An Electronic Judicial Identification Model Based on Evidence Chain

MA Guo-fu[1], Wang Zi-xian[2], Wang Kui-peng[3]

(1.Dept. of information management,The central institute for correctional police,Baoding Hebei,071000,China;2. Modern education center, The central institute for correctional police,Baoding Hebei,071000,China;3. Dept.of scientific research, The central institute for correctional police,Baoding Hebei,071000,China;)

Abstract**:** The concept of electronic data and judicial identification is first introduced, basing on the in-depth study on the current models of electronic forensics, an electronic judicial identification model based on three-dimensional trusted electronic evidence acquisition model is proposed. The model implements linear process control, evidence supervision, time constraints and legal constraints and trusted fix of electronic data for the whole process of judicial identification. By establishing political and judicial certification authority, it achieves mutual trust and mutual recognition between relevant agencies and the court in the whole process of evidence collection and identification, and ensures their own safety and legal effect on evidence supervision chain. At last, it verified the correctness of the model by case analysis.

Keywords: judicial identification; evidence ring; evidence chain; evidence supervision chain; trusted fix

1. Introduction

At present, the sharp rise in all sorts of electronic crime cases and the related economic and civil dispute cases are causing unpredictable consequences and enormous financial loss to our society and our country. The key to fighting against crime is to gain the full, reliable and legal-effective evidences. In March 14th, 2012, the 5th conference of the 11th National People's Congress has decided to revise the Criminal Procedure Law of The People's Republic of China. In the revised Criminal Procedure Law, it is clarified that electronic data can be used as independent evidence. Specifically, 13, the Article 42 was changed to the Article 48 to Materials that can prove the true circumstances of a case shall be evidence. Including material evidence, documentary evidence, testimony of witnesses, statements of victim, statements and exculpations of criminal suspects or defendants, expert opinions, records of inquests, inspection, identifications and investigations, audio-visual materials and electronic data. Although electronic data being independent evidence has been legally determined so far, it is not certain about the standardization of the process of obtaining electronic data evidence and identifying it judicially in China. However, in the recent filed cases, electronic evidence usually needs judicial identification to become a direct evidence of a case. The fact that we don't have integral and legal-practice-helping standardization to the judicial identification of electronic data makes it questionable in its impartiality, authority and neutrality. So it is vital for improving the legal effect of electronic data to learn the existed standard and experience of judicial identification to electronic data from other countries, and set up an electronic judicial identification model, which is based upon the chain of evidence and evidence supervision, legally and technically, so that we can standardize the whole process of judicial identification of electronic data.

2. The Existed Electronic Data Forensic Model

In our current legal practices, an electronic data can only make it to the case deciding evidence by being submitted to the court and admissible during cross-examination after being

identified by the identifying agency. Reference [1] defines electronic judicial identification as an activity that experts use science technology or professional acknowledge to give out opinions after identifying or determining the specialized question involved in the lawsuit. Reference [2] defines electronic judicial identification as a judicial identifying technology that experts analyze the electronic data which are legally collected, identify the type and character of them, and verify its capacity of proving after finding out the objective relation between the truth of the case and them. The judicial identification of electronic data needs to identify not only the original gesture of the evidence, but also the relative information of the case, to make sure the realization of the objection, correlation and legality of electronic data. The processes must follow the operating standard strictly, conforming to the law. Otherwise, it would lead to the drop of credibility and lack of legality of evidences. With regard to this, people proposed numbers of evidence obtaining model, including the Process Computer Forensics Model, the Level Computer Model, the Distributed Computer Forensic Model, etc.

In the Process Computer Forensics Model, there are some disadvantages, for example, no time limit to the evidence obtaining process, uncertain statement about the cross work and repeat work, lack of effective supervision in the whole process, uncertain legal constraint on the process and so on. The Level Computer Model assigns the evidence obtaining process to 5 levels—discovery,regulating,extracting, analyzing and stating. While stressing the law-related character, the Level Computer Model neglects or reduces the significance of technology supporting. Comparing to the Process Model, the Level Model has any kinds of problem except for legal constraint, indicating the operation process blurrily and poor in actual operability. In the Distributed Computer Forensic Model [3], there is no supervision in the whole process or time limit. Therefore, it is difficult to identify the legal effect of electronic data.

