# Research On Some Relevant Problems in Computer Forensics

Yongquan Wang [1, 2]
1. Department of Information Science and Technology
East China University of Political Science and Law
Shanghai 201620, P. R. China
e-mail: wangyongquan@ecupl.edu.cn

Henry C. Lee [2]
2. The Henry C. Lee Institute of Forensic Science
University of New Haven
CT 06516, U. S. A
e-mail: hlee@newhaven.edu

***Abstract*—In order to effectively combat and control the cybercrime, the crucial precondition to solve those problems is to study how to quickly and efficiently collect evidences which can be accorded with legal requirements. From the features of computer forensics and Based on the thought, theory and method of traditional crime scene investigation, this paper has made a thorough thinking, research and analysis on computer forensics and its relevant problems involved in it, such as the law, the theory, the technology and the procedure rule by combining law and technology. At last, the future direction of computer forensics has been presented. That will be benefit to the justice practice and the development of theory and technology of computer forensics.**

***Keywords-computer forensics; black box; law; technology; procedure rule***

## I. INTRODUCTION

With the rapid development of information technologies and wide use of computer networks, computer forensics has become an active research area due to increasingly criminal activities in communication networks and information security.

According to the 30th Statistical Survey Report on Internet Development in China [1], as of 30 June 2012, the number of Internet users has reached 538 million along with an increase of 39.9% in the use of Internet. We have also witnessed an explosive growth in the number of blog users from over 63 million in 31 December 2010 to more than 353 million with an about increasing rate of 560.3%. E-commerce activities such as online shopping and network transaction such as online bank and online paying have also expanded rapidly. Network applications such as instant messaging, search engines, business transactions, online music, online news, online video, and micro-blog have also become the major interests of Internet users. Therefore, there is an increasing demand on Internet and network applications. In USA, more than 90% large enterprises and 80% small medium enterprises use Internet for business transaction. Computers and networks have become an important part of social and economic life.

Computer and network crimes such as attacks caused by computer virus or Trojan, network Infringement disputes, network frauds, online pornography and gambling are getting worse because of the wide penetration of computers and Internet which leads to tremendous economic loss and increasingly prominent social problems.

Recent years, with the appearance and promotion of the new technologies such as the Internet of things, cloud computing and the confusion of the three networks, the technologies of computer network are improving. At the same time, computer (cyber) crimes are presented with new variations with characteristics of difficulties of discovering, capturing, proving and controlling.

To solve these civil disputes or fight with the criminal activities in computer communication networks, we will need to find adequate, reliable and convincing evidence.

Computer-related crime cases usually play three roles - the target of hacking, crime tools and criminal information storage [2], with each case having a large amount of data retained in computers and their peripherals. It is of vital important to find the evidence of a crime case using relevant techniques and methods. Therefore the research on computer forensics related to criminal activities in communication networks is receiving more and more attention in the interdisciplinary field of computer and law. Currently, computer forensics has many definitions. We argue that computer forensics is a process of finding evidence from computer systems to prove the existence of an objective fact making use of computer related technologies and approaches.

Computer evidence refers to computer materials and their derivatives which can be used as evidence against criminal activities. It is related to electronic evidence but they are not equally equivalent. In most cases, computer evidence is different from the electronic evidence in the extension, due to the reason that mechanical computer, optical computer, bio computer based evidence can only be used as electronic evidence with an equivalent function. In addition, computer evidence is different from electronic evidence in the aspect of content. For example, the fixed telephone is a modern communication means which builds on semiconductor technology using analog electronics. The recorded materials belong to electronic evidence but not computer evidence. Electronic technology made of modern communication tools, it recorded telephone information on electronic evidence are not part of computer evidence. Although computer evidence differs from electronic evidence in the aspects of connotation and extension of the concept, we normally do not differentiae them. We can follow a standardization approach to specify the complete or partial evidence type. This paper uses the word of computer forensics and presents in depth an analysis and an exploration on criminal activities in communication networks based on forensics tools or software being used.

Published by Atlantis Press, Paris, France.

In order to effectively combat and control the computer crime or cybercrime, the crucial precondition to solve those problems is to study how to quickly and efficiently collect evidences which can be accorded with legal requirements. From the features of computer forensics and Based on the thought, theory and method of traditional crime scene investigation, this paper has made a thorough thinking, research and analysis on computer forensics and relevant problems involved in it, such as the law, the theory, the technology and the procedure rule by combining law and technology. That will be benefit to the justice practice and the development of theory and technology of computer forensics.

