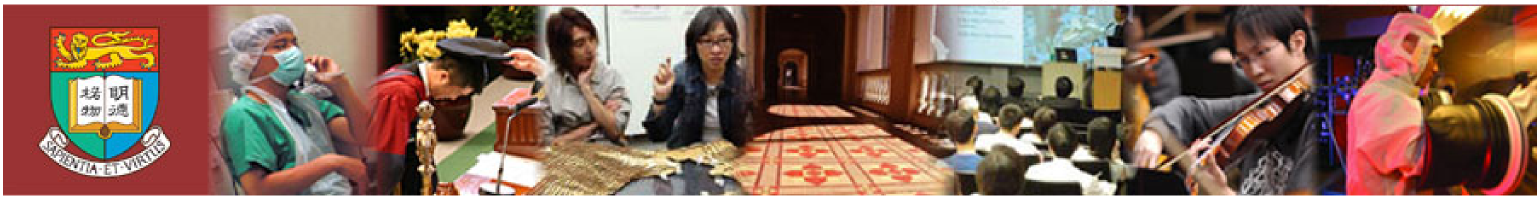

2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing

Development of Domestic and International Computer Forensics

Rongsheng Xu[1]
Institute of High Energy Physics,Chinese Academy of Sciences
Beijing, China
e-mail: xurs@ihep.ac.cn

K.P. Chow[2]
The University of Hong Kong, Hong Kong
Hongkong , China
e-mail: chow@cs.hku.hk

Ying Yang[3]
Shandong Computer Science Center
Jinan，China
e-mail:yangy@keylab.net

***Abstract*—with the increasing of computer crime, instant emergence of new digital product, new computer technology and computer forensics technology is promoted, developed constantly. This paper described basic information/content of computer forensics, and elaborated the development of current computer forensics at domestic and overseas market. The trends of computer forensics are pointed out and recent hot topics of research are introduced.**

Keywords-Computer forensics; computer crime; digital evidence；forensics tools

I. OVERVIEW OF COMPUTER FORENSICS

Many concepts have been presented to describe computer forensics; and many scholars and institutions have given definitions to computer forensics, for example the definition given by SANS[1]. According to some pre-defined programs for comprehensive examination of computer systems, computer forensics uses software and tools, to extract and protect the evidence of computer crime. Therefore, computer forensics is a process to recognize, protect, extract and archive electronic evidences that are able to be accepted by the court, sufficiently reliable and persuasive, existing on the computer and related peripherals. Judicial forensics must be subject to the main body of the law, and must be executed in accordance with the manner required by law and procedures.

The basic principle of computer forensics is to gather evidence as soon as possible, and to ensure that it is not breached. Chain of custody shall be assured, it means when the evidence is formally submitted to the court, it must be able to record any changes of the evidence from the state when it is first available to the state to the state when it appears in court. Of course, no change is the best. The entire examination and evidence collection processes must be supervised, that is, all investigation and evidence gathering by the experts appointed by the plaintiff shall be monitored by the experts appointed by the other parties.

Thus, computer forensics involves a wide range of technologies. Comprehensive utilization of a variety of technical knowledge is needed to solve practical problems. Related technology areas include file operation system, network system, encryption technology, forensics, and evidence search. Disciplines associated with computer forensics include computer application technology, information security, law and jurisprudence, and criminal science. The contents of computer forensics research is based on each process of the computer forensics processing steps for corresponding research, including evidence identification, acquisition, analysis, presentation, and recording etc. For decades, computer forensics research in and out of China has experienced a very impressive development from beginning to advanced level, from a few people to a large-scale development.

II. HISTORY AND CURRENT SITUATION OF OTHER COUNTRIES IN DEVELOPMENT

According to Professor Mark M. Pollitt, from National Forensics Science Technology Center, University of Central Florida [2], the development of overseas computer forensics can be divided into four stages: prehistoric period (before 1985), infant period (before and after 1985-1995), childhood (before and after 1995-2005), puberty (before and after 2005 - present):

In prehistoric period, there is only a small number of people, such as information management system developers (MIS), company security officers, a handful of federal law enforcement officers, were engaged in these areas because they came into contact with similar events. This was the beginning of computer forensics.

