International Journal of Digital Crime and Forensics
Volume 12 • Issue 3 • July-September 2020

Research on the Rules of Electronic Evidence in Chinese Criminal Proceedings

Jin Du, Digital Forensics Lab, Institute of Software Application Technology, Guangzhou, China & Yunnan Police College, Kunming, China

Liping Ding, Digital Forensics Lab, Institute of Software Application Technology, Guangzhou, China & CAS, Guangzhou, China

Guangxuan Chen, Zhejiang Police College & Institute of Software, Chinese Academy of Sciences, Beijing, China

ABSTRACT

As a new object in judicial practice, electronic evidence is of great practical significance. To locate the probative force of electronic evidence, which can be used to prove the facts of the crime, judging the electronic evidence validity, and how to establish scientific rules of electronic evidence, which not only effectively contains crime, but also protects civil rights from illegal infringement of state power becomes very important. This article outlines the definition of electronic evidence and rules and establishes a suitable electronic evidence system of China's criminal procedure system based on the analysis of problems in each link of judicial proof in judicial practice and the four aspects of judicial proof.

KEYWORDS

Electronic Evidence, Evidence Rule, Judicial Proof, The Ability of Evidence, The Validity of Evidence

1. OVERVIEW OF ELECTRONIC EVIDENCE AND RULES

There is no uniform evidence law in the judicial practice in China, and the relevant evidence systems are divided in the three big procedural laws. In the context of the new criminal procedure, the provisions are lack of maneuverability, although there are evidence provisions in the judicial interpretation, it still cannot meet the needs of judicial practice.

To establish a rational criminal evidence law, we must start from the rationality and procedural justice, to analyze the characteristics of different evidence, and construct the relevant evidence rules. Thayer, a famous jurist of evidence, believes that the core content of the evidence is a set of technical rules that are essentially negative norms and rules of exclusion. These specifications and technical rules make clearly defined which facts may appear in the court as well as how to prove the facts appear in the court (Chongyi, 2014; Shuhou, 2015; Jianlin, 2014; Jiahong, 2014; Jiahong, 2014).

Scientific evidence rules are an important embodiment of the procedural justice and the guarantee of human rights. Professor Baoguo Fang has three points about the functions and roles of evidence: first, evidence rules help identify the case facts, but also restricts the fact investigation to a certain extent. Second, evidence rules enhance the operability of the proceedings, and restrain the discretion

DOI: 10.4018/IJDCF.2020070108
This article, originally published under IGI Global's copyright on July 1, 2020 will proceed with publication as an Open Access article starting on January 27, 2021 in the gold Open Access journal, International Journal of Digital Crime and Forensics (converted to gold Open Access January 1, 2021), and will be distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

of the judges (Ping, 2013). Third, evidence rules help to protect human rights, specific social relations, and social interests.

1.1. Definition of Electronic Evidence

With the development of computer technology and extensive application, in the earliest 50s in the last century, the emergence of the concept of computer evidence, which generates electromagnetic records during the computer or computer system running in the process and uses to prove the facts of cases. Later, with the application of network technology, there appeared the concept of network evidence, which refers to the electromagnetic records in the network environment and uses to prove the facts of cases. Until the 90s in last century, besides computer and network, the emergence of a large number of digital products, and the advanced digital signals of telephone, Telegraph and television which were used to transmission signals by analog signal. At this time, the jurisprudential circle called this "electronic evidence" which differs from the traditional forms of evidence "record" (Ping 2013).

In this paper, in order to cover different forms of electronic evidence, we choose the carrier form of electronic evidence for the generalized definition: exist in electronic form, used as the information technology or information equipment evidence form, all the data and its derivatives. This definition indicates that the electronic evidence should have legal characteristics firstly, and it is used as a proof material to prove the case facts. Secondly, the electronic evidence are present in electronic form and information technology, so their generation, transmission, resulting, acceptance and storage have a certain commonality. Finally, the carrier of electronic evidence must rely on electromagnetic media, such as disk, CD type, so the data information always leave some traces in these electromagnetic media.