## II. THE LEGAL ISSUES OF COMPUTR FORENSICS

The legal issues of computer forensics main focus on the following three topics: computer crime, computer forensics, the subject and procedure of computer forensics, and electronic evidence.

### *A. Implications of Computer crime and computer forensics*

Computer crime refers to the severe act against society which endangers the order of the computer industry, violates the laws and regulations for the protections of computer software and information security system, infringes the rights and interests of obliges, and other acts who severely poses dangers to society, it is usually a covert, cross-border act implemented by intelligent, anonymous criminals with low cost but high loss to the society. It involves a wide range of interesting, it is difficult to let the victims to start proceedings [3-5].

Computer forensics refers to the process of verifying, protecting, extracting and documenting the electronic evidences in computer and related equipment which should be reliable, persuasive and sufficient enough to be accepted by the count. Compared with the traditional crime scene investigation and evidence, Because computer data is vulnerable to tampering, forgery and deletion, in order to make electronic data be collected as evidence, its probative force must be strengthened to ensure that, in its generation, storage and delivery process it should maintain its originality, credibility and integrity, and the continuity of the evidence, so as to be accepted by court. To meet these requirements, the following points must be paid attention to in the process of computer forensics: (1) Do not analysis the original data directly. (2) The software for data analysis must be ensured to be safe and credible. (3) Analysis of the data should have digital signature before analyzing the data. (4) It is necessary to describe in detail and file the damaged computers, including the original state and surrounding environment of damaged computer system, analysis methods, the specific operation, results and the result of analysis. (5) It must be backed up after the analysis is complete each time. (6) The evidence obtained must be preserved properly to prevent it from being damaged, altered, which causes it to lose the legal effect. The common forensics technology includes: monitoring technology for electronic evidence, physical evidence, and access to technology, electronic evidence collection and preservation of electronic evidence handling and identification techniques, electronic evidence examination and submission technology and so on.

### *B. Problems of the main body of computer forensics and procedure law*

Because of the high requirements of electronic evidence collection techniques, the main body of computer forensics needs to have some computer knowledge and to follow strict standards and procedures in the process of forensics [6, 7]. In computer forensics, we need to delegate or to employ a particular group of electronic technical experts or computer experts to assist in evidence collection. In criminal proceedings, the evidence given by electronics expert or computer expert needs to be under the guidance of the investigators or the network police.

For the program of computer forensics, electronic evidence obtaining should follow the principle of fairness, voluntariness and truth, and the parties shall not trespass computer information system to obtain evidence. If the evidence is provided by a third party, the third party should be issued to ensure that the evidence generated or received must always maintain the original state and that he will provide documents of evidence of digital signature voluntarily. Due to the fact that it is difficult to obtain other evidences for the parties, the burden of proof in disputes due to the infringement shall be borne by the tortfeasor. There are many ways to obtain evidence, but they must be in the form of legislation, which offers procedures and authority to obtain electronic evidence. In particular, when asking for an item of evidence from the ISP, professional network companies or a data company, one should strictly abide by the confidentiality agreement and the terms of service signed with the customers because it is not allowed to disclose users' personal information and usurp the privacy materials and confidential information in the name of litigation needs. Electronic evidence collection, application and determination should undergone a process of improvement and standardization gradually, which depends on the development and promotion of technology to a large extent. Therefore, the legislation should advance with flexibility, and not develop the terms with large quantity. At the same time, we should have to note a harmful tendency: as electronic evidence is both invisible and destructive, we demand harsh requirements for electronic evidence. It seems that all the electronic evidence can only be counted as indirect evidence and that we cannot ensure its credibility unless it is in complete safety. But this incline should not be taken. In fact, virtually any kind of evidence can be forged, altered and destroyed, and any traditional evidence has the threats of loss and the difficulty of reproduction. With regard to selection and recognition of the evidence, each contractor has different levels of using of the principle of free evaluation of evidence, so the law should set too many obstacles for judicial officials to judge the evidence.

### *C. Legal issues of electronic evidence*

Electronic evidence, also known as computer forensics, computer data evidence, documentary evidence, generally refers to that, in the process of computer crime, evidence is

physically stored within the computer system memory to prove the computer crime. Compared with traditional types of evidence, it is accurate, fragile, perishable, concealed, complex, diverse and easy to diffuse. In addition to that, electronic evidence collection is rapid to collect, easy to store, taking up little space with great capacity, transmission and convenient transportation. It can be reproduced, with simple application and operation.