Infant period (ten years) is time when U.S. saw the popularity of personal computers and the appearance of Internet, also the time when U.S. saw a large number of computer crimes. Most of the operating systems were Unix, DOS systems, Macintoshes and early Windows. Ordinary Internet users use telephone dialing, such as AOL to access

978-0-7695-4517-2/11 $26.00 © 2011 IEEE
DOI 10.1109/IIHMSP.2011.98

Internet. Cyber crime became the focus of the society; the telephone system was an important target for forensics.

In childhood stage, there were many changes of computer forensics. "911" event caused more attention from government, military and intelligence agencies on computer forensics, as well as all digital forensics technologies. During this stage there was emergence of Windows-based GUI tools, such as Expert Witness, Encase, FTK, iLook, ACES, and other large-scale forensic software products; also the development of Linux-based tools, such as TSK, SMART, HELIX etc. Moreover, the subsequent emergence of forensics tools on network and memory acquisition. Academia and business circle's interest was greatly enhanced for staff workers from the individual to the institution participated in the evolution. And there was emergence of government-funded institutions, with well-trained, well-equipped team.

Puberty stage marks the cause of computer forensics has grown stronger. To the present, there have been the emergence of many large-scale enterprises and advanced products, including enterprise-class tools: Encase, FTK, bootable file systems: Helix, SPADA, as well as specialized electronic evidence discovery tools. Forensic objective is developed from simply mainframe computer forensics to a variety of media, digital evidence forensics, not only for file system, network, but also for telephone, MP3 players, game consoles (such as XBOX), social media, business system and e-mail evidence. This stage of maturity is also reflected in a number of academic and technical communities which has been active for many years. For instance, DFRWS continues ten years, IFIP WG11.9 continues six years and SADFE continues five years and so on.

Throughout the development of overseas computer forensic, after years of demand stimulus and sustained progress, it has been developed to a considerable extent. For example, tools are mature, technology advanced. New ideas and methods are emerging one after another, and different tools can adapt to different needs. Russia was mature in password recovery and introduced GPU technology (Passware Company[3], Elcomsoft Company[4]). United States, Canada, Australia and Brazil police authorities have accumulated extensive experience on computer forensics. For instance, many universities have also carried out in-depth theoretical research and technological research and development in computer forensics; Moreover, there are several outstanding competition organizations, who launch competition conference every year. It lectures and competition during the event has always been rich in new ideas accommodating forefront demand, and leading the technology trend. For instance, "Black Hat" Technology Security Conference [5].

III. Domestic research

In China, the popularity of computers and the Internet appeared in 1996, then there were occurrences of computer network crimes around the country. China's public security departments were charged with dealing with computer crime cases. Computer forensics research also saw a greater start driven by scientific research institutes, but many gaps still existed then. Formal launch of the research started in 2000.

A. Domestic universities and research institutions

Universities and research institutes that launched computer forensics research work at the early stage in the country are as follows:

Institute of Software, Chinese Academy of Science, is well-known for its research highlights in system security, covert channel analysis and real-time forensics[6];

Network Security Laboratory, Institute of High Energy Physics, Chinese Academy of Sciences, carried out research work in network forensic, disk analysis, virtual machine, fragment recovery and cell phone forensics;

Shandong Computer Science Centre, Shandong Academy of Sciences, established Sino-US International Joint Lab at early time, and carried out research work on Internet communication tool forensics and memory acquisition;

Peking University carried out a lot of work on computer crime, evidence fixation and preservation techniques, as well as the full-time post-graduate training programs;

Chongqing University of Posts and Telecommunications conducted in-depth study on fine-grained data integrity tests[7];

Hubei University of Police established Computer Electronic Forensic Lab, having done a lot of practical work on handling of cases;

Forensics Lab, East China University of Political Science and Law, had reaped plentiful and substantial achievement in the research and evaluation evidence on video and image.

