Chapter 17
Applications and Trends of Digital/Electronic Evidence in Chinese Litigation

Baosheng Zhang and Huangxun Chen

17.1 Introduction

The development of information technology has greatly changed our lives and had important impacts on judicial practice in both civil and criminal cases. Digital evidence has become one of many new types of physical evidence. Since the first civil law case involving digital evidence was tried by the Beijing Haidian District Court in 1996, there has been a tremendous increase in the use of digital evidence in the litigation process within China.[1]

Digital evidence has two unique properties, making it different from traditional written evidence: (1) The method of storage and type of information rely on computer hardware or software as electronic carriers subject to alteration or recovery[2]; (2) The collection and the presentation of digital evidence require computer knowledge and skills and therefore display characteristics of scientific evidence.

Although digital evidence has its own unique features, it still shares some of the general properties of evidence. Therefore, the general rules of evidence should still

[1] See Chu Zhang and Likai Liu, "An Email with a Fake Name: Yange Xue v. Nan Zhang for a Fraudulent Email," in *Case Studies on Telecommunication Law,* 136–41 (Beijing: Law Press, 2005).

[2] Chunyu Zhao and Yunquan Zhang, "Characteristics of Digital Evidence and Their Impacts on Evidence Collection," in *Journal of Heilong Jiang Political Science & Law Management College* 1 (2006).

B. Zhang (✉)
Key Laboratory of Evidence Science, China University of Political Science and Law (CUPL), Beijing, China

Ministry of Education, Beijing, China
e-mail: bensenzh@cupl.edu.cn

H. Chen
China University of Political Science and Law (CUPL), Beijing, China

M. Kengyel and Z. Nemessányi (eds.), *Electronic Technology and Civil Procedure*, Ius Gentium: Comparative Perspectives on Law and Justice 15,
DOI 10.1007/978-94-007-4072-3_17,

apply to the standard use of digital evidence. This paper analyzes several recent cases and recommends general regulations governing the collection and the presentation of digital evidence in China.

17.2 Case Examples

17.2.1 Futaihong Precision Industrial Company v. Xiangjun Liu and Shaoqing Si

In June of 2006, Futaihong Precision Industrial Company Ltd (Plaintiff) (a part of Foxconn Group in Shenzhen Municipality) filed a civil lawsuit in Shenzhen Municipal Intermediate People's Court (hereafter, Shenzhen Court) against Xiangjun Liu and Shaoqing Si (the Accused) from Biyadi Company for invasion of commercial secrets and demanded RMB 70 million in compensation for damages.

On 10 August 2006, the Shenzhen Court preserved the evidence by copying all of the documents from the computers belonging to both of the accused and transferred them onto a portable external drive (hereafter, Disk A).

On 20 August 2007, the Shenzhen Court requested Jiuzhou Forensic Examination Centre of Intellectual Property in Beijing (hereafter, Examination Centre) to perform a forensic examination. The Examination Centre transferred the documents from Disk A onto four smaller disks (hereafter, Disk B), conducted its examination, and submitted its Forensic Examination Reports (Reports No. 117 and No. 118) on December 24, 2007.

On February 25, 2008, the Shenzhen Court opened the trial and allowed a discussion of the reports in court. During the debate, the defence examined both sets of disks and argued that Disk B contained an extra 17 documents (an extra 20 megabytes of additional information) that Disk A did not have when examined during a preliminary hearing on 28August 2006. The defence argued that Disk B was altered and the examiner from the Examination Centre could not provide a reasonable explanation. On 27 February 2008, the plaintiff withdrew the lawsuit from the Shenzhen Court and received permission from the court to abandon the suit on March 6, 2008.

17.2.2 Foxconn Group v. Xiangjun Liu

In June 2006, Foxconn Group filed a separate complaint at the police station in Baoan District in the Shenzhen Municipality, accusing Xiangjun Liu, an employee of Biyadi Company, of invasion of commercial secrets. The police subsequently conducted a criminal investigation.

In November 2007, the police copied the documents from Disk A from the Shenzhen Court onto an external drive (hereafter, Disk C) and asked the Jiuzhou Forensic Examination Centre of Intellectual Property in Beijing for its own forensic

examination (the same Examination Centre that had previously been appointed by the Shenzhen Court). The Examination Centre transferred the documents from Disk C onto Disk D for its examination and submitted its Forensic Examination Reports (Reports No. 124 and No. 125). The Examination Centre alleged that the computer data contained a total of 100 documents belonging to Foxconn Group and, amongst them, 55 were considered to contain commercial secrets with an estimated value of RMB 2.28 million.

On 26 September 2007, the police station forwarded a formal charge to the Baoan District Procuratorate Office. On January 24, 2008, the prosecution brought an official charge against Xiangjun Liu for invasion of commercial secrets based upon digital evidence from the Forensic Examination Reports (Reports No. 124 and No. 125).

On March 31 of 2008, the Baoan District People's Court opened a trial, reached a guilty verdict for Xiangjun Liu and sentenced him to 4 years imprisonment. The Defendant Xiangjun Liu immediately entered an appeal against his conviction.

17.3 Rules of Digital Evidence Applied in Chinese Litigation

17.3.1 Collection Rules of Digital Evidence

Due to its unique nature, the collection and examination of digital evidence requires strict compliance with technical protocols.

