

The Dilemma and Countermeasures of the Practice of Electronic Forensics in Criminal Procedure

Yubao Wu

Department of Information Technology, Nanjing Forest Police College, Nanjing, Jiangsu, 210023, China
eice_wu@126.com

Keywords: Formal Litigation, Electronic Forensics, Dilemma, Countermeasures.

Abstract: With the development of Internet electronic technology, electronic evidence occupies a very important position in the judicial practice of our country. However, because the electronic evidence is listed as the kind of legal evidence in the judicial practice of our country for a relatively short time, there are many difficulties in the practice of obtaining evidence. How the legal person overcomes these difficulties, consummates the electronic evidence collection work, constructs the relatively complete operation mechanism from the legislation, the judicature and so on, enhances the electronic evidence proof power, is the key question which needs to discuss..

1. Introduction

Nowadays, with the further development of computer network, there are more and more criminal cases on the network. For example: Internet fraud, Internet hacking computer crime and so on. When legal workers face such cases, they can not help but involve the evidence of electronic evidence and the identification of evidence. However, in the present situation, there are many problems in the practice of electronic forensics in criminal proceedings, such as: the process of obtaining evidence is difficult, the process of determining evidence is difficult, the legislation of evidence collection is not perfect, and so on. The change of information age is unprecedented, and the leap of information existence and acquisition makes the study of evidence and even the legislation of evidence face many tests. Under the general trend of evidence informatization, the electronic data based on computer and its network plays an increasingly important role in the process of proving the facts of the case. Therefore, according to the actual situation, we should take appropriate measures to improve the plight of existing electronic evidence collection, so that electronic evidence can play its full role.

2. Summary of Electronic Evidence

2.1. Concept of Electronic Evidence

Electronic evidence is litigation evidence stored in magnetic media in the form of electronic data. The new Code of Criminal Procedure has included "electronic data" as one of the types of evidence.



Figure 1 The concept of electronic evidence

In general judicial practice, electronic evidence mainly includes: email, telegram, chat record, announcement information, call recording and so on. The application of electronic evidence in criminal proceedings can greatly improve the efficiency of judicial practice, which is an important measure in line with the trend of the times[1].

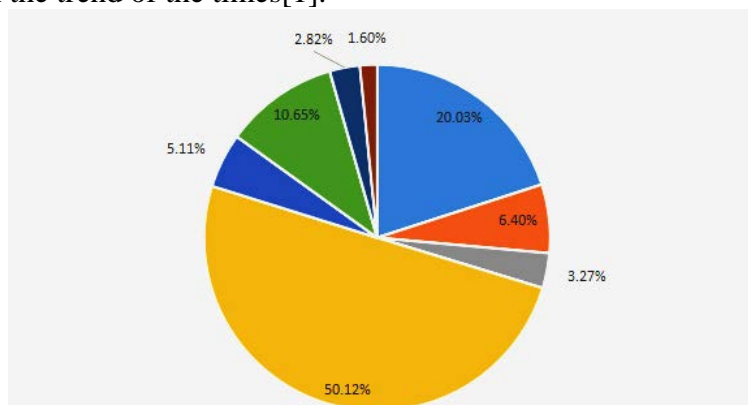


Figure 2 People's primary use of mobile phones today

3. The Difficulties Faced by the Practice of Electronic Forensics in Criminal Litigation in China

3.1. Legislation Lags Behind

Although the new Criminal Procedure Law of our country stipulates that electronic evidence is one of the valid legal evidences, it lacks the corresponding practical experience in practice. In addition, the electronic evidence itself is difficult to preserve, easy to be tampered with and so on, which makes it difficult for the electronic evidence to have the same persuasion as other traditional evidence.

3.2. Lack of Evidence Testing and Identification

In the present case, there is an increasing number of criminal cases requiring proof by electronic evidence. However, the judiciary does not have a special electronic evidence collection department to obtain evidence of this kind of evidence, which is sufficient to reflect the current situation of imperfect electronic evidence detection and identification institutions. Although some regions have established the corresponding evidence testing and identification agencies, the lack of corresponding equipment and talent has limited the role of such institutions. These difficulties make it difficult to guarantee the persuasion of the electronic evidence itself and bring difficulties to the work of the national judicial personnel to solve the case.