Concerning electronic evidence eligibility, the hearsay rule and the best evidence rule hinder the electronic evidence to be admitted into evidence in common law, but countries make the evidence qualifications by extending the original connotation and replacement of the original method. Countries in continental law system generally require it to provide original evidence. Provisions in many countries of continental law system are relatively broad and general principles recognize the electronic evidence. Procedure laws of China holds that "facts that prove the real situation of the case are all evidence" and this general provision offers the space and the legal basis for the use of electronic evidence in litigation. Therefore, whether the electronic evidence can be evidence is not so controversial in China.

We can also use positive identification method to prove the power of electronic evidence, i.e., to start from identifying the evidence itself, or the other side of evidence. We review the following aspects using the positive methods to find the probative force of electronic evidence: (1) The generation of electronic evidence; (2) The storage of electronic evidence; (3) The transmission of electronic evidence; (4) Electronic evidence collection; (5) Whether the electronic evidence has been deleted. Positive method proves the power of electronic evidence based on the identification of the ordinary evidence principles. However, due to the fact that electronic evidence is vulnerability, easy to be altered, increased and deleted, which is often difficult to detect, it is unrealistic to have the integrity of electronic evidence from being tampered, increased and excision. Then we must use the presumption to ensure the integrity of electronic evidence. Of course, the defence can research on the electronic evidence in computer crime and its rules of evidence to debate.

For the position of the electronic evidence, this subject identities it as independent types of evidence. The reason is that it is different from the audio-visual materials, the traditional evidence and the mixed evidence.

In making the electronic evidence into the audio-visual materials, we need to expand the interpretation of audio-visual materials, and to break the boundaries of audio-visual materials on the evidence of the tapes, video tapes and so on; In addition, the electronic evidence is expressed in binary data to a digital signal, which the other kind of evidence does not possess. Finally, the position of the audio-visual materials in the law of evidence is limited. At best, it is a tool for confirming the parties' statements, evidence, and so on. Therefore, we believe that bringing electronic evidence into audio-visual materials simply will limit its effectiveness of evidence, and it is not conducive to the facts of the case.

Electronic evidence should also not be included in the traditional documentary evidence. First, it is difficult for the electronic evidence's long-term storage and safety. Electronic evidence in computer and network may be exposed to viruses, hacker attacks, misuse, and also be easily damaged or eliminated, while the traditional documentary evidence do not have these troubles; Secondly, electronic evidence can not be read directly and its access and transmission depends on the support of modern information technology service system. If there is no appropriate IT equipment, it is difficult to see the fact that the evidence reflected upon, and the extraction of electronic evidence is much more demanding than traditional documentary evidence; finally, although the content recorded in the tradition documentary evidence is also easy to be changed, as in judicial practice, there have been many situations that the parties change or add the contents of the documentary evidence for self-interest, the electronic evidence stored in the computer is more convenient for the correction, modification or supplement of a variety of data, even if the data encrypted has the possibility to be decrypted.

Electronic evidence is different from the mixed evidence. For mixed evidence, we believe that the mixed evidence is open to question for the classification. First, the information stored in a disk and CD-ROM is not the objective existence for its own property, the external characteristics or existence to prove the case. Therefore, the disk or CD-ROM is not the evidence; Secondly, using computer for simulating crime to determine the possibility of a crime is not the record of inspection; Finally, the evidence from computer and its testing system must be divided into two parts.

Because the standards and methods for reviewing electronic evidence are different from the traditional ones, the rules and methods for collection, extraction, application rules and preservation of electronic evidence are different from the traditional ones. Only by giving electronic evidence independent legal status, can it provide effective protection for the sound and orderly development of the application of information technology for e-commerce.

## III. THE TECHNICAL AND THEORETICAL QUESTIONS OF COMPUTER FORENSICS

This part, we investigate the technical methods and models, then propose a computer forensic black box system model.