1.2. Definition and Function of the Evidence Rules

The formulation of rules of evidence mainly comes from the Anglo-American legal system, which is called "of evidence rules" in English. And it is called "the law of evidence" in Taiwan area. The evidence rules in Anglo-American legal system countries are used as customs, cases, or judicial interpretations (Pinxin 2013). However, since the second half of the 19 Century, the system of evidence in the Anglo-American legal system countries has been gradually got codification, such as India's evidence law, "the rules of the federal rules of evidence" (Chinese People's Public Security University Press 2013), etc. Generally speaking, the rules of evidence in Anglo-American legal system mainly refer to the various basic rules and a series of exceptions and conditions, which are used for the correct use of evidence. The content mainly includes: the rules of the burden of proof, the rules of the association rules of evidence and the rules of hearsay evidence.

At present, the domestic scholars have different views and interpretations in defining the rules of evidence. Some scholars believe that the evidence rules are the general term of confirming the scope of the evidence, adjusting and restricting the legal norms, which is a concentrated expression of the law of evidence. Some scholars believe that the rule of evidence refers to the norms of the collection, review and evaluation of normative evidence. There are scholars that believe that the rules of evidence have broad and narrow points. In a narrow sense, it refers to a dominant role in the trial or hearing rules, which refers to admissibility rules; in a broad sense, it refers to the evidence rules and guidelines of collection and use. In a narrow sense, it belongs to the Anglo-American legal system, this article adopts the theory of broad sense which proceed from China's reality.

2. THE EXISTING PROBLEMS OF CHINA'S CRIMINAL ELECTRONIC EVIDENCE RULES

Nowadays, we have entered the era of information with the development of electronic information technology and the wide application of electronic products. Information is everywhere, the electronic evidences exist in the form of electronic information and use for being evidences. They are the data information and various of its derivatives with the assistance of information technology or equipment.

There are various forms of electronic evidence, not only the traditional telegraph, telephone and fax etc., but also the electronic bulletin (BBS) data network, IP address, router's MAC address and digital signatures are included. The electronic evidence also faces some problems in the China's criminal proceedings, one is the question of electronic evidence's position, and the other is the lack of electronic evidence rules in different forensics, quote, certification and cross-examination.

2.1. Positioning of Electronic Evidence

To use evidence which exists in the form of electronics and its derivatives, in general, all countries in the world hold a positive attitude, and so does China. It is not a problem, because we have a relevant provision, which is anything that can prove a case, is evidence (Guomin, 2012). But the question of what position should be given to the electronic evidence has been a constant dispute among the academic community.

This has been an age-old discussion for electronic evidence among the law circle. There are three points now through the previous debate: "classified", "independence" and "mixed theory". These points of view have their own advantages and disadvantages. January 1, 2013 the new "Criminal Procedure Law of the People's Republic of China" provisions of article 48 lays down the electronic evidence is one of the stipulated legal evidence types. Since then the debating legal status of electronic evidence had ended and the electronic evidence won its legal status in criminal proceedings (Joachim 2012). It is the first time for the two new civil and criminal procedure law that combines the electronic evidences and the traditional evidences at the same time. It is also the first time that China law made electronic evidence clear to be a kind of legal evidences.

To be grouped in documentary evidence, audio-visual material is only a makeshift for electronic evidence before the revise of criminal procedure law. It cannot reflect the different texture of electronic evidence. Electronic evidence is a new social phenomenon in the information age, which obviously does not belong to the traditional types of evidence. Even if the manifestation forms are seemly related to some traditional evidence, but the electronic evidence relying on its strong proof ability becoming an exceptional independent type of evidence in the lawsuit, and playing an important role of evidence, which cannot be replaced in the case, when there's a dilemma.