University of Hong Kong had done a lot of work, such as the p2p protocol analysis and evidence collection, online auctions, fraud founding, internet piracy forensics, as well as video analysis, forensics and cell phone forensics and so on;

In summary, the characteristic of domestic computer forensics work is to track overseas advanced theory and technology, and develop forensics technology with its own characteristics. For example, evidence acquisition mechanism deployed in operating system, Chinese e-mail forensics research based on fragment recovery, and cell phone forensic research and future cloud computing forensic research, Internet-for-things research and so on.

B. Domestic organizations to implement computer forensic

In China, public security system began forensic work early because criminal and civil cases are most directly related to the activities of computer crime cases. Network Monitoring Unit of each department and bureau began computer forensics work, main focusing on forensic and surveillance of cyberspace cases.. In the last two years, criminal investigation department also came into contact with computer crime cases, and gradually came equipped with a variety of resources to carry out computer forensics work.

According to actual work, the procuratorate, public security directorate, the military, etc. also involved in computer forensics work related to their own business according to their responsibilities.

C. Companies engaged in computer forensics

Computer forensics becoming a technology hot spot, more and more companies started work in this area.

Xiamen Meiya Pico Information Co., Ltd., not only provides electronic data forensics products, but also electronic data identification services, Meiya products have formed into series, with all-encompassing functions, including electronic data-acquisition equipment, electronic data analysis system, electronic data destruction equipment and other mature products. Having set up its own training center, it is the only one listed domestic company specialized in computer forensics.

Beijing FuHua Technology Development Company, familiar with advanced computer forensics tools from both domestically and internationally. On the basis of digestion and absorption of these products, in combination with the actual needs of our country, has researched and developed computer forensics products with indigenous intellectual property rights in line with national conditions and practical needs. The company can provide the professional computer forensics training programs and related services. The research includes mainly password cracking software and hardware, iPhone cell phone forensics, file fragmentation analysis system, computer simulation and other directions.

Pansafe Software (Shanghai) Co. LTD. focuses on the development of computer forensics software and technical services. The main products include cell phone forensics, media forensics, field forensics, simulation forensics, association analysis, etc.

Domestic companies can do some original research and development work, or track overseas technology, and complete a number of researches and development of overseas alternative products. However, there are also some companies draw support from overseas advanced products, for the second development or packaging, or direct do domestic sales by being an agent of the overseas product.

D. Legal issues of electronic evidence

Computer forensics is an interdisciplinary between computer technology and jurisprudence. The issue that facing the computer forensics personnel is how to make the data obtained by computer meets the requirements of evidence in court. China needs to get this work done as soon as possible under the condition that computer crime and legal status of electronic evidence in the country are still yet to be perfected. Renmin University of China School of Law conducted a feasibility study and make recommendations in terms of the legislative basis of electronic evidence, e-discovery rules, cyber law, to promote the development of standardization in the legislation of electronic evidence in China.

IV. Computer forensics conferences

A. National Computer Forensics Workshop

National Computer Forensics Workshop, the academic conference sponsored by Committee of Computer Forensics Experts in Chinese Electronic Institute, is dedicated to the construction of academic exchange platform, the promotion of understanding of R&D Engineering staffs in the field of computer forensics technology. The Workshop has now been held three sessions, focusing primarily on basic theoretical study and the direction of new technologies.

B. IFIP Working Group 11.9 on Digital Forensics

IFIP Working Group 11.9 on Digital Forensics is hosted by Security and Privacy Protection in Information Processing Systems under International Federation for Information Processing. The conference is an international high-level computer forensics academic conference, with the aim of promoting scientific and technological research and development on digital forensics by jointly working with the scientists, engineers and practitioners who are engaged in international digital forensics. Advances in Digital forensic, the accepted papers of the annual conference, will be published by Springer Publishing Company.

C. CCFC (China Computer Forensics Conference)

CCFC was hosted by China Computer Forensics Research Center(CCFRC) every year. It is a grand event for researchers, engineers, business personnel in Chinese forensics field to communicate with each other. The CCFC plays a leading role in accelerating the development of China's computer forensic technology by inviting domestic and international experts and professors in the field of computer forensics, original authors of computer forensic tools and the leading forensic vendors in the industry, to discuss and conduct training programs focusing on the latest technology, latest products, demonstrations, and experience and so on related to computer forensics.