### *A. Technical methods of computer forensics*

- Forensic Technologies based on Algorithms and Software Analysis. (1) Cryptography. In many cases, computer forensics needs to deal with the problems on how to decrypt the encrypted data. Currently there are a number of encryption and decryption algorithms and relevant tools. The cryptographic techniques and methods used in computer forensics mainly include: ① Cryptanalysis: The technology requires that a password forensic expert have specialized knowledge in the field of cryptography. It is worth noting that the existing software tools are not practically applied. ② Password cracking techniques: These include passwords dictionary, key

guessing, brute-force techniques. Password dictionary is generally based on software and there are a variety of dictionaries available. Many dictionary-based password cracking software packages are available with a relatively high cracking rate. For example, AOPR is such a cracking tool dedicated to Office files. ③Password search: These include physical search in the physical environment around the computer, logical search in the documents of computer systems, and network eavesdropping in email messages and network environments. ④ Password extraction: In general, many of the Windows passwords are in plain text form and stored in the registry or other designated places. Therefore, passwords can be extracted from the registry files. ⑤ Password recovery: Using password recovery mechanism, password can be obtained from the system administrator. (2) Data Mining Technology. Data mining is a decision support process, mainly based on artificial intelligence (AI), machine learning, statistical techniques and methods, highly automated analysis of massive amounts of data obtained, and the inductive reasoning. In this way, knowledge can be obtained to predict the behaviour trends of the analyzed objects which can help decision-makers or managers to adjust strategies to make the right decisions. Data mining is highly valuable in analyzing criminal behaviours. The criminal patterns, trends, and the associations among criminal behaviours can be found by designing high quality data mining algorithms to analyse large amounts of historical criminal records which are stored in data warehouses and maintained in a consistent way. The obtained knowledge is of value to police and judicial departments.

- Hardware-based Forensics. (1) Data Recovery Technology. Data recovery technology is primarily used to recover the data from the deleted files and formatted disk of the suspects. Disk formatting only re-organizes the entries to file systems. Data will still be available if it is stored before disk formatting. Disk formatting will create a new blank index table links with unallocated data blocks. The operation of deleting files does not permanently remove the files from disk, but put the data blocks back into the file system which is invisible for normal read and write operations. Therefore, we can use popular and promising forensic software tools such as TCT and ENCASE to recover data. Based on optics principles, these tools recovers data by analyzing the refraction, spectral radiation and diffraction. Many companies provide such data recovery services such as Ontrack company and Ibas laboratory. (2) Computer Forensics Chip Design. It is understood that among the products in computer forensics in China, the "forensics machine" produced by the Computing Center of the Institute of High Energy Physics, Chinese Academy of Sciences can detect the ways that hackers intrude and produce analysis reports which can be used as legal evidence. In addition, the detection box of computer evidence mainly developed by Xiamen Meiya Pico Information Co. Ltd. in Xiamen city, China, has the functions such as evidence extraction, cracking, analysis and recovery. Many forensic tools are also available in other countries, notably TCT and EnCase. TCT can analyze the activities of the running machines in real time and capture the current state information. EnCase is a product that is recognized by the U.S. government for computer forensics. EnCase is an integrated forensics application based on Windows interfaces. Its features include data browsing, search, disk browsing, creation of evidence files, saving cases. Among the existing computer forensics tools, hardware based products are mainly focused on the aspects of "data erase forensics interface of hard disk", "hard disk data cloning" and "network monitoring", whereas software products are mainly on "file content browsing (text and images)", "text search using keywords", "undelete ", "drive imaging (copying the full storage space bit by bit). Currently there are no uniform standards and specifications that forensics tools can follow in the study of computer and network related crimes. It is therefore hard for users to compare the effectiveness and reliability of these tools. To this end, Brain Carrier proposed to use open source tools to ensure the reliability of the forensics tools [8]. Although the reliability can be improved through the testing work contributed by many researchers, the ownerships and interests of these tools have to be reflected.
- Forensics based on Tightly Coupled Hardware and Software. (1) Post-Event based Static Analysis. Regardless of the roles that computer crimes play like "hacker intruder", "crime tool" or "criminal information storage", a large amount of crime-related data will be left in the computer and its peripheral equipment. Therefore, this data can be obtained through static analysis (i.e. static computer forensics which is also referred to as computer forensic) to be used as the evidence of litigation. The nature of static analysis is that it considers computer as a crime scene, and analyzes the criminal behaviours in network communications in the form of forensic anatomy and also conducts a detailed analysis on the data stored in various computing medias. In this way, the important data and reports associated with the facts can be obtained. Post-event based static analysis includes two stages: " physical evidence acquisition" and "information discovery". The former refers to the process that investigators search for relevant computer hardware at computer crime or intrusion scene and keep it for investigation. The latter searches for evidence from the original data including files and logs which can be used to support the associated facts or refute them. Similar