3 An Electronic Judicial Identification Model Based on Evidence Chain and Evidence Supervision Chain

From the analysis mentioned above, giving the poor versatility of our current forensic model, it’s hard to guarantee the legality of the obtained evidence. In this article, there will be a proposal of the judicial identification model that based on evidence chain and supervision chain as the evidence circle and evidence chain are applied to electronic forensic and judicial identification. An evidence circle is used to achieve the mutual confirm of multiple electronic data, so that the originality, objectivity and correlation of electronic data will be assured. An evidence chain is used to protect the truth and integrity of electronic data. What is used for protecting the legality and the legal effect of electronic data is the regularizing of the credibility of electronic data and the evidence supervision chain. This model combines the theory and judicial practice, as well as the technicality of the electronic identifying model and the legality of the identifying process. That means this model can be used not only in criminal, civil and administration fields, but also in evidence obtaining inside a company and other demands apart from electronic crime. And it can change over time.

3.1 Evidence Circle

As we all know, a single piece of evidence is always not able to confirm a crime, and it is not clear in electronic judicial identification. That is to say, with multiple evidences supporting each other, the identification can be more legally effective. Evidence circle is a horizontal analysis that mainly horizontally analyzes the time, user, device and some other information in

multiple evidence data in a certain time by association rule mining. After analyzing, it digs out the correlations between all kinds of evidences, which make sure about the multiple evidences confirming and supporting one another, so that the evidence circle is developed, assuring the objectivity and correlation of evidences. The association rule algorithm is involved in the similarity of crimes, timing and multiple evidences. The evidence circle is a reflection of the correlation of multiple evidences and its crossing in space, as is shown in Figure 1.