V. The development of future computer forensics

A. Development of tools (technology)

Development of computer forensics tools must meet the development of the need of the forensics, which is reflected in the achievement of better forensics performance, and the analysis and forensics of data in the form of a new medium.

Real-time forensics (technical) tool -- the existing forensics trends tends to the forensics of running machine. Forensics requests the ability to obtain the computer evidence that is under the current operating state in a real time manner whether in the network or a separately running machine.

The cell phone(smart terminal forensics analysis Tools-- IT giants are constantly introducing new cell phone devices, introducing a new intelligent operating system, such as IOS's iPhone and iPad2 (has just launched); smart phone using Google's Android system; Tablet Personal Computer using Microsoft's operating system. These newly-emerged intelligent terminals are challenging the existing computer forensics techniques and tools,

Massive data acquisition, storage and analysis tool -- web data extraction and analysis in the internet are the research field of information and intelligence professionals. Today, they are increasingly applied to the internet forensics, which involves in a huge amount of data that cannot complete storage and processing by single machine or several single-machine clusters. In some cases, the suspect computers are related to excessive scope and data, which cannot be processed in the time required by the case with the usual forensic tools. Thus, more rational processing method is demanded in the field of computer forensic.

A**utomated intelligence analysis tool** -- the use of artificial intelligence, machine learning, neural network technology to develop intelligent analysis tools. Although there are numerous papers elaborating artificial intelligence, machine learning, neural network theory and technology, how these theories and techniques can really play a role in forensic are still yet to be solved.

The evidence visualization (technical) Tools – there have been a lot of sophisticated tools to access to digital evidence at this stage, but it is still a major problem of research demanded in the confused data. How to conduct logical analysis for obtaining the evidence or the relationship between data, providing greater support and help for computer crime investigation and analysis; or how to let the judicial officers have an intuitive understanding of the evidence submitted to them for the recognition of effective digital evidence. According to various data obtained, evidence visualization can reveal the associated data obtained in a graphical manner using correlation analysis, visualization technology and automatic graph layout drawing algorithm, to help investigation and evidence collection personnel carry out further analysis, and make the result as the evidence presented[9].

Facing anti-forensic work -- computer anti-forensic uses data erasure, data hiding, data encryption method to avoid traces and evidence of crime being caught. With the development of computer technology, anti-forensic will be ongoing, and might become more difficult and require more effort to ensure that traces can still be tracked, and evidence be obtained even under the interference of anti-forensic. This is a process of constant struggle. While the priest climbs a post, the devil climbs ten.

Trusted computing technology(TPM) and forensic tool -- an impossible task. Trusted computing technology is to introduce hardware security features on the PC platform, and to improve the terminal system security by the security features provided. The core technology of “trusted computing” is the security chip called TPM (trusted platform module). Trusted computing security established in the chip-level is a great challenge to computer forensic technology.

Forensic by Internet of Things and forensic by cloud computing – “Internet of Things” and “cloud computing” are two hot topics in the latest IT field. The internet of Things has extended nodes from the computer to the other media. For instance, automotive, home appliances can all become network nodes, providing data for the network. Cloud computing, however, will conduct centralized resource management of the resources. These operations and application models different from the traditional networks have brought great challenges and opportunities to forensic technology.

Forensic analysis pertaining to video and audio -- in internet applications, some conventional chat tools(Instant messenger) such as QQ ,MSN,Yahoo, not only provide text chat, but also audio and video chats. Skype put audio chat as top priority . Therefore, forensic is not only based on text, but also on the related video and audio. Seeing that chat tools have their own information transmission and storage modes, or even encrypted in a special way, forensic has seen some difficulty; Another hot spot of video is how to handle the massive video data being monitored to get the information needed without having to browse through video data in a manual way. The development trend of video surveillance field is the use of intelligent video analysis, computer vision and machine learning theory and technology, supporting goal judge and alarm. This is a means for computer to handle rapid forensic.