3.3. Lack of Certification Personnel

We need to be clear: the evidence of electronic evidence not only needs the forensics personnel to have the relevant legal knowledge, but also needs the forensics personnel to have the corresponding investigative and computer knowledge. In the present case, however, such talent is extremely scarce. This leads to the relevant departments in the electronic evidence collection, because the quality of the forensics personnel is not high and easy to lead to the destruction of evidence or evidence acquisition process is not standardized and so on, which is very unfavorable to the detection of the case.

3.4. Backward Certification Technology and Equipment

Electronic evidence, as evidence of high scientific and technical content, requires the technology and equipment to better ensure the authenticity and legitimacy of the evidence. However, as far as the present situation is concerned, our country is backward in the technology of collecting evidence of electronic evidence, and the replacement of evidence collection equipment is not very timely, which is very unfavorable to the detection of relevant criminal cases.

4. The Effective Perfecting Strategy of 4. Electronic Evidence Obtaining in China

4.1. Increase the Training of Electronic Evidence Forensics Personnel

In view of the shortage of professional electronic evidence-taking talents at present, the state and relevant departments should strengthen the training of electronic evidence-taking talents so as to further strengthen the judicial team in China.

The relevant departments shall conduct corresponding legal training on evidence and computer for personnel conducting on-site exploration and inspection. In order to enable the current staff to have the corresponding protection of evidence and the awareness of the discovery of evidence, but also to be able to find evidence and evidence of the correct methods. Relevant departments can promote the further strengthening of the judicial team in China by combining online and offline education to improve the professional quality of the current staff.

In view of the shortage of professional electronic evidence, we can reserve talents from the perspective of higher education. The National Bureau of Education may issue effective training programs, requiring the major law colleges to set up corresponding training courses in the direction of electronic evidence, and demanding that the professional direction should carry out personnel training according to the training plan issued by the state, so as to further expand the talent reserve in the field of electronic evidence collection in China.

Besides the method of cultivating talents, the relevant departments can expand the scale of electronic evidence-taking talents in the judicial department by applying the appointment system. The relevant departments may form an expert group on electronic evidence by employing experts in various fields, such as computer, investigation and law, so as to involve the expert group on electronic evidence in the work of obtaining evidence in major criminal cases. This will make the evidence of electronic evidence, reduce resistance and improve efficiency.

4.2. Standardized Forensic Process

Although the process of obtaining evidence of electronic evidence has been stipulated in Chinese legislation, the process of obtaining evidence is not standardized. Therefore, the relevant departments should further strengthen the law enforcement, standardize the process of obtaining evidence of electronic evidence, so that the legitimacy of evidence can be guaranteed.

Site protection. Before collecting evidence, the computer should be cut off all contact with the outside world, all equipment on its periphery should be seized, and on-site personnel should be required to prohibit any unrelated operations.

Search evidence. Search the evidence personnel should immediately detect other information systems connected to the target computer, check the network, cable, power supply and other connections to see if the target system is connected to other LANs or information systems[2]. In addition, search personnel should also pay attention to the corresponding storage media, such as: USB disk, hard disk, but also timely ask the relevant personnel to replace the corresponding electronic equipment. If there is a history of equipment replacement, it is necessary to pay close attention to the specific direction of the replaced equipment. Only in this way can the integrity of electronic evidence be guaranteed to the greatest extent, and the later stage of evidence testing be facilitated.

Evidence extraction. Lost evidence needs to be kept and backed up in a timely manner, and other evidence that may be left over from electronic devices such as fingerprints, handprints, blood stains, etc.