One of the unique characteristics of digital evidence is the fact that it can be duplicated—the evidence can be reproduced if the command of "copy" is executed on a computer. In general, under normal working conditions, there should be no discrepancy between a copied version and the original version. The *U.S. Federal Rules of Evidence* (FRE) 1001 defines "writings" and "recordings" as evidence consisting of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostatting, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation. According to FRE 1003, "('Admissibility of duplicates') the preference for original writings or recordings can be excused and other 'secondary' evidence or copies of the contents can be admitted if the absence of the original can be explained or justified."[3]

Duplication of digital evidence, however, presents certain differences from traditional written evidence, suffering from any modification or being subject to fraud, alteration, deletion and damage during its storage, delivery or use in a much more accessible manner. The key element in collecting digital evidence is to ensure that the evidence has not been subject to any alteration or damage. In the ligation process, the use of duplicates must comply with strict procedures and standards,

[3] See Ronald J. Allen, Richard B. Kuhns and Eleanor Swift, *Evidence, Text, Problems, and Cases* (Austin: Aspen Law & Business, 2002), 693. [hereinafter Allen et al., *Evidence*].

ensuring that the duplicated version is exactly the same as the original version. According to FRE 1001 (4): "A duplicate is a counterpart produced …by mechanical or electronic re-recording,… or by other equivalent techniques which accurately reproduces the original." The phrase "Accurately reproduces the original" contains the fundamental requirement in reproducing any digital evidence.

In 2000, the experts from the G8 (Canada, Britain, France, Germany, Italy, Japan, Russia and the U.S.) proposed six principles in governing the collection of digital evidence[4]:

1. All general forensic procedures must be applied;
2. Upon seizing digital evidence, action must be taken to ensure no changes have been made to the evidence;
3. If a person requires access to the evidence, the person must be trained to handle the evidence;
4. Any seizure, access, storage, or transfer of digital evidence must be fully documented;
5. Any person possessing digital evidence must be responsible for all the actions relating to the handling of it; and
6. Any agency responsible for seizure, access, storage or transfer of digital evidence must fully comply with these principles.

In 2005, China's Ministry of Public Security issued its *Regulations on Examination of Computer Crime Scenes and Digital Evidence* (hereafter, *Examining Regulations*). The *Examining Regulations* specify similar principles as operational protocols governing the collection and examination of digital evidence.

The *Examining Regulations* provide: "the purpose of preserving and sealing digital evidence is to ensure its integrity, authenticity and originality. As evidence, all the storage means, electronic devices and digital data shall be preserved and sealed at the scene for future use."[5] It specifies the method of preserving digital devices and storage means: "(1) The sealing method in use shall ensure that no one shall have an access to the sealed storage means and digital devices unless an unsealing procedure takes place; (2) Photos shall be taken before and after the sealing procedure of the sealed digital and storage devices, and a 'Sealing Log of Digital Evidence' shall be prepared. Photos shall be taken from different angles, displaying the condition before and after the sealing, especially the sealing location and the sealing tag."[6]

Article 14 then states: "Methods of preserving storage devices and electronic/digital data shall include the following: (1) The Integrity Value Method shall measure the integrity value of electronic/digital data and storage devices, and shall record the information in the 'Preservation Log of Digital Evidence.' (2) When storage

[4] Scientific Working Group on Digital Evidence and International Organization on Digital Evidence: Standards and Principles, in Forensic Science Communication, 2000.

[5] Regulations on Examination of Computer Crime Scenes and Digital Evidence, Art. 12.

[6] Ibid. Art. 13.

devices and duplicates are immeasurable by the integrity value or unduplicated, the Sealing Method shall be used and the reasons be explained on the field note or the examination report according to Article 13 mentioned above."[7]

Article 29 also provides: "Duplication or copying of the original storage means shall comply with the following principles: (1) After duplication, reseal the original storage devices. (2) Camera recording shall be used if an examiner performs any critical action, such as unsealing, beginning of duplication, end of duplication, and resealing. (3) After the duplication is complete, a new sealing shall be conducted and a 'Preservation Log of Digital Evidence' should be prepared and all the actions taken shall be recorded according to Article 13."[8]

During the investigation process of two example cases, however, the examiners did not comply with the regulations discussed above, making the following serious mistakes in retrieving and handling the digital evidence:

1. What the police station in the Baoan District sealed and retrieved was not the original data, nor did the duplicated data reflect the original. According to Article 12 in the *Examining Regulations* all the storage, electronic devices and digital evidence must be preserved and sealed at the scene for future use as evidence. In the case under discussion, the Shenzhen Court copied the original documents and produced only the duplicated Disk A. However, the Shenzhen Court did not preserve or seal the duplicate and therefore failed to comply with the requirement set by Article 13 of the *Examining Regulations*, that states that when storage devices and duplicates are immeasurable by the integrity value, the Sealing Method shall be used, indicating the reasons on the field note or examination report. In fact, the police station in the Baoan District only copied the digital data from Disk A onto an external drive (Disk C), without any measures of ensuring "integrity, authenticity, and originality". From a stricter technical approach, before duplicating a computer hard-drive, technical measures should have been taken to remove any information left on the storage device to ensure it is in zero-contaminating condition. Along the same line, instead of some common copying methods, a RAID mirroring technology should have been used (from the Disk A to Disk C). Without this mirroring technology, a duplicate via a Windows system may produce discrepancies, such as a change of data sector and an increase or decrease of supplementary information.
2. The police station in the Baoan District did not comply with the requirements set by the *Examining Regulations*. Firstly, Article 13 (2) provides that before and after sealing Disk C, "photos shall be taken and a Sealing Log of Digital Evidence prepared". In addition, "photos shall be taken from different angles, displaying the condition before and after the sealing, especially the sealing location and the sealing tag." Secondly, Article 29 provides in particular that camera recording shall be used if an examiner performs any unsealing, beginning of duplication, end of duplication, and resealing.