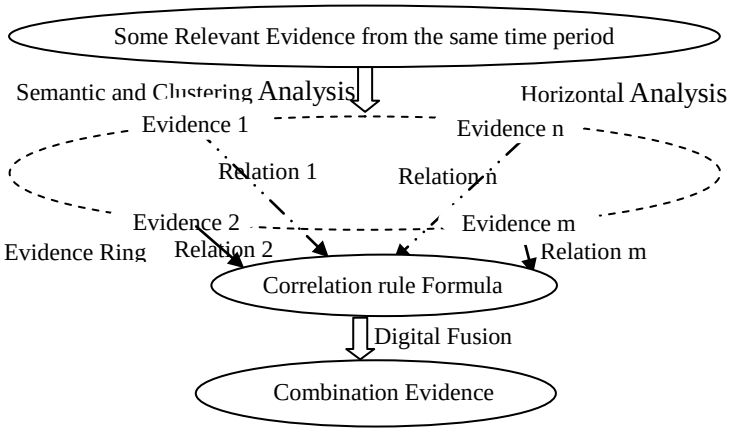

Fig 1 Evidence Ring

3.2 Evidence Chain and Evidence Supervision Chain

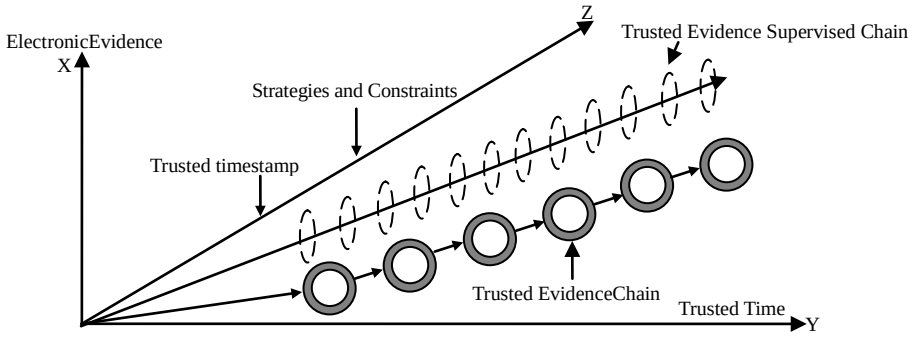

Fig 2 Three-Dimensional Trusted Evidence Chain Model

It is necessary to build up an evidence chain due to the request of judicial practice and the fact that there is work-repeating and backward work existed in every phase of the judicial identification. Because the identifying strategy will change along with the changing of identifying request during building up an evidence chain, we can say that the process of identifying is the process of forming the evidence chain. Or the evidence chain is a reflection of analyzing the evidences longitudinally. Reference [4] proposes an idea of trusted forensic and trusted time stamp technology which is based on the combination of trusted forensic and time stamp technology. By adding the trusted time stamp and different evidence properties to the different phases of the identifying model, the trusted evidence chain can be built basing on trusted time stamp, and the objectivity, continuity and consistency of the evidence could be guaranteed.To build up the trusted evidence chain which is based on trusted time stamp synchronicity, as well as guarantee the legality and usability of the evidences, we should practice legal constraints—use different legal properties and add different constraints in different phases of the identifying model to supervise the whole process of identification. Based on the trusted time stamp, strategies of identification and constraints, trusted evidence

supervised three-dimensional trusted electronic chain of evidence and evidence of supervision chain model as shown in Figure 2

3.3 An Electronic Judicial Identification Model Based on Evidence Chain and Evidence Supervision Chain

An Electronic Judicial Identification Model Based on Evidence Chain and Evidence Supervision as shown in Figure 3.The model including the identified preparation,fixed preservation of evidence,analysis and identification of evidence,supervision of evidence,identification opinions and evidence presented in court.In the same time,these stages can also be appropriately adjusted according to the actual need. The large data volumes and the potential of hard drive encryption may arise in forensics and judicial identification, meanwhile, the results generated by each stage in the future can reproduce scene, therefore, each stage results of forensics and judicial identification need to generate a unified XML format.In this way, each stage results of forensics and judicial identification can be presented separately, may also constitute evidence chain.

3.3.1 Identification Preparation

Identification Preparation includes forensic personnel qualification preparation, the recognition of electronic identification tools, the consignor of forensic, identification Knowledge database based on the rule of law, criminal behaviour case database, trusted time-stamp authority (TTSA), certificate from political and judicial CA and evidence storage centers etc. Knowledge database based on the rule of law,criminal behaviour case database can change with the actual needs changes.Evidence supervision ensures legal requirements in the preparatory stage of identification, at the same time if necessary, can be traced back,adjust or update the identification prepare content. Political and judicial CA can improve the authority and unity of the legal sentencing, the relevant institutions become members of its certification and receive a certificate for mutual authentication and establish evidence storage center, the certificate from the political and judicial CA is used to authenticate each other and legal agencies, evidence storage and extraction, thereby ensuring the legal effect of identification supervision itself.

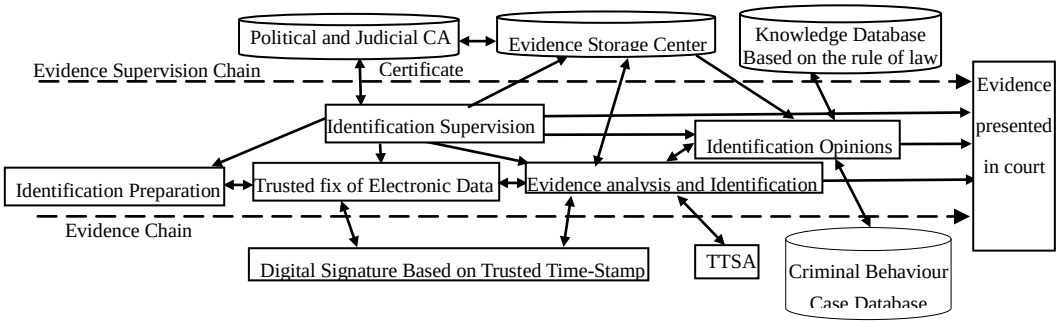

Fig 3 An Electronic Judicial Identification Model Based on Evidence Chain and Evidence Supervision