In the long run, with the development of science and technology, there will be more and more new evidence in the human society, which will also be faced with the problem of legal orientation. Therefore, the division of evidence should be carried out according to its nature, characteristics and proof mechanism. For the status of electronic evidence, the author believes that we should build an open system of evidence classification in Mr. Pei Candling's method, and classified them into: material evidence, documentary evidence and witnesses. In this system, it has been divided into 4 basic types according to the characteristics of the material: physical evidence, vestigial evidence, traces evidence and intangible evidence. Documentary evidence has been divided into 3 basic types: texts, pictures and video documentaries. The witness has been divided into 3 basic types: the testimony of witnesses, statements of victims, the criminal suspects or defendant's confession and defense etc. Then the evidences will be classified into these 3 categories according to the mechanism of the electronic evidence. For example, using e-mail as evidence, the parts of expressions in the mail are going to belong to the documentary evidence. And the automatically generated records such as the email headers, message source and target address, e-mail system records are belonging to another documentary evidence of mail authenticity. If the message was deleted after the suspect by the evidence, forensic experts restored e-mail by technical means, then it is and evidence of expert testimony which is issued by the expert witness, so it belongs to witness evidence.

2.2. The Issues of Electronic Evidence in the Process of Obtaining Evidence

The development of information technology and the extensive application has bound crime detective and the electronic evidence ever more tightly together. People often get more clues and evidence by means of modern technology, but in judicial practice, the material is often used as investigators

clues, rather than the final material. This is due to the easy destroy and modify characteristics of electronic evidence, if taken as a material, in the aspects of cross-examination, especially in the criminal proceedings, which requires a higher standard of proof, "beyond reasonable doubt", due to the characteristics of electronic evidence, the real essence of electronic evidence will be questioned, so, it is indeed regrettable for many cases that cannot be convicted with hard work in obtaining the electronic evidence. And all this is because the lack of necessary legal rules of electronic evidence collection in our country (Yuan 2012). The specific performance is that investigators do not know where to implement the legal limits of electronic evidence, but the fact that this activity in today's China is no specific legal constraints. Under the case of no specific law to constrain the behavior of electronic evidence, will it lead to some of the problems of improper infringement to civil rights when investigators use the software and technology? There is still an insufficient interaction between legal norms and electronic evidence in today's China.

From the point of the practice in electronic forensics, the electronic evidences are using more concentrated in online gambling, online fraud and Internet pornography cases when identify the facts of crimes. In the investigation, if the server is not in the scope of the jurisdiction in our country, due to lack of methods in obtaining the original ones, investigators usually use the "screenshot" or "download" to approach the preservation of evidence. Under the ways of evidence preservation, which are in the absence of other evidence to protect its forms of authenticity. Will these kinds of evidence withstand the scrutiny?

In addition, search and seizure is an important part in the evidence collection. Search is a major way of obtaining evidence in criminal cases, and it is also an investigating act directly relating to the rights of privacy, personal rights and property rights. Therefore, the implementation should be taken strict examination and approval procedures, and ensured strict observance of laws (Shan 2012). The act of obtaining the electronic evidence is in the virtual space, so it is important for us to think about what kind of legal regulation should be taken in the virtual space when search and seizure, so that we can guarantee to obtain the evidence and not infringe the legal rights of others at the same time.

To sum up, from a technical point of view, the scope of electronic evidence forensics will become increasingly larger and larger, forensics technology will sooner away from "download", "screenshot" this kind of original methods, but to a more professional forensics. Moreover, the process of obtaining evidence is bound to move towards the standardization management. From a legal point of view, electronic evidence forensics system also belongs to the scope of forensics regulation. And the electronic forensics technology and standards must accept the regulation by law. Only by these, can the electronic evidence really have the ability as to make to withstand interrogation. Therefore, with the development trend of electronic evidence, this is an emergent need for China to have dual constraints in technology and laws.

2.3. The Issues of Electronic Evidence in Proof

The "proof" means the activities of the parties in the case which provide evidence to the court to prove its claim during the trial or the evidence exchange. Both sides' evidence need to be reviewed before the proof, the review is mainly examining the competence of evidence and the probative force. The review of the competence of evidence is a procedural review (Eoghan 2012). It is primarily to deal with the evidence qualifications. Meanwhile, the review of evidence competence plays a legal restriction on the probative force. This requires the legitimacy review of the evidence subject, sources, methods and other aspects. The probative force review is a substantive examination of the evidence. Using evidence to prove the facts of the case, some logical links between the evidence and the case are required. Because the world is a common link as a whole, as a result, the requirement of the relevance evidence and the facts in the lawsuit must reach a certain degree. Which all of these are in order to improve the efficiency of litigation, to prevent the unlimited expansion scope of the evidence investigation in the court. It will be abandoned if there is no or almost no relationship between the

evidence and facts that should be confirmed. So the review of probative force needs to be satisfied with the "minimum probative force".