[7] Ibid. Art. 14.

[8] Ibid. Art. 29.

3. When sealing Disk C, the Baoan District police did not comply with Article 14 on the requirement of the "Integrity Value." The investigation team simply copied the digital information (allegedly involved in the commission of a crime) from Disk A (an external drive) onto Disk C (an external drive) without measuring the integrity value. The police should have verified whether the duplicated data was identical to the original data using special verification software and recorded the results in the Preservation Log of Digital Evidence. In fact, the police did not measure "the integrity value of the digital data and storage device", nor provided "any reasons on the field note or the examination report". Thus, there was no measure taken by the police in this case to ensure that the digital evidence was not altered.

In summary, during the retrieving and examination process, the investigators in the case did not strictly follow the requirements of preserving and sealing digital data set forth by the *Examining Regulations*. As a consequence, the integrity, authenticity, and originality of the digital evidence obtained in the case were not guaranteed and its capacity to act as proof as legal evidence was fundamentally jeopardized, giving rise to an appeal.

17.3.2 Examination Rules for Digital Evidence

In litigation, an examination requires a scientific approach to evidence investigation. A forensic examination refers to the process where an examiner employs scientific technology or special knowledge, examines evidence through analysis and judgment, and provides forensic expertise on technical issues related to the litigation.[9] Forensic expert evidence is recognized as scientific evidence and classified as one of the types of evidence in China. An examination develops into forensic evidence when an examiner or expert performs an examination, analysis, makes a judgment, and draws inferences. "Experts can generate evidentiary facts themselves. Such individuals provide basic facts for the fact finder. Experts may present inferences and conclusions to which fact finders may defer."[10]An examination of digital evidence can provide important guidance to the fact-finding process and therefore should be standardized through the use of strict regulations.

In 2005 the Ministry of Public Security in China issued its *Examination Regulations* stating: "[e]xamination of digital evidence in the *Examination Regulations* refers to an examination process of designated sample(s) in which an examiner from a digital evidence examination unit within a public security agency employs special knowledge, equipment and devices, and technology, performs

[9] Decisions on the Issues from Management of Forensic Examination, Article 1, Standing Committee of National People's Congress, 2005.

[10] Allen et al., *Evidence*, supra, note 3, 732–33.

examination, analysis, verification, and judgment, and provides an examination conclusion."[11]

During the examination process of the related cases mentioned above, however, the examiners did not comply with the 2005 *Examination Regulations*. As a consequence, there were many serious mistakes in the Examination Reports issued by the Examination Centre.

Examination Reports No. 124 and No. 125 issued by the Examination Centre were based on an examination of Disk D which was a copy from Disk C which in turn was a copy from Disk A. The duplication process did not comply with the related regulations on preserving and sealing storage means on the scene. Therefore, the integrity, authenticity, and originality of the digital evidence were not ensured at all.

From the transcript of the preliminary hearing on 28 August 2006 at Shenzhen Court, the information belonging to "Xiangjun Liu" in Disk A amounted to 9.62 gigabytes in 7,440 documents (contained in 99 folders); the information belonging to "Shaoqing Si" in Disk A amounted to an additional 3.41 gigabytes in 2,757 documents (contained in 292 folders).

The Baoan District police made Disk C from Disk A at the Shenzhen Court and submitted Disk C to the Examination Centre in Beijing. The Examination Centre in turn made a further copy (Disk D) from Disk C and performed an examination on Disk D. The Examination Report (No. 124), however, indicates that the information belonging to "Xiangjun Liu" is equal to 9.64 gigabytes in 7,455 documents (contained in 99 folders), which contains an extra 0.02 gigabytes and extra 15 documents. According to examination report (No. 125) the information belonging to "Shaoqing Si" is contained in 2,759 documents with an extra two documents. In conclusion, the examination process failed to comply with Article 41 in the *Examination Regulations* that "the examination unit of digital data from a public security agency shall take technical measures and ensure no alteration to any original storage means and electronic devices during a forensic examination."[12]

In addition, Examination Reports No. 117 and No. 118 issued on December 24, 2007 by the Examination Centre dealing with Disk B (a supposed duplicate of Disk A) indicated that Disk B had been altered from the original. According to the trial transcripts on October 25, 2006 by the Shenzhen Court, the court printed out 13 files belonging to "Shaoqing Si" on Disk A. Among the 13 documents with the Foxconn labels and personal signatures, ten files have the name of "Foxconn Material Management Regulations for Product Information and Environmental Management." However, the Examination Report (No. 117) from the Centre did not record these files in Disk B.

The names of the first file (Operational System) and the fourth file (Foxconn Product Environment Quality) were not identical to the names of the first file (Operational System) and the fourth file (Environmental Quality of Foxconn

[11] Regulations on Examination of Computer Crime Scenes and Digital Evidence. Art. 2.

[12] Regulations on Examination of Computer Crime Scenes and Digital Evidence. Art. 41.