B. Development of law

1) International law

For now, a definite legal force on electronic evidence has not been available so far in the international legal system. In 1996,The United Nations Commission on International Trade Law (UNCITRAL) passed Model Law on Electronic Commerce (MLEC), which stipulated that electronic evidence can be used to prove the objective facts. MLEC Article 8 stipulates “On the occasion that the law requires the information submitted or maintained in its original form, a piece of data is to confirm the primitiveness of the electronic evidence and the effectiveness of the direct forensic." Article 9 stipulates " In any legal procedure and in any rule which apply relevant evidence , the acceptability of a piece of data as evidence should not be denied." Thus, from the perspective of international law, electronic evidence is an independent type of evidence, which can be used in judicial practice, and has an independent probative force and credible force.

2) Professional ethics and conduct of forensic officers

In this regard, the law in each country has its own provisions, and has established relevant professional ethics and conduct for the forensic officers need to comply with. For instance, HTCIA（High Technology Crime Investigator Association）proposed a set of ethical conduct and practice guidelines for its members, and requested its members to put them into practice. Once a member is found to have violated these guidelines, his/her membership will be cancelled, and he/she will be reported to the relevant judicial body.

3) Rules of evidence identification

In this respect, the overseas evidence laws have strict rules. For example, the 1998 Canadian Uniform Electronic Evidence Act, the 1999 British Electronic Communication Privacy Act, the U.S. Federal Rules of Evidence[10] all have been similar provisions, which have made judicial provision to determine the legality of electronic evidence and forensic specification .

However, in China, electronic evidence has not been clearly defined as the type of legal forensic. For instance, the seven categories of evidence in the three procedural laws (civil, criminal and administrative) have not clearly defined the effectiveness of electronic evidence, as legal evidence categories. However, some provisions are available in some lower-level laws, such as Contract Law, Electronic Signature Law. Moreover, the Supreme People's Court and the Supreme People's Procuratorate have both made a number of judicial interpretations and rules, which are applied to electronic evidence.

C. Development of standard

1) System construction of relevant law and technical standard

For electronic evidence is the cross area of technology and law, so the standard of law and technology, which can be used in electronic evidence has been the focus of the researchers and justice practitioners. As the justice has always lagged behind the reality, the judicial organs start to solve the problem only after the problem occurs in the national judicial and technical standards. In this sense, the judicial development of electronic evidence is not slow in progress, but keeps pace with the times[11].

2) Forensics principle, process, method

There has always been research and development on forensics's principle, process and method, since the emergence of forensics.

Dan Farmer and Wietse Venema were the first to propose the basic forensics' process, to define the whole process of the forensics on UNIX system, and put forward the basic principles that should be followed in each step of the operation. The main idea is applicable to most computer systems. And they developed TCT (The Coroner's Toolkit) toolkit for forensics work. Subsequently, the relevant advanced incident response model, abstract model, etc. the U.S. Department of Justice (DOJ) proposed a Model for Computer Forensics Investigation Program, and the U.S. Air Force Academy proposed Abstract Process Model, both of which have given a detailed description on the process , method and principle of electronic evidence.

3) Accreditation of computer forensics agencies and staff workers

Since computer forensics is an emerging technology industry, such issues still remain as how the organization conducts computer forensics with uniform, recognizable, repeatable work, and how related staff proves their professional capabilities with their relevant qualifications. However, in this respect, there is no public authorized standards and regulations in and out of China. There are only requirements for Judicial Expertise Institutions .

American Society of Crime Lab Directory/Laboratory Accreditation Board, ASCLD/LAB started to use ISO17025 General Requirements for the Competence of Testing and Calibration Laboratories to conduct accreditation for All-American Electronic Data Forensics Identification Laboratory in 2004. For instance, it accredited the Defense Computer Forensic Laboratory, DCFL, the world's largest digital forensics lab, and FBI-based Regional Computer Forensic Laboratory, RCFL across the United States, etc. Thus. This certification has become the industry qualification for computer forensics agencies, and authorized by the U.S. judicial body.

England has also adopted ISO17025 to conduct accreditation for its computer forensic agencies. For example, the FORENSIC Science Service，FSS, the world's largest of its kind in England provides computer forensic and identification service for all the police agencies cross the nation after it was accredited by UKAS(United Kingdom Accreditation Service).