to other evidence, computer evidence or electronic evidence must be true, reliable, complete and complies with relevant laws and regulations and judicial procedures. It should be pointed out that physical evidence acquisition is the basis of the whole forensics process. When obtaining physical evidence, the most important thing is to ensure that the evidence obtained is original without any damage. It is extremely difficult to find all the relevant data as computer crime evidence may exist in the system log, data files, hidden files, registers, swap buffer, user process memory, stack, file buffers, the file system itself, free disk space, the printer buffer, network data buffer, and the counter location. To this end, trade-offs have to be made through a thorough analysis and judgement. In static computer forensics, information discovery comes after physical evidence has been obtained. Computer crime cases have different requirements on information discovery. Some cases only need the key documents, pictures or email messages, while others might need to reproduce the details of the work happened. Unless there are special needs, under normal circumstances, information discovery is a process that makes a physical copy of the original data with an aim to protect the original data. Typically, forensics experts also use MD5 algorithm to summarize the data in the original evidence and keep the evidence and the summary in a safe place. Considering the files that contain evidence of a crime may have been deleted, data recovery is needed to recover the key files, communication records and other clues. In the mean time, this process also facilitates acquisition of file attributes and document processing. After data is recovered, forensics experts should carefully conduct queries based on keywords, analysis, analyze file attributes and digital summary, search for system logs, decrypt documents, access Windows swap buffers. The results of information discovery largely depends on forensics experts' experience and wisdom due to the lack of tools for comprehensive data analysis. This requires that a qualified forensics personnel must have a profound understanding of information systems with an expertise in computer architecture, operating systems, distributed computing, database theory and applications, network architecture and protocols. In this way, forensics experts can produce comprehensive reports based on the results of information discovery which will become an important basis in against crime. (2) Pre-Event Prediction and dynamic Detection. With the popularity and penetration of network applications, it is difficult to use static analysis which is mainly used for standalone computer forensics to detect and acquire evidence in real time to meet the growing number of cyber crimes. To minimize the defects of passive firewall technologies and intrusion detections, forensics can be conducted via pre-event prediction and dynamic detection method referred to as dynamic computer forensics (DCF). DCF incorporates forensics technology into firewall systems, intrusion detection systems and honeypots to dynamically detect all the possible computer crimes in communication networks, capture data in real-time and analyze the intentions of intruders. DCF takes effective measures to cut off the network connections or to induce the intruders to provide more information. In this way, as much as possible data can be obtained and analyzed with a safe running of the system. It can be noted that DCF can produce complete and true evidence. In the mean time, it can also analyze the means and motivations of crimes for right decisions which triggers relevant firewall and detection systems to action on intrusions. This facilitates the interactions between computer forensics, firewall and detections systems. Through system self structure changes and backup strategies, all the aspects in the communication network can be protected which leads to an integrated security infrastructure. DCF can record the working status of the system especially the whole process of hacker intrusion. It can capture and analyze the intrusion behaviours through which self defence strategies can be generated. DCF mainly involves the stages of data acquisition, data analysis, evidence identification, preservation of evidence and evidence submission as following in detail [9]. ① Data Acquisition: The volume of data in data acquisition phase is very large and data is updated from time to time, (e.g. on a daily basis, millions of event records may be generated on a Web). This kind of data includes system logs, logs related to firewall, FTP, WWW, and anti-virus software, system audit records, network traffic monitoring, the relevant operating system (such as the Windows operating system) and the hidden files or temporary files of databases, database operation records, hard drive swap, slack data and free buffers, software configuration data; script files, Web browser data buffers; e-mail; real-time chat records, bookmarks, history records or session logs. For the acquisition of these massive data, the network data can be obtained via a dedicated hardware. The core idea is to set the network card to promiscuous mode in order to monitor the data passing through the network segment. The header of every packet received will be analyzed and matched with certain rules. The matched data will be stored in network data files. Unmatched data will be discarded. In general, network data files are stored in a binary format based on time intervals for subsequent analysis. ②Data Analysis: In the data acquisition stage, the use of data acquisition software (technology) to collect large amounts of data. The key to DCF is to mine meaningful information from massive data sets, to identify its association with a certain case, to reflect the objective facts of the case which can be accepted