3.3.2 Trusted Fix of Electronic Data

Trusted fix [5] is trusted fix method that does not destroy the static properties of the electronic data or ensure the trust of the static properties of the electronic data.By multiplayer digital signature based on the trusted time stamp of the original data submitted for the consignor to conduct trusted fix to avoid invalidity of digital signatures after the digital certificate validity period has expired. The computer or storage media to be identified is

referred to the target machine M; multiplayer digital signature participants include the signer S (the consignor or suspect), the certifier C (the third-party identification agency), the verifier V (the relevant functional departments of public security, etc.).The trusted time stamp authority(TTSA)is granted by time stamp service authority(TSA)of national time service center (the only authoritative time service agencies) ,it promulgate electronic documents that prevent electronic data from tampering and counterfeiting.Multiplayer digital signature participants obtain U Shield certificate for signature and encryption via online real-time certificate application center based on an intelligent terminal.Figure IV shows the electronic data trusted fix flow.

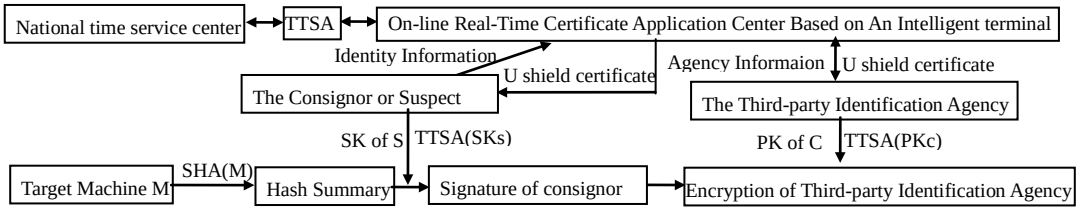

Fig IV The Electronic Data Trusted Fix Flow

(1) First, generates Hash Digest SHA (M) by calculating Hash using the SHA algorithm on the target machine.

(2)Second, the consignor or suspect obtains U Shield certificate based on RSA by submitting identity information to on-line real-time certificate application center based on an intelligent terminal, and then sign Hash Digest by using the TTSA (SKs) .

(3) Third,the third-party identification agency encrypt the above signature by using TTSA(PKc) of U Shield certificate based on RSA by submitting agency information to the on-line real-time certificate application center based on an intelligent terminal,and then achieve trusted fix for electronic data based on trusted time stamp.

3.3.3 The Evidence Analysis and Identification

The raw data submitted for the consignor to be analyzed and identified for the authenticity, integrity, legitimacy and relevance.It can identify the "original" features of electronic data and distinguish the relevant information of the cases.Due to concealment and intangibility of electronic data,the electronic data need to be converted the state which people can be perceived to be analyzed.The reliability and authenticity of conversion is foundation and key of the relevance of evidence,is also the difference with examining relationship of the traditional evidence. According to identification strategy based on the requirements of identification,the original data can be extracted and analyzed on the basis of additional trusted time stamp and identification supervision, when necessary for data recovery; evidence ring can be formed by semantic analysis of of multi-source data for the same period of time,computing the correlation of each evidence in ring evidence, synthesizing evidence according to association rules algorithm of evidence, signing the electronic evidence the by using of TTSA (SKc) in U Shield certificate and additional trusted time stamp obtained from a trusted time stamp service authority(TTSA) for ensuring the integrity of evidence, thus forming a evidence of evidence chain. The evidence of signature will be submitted according to the XML format to the evidence storage centers.In order to ensure the legitimacy of the identification agencies and evidence storage center, political and judicial CA authorized the two sides to authenticate each other by using certificate.