Products) in Disk B.[13] According to the trial transcript on Disk A, on a second review on October 25, 2006 by the Shenzhen Court, the court located 24 documents that revealed suspected invasion of commercial secrets, printed these files, and sealed these documents including the 2nd file named "Operational Procedure for Benchmarking Products" and the 17th file called "Operational Procedure for Recognizing External Purchase of New Products." However, the Examination Report (No. 118) did not contain any reference to these two documents.

In summary, the examinations of Disk B and Disk D by the Examination Centre lost credibility due to the suspicion that it had been tampered with and the Examination Centre has lost its probative force in its reporting, since it has reported unreliable digital evidence.

17.3.3 Rules of Proof of Digital Evidence

A fact-finding process consists of three main components: proof, cross-examination, and ratification.

The proof stage refers to the activities by which a party attempts to prove or disprove *factum probandum* with evidence. The proof includes production and cross-examination.

Production of digital evidence refers to those activities that testify to alleged statements recorded therein. An electronic file is one type of document that may not represent a typical document in a strict sense, yet the *Regulations* on writing documents still apply to it.[14] In several countries, the best evidence rule has been applied to written documents and digital evidence. The best evidence rule creates a preference for the production of originals.[15] In FRE 1001 (3) "an 'original' of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it.…If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is considered an 'original'." The original does not exclude any duplication. However, it must fulfil the requirement that it "reflect[s] the data accurately." In Canada, the *Uniform Electronic Evidence Act 4* states "where the best evidence rule is applicable in respect of an electronic record, it is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored."[16]

---

[13] See Table 3 "Examination Report" (No. 117), 158: "Nonpublic Examination Results of 116 Files from the Plaintiff in the Computer Hard Drive."

[14] Electronic Evidence: Computer-Produced Records in Court Proceedings, Introduction [2], Ken Chasse, Toronto, Ontario, June, 1994.

[15] Allen et al., *Evidence*, supra, note 3, 693.

[16] Canada Uniform Electronic Evidence, Act 4.

The current laws and regulations in China also specify the best evidence rule regarding written documents and digital evidence. For example, the *Judicial Interpretation for the Execution of Criminal Procedural Law* of the Supreme People's Court (*"SPC")* provides: "Documentary evidence by investigation shall be the original document. If it is difficult to provide the original carrier, copies or reproductions may only be provided."[17] The *Specific Provisions on Evidence in Civil Actions of the SPC* ("PECA") provide: "the investigators who investigate upon and collect computer data or audio-visual materials such as sound recordings and visual recordings, etc. shall request the person investigated to provide the original carrier of the relevant data. If it is difficult to provide the original carrier, a reproduction may be provided. In the case of a reproduction, the investigators shall specify the source of the evidence and the process of its making in the investigation notes."[18]

The *Specific Provisions on Evidence in Administrative Actions of SPC* ("PEAA") provide: "Any computer data or audio-visual materials such as sound recordings and visual recordings, etc. provided by a party concerned to the People's Court should meet the following criteria: (1) Submit related original carrier. If it is difficult to submit, a reproduction may be provided; (2) Indicate clearly production method and time, the person in charge, and purpose of reproduction."[19]

17.3.4 Rules of Cross-Examination Relating to Digital Evidence

Cross-examination refers to "The questioning of a witness at a trial or hearing by the party opposed to the parry who called the witness to testify."[20] Because digital evidence can be easily falsified and altered, it is important to have valid cross-examination during the fact-finding process. For instance, the Canadian *Uniform Electronic Evidence Act* provides: "(1) A deponent of an affidavit referred to in Section 7 that has been introduced in evidence may be cross-examined as of right by a party to the proceedings who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced. (2) Any party to the proceedings may, with permission of the court, cross-examine a person referred to in paragraph 5(c)."[21] In China, cross-examination refers to any party concerned or the legal representative designated or appointee who can challenge the evidence

[17] The SPC Judicial Interpretation for the Execution of Criminal Procedural Law (1998) 3 Gazette of the Supreme People's Court of the People's Republic of China 101. Art. 53.

[18] Specific Provisions on Evidence in Civil Actions of the SPC (2002) 1 Gazette of the Supreme People's Court of the People's Republic of China 22 [hereinafter PECA]. Art. 22.

[19] Specific Provisions on Evidence in Administrative Actions of SPC (2002) 4 Gazette of the Supreme People's Court of the People's Republic of China 132 [hereinafter PEAA].Art. 12.

[20] *Black's Law Dictionary,* 7th ed., (West Group, 1999), 383.

[21] Canada Uniform Electronic Evidence Act 8.

presented by the opposing party through inquiry and questioning. The *Criminal Procedural Law* provides: "the testimony of a witness may be used as a basis in deciding a case only after the witness has been questioned and cross-examined in the courtroom by both sides, that is, the public prosecutor and victim as well as the defendant and defenders, and after the testimonies of the witnesses on all sides have been heard and verified."[22] The *Civil Procedural Law* also provides that: "evidence shall be presented in court and cross-examined by the parties concerned."[23] In summary, both criminal and civil trials in China require that digital evidence shall be presented and cross-examined.