The accreditation bodies recognized by CNAS (China National Accreditation Service), have become common computer forensic and identification bodies in the country's judicial body. Especially after CNAS issued the Guidance on the Application of Laboratory Accreditation Criteria in the Field of Electronic Forensic (CNAS-CL27) in 2010, the domestic-related computer forensic and identification bodies can become recognized computer forensic and identification bodies as long as they have passed the accreditation.

Unfortunately, a qualification standard to recognize practitioners in and out of China has not been available so far. Few companies have provided accreditation for their product operations. For instance, ENCE(Encase Certified Engineer)introduced by Guidance Company, ACE(ACCESSDATA Certified Engineer)by Accessory Company, and MCE(Metal Certified Engineer)by domestic Dampen Metal Company. These qualifications only recognize the owners in a high lever on applying these tools , but cannot prove their computer forensic and identification practice standards.

4) Forensic tool evaluation criterion

In this regard, Computer FORENSIC Tool Testing，CFTL, under National Institute Of Standards and Technology, NIST, has played a role of norms and standards. The program is based on well-recognized international methodologies for conformance testing and quality testing, such as ISO/IEC 17025:1999, General requirements for the competence of testing and calibration laboratories. It established a methodology for testing computer forensic software tools by development of general tool .This approach, as standardization and standardization requirement for forensic tools, has been recognized by many countries in the world.

China National Technical Committee on Criminal Technology of Standardization Administration also organized and completed Software Identification Technical Specifications of Electronic Forensic. This has proven that the domestic computer forensic tools evaluation criteria and approval have been standardized and recognized according to internationally accepted norms and practices.

D. Cooperation

Electronic evidence is related to many technologies, hence more complex and professional. Average computer technicians do not necessarily mean that they can understand all the technical fields. The judicial officers are more proficient in evidence, but it does not necessarily mean that they can understand the characteristics of electronic evidence. They have also certain problems in understanding and using its probative force, reliability and repeatability. Thus, it is very necessary to strengthen the cooperation between the electronic forensics' professionals and the non-professional judicial officers. In this respect, the United States has adopted a way of expert witnesses. However, this method also has certain requirements for the majority of judicial officers, for instance, the level of computer knowledge and their understanding and so on. Furthermore, the language level and prejudice of expert witnesses are likely to mislead the relevant judicial officers. As there are still some legal issues in the domestic use of electronic evidence and probative force, and China's continental legal system needs a clear judicial provisions when electronic evidence is to be adopted. Thus, China needs to carry out international cooperation with those countries which have advanced experience in electronic evidence. For instance, the countries include United States, Canada, Germany, etc. The cooperation in the areas such as electronic evidence forensic, identification, recognition, training program and qualification recognition, to enhance the level of domestic electronic evidence forensic. The CFEG(China Forensic Expert Group) had taken the first step.The annual computer forensics conference that CFEG organizes has become a large exchange place for the professionals from both domestically and internationally to conduct computer forensic technology and judicial practice, and also to promote the development the level of domestic forensic.

VI. China's New Research Focus

A. Cell phone forensic

For the specific cell phone forensics, forensic mainly focuses on the logical file system in the cell phone internally. It is better to use non-invasive physical forensic as far as possible. If necessary, use the jailbreak tools, implement non-invasive physical forensic. IPhone and iPad have become hot, the number of people using the two devices has seen a sharp increase. Forensic based on iPhone has also seen more urgent needs. Another cutting-edge technology,chip level forensic pinpointing damaged copycat cell phones, is directly reading telephone chip to get the file system image and conduct analysis, and access to the data.

B. Cloud computing forensic

1) The main content of cloud computing forensic includes:

a) Problem identification, that is, how to confirm the location of the data concerned stored in the cloud terminal and virtual machine, and confirm the cloud service functions and the condition of the operating system.

b) Record monitoring system, in the cloud system, to collect, analyze and create the relationship pinpointing to the recorded data, to assist the audit of due management practices.

c) Data and system recovery, data recover intentionally or unintentionally deleted or changed in the cloud, and recovery of the damaged system caused by invasion, and acquisition process of cloud side evidence and preservation techniques.