by court for computer evidence (or electronic evidence). Therefore, data analysis is the key stage of DCF. Data mining techniques such as association analysis, classification analysis, link analysis [10] are used in order to ensure the timeliness, effectiveness, intelligence, adaptability and scalability of forensics data in DCF. ③Evidence Judgement: Through data analysis and filtering, the course of commission of the crime can be determined based on criminal behaviours and pattern in communication networks which include the invasion time, the IP address used, files added or deleted, files uploaded and downloaded. In this way, crime evidence can be obtained and processed by court. ④Preservation of Evidence: Through analysis, once the evidence is identified, the next step is to preserve the evidence to prevent tampering or deleting from internal and external unauthorized users. Disk encryption technology is commonly used for storing encrypted evidence. The main disk encryption methods are hard coding some software, laser perforation, mask encryption and encryption chips. Encryption can also be done by modifying the disk parameter table (such as sector space, free high-track). In addition, stack overflow protection can be applied to prevent hackers to attack the system. ⑤ Evidence Submission: The whole process of computer forensics must not be tampered. To this end, the evidence obtained should be submitted to court following the legal procedure of judicial practice which can be used as the basis for sentencing of computer and network crimes. Certain technological approaches must be in place when submitting evidence. For example, in the process of transmitting evidence or data, these approaches not only have the ability to resist the illegal invasion of hackers, but also to improve the confidentiality of evidence (or data) submitted remotely. To this end, encryption technologies are use such as IP encryption, VPN encryption, SSL encryption, to ensure secure transmission of data or evidence. In addition, the message authentication code (MAC) can also be used to ensure the integrity of evidence or data during transmission.

### *B. Computer Forensics Models*

Many fruits have achieved in computer forensics research, most of them are in the law and computer science fields. The research of Computer forensics in computer science area includes two aspects: Theoretical research and Practical research. Theoretical research has higher abstractness, which is emphasized on finding the scientific foundation of computer forensics, focused on the research of computer forensics models and the universal problems in the computer forensic process. Practical research stressed more on the practice, which applies abstract theory into judicial practice and points out its exploratory trends.

Up to date, more than ten kinds of common computer forensic models have been proposed [11-17], such as Basic Process Model, Incident Response Process Model, Law Enforcement Process Model, The Integrated Digital Investigation Mode, The Enhanced Digital Investigation Process Model, Requirement Based Computer Forensics Process, Level Computer Forensics Model, Multi-Dimension Computer Forensics Model, and Multi-Dimension Computer Forensics Model Based on Trust, Computer Forensics Model Based on Dynamic-Collection, Simulation Analysis of Forensics Model, and Model of Digital Data Forensics Based on Trusted Probability. Each of them has their strong point to solve different problems, but until now, we haven't found a model that can solve all of these problems, so researches in this area are still going on.

### *C. Computer forensic black box system*

Current researches mainly focus on the computer forensics itself, in other words, they are the researches of how to collect evidence from the massive data in the existing network system, however, there haven't any research that lay emphasis on how to form a lawful, valid and standardized evidence automatically when the crime occurred ("black box" evidence), so that the police and procurator organs (investigative organs) can easily obtain computer evidences that are related to the case. In brief, without good "black box", we have no effective evidence. Study on the computer forensics technology is actuality one side, while the study of the standardized evidence and the design of the "black box" are of significantly importance.

Now, we present the view that we should embed the computer forensic black box into the computer and network system. At the same time, we think that the black box should have the following function: which is that it can automatically record the data, logs and reports that are related to the running state of the computer system and its safety, and can let the law enforcement or management officers easily obtain the data in the black box, and then use them as digital evidence. In other words, the black box can locate digital evidence rapidly, so as to improve the reliability of the related digital evidence, drop the cost of controlling crime. Furthermore, in order to do those basic functions, as a system model, we think that this black box system should include the following modules such as the application layer, transition layer, data process layer and interface layer (see Fig. 1). The application layer is responsible for accomplishing all user requests, which includes User Management, Register Module, Data Query, Key Update, Time Update, personal data process and so on; The transition layer is responsible for accepting the data manipulations that are identified by the application layer, and transform them into a series of inner manipulations that can be managed by the black box core process layer; The data process layer is the kernel of the black box, which includes three parts: black data warehouse, key relational database and the black box data process sub-system; The interface layer is the data interaction interface between the black box system and other data source related systems. Based on the different requirements, the data source related systems can be operation systems, application systems and computer networks.

Computer forensic black box system constructed as above presents a data generation and protection method, which can be compromise well with existing technologies, there are two ways: One way is to use the existing theory and technology in the data source part; the other is to use them in the application layer. In short, we can use the outcome data of the existing computer forensics technologies as source data of the black box system or using the black box system data as source data of other computer forensics technologies.