17.3.5 Ratification Rules of Digital Evidence

Ratification refers to the process by which judges evaluate evidence in court in terms of its relevance, competence and probative value based on certain regulations and experience.[24] No evidence which includes digital evidence has any predesigned abiding force. Judges must apply logical reasoning and rules of experience to evaluate and verify all the evidence of the case comprehensively, objectively, and justly, weigh and balance the relevance, admissibility and probative value of evidence, and provide explanations for the reasons behind their decisions.[25]

17.3.5.1 Relevancy and Admissibility of Digital Evidence

Both PECA and PEAA clearly exclude the admissibility of the following digital evidence: "evidence that cannot exclude alteration," "evidence that is associated with doubts" or "evidence that cannot match the original file."[26] When one party challenges the probative value of evidence, the other party must asks its producer, witness, and person in charge of the custody of it to identify or authenticate it in court. The Civil Procedural Law provides:

> The People's Court shall verify audio-visual materials and determine after their examination in the light of other evidence in the case whether they can be taken a basis for determining a fact.[27]

---

[22] The Chinese Criminal Procedure Law (1996) 2 Gazette of the Supreme People's Court of the People's Republic of China 39. Art. 47.

[23] Ibid. Art. 66.

[24] See Jiahong He, *Brief Evidential Law* (Beijing: China Renmin University Press, 2007), 185.

[25] See PECA, supra note 18, Art. 64. Also see PEAA, supra note 19, Art. 54.

[26] See PECA, Ibid., Art. 69. Also see PEAA, Ibid. Art. 71.

[27] The Chinese Civil Procedural Law (1991) 2 Gazette of the Supreme People's Court of the People's Republic of China 3. Art. 69.

The relevance of digital evidence includes the requirement of evidence sufficient to support a finding. When presenting evidence, the producer can be identified based on the content of the digital evidence. However, digital evidence does not necessarily share this characteristic. It is relatively difficult to identify the producer of digital evidence without other relevant evidence or computer techniques.

For example, in once instance police in China received a report from a person named Li who alleged that his email account has been stolen and somebody was using his email account to distribute pornography. The police examined the content of several pictures and searched the server's log from the City ISP. The police examination uncovered the IP address, the telephone number and the internet account details. All three accounts were under the name of "Liang." The police also knew that the server of the City ISP, the computer name from which the emails were sent, matched the computer name under "Liang." In addition, Liang did not have an alibi: he was at home online at the time of the alleged crime. He had the opportunity to commit the crime. As a result, the police questioned him, confiscated his computer, issued a warning and fined him 1,500 RMB. Liang contested the police's decision, arguing it may have been done by a hacker and demanding a withdraw of the administrative lawsuit.[28]

This was the first case in China using IP information as evidence at trial. During the trial, the key point was whether the act of distributing the illegal pornography could be verified by the existing digital evidence, which included the IP address, emails, and server's log, together with the statements from both parties and the testimony from witnesses. The Court of first instance concluded that the pornographic emails at the recipient's end were sent from Liang's computer. The IP address, online telephone number, and email account all belonged to Liang. The server's log from the ISP indicated that Liang was using his telephone line for an internet connection. The police later confirmed from examination of Liang's computer that there was no hacking during that period of time of the offence. Based on the IP address of the internet, online account, and password used, the police concluded that the emails were sent by Liang.

However, the case was later challenged by experts. In 2005, Mr. Zeming Yang from the China Academy of High Energy Physics explained the case in detail at an academic conference. He argued that it was not sufficient to just rely on the IP address or "Internet behaviors." The trial court should obtain evidence from the internet, recovery of disks, or disk sectors, and conduct thorough analysis and examination.[29]

---

[28] Jun Deng, Nanjiang Zhao, Qichun Zeng, Jin Yang and Zeming Mao, "A Lost Lawsuit for Internet Users with IP Address as Evidence," *Southern Daily*, May 27, 2003.

[29] See Zeming Yang: *Computer As Evidence and Daily Journal Analysis*, the Annual Reports from China Internet Society and Computer Network and Information Security at the Annual Urgent Meeting of China's Computer and Network Security, 2005.

17.3.5.2 Probative Force of Digital Evidence

"Probative force" denotes the strength to support or negate *factum probandum*.[30] Whether or not digital evidence has probative force relies on the reliability and integrity of the digital records system. Therefore, the *United Nations Commission on International Trade Law Model Law on Electronic Commerce* in 1996 provided useful guidance "as regards the assessment of the evidential weight of a data message, and how the evidential value of data messages should be assessed (e.g. depending on whether they were generated, stored or communicated in a reliable manner, and whether such reliability method of information integrity was maintained, so that the methods or factors to identify the sender can be established)".[31] The probative force of digital evidence depends on the reliability of its generation, storage, delivery, and chain of custody. *Digital Signature Law of PRC* provided a similar regulation, requiring that "to verify the authenticity of digital documents as evidence, the following elements shall be included (1) reliability methods of maintaining generation, storage, and delivery of digital documents; (2) reliability methods of maintaining content integrity, (3) reliability methods of identifying the sender; and (4) other related factors."[32]

The *Uniform Electronic Evidence Act of Canada* clearly provides: "In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed (a) by evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record, and there are no other reasonable grounds to doubt the integrity of the electronic records system; (b) if it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or (c) if it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record."[33]

Chinese scholars have proposed three rules for determining the probative force of digital evidence: (1) The probative force of digital evidence by a public notary service is greater than that of digital evidence without any public notary; (2) The probative force of digital evidence made during regular business activities is greater than that of digital evidence made for a litigious action; (3) The probative force of digital evidence by the adversary party is greatest, followed by digital evidence by a neutral party, and the weakest one made by own party.[34] Mr. Xing Lu added the

[30] Terence Anderson, David Schum and William Twining *Analysis of Evidence*, 2nd ed., (Cambridge/New York: Cambridge University Press, 2005), 44–5.