In China's judicial practice, due to the lack of the relevant provisions and probative force of electronic evidence, there's few electronic evidence mentioned in the process. Even in some cases that need electronic evidence, the effect shows insignificant. In the trial, the traditional proof is not suitable for the electronic evidence revealing. Especially when the defense questions the content of the evidence presented by the accusing party, the judge requires the accusing party to reinforce the evidence. Then the questions about how to reinforce and what standard constraints needed to be set should be regulated by each characteristics of electronic forensics. In judicial practice, there is the case of the judge who organized the parties directly to the Internet and obtained evidence of the case in the trial, so what kind of legal regulation should be set in this case.

So we must aim at the China's lawsuit system, combine the characteristics of the electronic evidence collection, research and construct the rule of electronic evidence in reviewing and proof.

2.4. The Issues of the Electronic Evidence in the Cross-Examination

In litigation activities, the cross-examination is the necessary prerequisite for attestation, which also act on it. The key of cross-examination is the question and doubt, so the cross-examination is an important means of both sides to refute and attack the other side of the evidence, but also an important way to help and affect the judge's attestation. Cross-examination may be different according to different types of evidence. It takes questioning or cross-examination for witness testimony and other words. It questions the contents or features for physical evidence and documentary evidence. As for the electronic evidence, it queries more questions because of its diversity.

In the proceedings, evidence can only be taken as a basis after subjected to cross-examination procedures. When taking cross-examination, both parties will question, explanations and argue the authenticity, relevance and legitimacy and the probative force on the evidence. And because of the authenticity of electronic evidence cannot be separated from the system environment, and some of the system environments and not in the jurisdiction of the law in our country. In this circumstance, it is kind of imposition for both parties who only to have a general knowledge to engage in cross-examination on the process of replication and generation, storage, transfer, and judge if there's any potential substantive changes in it. Cross-examination should be a fair game for both sides. And taking into account, the cost of litigation, judicial efficiency and other factors, the judge can except from some cross-examination with the compliance of a certain rules. Therefore, it is a must to set up a specific "rules of the game".

2.5. The Issues of Electronic Evidence in the Authentication Process

The authentication, refers to activities that the judge reviewing, judging and confirming the evidence in the trial process. Certification is the purpose and destination to the forensics, burden of proof and cross-examination, the judicial proof cannot be completed without the link of authentication. In the authentication process, the judge needs to make judgments for both parties' evidence. The traditional evidence, the judge can make a judgment by virtue of common sense in most cases. Due to their simple relationships and mechanisms (Binhua 2011).

The emergence of electronic evidence makes the authentication process getting complicated. Because of the various forms and a wide range of links of electronic evidence, the mechanisms are complex and hard to directly perceive. Moreover, at present, the evidence system of our country has not yet set the legal norms and rules of evidence. In this case, it is tantamount to ask judges to judge.

In the process of authentication, the questions about what constrains should be taken to the judges and what contents should be include for the electronic evidence authentication standard are closely connected to the final judgment. So constructing a suitable authentication rule of electronic evidence for China's judicial system is a burning issues which need to be solved.

3. CONSTRUCTION OF CRIMINAL ELECTRONIC EVIDENCE RULE SYSTEM

At present, with the development of electronic information technology and the wide application of electronic products, we have entered the era of information. However, due to the lack of the rules of electronic evidence, on the one hand, to achieve in the judicial practice often as material handling materials, rather than evidence; on the other hand, resulting in the electronic evidence collection, seizure and preservation methods was the defense questioned at the time of cross examination (Ruihua, 2009).

3.1. The Forensic Rules of Electronic Evidence

Forensic work, as the first part of the judicial proof, it involves the collection and preservation of evidence. The evidence collection and preservation are the premise of finding out the cases' facts, and it is also the necessary stage of handling cases. It is the basis of completion of the task, and the realization of the process. Thus, it is essential to establish the forensic rules of electronic evidence. First of all, the principle should be established before establishing the forensic rules of electronic evidence. The so-called principle of evidence forensic is a general criterion for search, collection and preservation of evidence. The author believes that the electronic evidence forensic activities should comply with the following two principles: firstly, the principle of legality of obtaining evidence. Secondly, the principle of tightly regulated processing.

