Collection and Preservation of Electronic Evidence

Yilin Zhang

Civil and Economic Law College, China University of Political Science and Law, Beijing, 102249, China

Keywords: Electronic evidence. Collection. Preservation

Abstract. With rapid development of social science and technology, the Internet is increasing applied into people’s daily life. Meanwhile, network crime also emerges at the right moment. A special evidence form is thereby caused in the evidence field, namely electronic evidence, which increasingly becomes people’s concern and research object. It is an integral part in the electronic evidence research field to legally collect electronic evidence and preserve it effectively at the same time. Therefore, it plays a decisive role in establishing and completing the evidence discovery system of electronic evidence and guaranteeing smooth works of judicial offices to collect and preserve electronic evidence properly and finally apply it into juridical practices.

Introduction

As a special evidence form in the evidence field, electronic evidence has higher concealment, complexity, technical requirements and other characteristics when compared with traditional evidence, which determine the uniqueness of electronic evidence collection and preservation. For a legal evidence discovery subject, electronic evidence can be easily collected and preserved through legal evidence discovery procedures and with correct methods, technologies or tools. Besides, it is of great importance to apply electronic evidence into juridical practices and thus to effectively prevent and fight against network crimes.

Collection of Electronic Evidence

Collection Subject of Electronic Evidence

It is stated in Article 50 of the Criminal Procedure Law that “Judges, procurators and investigators must, in accordance with the legally prescribed process, collect various kinds of evidence that can prove the criminal suspect’s or defendant’s guilt or innocence and the gravity of his crime. It shall be strictly forbidden to extort confessions by torture and to collect evidence by threat, enticement, deceit or other unlawful means”. According to Article 52, “The People’s Courts, the People’s Procuratorates and the public security organs shall have the authority to collect or obtain evidence from the units and individuals concerned. Physical evidence, documentary evidence, audio-visual recordings, electronic data, and other evidence gathered by an administrative authority in the process of law enforcement and case investigation may be used as evidence in criminal procedures.” It is stated in Article 3 of Rules of the People’s Procuratorate on Inquisition Procedures of Electronic Evidence prepared by the Supreme People’s Procuratorate that “Inquisition of electronic evidence are activities executed by inspection technicians who, in accordance with relevant theories and methods, assist investigators in promptly discovering, obtaining and fixing as well as inspecting electronic evidence or other kinds of evidence associated with a crime, in order to provide clues and evidence to the department of handling cases to help it judge the nature of a case and determine the handling direction.”

According to laws and regulations above, electronic evidence is collected by the following four subjects in criminal cases: judges of the People’s Courts, procurators of procuratorates, investigators of the public security organs, and administrative organ. Different from traditional evidence, higher requirements are set for electronic evidence collection subjects in juridical practices due to technical requirements of electronic evidence itself. Besides investigators of administrative organs and judicial
offices, electronic evidence collection subjects also include professional electronic technicians approved by judicial offices. In cases related to electronic evidence, investigators of administrative organs and judicial offices, due to insufficient related knowledge, always take improper actions when they encounter professional, technical or other issues related to electronic evidence, although they have mastered abundant legal knowledge and had extensive experiences in handling cases. For instance, such investigators collect electronic evidence just by simply detaining or checking computer, mobile or other electronic devices used by a criminal suspect committing certain crime, which easily leads to damage or even loss of electronic evidence and thereby to weakened or even lost probative force of electronic evidence. In such cases, it is necessary for professional personnel proficient in electronic technology related knowledge to assist investigators of judicial offices in collecting electronic evidence, so as to avoid effects or possible effects of evidence damage or loss caused by above circumstances on probative force of evidence. It’s important to note here that professional electronic technicians can only act as assistants rather than subjects in the collection of electronic evidence. The collection of electronic evidence is far from simple technical works, however, it is more associated with legal works. Although they have professional knowledge related, the collection will make no sense if such technicians without professional law knowledge related collect electronic evidence against modes or procedures stipulated by relevant laws and regulations. In conclusion, electronic evidence in criminal procedure cases shall be collected in a form with investigators of judicial office as well as administrative organs as major subjects and professional electronic technicians as minor subjects.