[31] The United Nations Commission on International Trade Law Model Law on Electronic Commerce: Section 2 of Article 9.

[32] Digital Signature Law of PRC. Art. 8.

[33] Canada Uniform Electronic Evidence. Act 5.

[34] Jiahong He, *Research on Digital Evidence Law* (Beijing: Law Press, 2002), 158.

following three additional rules: (4) Digital evidence with forensic expertise has greater probative force; (5) Digital evidence that has been verified has greater probative force; (6) Digital evidence that has been recognized by a certification agency has greater probative force.[35] Finally, Mr. Ye Li supplemented: "The digital evidence provided by a certification agency has greater probative force than that provided by any party concerned."[36] These rules collectively provide important referential values to judges for evaluating the probative force of digital evidence.

17.4 Future Trends

As the pace of the application of digital evidence in China's litigation increases, more issues with the current legislation governing its application have become exposed to the public. Currently all specific rules and regulations of digital evidence are limited to those found in judicial interpretation by the Supreme People's Court or governmental provisions. In the future, we can expect Chinese uniform provisions of digital evidence.

17.4.1 Trends for Further Standardization of Digital Evidence Collection

While there have been no clear regulations set for collecting digital evidence in China, academics are engaged in active discussion on how to introduce stricter provisions for gathering digital evidence, necessary on account of its unique characteristics. Several American scholars represented by Kevin Mardia propose detailed labels for each carrier during evidence collection, chain of custody for evidence integrity and prevention of potential alteration during collection and maintenance.[37] Chinese scholars suggest the following procedures: (1) Investigation and collection of evidence should consist of two stages: delegation and acceptance of the case, and; examination and identification.

During the first stage, specific requirements should be made known for the delegation of responsibilities to relevant professional units, as well as setting out time frames for acceptance and processing of the case.

During the second stage, examination and identification involves collection and sealing of digital evidence as well as requirements and flow charts for examination

[35] Xin Lu, *Research on Digital Evidence in Civil Proceeding* (Beijing: China University of Political Science and Law Press, 2006), 46.

[36] Hua Li, *Research on Probative Force of Digital Evidence* (Guangzhou: Jinan University Press, 2007), 32.

[37] Kevin Mardia, Chris Prosise and Matt Pepe, *Emergent Responses and Forensic Examination*, trans. Qingqing Wang (Beijing: Qinghua Press, 2004), 167–8.

and analysis. (2) Search warrants shall be presented when searching for evidence and the search procedure shall be prescribed by the scope set out in the warrant. Specific items such as computers, internet servers, terminal storage, and IP addresses shall be clearly identified. (3) After collecting the evidence, the following shall be indicated clearly: source, time, personnel involved, detailed records, the whole process of chain of custody, and information under custody and signatures on the records from two different witnesses. (4) Special attention shall be paid to the individual privacy of the party concerned during the collection and use of digital evidence.[38]

It is absolutely necessary that forensic evidence should be made from the evidential sample according to the appropriate technical procedure and methods. Similar regulations on digital evidence have also been proposed by local municipalities. For instance, the *Collection of Digital Evidence and Examination Protocols by People's Procuratorate of Huangpu District in Shanghai* established a basic system for forensic examination of digital evidence. Because digital evidence has certain characteristics, such as being high-tech, secret, easy to alter, and coming in a variety in forms, the following principles were established: (1) Standardization Principle, involving a flow chart of steps and requirements for a strict procedure; (2) Monitoring Principle, to ensure reliable evidence examination involving video tape recording of the main procedures for collecting digital evidence and having a third party as an independent witness; (3) Safety Principle, using stable and reliable equipment for non-destructive examination ensuring no damage to the original source file (it is necessary to use the Hash value to ensure the identification between an original file and a duplicated file) which must be sealed, with only a duplicated file being used for analysis and recovery, and; (4) Confidentiality Principle, whereby it is necessary for any operating personnel involved to maintain the privacy of personal information and case details, following related confidentiality requirements.[39]

17.4.2 Trends for a System on Provisions of Digital Evidence

To date there is no uniform law of evidence in China. Regulations on digital evidence come from five uncoordinated sources: related laws, judicial interpretations, agency regulations, related international regulations, and other standard official documents.[40] Justice Deyong Shen of the China People's Supreme Court once stated that: "The articles of many laws, regulations and judicial interpretations are inconsistent, and do not operate in a harmonized manner. To some extent, that situation creates

[38] See Feng Gao: *Prosecutorial Organization's Forensic Examination of Electronic Evidence* at: http://www.procedurallaw.cn/zjfx/zdwz/200905/t20090508_216810.html [08.05.2009].

[39] Ibid.