The forensic rules of electronic evidence are abiding by the previous 2 principles premise; construct the specific activities criteria for the construction of electronic evidence searching, collection and preservation. From the perspective of legal regulations and technical norms, the following rules can be constructed as following:

- First, in addition to the exception of the special provisions of the law, the search for criminal electronic evidence must have a search warrant;
- Second, the criminal electronic evidence warrant need to meet 3 conditions: (1) the investigators have found evidence that the evidence involved in electronic equipment from the searched person or private virtual space; (2) a detailed description for the search or seizure of equipment and private virtual space; (3) issue a warrant according to the law;
- Third, the search scope of electronic evidence should be as clear as possible;
- Fourth, a complete chain should be established for the preservation of criminal electronic evidence.

The author thinks, since the search scope of electronic evidence is difficult to be cleared, and the storage medium may also have relevant evidence, the investigators can use the query and search functions in computer forensics software or other technical equipment, take forensic activities within scope and at the same time record the definition of storage in order not to miss any evidence. Searching for evidence in a limited scope, due to various reasons, the investigators are sometimes impossible or there is no need for all data in the storage media to be traverse viewed, so that there may be missing evidence. This requires investigators record reasons for files that are not be able to implement a thorough search. A regular chain of evidences in the forensic of criminal process should be established during taking collecting, fixing and filing the technical means. In criminal proceedings, the purpose of establishing the chain of evidence is not only to protect the integrity of electronic evidence, but also to indicate whether there is a possibility of tampering in the regulatory process. The chain content of electronic evidence should include: the personnel, location and time that are involved in the process of searching and fixing the electronic evidence, the technical means and the reasons for the disposal of the process.

3.2. The Rules of Electronic Evidence Proof

The rules of electronic evidence proof is the process of providing electronic evidence in prosecution and defense. The rules of proof also include the rules of evidence before trial. The review of the evidence before the trial, is mainly to judge the using evidence in the prosecution and the defense. The reviewing content includes the competence of evidence and probative force. From the perspective of legal regulations and technical norms, the following rules can be constructed as following:

- First, the content of the reviewing in competence of electronic evidence mainly includes the qualification of the subject and the examination of the source;
- Second, the content of the reviewing in probative force of electronic evidence mainly includes the reliability and integrity of electronic evidence;
- Third, in the process of proof, the participation of professional and technical personnel should be deemed as necessary permission to assist the trial.

The author believes that the organs, institutions or individuals should be fundamentally denied if there is no subject qualification for collecting, fixing and analyzing the identification of electronic evidence. For the examination of the source of electronic evidence, mainly to ensure the obtaining the time, method and place of electronic evidence, which proof its "formal authenticity". If the source of the electronic evidence is defective, the denying method should be different from the "fundamental negation" of subject qualification. Because the data source network environment is easy to change, this flawed evidence does not necessarily constitute a defense to the entity against. Therefore, this type of evidence does not need to be ruled out for the referee, the admissibility of the evidence won't be affected by its technical violations, and it can be identified by data and other technical measures to reinforce.

There are three ways to determine the reliability of the system: first, the computer system of a certain electronic evidence is reliable, and it is presumed comes that the electronic evidence is reliable. Second, an evidence preserved or provided by an adverse side party, and the presumption comes that the electronic evidence is reliable. Third, an evidence that can be proved as generated and stored in normal operation of the business activities, and the presumption comes that the electronic evidence is reliable. For the identification of integrity can also have two ways: first is the direct determination, this way is a prerequisite for a further compare of the original sample of electronic evidence, one by one check than by checking software. Second is the indirect identification, make presumption of the electronic evidence reliability through the normal operation of the computer system that the electronic evidence relies on. And at the same time, some electronic evidences are not completely in practice, but they can be also considered to have integrity. For example, in some cases of Internet pornography, the suspect's chat records can be used as evidence. In this kind of cases, though the suspect's chat record is not completely, the contents of the record has been enough to allow the judge to believe that the occurrence of criminal facts. Such evidence shall be determined in terms of its content to be proved.