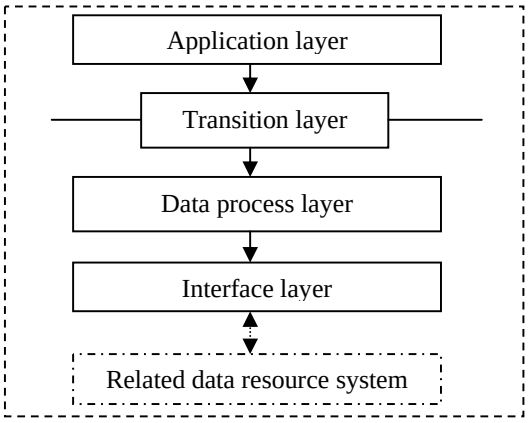


Fig. 1 Black box system

## IV. THE PROGRAMS AND RULES OF COMPUTER FORENSICS

### A. *The principles and procedures of Computer Forensics*

In order to ensure of the scientificality and legality of the computer forensic, and also obtain the evidence with high quality and at the same time be recognized for more people, in computer forensics, some basic principles are needed to be followed. These principles include scientific principles, legal principles, promptly principles, standardization principles, repeatability principles. Scientific principles mean that the information obtained in computer forensics should meet the objective factual circumstances, and computer forensics should be implemented in accordance with standard methods and procedures. Legality contains the legitimacy of starting the program and implementing the program of the computer forensics.

Accords with the analysis of the existing computer forensics model, combines with the common characteristics of the different legal activities, divide the procedures of computer forensics into three important subprograms: the start of the program, the implementation of the program, the show of the program.

The start of the program includes: obtaining the permission by law of the computer forensics, planning of the program strategy of the detailed computer forensics, human and financial resources must be equipped with the Computer Forensics.

The implementation of the program of the computer forensics is carried out after the start up program in computer forensics. Because of legal activities of a different nature and the different technical methods it uses, computer forensics implementation of the program differs. Usually, several or all of the activities below are needed to be completed: site disposal and survey activities, electronic data or evidence to be obtained and fixed activities, analysis and identification of activities of electronic data, tracking activities of computers or persons involved, assessments of computer forensics implementation activities, computer forensics related legal instruments or review activities.

The program of computer forensics also includes the show of computer forensics. When inquests are displayed and judicial expert opinion or other legal instruments are issued according to the results of the implementation of activities under the computer forensics, the digital evidence collected by the computer forensics activities and related survey results may be applied to the proceedings. Finally, accepting litigation involved in the investigation or cross-examination. At this point, the computer forensics process is not over, it also includes a series of preparedness and response activities involved with computer forensics evidence presented in court.

### B. *Quality control of the Computer Forensics*

Currently, we counter an important problem is how to find an efficient way to improve the identification quality from the perspective of forensic institutions to manage. However, it is very important that the management and quality control in computer forensics (forensic field) must meet two basic principles: one is that the management of the identification of activities must comply with the principle of combining internal management with external supervision; the other is that forensic activities are required to comply with the full range and multi-level control principles.

## V. CONCLUSIONS

In recent years, although a significant progress has been made in computer and network forensics from the aspects of both theory and practice, limitations still exist which is hard to meet the objective requirements of forensic technology of social and judicial practice. In summary, forensics is moving towards the following directions:

### A. *Intelligent and automated*

Computer forensics will be further integrated, intelligent and automated. On the one hand, forensic technology in data acquisition and data analysis phases will continue to use the new intelligent information processing techniques such as data mining, a variety of effective, intelligent computing methods (fuzzy sets and fuzzy reasoning, rough set theory and methods). On the other hand, research is needed to facilitate forensics tools to automatically generate legal, effective and standardized evidence when computer and cyber crimes occur for use by police and inspection departments.

### B. *Integrated*

Computer forensic technology is integrated with system design and implementation. The future computers, network systems and software will be designed with forensics or forensics tools which considers computer forensics as a major component of computer networks and information

Published by Atlantis Press, Paris, France.

security systems to maximize the data volume in evidence within a certain level of cost in design.

### C. Specialized computer forensic tools [18, 19]

In cyber crimes, in addition to computers and networks and workstations, the current extensive use of mobile devices such as portable computers, PDAs, mobile phones may become the targets or instruments of crime. Evidence of a crime will be distributed in computers, portable devices, routers, switches, mobile phones in various forms. Therefore, the design of specialized and effective forensic tools and products (including hardware and message formats) for different cases is also an important direction in research.