[40] See Jiahong He and Weiping Zhang, *Brief Evidential Law* (Beijing: Renmin University of China Press, 2007), 8–12.

confusion in the application of evidentiary rules in the trial. For instance, some insufficient laws are being used to guide the application of electronic evidence, etc. The reformation and improvement of the evidence system has become an important and urgent task for current Chinese judicial reform."[41]

Since 2001, China's academic community has engaged in some lively discussions on improving evidential legislation and scholars have proposed several different "Expert Proposals on Evidence".[42] In August 2006, with the support of the China Supreme Court's research office, the Institute of Evidence Law and Forensic Science of the China University of Political Science and Law undertook the task of drafting the *Uniform Provisions of Evidence of the People's Court: A Proposal for Judicial Interpretations*[43] (hereafter, the *Proposal*). The draft was completed in September 2007 and currently is being tested as part of a pilot program in seven local courts.

The *Proposal* provides systematic regulation of digital evidence based on case experiences from Chinese judges and foreign regulations on digital evidence.

First, as to Forms of Electronic Evidence, the *Proposal* provides: "Audio-video and electronic evidence shall have explanatory labels indicating the name of the author or collector and the time, place and process of the creation or collection… Electronic evidence shall have written explanations describing the handling and reproduction process, noting the time and place of the handling and reproduction, the form, category, file type as well as the handler, possessor and custodian who handles and reproduces the electronic data."[44]

Second, in regard to exhibition of electronic evidence, the *Proposal* provides: "Electronic evidence shall be exhibited in a recognizable means such as monitor, printout or word descriptions with a clear subject matter to be tested. When audio/video or electronic evidence involves business secrets and personal privacy, exhibition shall be conducted in a setting not open to the public."[45]

Third, in terms of the content of digital evidence in a cross-examination, the *Chinese Procedural Law* does provide certain regulations that can be applied to digital evidence, yet the regulations are vague on what content shall be debated. Cross-examination on digital evidence shall focus on the congruence between the reproduction and the original document. The *Uniform Digital Evidence Law of*

---

[41] See Chief Justice Xiao Yang, China Intensifies Its Efforts for the Reformation of Evidential System (May 30, 2006) in Xiao Yang, *The Central People's Government of the People's Republic of China*, at http://big5.gov.cn/gate/big5/www.gov.cn/jrzg/2006-05/30/content_295901.htm [28.05.2009].

[42] See e.g. Yuqiang Bi, etc.: *Draft for China Evidential Law with Suggestions and Argumentations*, 2004; Guangzhong Chen: *Expert Draft for PRC Evidential Law (Articles, Interpretations, & Argumentations)*, 2004; Wei Jiang: *China Evidential Law Draft (Proposal) & Legislative Reasoning*, 2004.

[43] See Baosheng Zhang, *Uniform Provisions of Evidence of the People's Court: Proposal for Judicial Interpretations and Drafting Commentary* (Beijing: China University of Political Science and Law Press, 2008). [hereinafter Zhang: Uniform Provisions of Evidence].

[44] Zhang: *Uniform Provisions of Evidence*, supra note 43. Art. 20.

[45] Ibid., Art. 92(2).

Canada provides: "This Act does not modify any common law or statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence."[46] This Canadian regulation points out that authentication and best evidence are the main focus of a cross examination on digital evidence. Therefore, the *Proposal* also provides clear regulations on authentication and best evidence for digital evidence, stating that "When electronic evidence and demonstrative evidence is exhibited but before being admitted into the court, if the opposing party objects, the proponent of the evidence shall introduce the producer, the collector and/or the custodian of the evidence to testify in court in order to confirm the identification and authentication of the evidence."[47] The precondition here lies in the objection of the opposing party which constitutes an important measure for a cross-examination requiring identification and authentication. Through identifying the sources and the chain of custody of the digital evidence, producers, handlers and custodians are able to ensure if a document is an original one, if the identification between the duplicated and original documents can be proved, if the new file still possesses original features, and if any alteration and changes have been attempted.

The *Proposal* states the authenticity of electronic evidence: "when the opposing party has raised an objection, it shall be identified and authenticated by its producers, witnesses, custodians and other persons who have the knowledge of the process of producing and custody of such evidence. The contents of identification and authentication of electronic evidence include, but are not limited to, the following elements: (1) Reliability of the methods for producing, saving, delivering and storage; (2) Environmental elements and agreements related to its producing, saving, delivering and storage; (3) Properties and characteristics of the electronic files; (4) Persons that may enter the information exchange system and their level of familiarity with the system; (5) For electronic evidence with a password, digital signature and account name and number, the password, digital signature, person who sets up the account, user and owner of the account and the use of the name or account; (6) De-encryption in the transmission; (7) Whether the system hardware is sound, whether the software is reliable, whether the system operates normally, whether it has been infected by a virus, whether it is possible that the stored data has been changed or altered; and (8) Whether the method of reproduction reflects the contents of the original accurately and completely."[48]

Fourth, with regard to ratification and admission of duplicates, Article 169 in the *Proposal* states: "If the other party in the lawsuit does not object, or although an objection has been raised, the identification and authentication of the evidence can be determined and proved, or when there is no sufficient opposing evidence to disprove such evidence, adjudicators may admit the following types of evidence presented by one party: (1) Photocopies, photographs, duplicates or excerpts that have

[46] Canada Uniform Electronic Evidence, Section One of Art. 2.

[47] Zhang: *Uniform Provisions of Evidence*, supra note 43, Art. 94.

