models vary somewhat, the models reflect the same basic principles and the same overall methodology.

Most of models reviewed have element identification, collection, preservation, analysis, and presentation. To make the step more clear and precise, some of them added addition detail steps into the element. Organizations should choose the specific forensic model that is most appropriate for their needs.

4.1 Kruse and Heiser Model

Kruse and Heiser have developed a methodology for computer forensics referred to as three basic components that is acquire, authenticate and analyze[12](Kruse and Heiser, 2002). These components focus on maintaining the integrity of the evidence during the investigation. In detail the steps are:

1. Acquire the evidence without altering or damaging the original. Consisting of the following steps:

a. Handling the evidence
b. Chain of custody
c. Collection
d. Identification
e. Storage
f. Documenting the investigation

2. Authenticate that your recovered evidence is the same as the originally seized data;
3. Analyze the data without modifying it.

Kruse and Heiser suggest that in computer forensics is the most essential element to fully document your investigation including all your steps taken. This is particularly important if due to the circumstances you did not maintain absolute forensic integrity then you can at least show the steps you did take. It is true that proper documentation of a computer forensic investigation is the most essential element and is commonly inadequately executed.

4.2 Forensics Process Model

The United States of America's Department of Justice proposed a process model in the Electronic Crime Scene Investigation: A guide to first responders. [13] This model is abstracted from technology. This model consists four phases:

1. Collection; The first phase in the process is to identify, label, record, and acquire data from the possible sources of relevant data, while following guidelines and procedures that preserve the integrity of the data.
2. Examination; Examinations involve forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest, while preserving the integrity of the data.

3. Analysis; The next phase of the process is to analyze the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.

4. Reporting; The final phase is reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed and providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process.

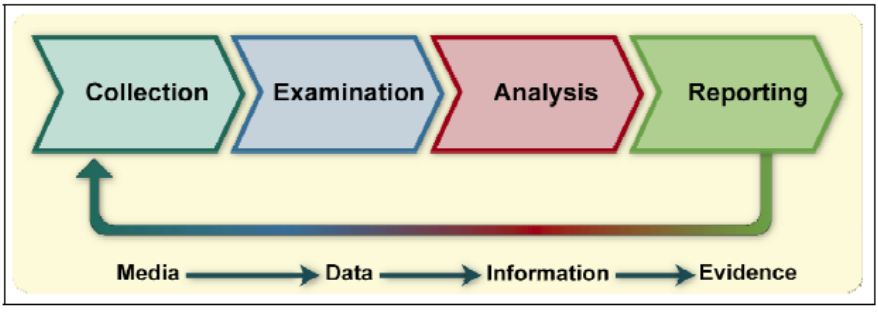

Fig. 1. Forensic Process [14]

There is a correlation between the 'acquiring the evidence' stage identified by Kruse and Heiser and the 'collection' stage proposed here. 'Analyzing the data' and 'analysis' are the same in both frameworks. Kruse has, however, neglected to include a vital component: reporting. This is included by the Department of Justice model.

4.3 Yale University Model

Eoghan Casey, a System Security Administrator at Yale University, also the author of Digital Evidence and Computer Crime (Casey, 2000) and the editor of the Handbook of Computer Crime Investigation (Casey, 2002), has developed the following digital evidence guidelines (Casey, 2000).

Casey: Digital Evidence Guidelines. [15]

1. Preliminary Considerations
2. Planning
3. Recognition
4. Preservation, collection and documentation

a. If you need to collect the entire computer (image)
b. If you need all the digital evidence on a computer but not the hardware (image)
c. If you only need a portion of the evidence on a computer (logical copy)

5. Classification, Comparison and Individualization
6. Reconstruction

This model focuses on processing and examining digital evidence. In Casey's models, the first and last steps are identical. Casey also places the focus of the forensic process on the investigation itself.

4.4 DFRW Model

The Digital Forensics Research Working Group (DFRW) developed a model with the following steps: identification; preservation; collection; examination; analysis; presentation, and decision. [16] This model puts in place an important foundation for future work and includes two crucial stages of the investigation. Components of an investigation stage as well as presentation stage are present.