### D. Cloud forensics

Computer Forensics in emerging network environments. With the development of emerging information network technologies such as Cloud Computing and the Internet of Things, new computer forensics technologies such as cloud forensics based on Cloud Computing or forensics cloud platform have to be investigated to meet these requirements.

### E. Combination

Combination of "black box" and other computer forensic technologies. How to construct a better or efficient "black box" and combine the black box with data mining technology, fuzzy set theory and rough set theory after demonstrating the function and model of black box system.

In addition, computer forensics is a multi-disciplinary field which involve law, computers and networks (e.g. disk analysis, encryption, graphics and image processing, audio files, log information mining, database technology, operating system), applied mathematics and physics (such as the physical properties of media). It has become a high priority in developing forensics techniques and tools which meet the objective requirements of legal norms and judicial practice of China taking into account the emergence of new information and communication technologies. Also, it is worthy to do that we absorb the modern crime scene investigation theory, technology and methods to serve computer forensics, and combine the situation of crime scene to aid computer forensics.

## ACKNOWLEDGMENT

This work was supported by National Social Science Foundation of China (No. 06BFX051), National Natural Science Foundation of China (No. 60775038), Judicial Expertise Construction Project of 5th Key Discipline of Shanghai Education Committee (No. J51102), and also was supported by the training fund of The Henry C. Lee Institute of Forensic Science at the University of New Haven, USA.

## REFERENCES

[1] Cnnic, "The 30th Statistical Survey Report on Internet Development in China" (in Chinese), http://www.cnnic.cn/research/bgxz/tjbg/201207/t20120719_32247.html.

[2] Ling Wang, Hualin Qian, "Computer Forensics Technology and Its Development Trends," Journal of Software, Vol. 14, No. 9, pp. 1635-1644, 2003.

[3] H. Maher, "Online and Out of Line: Why is Cybercrime on the Rise, and Who's Responsible," http://abcnews.go.com/sections/us/DailyNews/cybercrime000117.html, June, 2002.

[4] Computer Security Institute(CSI)&FBI, CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 2006, 17.

[5] Australian Hightech Crime Center, Results of the 2006 Australian Computer Crime and Security Survey [R].

[6] R. Marcus, K, S. Kate, "The future of Computer forensics: A needs analysis survey," Computers and security, Vol. 23, No. 1, pp. 12-16, 2004.

[7] J. M. Patzakis, "Computer forensics-from cottage industry to standard Practice," Information System Control Journal, Vol. 2, No. 2, pp. 5-7, 2001.

[8] Brain Carrier, "Open source digital forensics tools, the legal argument, Stake, Research Report", October 2002.

[9] Yun Wang, James Cannady and James Rosenbluth, "Foundations of computer forensics: A technology for the fight against computer crime," Computer Law & Security Report, Vol. 21, Vol. 2, pp. 119-127, 2005.

[10] Jiawei Han and Micheline Kamber, Data mining concepts and techniques, Morgan Kaufmann Publishers, San Francisco, CA, 2001.

[11] D. Farmer and W. Venema, "Computer Forensics Analysis Class, Handouts," http://www.fish.com/forensics/class.html, 1999.

[12] K. Mandia and C. Prosise, Incident Response, Osborne/McGraw-Hill, 2001.

[13] Technical Working Group for Electric Crime Scene Investigation, Eletronic Crime Scene Investigation: A Guide for First Responders, 2001.

[14] Digital forensics Research Workshop, "A Road map for Digital Forensic Research," http://www.dfrws.org, 2001.

[15] Brian Carrier and Eugene H Spafford, (2003)Getting Physical with the Investigative Process, International Journal of Digital Evidence, Volume 2, Issue 2, Fall 2003.

[16] Venanslus Baryamureeba and Florence Tushabe, "The Enhanced Digital Investigation Process Model," http://www.dfrws.org/bios/day1/Tushabe_EIDIP.pdf.

[17] W. G. Kruse and J. G. Heiser, Computer forensics: incident response essentials (1st Edition), Pearson Education Inc., USA, 2001.

[18] Rongsheng Xu, K. P. Chow, Ying Yang, Development of Domestic and International Computer Forensics, 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing.

[19] Tang Tianbo and Gao Feng, "The application of visualization technology in link analysis," New Technology of Library and Information Service, No. 2, pp. 78-82, 2009