According to Article 64 of Civil Procedure Law, “A party shall have the responsibility to provide evidence in support of its own propositions. For the evidence that cannot be obtained by any parties or their litigation representatives because of some realistic reasons or for the evidence that the people’s court considers necessary for adjudicating the case, the people’s court shall investigate and collect such evidence.” According to legal provisions above, evidence in civil procedure cases is mainly collected by the party involved and its litigation representatives or the people’s court.

According to Article 32 of Administrative Procedure Law, “The defendant shall have the burden of proof for the specific administrative act he has undertaken and shall provide the evidence and regulatory documents in accordance with which the act has been undertaken.” It is stated in Article 33 that “In the course of legal proceedings, the defendant shall not by himself collect evidence from the plaintiff and witnesses.” In Article 34, “A people’s court shall have the authority to request the parties to provide or supplement evidence. A people’s court shall have the authority to obtain evidence from the relevant administrative organs, other organizations or citizens.” According to legal provisions above, evidence in administrative procedure cases is mainly collected by either the two parties or the people’s court.

Collection Procedures of Electronic Evidence

At present, collection procedures of electronic evidence are still incomplete in China. Many problems need to be addressed urgently. Different kinds of electronic evidence have different characteristics and different technical requirements. Accordingly, collection procedures are also different to some extent. Even so, collection procedures of electronic evidence are approximately the same. Specifically, electronic evidence in civil procedures and administrative procedures cannot be recorded, obtained or fixed without the authorization or permit of relevant organizations or the party involved. In criminal procedures, collection of electronic evidence mainly includes the following steps:

**Cordon off and inquest the crime scene**

To collect electronic evidence, first cordon off the crime scene for inquisition; cut off all contact with the outside world; stop relevant electronic devices; videotape relevant electronic devices on scene, and put all these into records at the same time.

**Protect electronic devices**

Inspect relevant electronic devices, and take effective measures to protect such devices against any damages.
Make a preliminary check on electronic devices
Relevant personnel shall make a preliminary check on electronic devices (such as system, software & hardware and other basic parameters), and make relevant preparations, which is more beneficial to smooth obtaining of evidence in the next step.

Backup electronic evidence
Before being obtained and fixed, electronic evidence shall be backed up to avoid damage or loss of such evidence in later works.

Obtain and fix electronic evidence
After relevant preparations are made, personnel involved shall obtain electronic evidence with legal technologies and tools. Electronic evidence obtained shall be promptly fixed to prevent any damage or loss in the process of collection. In the fixing process, any damage is not allowed for original data in electronic devices. Moreover, relevant pictures shall be shot and videotaped in the process of obtaining and fixing. At the same time, relevant details shall be recorded for integrity and authenticity of electronic evidence.

Preservation of evidence in unexpected cases
In case of any other unexpected circumstances (for instance, failure of relevant evidence obtaining equipment or tools to obtain relevant evidence), electronic devices involved can be properly preserved and taken out of the crime scene for evidence obtaining. However, relevant reasons for taking such devices out of the scene must be explained in relevant records.

Additional record of relevant information
The last step for collection of electronic evidence is to record the evidence collected, and note its source, obtaining time & process, name of the obtainer and other information, so as to ensure authenticity and legality of electronic evidence collection.

Preservation of Electronic Evidence

Concept of Preservation of Electronic Evidence
For the concept of preservation of electronic evidence, no unified definition is available in the research field of electronic evidence. In the author’s opinion, the preservation electronic evidence refers to legal act of the electronic data preservation subject who, under legal preservation procedures, uses valid storage methods to protect and manage the collected electronic data probably proving, in a legal sense, facts of a case.

Preservation Subject of Electronic Data
Electronic data preservation subject is mainly divided into two categories: i) the first category refers to electronic evidence collection subjects as mentioned above. Based on the nature of different cases, such subjects are divided into three categories: preservation subject in civil procedures, preservation subject in criminal procedures, and preservation subject in administrative procedures. After the collection of electronic evidence, the collection subject shall promptly and properly preserved the evidence collected, and make sure that the collected evidence can be used as evidence to prove facts of a case in a legal sense; ii) the other category refers to professional evidence preservation subjects. In civil procedures or administrative procedures, the electronic data is preserved by professional evidence preservation organizations or departments designated by both parties. In criminal proceedings, the electronic data is preserved by professional evidence preservation organizations or departments designated by judicial offices or administrative organs.