[48] Ibid. Art. 100.

been verified to be identical to the original document evidence; (2) Duplicates, photographs, records or demonstrative evidence that have been verified to be identical to the original document; (3) Duplicates that have been verified to be identical to the audio/video and electronic evidence."[49] Chinese scholars further emphasize the identification and authentication of digital evidence. Great attention shall be paid to the accurate results of the duplication and the systems of digital evidence for identification and authentication. "When one party in the lawsuit does have objections to the authentication of a fact or its related document, the proponent of the evidence shall present to court the time logs, online records, recipient's phone number, IP cards or the information of the computer in use, its operational information, disks, decoded files, and related CDs/DVDs. Related witnesses shall also be summoned to court."[50] The new development of electronic information technology, especially in the area of e-commerce has raised some unique issues to identification and authentication of digital evidence. For instance, "for digital evidence with encrypted files, accounts with digital signatures, or regular accounts, the party concerned or public prosecution agencies shall present and prove the identity of the person who sets up the account, who uses it, or any related persons in relation to the encryption, digital signature, and account, as well as any information related to the account or the name associated with the account. If necessary, the court shall consider the consequence of revealing the code to the public during a trial as digital evidence and may rely upon indirect evidence to prove the identity of the person who sets up the account, who uses it, or any related persons in relation to the encryption, digital signature, and account, as well as any information related to the account or the name associated with the account."[51]

Fifth, in terms of the greater role of the expert witness for digital evidence during a cross-examination, the *Proposal* specifies that: "Parties to a lawsuit may invite persons with specialized knowledge as an expert witness who—with permission of the People's Court—will appear in court to express opinions on specialized issues."[52] In any litigation related to digital evidence, if the attorney does not have relevant knowledge such as a scientist or an engineer should have, he can invite experts in the area to assist his duties, for example, to provide explanations of the digital evidence or forensic expertise presented to court, to question the examiner of digital evidence from the opposing party and cross-examine the forensic expertise, or to rebut the expert evidence from the opposing party, to answer questions from the judge or the party concerned with the purpose of advising any questions related to unique issues or specialized knowledge from digital evidence.

---

[49] Ibid. Art. 169.

[50] Wei Tang, *Evidential Law in Civil Proceeding*, Article 210, Expert Proposal.

[51] Wei Jiang, *China Evidence Law Draft (Proposal) & Legislative Reasoning* (Beijing: Renmin University of China Press, 2004), 542.

[52] Zhang: *Uniform Provisions of Evidence*, supra note 43, Art. 107.

17.4.3 Our Thinking on the Admissibility of Digital Evidence

Digital evidence is one type of scientific evidence available to litigators. Questions remain whether the admissibility of digital evidence should be founded upon the reliability of scientific principles and methodology, or the reliability from inference based on scientific principles and methods. In the *Daubert* case, the Court said that in determining admissibility of expert testimony the "focus, of course, must be solely on principles and methodology, not on the conclusions that they generate".[53] In other words, even if an expert applies a reliable methodology, the expert can still draw an inference that may ultimately fail in a test. If this is true, what is the significance that can be placed on the reliability of scientific principles and methodology? In judging the reliability of digital evidence, in addition to the reliability of scientific principles, should we put more emphasis on the reliability of scientific inference?[54] While the admissibility standard of scientific evidence shall be applied to admission of digital evidence, how does the admissibility standard of general evidence relate to the admission of digital evidence?

Although the admissibility of scientific evidence can be improved on a continuous basis, judges are laypersons to science and less experienced to evaluate the suitability of scientific principles and methodology. In essence, judges, as legal experts, can skilfully apply the general admissibility standards giving weight to the admission principles of scientific evidence.

There are two limitations to the admissibility of duplicates in the *U.S. FRE* 1003 states: "A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original."[55] In the *Bryant v. State* case, the defendant was accused of child abuse and the only evidence in the case was a piece of digital image that had been edited and enlarged by the prosecution for the trail. The appellant court held that "only if the proponent can ensure a fair and accurate duplication of the fact to be proved and reflect the truth of the incident, can the duplicates be admitted as evidence."[56]

Chinese scholars generally agree that the general rules of traditional evidence in the law shall also be applied to the collection and proof of scientific evidence. It is fair to delegate discretion to judges in determining if the admission of scientific evidence exceeds its proved value in substance, or if the admission is consistent with the requirement of a fair trial. For example, it is a legal issue to obtain delegation and permission from agencies or parties concerned in collecting digital evidence. In criminal proceedings, the police must follow the law in conducting a

[53] Allen et al., *Evidence*, supra, note 3, 753–4.

[54] See Baosheng Zhang, *Evidence* (Beijing: China University of Political Science and Law Press, 2009), 228–9.

[55] FRE 1003. ADMISSIBILITY OF DUPLICATES.

[56] Bryant v. State, 810 So. 2d 532 (Fla. Dist. Ct. App). [2002].

search, placing the evidence in custody, or making online interception with approvals from agencies of authority and without any invasion of citizen's rights.[57] In civil proceedings, any party shall obtain permission from the owner or the custodian of evidence and then collect related digital evidence.

In conclusion, in order to provide for greater application of digital evidence in fact-finding, the following considerations are important: stricter technical protocols and standards should be written into the law in China; general rules in the law of evidence should not be ignored but applied to digital evidence with the emphasis upon uniqueness and technicality of digital evidence; and the judge's discretion carries very great weight.

[57] Yinghui Song, "Issues Related to Legislative Improvement of Search and Taking Custody of Digital Evidence," in *Evidential Forum* 7 (2004).