3.3.4 Evidence Supervision

The full supervision of the identification process can achieve the full playback of the identification process, and supervise the evidence storage center to ensure legality of evidence, there is no forgery and tampering with the original data; Evidence supervision is also used to obtain a certificate from political and judicial CA, awarded to those forensics and identification agencies for the authorization and authentication.

3.3.5 Identification Opinions

Identification Opinions can be issued by summarizing the whole identification process. Update identification knowledge database based on the rule of law and criminal behavior case database.

3.3.6 The Evidence Presented in Court

Submit the chain of evidence and evidence of supervision chain of whole identification process to the court in form of identification opinions recognized by the court.

3.4 Characteristics of Model

Compared with the other forensic and identification model, the model has the following characteristics:

(1) Compatible with Existing Models

The model was proposed on the basis of summing up the existing model.It can be turned into the traditional forensic model, when changes of the time and other policy of three-dimensional evidence chain.

(2) Evidence Supervision

The model Supervises the whole process of identification,forms evidence supervision chain, and submits to the court.The identification process can reproduce via the form of playback for proving the legitimacy, integrity and objectivity of evidence.The formation of network relationships between the whole identification process and evidence supervision resolves the fusion of legal and technical,integration and availability of evidence.

(3) The Tusted Time Stamp

With the continuing upgrade and update of the crime techniques, technology strategy of identification should also adapt to the change. At the same time in the identification process, implementation of trusted time stamp, the time line merges into the evidence for the continuity consistency, undeniable and resistance of the evidence.

(4) Evidence Ring and Evidence Chain

Evidence ring can be formed via semantic analysis of multi-source data at the same period of time, realize mutual authentication, ensure the relevance of the evidence.According to the correlation degree of evidence, the evidence can be synthesized by using the association rules algorithm.The evidence chain can be formed by executing linear control in the identification whole process, ensuring the continuity of time and cross of space of the evidence.

(5) The Mechanism of Authorization and Authentication

The national political and judicial CA realizes mutual trust and authentication of identification process among the relevant agencies, also ensures safety of evidence supervision chain and legal effect.

(6) The Identification of Knowledge Database and Crime Behaviour Case Database

The communication among identification knowledge database and crime behaviour case database and evidence storage center used common XML format, identified knowledge

database improves the effect of the identification, and crime behaviour database improves availability of the evidence.

4 Case Analyses

4.1 The Construction of the Evidence Chain

Reference [6] described in identification case analysis of panda virus. After the trusted fix of the electronic data on the identification materials provided, the evidence chain in accordance with the three-dimensional trusted electronic chain and evidence supervisory chain model constructed as follows:

Software environment for the related experiments ->interests, abilities and qualities of the suspects produced computer viruses-> the motives of the suspects produced virus-> the original virus code and mature products-> benefits obtained from the suspect.

4.2 The Construction of the Evidence Ring

(1) Software Development Environment Ring

Delphi7, VMware, ICQ and other software were found in the suspect 's mobile hard disk partition 1, Delphi7 of above three tools is a programming tools software that is widely used in the programming, can be used to write and debug virus code; Vmware is a virtual operating system software, the experiments of virus infection and destruction can be executed repeatedly in the virtual operating systems,which doesn't infect on virus writer own computer; ICQ is a tool used to change the program icon,the icon of any executable program can be modified into a panda icon. Thus, the above three tool software supports each other between production of virus and virus experiments, construct the virus development environment ring.