The electronic evidence in essence is a binary sequence of numbers, so its show not only need the help of storage media as a carrier, but also need related display software and systems to convey the real message out. Therefore, electronic evidence's producing is sometimes needed the operation by professional and technical personnel, in this case, we may file an application to the court, the court reviews the status and qualifications of professional technical personnel, and they shall be permitted. In the display of electronic evidence, professional technical personnel should have a certain explanation of electronic evidence.

3.3. The Rules of Electronic Evidence Cross-Examination

Wig more, an expert on evidence, once said, "The cross-examination, the greatest legal engine for the discovery of the truth of human beings ". As a matter of cross-examination, which plays an important

role in reviewing and judging for the evidence. The rules of cross-examination of electronic evidence is the electronic evidence and proof testimony by both parties in the trial. From the perspective of improving the quality of the cross-examination and the judicial efficiency, the rules can be constructed as following:

- First, it should be allowed for both parties to apply for professional technical personnel to examine the technical issues in cross-examination;
- Second, in criminal proceedings, for those approved evidence by both parties, or evidences involving state secrets, commercial secrets or personal privacy which not allow the other party to know the specific content, the judge can directly identify the evidence by self-review.

The author believes, for the protection of both sides' defensing quality, especially the legitimate rights and interests of both parties, the judge should allow them to apply for professional technical personnel to dispute the technical issues in the case. The purpose of the rules is to improve the efficiency of litigation, and control its cost, which based on the protection of defendant's rights. Therefore, not all of the electronic evidence that involve state secrets, trade secrets and personal privacy can be exempted from cross-examination. There is some evidence, such as forensics means and technology which can open to both parties but not to the public. So it still can be cross-examined with an unopened way. In the trial of criminal case, the prosecution cannot invoke the cross-examination of forensic methods of electronic evidence by this rule while the defense raise an objection. The judge must have sufficient reason to use it to avoid cross-examination.

3.4. Attestation Rules for Electronic Evidence

The attestation rules of electronic evidence is the activity for the judge to examine, evaluate and confirm the electronic evidence provided by the two parties in the course. The attestation rules of electronic evidence depend on the authentication of the contents and methods. There are certification rules to adapt to each content and methods. The construction of attestation rules of electronic evidence should be based on the facts and the legal regulation of forensics behavior. And starting from the existing technical level, judge the competence of evidence, probative force and the value of electronic evidence. The author believes that the construction of the attestation rules for electronic evidence should be as follows:

- First, in the investigation of criminal cases, it should be recognized its legitimacy in accordance with the legal procedures when use secret way to obtain electronic evidence. With the development of computer network technology, more and more criminal investigation using electronic technology to obtain the investigation of criminal suspects, which many countries have developed similar investigation measures, such as the United States developed a "The Law of Wiretap", the British "The Law of Eavesdropping ", Japanese "The Law Communication Interception Supervision". There is no such legislation in our country at present, but in judicial practice, there are great number who use this method to carry on the criminal investigation. And because the lack of legal norms, the investigation inevitable violation the right of freedom for whom being investigated. And getting information can be only as a clue, but not an evidence as a result. China's legal system at present, the legitimacy identification of electronic evidence should be based on the construction of the exclusive rule. The author thinks that we should set up the following rules: in violation of the law, conduct search and seizure of electronic evidence, causing serious consequences shall be excluded; in violation of the law, obtained the electronic evidence by interception shall be excluded; and other serious illegal plots shall be excluded;
- Second, the attestation of electronic evidence identification. In the attestation of the identification of electronic evidence, the authenticity can be deduced if both parties make recognition, or

distinguishing that it has not been altered by experts qualification, or obtain relevant evidence the original evidence generation environment through other means which are unable to obtain the original electronic evidence. For the "original electronic evidence", which is the data generated in original. "The original generating environment" refers to the storage media which is fixed in the first generation;

- Third, the association of electronic evidence. The authority of the association of electronic evidence takes the logical coherent argument. A certain extent on the facts of the relevant electronic evidence that can be proved to have a substantial impact. The judge should decide its relevance.