4.5 Proposed Model

The previous sections outline several important computer forensic models. In this section a new model will be proposed for computer forensics. The aim is to merge the existing models already mentioned to compile a reasonably complete model. The model proposed in this paper consists of nine components. They are: identification, preparation, collection, preservation, examination, analysis, review, documentation and report.

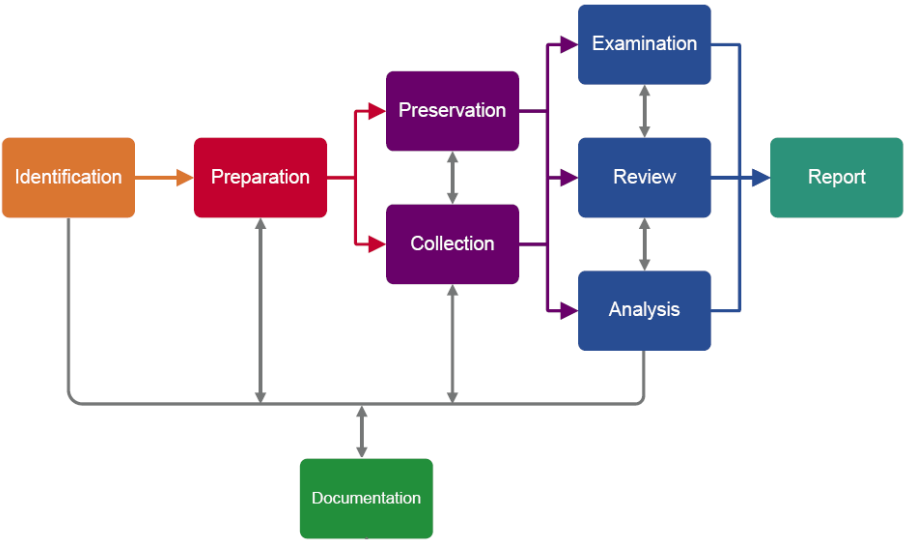

Fig. 2. Proposed Model of computer forensics

4.5.1 Identification

1. Identify the purpose of investigation.
2. Indentify resources required.
3. Indentify sources of digital evidence.
4. Indentify tools and techniques to use.

4.5.2 Preparation

The Preparation stage should include the following:

1. All equipment employed should be suitable for its purpose and maintained in a fully operational condition.
2. People accessing the original digital evidence should be trained to do so.
3. Preparation of search warrants, and monitoring authorizations and management support if necessary.
4. Develop a plan that prioritizes the sources, establishes the order in which the data should be acquired and determines the amount of effort required.

4.5.3 Collection

Methods of acquiring evidence should be forensically sound and verifiable.

1. Ensures no changes are made to the original data.
2. Security algorithms are provided to take an initial measurement of each file, as well as an entire collection of files. These algorithms are known as "hash" methodologies.
3. There are two methods for performing the copy process:

- Bit-by-Bit Copy:

This process, in order to be forensically sound, must use write blocker hardware or software to prevent any change to the data during the investigation. Once completed, this copy may be examined for evidence just as if it were the original.

- Forensic "Image"

The examiner uses special software and procedures to create the image file. An image file cannot be altered without altering the hash algorithm. None of the files contained within the image file can be altered without altering the hash algorithm. Furthermore, a cross validation test should be performed to ensure the validity of the process.

4.5.4 Preservation

1. Ensure that all digital evidence collected is properly documented, labeled, marked, photographed, video recorded or sketched, and inventoried.
2. Ensure that special care is taken with the digital evidences material during transportation to avoid physical damage, vibration and the effects of magnetic fields, electrical static and large variation of temperature and humidity.
3. Ensure that the digital evidence is stored in a secure, climate-controlled environment or a location that is not subject to extreme temperature or humidity. Ensure that the digital evidence is not exposed to magnetic fields, moisture, dust, vibration, or any other elements that may damage or destroy it.

4.5.5 Examination

1. Examiner should review documentation provided by the requestor to determine the processes necessary to complete the examination.
2. The strategy of the examination should be agreed upon and documented between the requestor and examiner.
3. Only appropriate standards, techniques and procedures and properly evaluated tools should be used for the forensic examination.
4. All standard forensic and procedural principles must be applied.

5. Avoid conducting an examination on the original evidence media if possible. Examinations should be conducted on forensic copies or via forensic image files.