The evidence is fixed. When the relevant evidence is extracted, the evidence extractor should properly number and preserve the evidence that has been extracted. Not only to avoid the natural environment of the political situation, but also to prevent other people through network hacking to damage the evidence or tamper with evidence, so that the authenticity of evidence.

Evidence. Every forensics officer should make a corresponding record after the end of the evidence, so as to protect the responsibility to the person. When there is a problem with the evidence, it is possible for the relevant authorities to be documented. The main contents of the evidence record include :(1) the cause of the case ;(2) the name and position of the forensics

officer ;(3) the witness ;(4) the procedure for extraction ;(5) the type and presentation of the electronic data extracted ;(6) the problems encountered in the course of acquisition and the measures taken; and (7) the signature or seal of the responsible person involved.

4.3. Construction of Electronic Evidence Transmission Authentication Platform

In view of the difficulties in the authentication of electronic evidence at present, the relevant departments can help the electronic evidence to solve the problem of authentication by constructing a special evidence inspection and identification organization and setting up a special evidence inspection and identification platform, so that the authenticity and legitimacy of electronic evidence can be further guaranteed, so that electronic evidence can play its real role in criminal proceedings[3].

The relevant departments can combine the current electronic big data with the transmission authentication of electronic evidence, construct the electronic evidence transmission authentication platform, so as to improve the efficiency of the collection and identification of electronic evidence, and help the judicial department to better solve the corresponding criminal cases. For example: Haining court based on the actual situation, build the corresponding block chain electronic evidence platform. The launch of the platform can not only effectively solve the problem of hard evidence collection and identification of electronic evidence, but also improve the judicial efficiency to a great extent, let the identification of evidence break the limitation of time and space, to a great extent, reflect the evolution of the Chinese judicial model in the Internet era, which is a further embodiment of China's judicial modernization. The related page is shown in Figure 3.

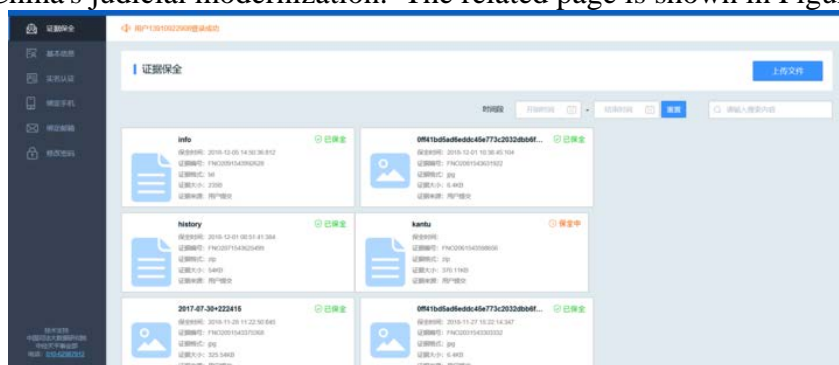


Figure 3 Electronic evidence cloud

5. Conclusions

To sum up, although the problem of electronic evidence collection is facing many difficulties, we can solve the multi-dilemma of electronic evidence collection by strengthening the training of electronic evidence collection talents, standardizing the process of evidence collection and constructing the authentication platform of electronic evidence transmission according to the actual situation, so as to give full play to the role of electronic evidence in criminal proceedings and help the judicial department to solve criminal cases effectively.

Acknowledgements

The 2019 major special support from Jiangsu Provincial Department of science and technology, Research and demonstration of key technologies for security protection of Jiangsu Police cloud (BE2019762)

References

- [1] Zhang, Zetao. On the procedural risk perspective of the connection between administrative evidence and criminal evidence —— on the rule of excluding illegal evidence in criminal procedure. Political and Legal Forum, vol. 37, no. 5, pp. 67-80, 2019.

[2] Wang Liping. A study on the rules of Electronic data Application in Cyber Crimes. Technological Wind, no. 24, pp. 112-113, 2019.

[3] Fu, Yangfu. On the Difficulties and Solutions of Electronic Evidence in Criminal Proceedings. Fujian: Overseas Chinese University, 2016.