2) Problems encountered in the cloud computing forensic listed in three areas:

a) Technical level, static data, dynamic data scattered and difficult to conduct forensic using conventional methods.

b) Organization layer, sub-cloud terminal server and client terminal in two parts, with large scope, difficult to do forensic. For example, forensic mechanism, including outsourcing services.

c) Legal aspect, facing a cloud under a mufti-jurisdiction and more commission or the least of host machine, the legal agreement between the customer and the cloud computing service provider is also an issue needs to be considered.

C. Forensic framework

Establish a knowledge base of massive data based on the past cases, conduct similarity computation using data mining technology, find the maximum similarity and the adjacent cases to make some adjustments for the conformity of the case demanded, and ensure the collection of evidence by adopting the best procedure. This architecture can be based on cloud computing service model, also known as "cloud forensic", including a complex password cracking service.

D. To obtain evidence from a wide range of on-line fraud cases

China's hacker economy industrial chain is showing a trend of the rampant phenomenon. China is in desperate need of making existing and underground economy, advertising, fraud and existing and other internet activities as its objects of study; and how to determine the appropriate way to capture evidence and accumulate forensic experience.

E. Extract evidence from VoIP

Three network convergence is the big move for the network development in China. All VoIP users based on the service only have user names and email addresses, it is not easy to do tracing. Moreover, compression and encryption have also been done to voice data.

1) Some researchers have done evidence acquisition:

a) Re-construct the information data packet;

b) Query and automatically record data packet;

c) To make sound document analysis adoption through decryption and routing protocols, use FFT digital signal processing to confirm its starting and completing locations and determine what kind of language used.

d) To track, and obtain voIP user information.

VII. Conclusion

Computer forensics has gone through four decades, and has grown from a limited evidence of a crime for the development of traditional information security to an important practical and theoretical area now. The development has exhibited the following characteristics: the rapid development of theoretical research； the more enriched practice content; many legal experts, forensic experts and technical experts work together to expand the field of study, enhance the application in practice.

Increasing development of computer technology and telecommunications technology emerging forms of crime caused by computer crime methods varied, the resulting forensic research and practice is also changing. This demands professionals in the field to move forward with times, strengthen research and application.

Thus, this area of research, practice, standardization and evaluation, etc. needs the joint efforts of professional, non-professionals, persons inside and outside the field, for the purpose that the computer forensics, information technology in the new era, is normally open all year round undefeated.

We hope that through our research and practice, the computer offense finds nowhere to escape, nowhere to stay. Through professional computer forensics evidence, of illegal activities based on information technology can be simultaneously found everywhere, a perfect chain of evidence can be given, so that law offenders is not able to find any excuse before the evidence. This is also the ultimate goal of this research.

References

[1] http://www.sans.org .

[2] Mark M. Pollitt. The History of Digital Evidence . Key Note on IFIC WG 11.9 nternational Conference on Digital Forensics) HongKong.

[3] http://www.lostpassword.com/

[4] http://www.elcomsoft.com/.

[5] http://www.blackhat.com/.

[6] WANG Yong-Ji,WU Jing-Zheng, ZENG Hai-Tao,DING Li-Ping1, LIAO Xiao-Feng.Covert Channel Research. Journal of Software, 2010,21(9):2262-2288(in Chinese).

[7] Chen Long, Wang GuoYin. An integrity check method for Fine grained data. Journal of Software, 2009, 20 (4) : 902-909 ,doi:10. 3724/ SP. J. 1016. 2011. 00847(in Chinese).

[8] Xiang Dawei,Mai Yonghao. Some comments on crime-scene and cybercrime evidence investigation.Netinfo Security, 2010, (11):12-14, doi:10.3969/j.issn.1671-1122.2010.11.004 (in Chinese).

[9] Tang Tianbo,Gao Feng.the application of visualization technology in link analysis. new Technology of Library and Information Service,2009(2):78-82(in Chinese).

[10] Greim .Federal Rules Of Evidence[M].Beijing：Law Press China,2000.

[11] Pinxin Liu andKun Liang.Legal Regulation Of E-DICOVERY[M].Beijing:China Legal.