(2) The Identification Ring of the Suspect's Abilities and qualities

In the favourite of division 1, 2, a large number of Website links of hackers base, Trojans, viruses technology were found, this shows that the hard disk owners has a very strong interest in knowledge of hacker attack and defence,the production and transmission the virus.At the same time in the division 5,found the manual, Ebook,videos and other information on a large number of hacking and tool software,production of Trojans and viruses,implementation of network attacks,including "gray pigeons remote management".And found in the history log, the hard disk user has visited many times these data and the directory;Still found a lot of source code file and Trojan programs that have programmed and packaged in Exe file with programming tools such as VB,VC and Delphi, these Trojan can run directly. in"\Source Code\Delphi\My_Work\Wuhan boy process monitoring\Code "directory, found "Wuhan boy" source code file.In"\Source Code\Delphi\ My_work\infection" directory,also found the multiple versions of the virus source code files,chronological order and clearly marked:" 2006.10.16,2006.10.25,2006.11.7,2006.11.8,2006.11.25,2006.11.30, 2006.12.1", etc.The code content than multiple versions of the code is basically the same and the function is gradually improved, reflecting the process of the authors maintenance and improvement.These website links, tools software, manual, Trojan source code and program and Wuhan boys source code mutual support and collaboration, constructing identification ring of the suspect's abilities and qualities,Wuhan boy source code in chronological order itself constructs a time ring at the same time.

(3) The Suspect's Benefit Ring

In Xiaojun document, found a lot of IP address,the computer's name, and login user name and password of Online Game ("hangame","itembay","journey","adventure island");

In"MyHacker\articles seen frequently\bill" directory,found accounts totaling more than 40 ten thousand yuan in January 2005 to July 2006,by extracting chat logs of Lijun with another persons, the contact person know what Lijun is doing, and put forward his demands,the two sides discuss the price of Trojan viruses and Trojan code generator. From obtaining game account and login password of else's computer using Trojan to the sale price of the Trojan code and Trojan generator Trojan, we can conclude that the author is not simply out of interest in the production of the Trojan program only to gain the economic benefits,thus constructing the suspect's benefit ring.

Due to limited conditions, the paper can not analyze international case.Therefore; the next step is to achieve international case analysis by broadening the channels of the collection of all relevant international case.

5 Conclusions

This article first proposed a three-dimensional trusted electronic evidence chain model based on analysis of existing forensic model, and then proposed an electronic judicial identification model based on evidence chain and evidence Supervision,the model can realize trusted fix of electronic data by electronic data trusted fixed process; by increasing identification supervision,time constraints (trusted time stamp)and legal constraints for ensuring objectivity,legality and availability of evidence; and can used evidence ring and evidence chain for ensuring integrity,correlation,continuity and consistency of evidence;by increasing political judicial and CA authorization and authentication mechanisms for solving mutual trust and mutual recognition of evidence between courts and identification agencies,and ensuring evidence supervision their own legal effects. The model can be used not only in electronic judicial identification and electronic forensics for obtaining electronic evidence, can but also be used in the enterprise to obtain evidence of employee mistakes, and used to guide judicial practice affairs and theoretical studies.

ACKNOWLEDGMENT

The project is funded by Hebei Province Institute of Humanities and Social Sciences Research Project(NO.SZ2011104).

REFERENCES

[1] Mai Yong-hao, Sun Guo-zi, Xu Computer Forensics and Judicial Authentication Beijing: Tingshua University Press, 2009(In Chinese)

[2] Guo Qiu-xiang, Zhu Jing-yi.The Construction of the Electronic Data Examination System. Chinese Journal of Forensic Sciences, Vol.49,pp. 57-60.February 2010(In Chinese).

[3] Zhou Min, Gong Jian, Study on the Distributed Computer Forensics Model.Mciroelectronics and Computer, Vol.29, pp.40-43 February 2012(In Chinese).

[4] Ling Qing-xiu.Research on the Formalism of Trusted Forensic on Digital Data.College of Computer Nanjing University of Posts &Telecommunications, 2009(In Chinese).

[5] Sun Guo-zi, Chen Wei-ming, Chen Dan-wei.One Trusted Fix Method of Digital Data Forensics.Journal of Beijing University of Technology,pp.621-626.May 2010(In Chinese).

[6] Mai Yong-hao, Xiang Da-wei.Study on the Forensic and Identification Techniques of Panda Virus.Netinfo Security, Vol.112, pp.44-46.June 2010(In Chinese).