6. All items submitted for forensic examination should first be reviewed for the integrity.

4.5.6 Analysis

The foundation of forensics is using a methodical approach to reach appropriate conclusions based on the evidence found or determine that no conclusion can yet be drawn. The analysis should include identifying people, places, items, and events, and determining how these elements are related so that a conclusion can be reached.

4.5.7 Review

The examiner's agency should have a written policy to establishing the protocols for technical and administrative review. All work undertaken should be subjected to both technical and administrative review.

1. Technical Review

Technical review should include consideration of the validity of all the critical examination findings and all the raw data used in preparation of the statement/report. It should also consider whether the conclusions drawn are justified by the work done and the information available. The review may include an element of independent testing, if circumstances warrant it.

2. Administrative Review

Administrative review should ensure that the requester's needs have been properly addressed, editorial correctness and adherence to policies.

4.5.8 Documentation

1. All activities relating to collection, preservation, examination or analysis of digital evidence must be completely documented.

2. Documentation should include evidence handling and examination documentation as well as administrative documentation. Appropriate standardized forms should be used to document.

3. Documentation should be preserved according to the examiner's agency policy.

4.5.9 Report

1. The style and content of written reports must meet the requirements of the criminal justice system for the country of jurisdiction, such as General Principles of Judicial Expertise Procedure in China.

2. Reports issued by the examiner should address the requestor's needs.

3. The report is to provide the reader with all the relevant information in a clear, concise, structured and unambiguous manner.

5 Conclusion

In this paper, we have reviewed the definition, the principles and several main categories models of computer forensics. In addition, we proposed a practical model that establishes a clear guideline of what steps should be followed in a forensic process. We suggest that such a model could be of great value to legal practitioners.

With more and more criminal behavior becomes linked to technology and the Internet, the necessity of digital evidence in litigation has increased. This evolution of evidence means that investigative strategies also must evolve in order to be applicable today and in the not so distant future. Due to this trend, the field of computer forensics will, no doubt, become more important to help curb the occurrences of crimes.

References

1. Hui, L.C.K., Chow, K.P., Yiu, S.M.: Tools and technology for computer forensics: research and development in Hong Kong. In: Proceedings of the 3rd International Conference on Information Security Practice and Experience, Hong Kong (2007)
2. Wagner, E.J.: The Science of Sherlock Holmes. Wiley, Chichester (2006)
3. New Oxford American Dictionary. 2nd edn.
4. Tilstone, W.J.: Forensic science: an encyclopedia of history, methods, and techniques (2006)
5. Peisert, S., Bishop, M., Marzullo, K.: Computer forensics in forensis. ACM SIGOPS Operating Systems Review 42(3) (2008)
6. Ziese, K.J.: Computer based forensics-a case study-U.S. support to the U.N. In: Proceedings of CMAD IV: Computer Misuse and Anomaly Detection (1996)
7. Hailey, S.: What is Computer Forensics (2003), http://www.cybersecurityinstitute.biz/forensics.htm
8. Abdullah, M.T., Mahmod, R., Ghani, A.A.A., Abdullah, M.Z., Sultan, A.B.M.: Advances in computer forensics. International Journal of Computer Science and Network Security 8(2), 215–219 (2008)
9. National Institute of Justice.: Electronic Crime Scene Investigation A Guide for First Responders, 2nd edn. (2001), http://www.ncjrs.gov/pdffiles1/nij/219941.pdf
10. RCMP: Computer Forensics: A Guide for IT Security Incident Responders (2008)
11. International Organization on Computer Evidence. G8 Proposed Principles for the Procedures Relating to Digital Evidence (1998)
12. Baryamureeba, V., Tushabe, F.: The Enhanced Digital Investigation Process Model Digital Forensics Research Workshop (2004)
13. National Institute of Justice.: Electronic Crime Scene Investigation A Guide for First Responders (2001), http://www.ncjrs.org/pdffiles1/nij/187736.pdf
14. National Institute of Standards and Technology.: Guide to Interating Forensic Techniques into Incident Response (2006)
15. Casey, E.: Digital Evidence and Computer Crime, 2nd edn. Elsevier Academic Press, Amsterdam (2004)
16. National Institute of Justice.: Results from Tools and Technologie Working Group, Goverors Summit on Cybercrime and Cyberterrorism, Princeton NJ (2002)