The above 3 points belong to the identification of the competence of evidence e of electronic evidence.

- Fourth, the reliability of electronic evidence. In determining the reliability of electronic evidence, if the equipment and software of evidence generation, storage, transmission and fixed can run normally, or state it does not affect the reliability of electronic evidence when its abnormal, it can be presumed the electronic evidence is reliable; if the electronic evidence is automatic generated by an independent third party in normal business activities and it can be deduced that the electronic evidence is reliable;
- Fifth, the value of electronic evidence. A copy of the electronic evidence is with the same value of its original one, unless the authenticity of the original one or other independent evidence is being questioned; or from the overall situation of the case, the allowance of copy original ones will lead to substantial injustice;
- Sixth, the probative force of electronic evidence. In determining the force level of electronic evidence, when several copies of electronic evidence point to prove one fact, using the following rules to evaluate the respective proof force: the probative force of electronic evidence is generally greater than that without justice, such as after justice, electronic evidence registration. The probative force of electronic evidence is generally greater than that is made for the purpose of litigation when the electronic evidence is custody in normal business activities of the third party. The strength of the evidence is generally greater than the electronic storage devices. The probative force of electronic evidence is generally greater than not affiliated information and system environment information.

4. CONCLUSION

Based on the analysis through the current system of criminal electronic evidence rules in China and the construction of the environment, based on the research of evidence classification system, a detailed analysis of the drawbacks of the current classification of electronic evidence, and put forward the classification of electronic evidence on the solution, and the scientific positioning of electronic evidence. After the analysis of the judicial practice in our country, the forensics, proof, cross-examination and attestation of electronic evidence in the four aspects of the application of electronic evidence. Finally, the construction of electronic evidence system of criminal litigation system in China, and tries to solve the existing judicial proof through the evidence system.

The construction of criminal electronic evidence system, mainly rules the competence of evidence and the proactive force. It aims to set a dual constraint system and regulate forensics behaviors by the technical norms and legal norms. And make more technical standard to distinguish the probative force of electronic evidence. So as to make contribution to improve judicial efficiency and curb crime.

4.1. Job Grant

This project is supported by the National key R & D projects. Major special projects of science and Technology Department of Yunnan Province. Jiangxi provincial economic crime investigation and prevention and Control Technology Collaborative Innovation Center Project (JXJZXTCX-007) funding.

ACKNOWLEDGMENT

Dr. Liping Du, affiliated with Digital Forensics Lab, Institute of Software Application Technology, Guangzhou & CAS, Guangzhou, China, aided with the completion of this project by serving as the corresponding author.

REFERENCES

Bian, J. (Ed.). (2014). *Evidence Law*. China University of Political Science and Law press.

Chen, R. (2009). *On Legal Research Methods*. Peking University press.

Chen, R. (2010). *Procedural Sanction Theory*. China Legal Publishing.

Eoghan, C. (2012). *The Digital Evidence and Computer Crime*. The electronic industry publishing house.

Fan, C. (Ed.). (2014). *Evidence Law* (3rd ed.). Law Press.

Guomin, L. (2012). *Study on the Legal Issues of International Trade in EDI* (1st ed.). Legal Press.

He, J. (Ed.). (2014). *New Evidence Law*. Law Press.

He, J. (2014). *Liu Pin's new book: "Evidence Law*." Law Press.

Joachim, H. (2012). The German Code of criminal procedure, the Chinese version (1st ed.). China University of Political Science and Law press.

Liu, P. (2013). *The United States Rules of Electronic Evidence*. Chinese Procuratorial Press.

Ping, J. (2013). In L. Yang (Ed.), *Electronic Evidence*. Tsinghua University press.

Ping, J. (2013). *Computer Crime Research*. the Commercial Press.

The research of electronic evidence rules in criminal proceedings. (2013). Chinese People's Public Security University press.

Tu, B. (2011). Electronic Signature and Authentication Service Law. China legal Press.

Yuan, S. (2012). *The Introduction of Criminal Evidence Ability*. The people's court press.

Zhan. (2012). *Modern Administrative Process Theory, Legal Concepts, Principles and System*. Peking University press.

Zhou, S. (2015). *Evidence Law* (1st ed.). Newbury.