Preservation Procedures of Electronic Data
The electronic data itself is unreadable, and it is saved in various memory media in a series of forms including electrical, magnetic, or optical signal. Therefore, relevant memory media shall be stored first while preserving electronic data. As electronic data is backed up during the collection, relevant information shall be noted in details, including name and category of the original’s and the copy’s memory media. At the same time, detailed information of the electronic evidence preserved shall be indicated. Moreover, each step of the electronic evidence in the process from collection to
presentation on the court shall be recoded in details for legality, integrity and authenticity of the electronic evidence.

**Methods and Technologies of Electronic Data Preservation**

There are a variety of methods and technologies for preservation of electronic data. The author summarizes several common preservation technologies as follows:

**Data monitoring technology**

Data monitoring technology means that relevant technicians use specialized monitoring equipment to control relevant data information (i.e. flow and signal) of electronic devices within a certain spatial range and to monitor abnormal changes in data information of such devices, so as to protect relevant electronic evidence.

**Write-protection technology**

Read-only files are also termed as files with the write-protection function launched. A file can be protected by means of write-protection. In this way, the original file is protected to prevent misoperation and avoid attack from virus towards the file.

**Encryption technology**

Encryption technology is the main security and secrecy method used in e-commerce. It is the most frequently used security and secrecy means, which uses technical means to convert significant data into messy code (encrypted) for transmission and then restore (decrypted) the data with the same or different means after the data reaches its destination.

**Digital signature technology**

Digital signature (also termed as public key digital signature and electronic signature) is a method used to identify digital information, which is similar to a common physical one written on the paper, but it is realized with technologies in the public key encryption field.

**Establishment of Electronic Data Preservation System**

At present, the electronic data preservation system is still incomplete in China. Based on the existing theoretical knowledge and relevant data, the author proposes the following suggestions to complete the electronic data preservation system:

**Enhance storage of memory media**

Electronic data is saved in memory media in certain forms. If the memory media are damaged, the content of electronic data will inevitably be damaged as well. Therefore, storage of electronic data memory media shall be strengthened (for instance, adopt the write-protection technology to set it as read only). Moreover, such memory media shall be regularly inspected and maintained.

**Take security protective measures against remote invasion**

In the network environment, hacker can operate a computer in long distance through remote data transmission. Therefore, security protection measures shall be taken for relevant electronic devices during storage of electronic data.

**Adopt encryption and other relevant protection technologies for electronic data**

Relevant protection technologies can be adopted for some key electronic data, such as encryption technology and digital signature. Even in case of disclosure, such electronic data can be effectively protected, and its security is enhanced.

**Prevent electronic data loss caused by infection**

Relevant software may be used while encrypting or taking other measures to protect electronic data. At this time, virus invasion shall be prevented since virus may be carried while relevant software is downloaded. Virus invasion may be fatal to electronic data. Therefore, sufficient virus preventive measures shall be taken, for instance, install antivirus program to kill virus entirely for electronic devices used to save electronic data, and regularly update the virus database.

**Standardize daily operation, and regularly inspect electronic evidence**

The person for storing electronic evidence shall standardize his daily operation, and inquire professional technicians for any operation of electronic evidence beyond his professional knowledge. The person shall be guided face to face, if necessary, to prevent any damage to electronic evidence caused by misoperation. Besides, electronic evidence shall be inspected on a regular basis.

**Implementation of accountability**
Electronic data shall be saved by special person and in special room. Monitoring equipment shall be installed in the storeroom. Any organization or individual shall be liable for any damage or loss of electronic evidence caused by them accordingly.

References
[3] Zhang Hongwei and Guoxin: Principles and Methods for Collecting of Electronic Evidence, Procuratorial Daily, 2010-12-7 (3);