Study on Supervision of Integrity of Chain of Custody in Computer Forensics*

Yi Wang

East China University of Political Science and Law,
Department of Information Science and Technology,
Shanghai, P.R. China, 201620
wangyi@ecupl.edu.cn

Abstract. Electronic evidence becomes more and more popular in case handling. In order to maintain its original effect and be accepted by court, its integrity has to be supervised by judges. This paper studies on how to reduce the burden of judges' task to determine the integrity of chain of custody, even there is no technique experts on the spot.

Keywords: Electronic evidence, chain of custody, computer forensics.

1 Introduction

Nowadays, electronic evidence becomes more and more popular in cases handling. Sometimes it is even unique and only evidence. However, current Laws are not suitable enough to treat this kind of cases. Academia and practitioners are devoted themselves to facing the challenges. Besides, experts in field of information science and technology are also engaged in solving these problems, since it is complicated and referring to cross field research.

In technical field, several typical models for computer forensics had been proposed since last century. They are Basic Process Model, Incident Response Process Model, [1] Law Enforcement Process Model, an Abstract Process Model, the Integrated Digital Investigation Model and Enhanced Forensics Model, etc. Chinese scholars also put forward their achievements, such as Requirement Based Forensics model, Multi-Dimension Forensics Model, and Layer Forensics Model. Above researches are concentrated on regular technique operations during forensic process. [2] Some of the models are designed for specific environment, and can not be popularized to other situations.

In legislation, there are debates on many questions, such as classification of electronic evidence, rules of evidence, the effect of electronic evidence, etc. They try to establish a framework, guide lines or criterions to regular and direct operations and process.[3] However, since there are so many uncertain things need to be clarified, it

* This paper is supported by Innovation Program of Shanghai Municipal Education Commission, project number: 10YS152, and Program of National Social Science Fund, project number: 06BFX051, and Key Subject of Shanghai Education Commission (fifth) Forensic Project, project number J51102.

X. Lai et al. (Eds.): E-Forensics 2010, LNICST 56, pp. 200–206, 2011.

needs time to solve them one by one. It has been widely accepted that current laws lag behind the technology development, and need to be modified or appended to adapt new circumstances. But innovation can't be finished in one day.

One of the main reasons on slowness of current law innovation is lack of seamless integration between legislation and computer science field. Lawyers are not familiar with computer science and technology, when it comes to technique area, they can not write or discuss deeply. On the opposite, the computer experts are facing the same problem, when it comes to law, they are laymen. Therefore, when standing on the border of the two fields, there is no enough guidance telling you what to do next, and there is no explicit rules directing you how to operate exactly. Judges and forensic officers sustain heavy burden when they facing cases dealing with electronic evidences, on one hand they have no enough guidelines, and on the other hand, they have to push cases forward.

This paper first considers how to divding duty clearly between legislation and computer science. That is to say which areas are concerned by law, and which ones are left for technique. It is the base of further discussion. Then let things go ahead naturally.

2 Analysis of Forensic Process

In computer forensic, many forensic models are suggested to regular forensic process, which is related to a lot of technical tasks. The models considered more on technique problems. In order to apply these models properly, it is necessary to have forensic officers with strong technical background. On the other hand, from the lawyers' point of view, this is a legal process and should follow the legal program and must within certain restraints. Considering technique experts' and legislation experts' viewpoint, there is no discrepancy between them. Forensic process can be divided into different stages. Technical experts are focusing on how to divide the whole process reasonably and make each stage clearly and easy to manage. Some models introduce the thinking of software engineer into them.

Judges concerns more on whether the forensic process is performed under the legal disciplines, whether captured evidences are maintained their integrity attribute, and whether these evidences are relative with the case. Therefore, judges don't need to be proficient in every detail of forensic process, but they can supervise the chain of custody if necessary.

So regardless which forensic model is used, when chain of custody is checked, there should be enough data to prove whether the integrity is held or not. Of course the supervision needs technique support. But it doesn't mean if there is no technical expert on the spot, the supervision task can't be executed. Besides the technical details, other aspects should be censored in a standardized way, and after that, judges can draw the conclusion whether the integrity attribute is maintained. If they need to clarify some technical problems, they could decide whether it is necessary to ask technical experts for help.

Therefore, the boundary of technique and law is clear, that is the data offered during the supervision and the standardized way of supervision. As there is no unified forensic model, the data given should not be fixed tightly. In the following, we call

these give data as interface data. According to technical doctrine of equivalents, the interface data can't incline to certain technique. And the standardized supervision is also principle, not specific for any technique or model(s).

3 Interface Data and Supervision

From above analysis, the core of the problem is how to supply interface data and how to design a standardized supervision way. In order not to be lost in detail, we first divide forensic process into five phases. They are preparation, evidence capture and collection, evidence analysis, evidence depository, and evidence submission. In some models, the stage division is different, but it is not the point. Here logic order is important. Once the logic order is right, a step belongs to previous phase or next phase is not critical.

Through discuss the inner relationship between different steps and stages, this paper gives a logic order table, which declares that forensic progress has to comply certain programs in order to guarantee the integrity of whole chain of custody, and during the programs, interface data can be determined, which is the important information for supervision.

3.1 Interface Data

According to the five stages mentioned above, let's discuss them one by one.

1. Preparation
In this phase, the main task includes selecting qualified people or training people to satisfy computer forensic tasks, acquiring legal permission for investigation and evidence collection, planning how to execute forensics in detail, such as background information collection, environment analysis, and arrangement, etc.

2. Evidence Capture and Collection
This stage is engaged in evidence fixing, capture and collection. The evidences include physical evidences and digital evidences. The former can use traditional evidences capture technique, and the latter need computer forensic technique to get stationary and dynamic electronic evidences. Then the collected evidences need to be fixed, and electronic evidences need to calculate digital signature to avoid original data is tampered.

3. Evidence Analysis
It is based on former phase. Evidences captured on second phase are analyzed in this stage. The main tasks are finding out useful and hidden evidences from amount of physical materials and digital data. Through IT technology and other traditional evidence analyzing technique, extract and make up evidences.

4. Evidence Depository
When evidences are collected in second phase, and up to they are submitted in court, during this period of time, the evidences should be put in a secure and good environment. It can guarantee that they will not be destroyed, tampered and become invalid. Evidences stored here are managed well.

5. Evidence Submission

In this phase, evidences collected and analyzed from above phase will be demonstrated and cross examined in court. Besides necessary reports written on evidences analysis phase, evidences should be submitted follow certain format required by law. When it comes to electronic evidences, the data which guarantee the integrity of chain of custody are also need to submit.

From above analysis, the basic data generated from each phase are clear, and demonstrated in table one.

Table 1. Interface data

Phase Num.	Interface data
Preparation	1. Certificate for proofing person who does forensic tasks is qualified. 2. Legal permission for investigation and evidence collection. 3. Other data if needed by special requirements.
	Comments: Except emergency formulated by law that could obtain legal permission after evidence capture and collection, other cases are not permitted.
Evidence Capture and Collection	1. Investigation and captured evidences are within the legal permission. 2. Traditional evidences capturer and collection follow current law's regulation. They should supply spot records, notes, take photos, and sign signatures etc. 3. For each of electronic evidence, it should calculate digital signature so as to guarantee the originality and integrity. 4. For dynamic data capture, if condition permitted, it should take video to record the whole collection process. Or 2 or more people should on the spot, and record the whole procedure.
	Comments: In this phase, if during executing tasks, accident happens, such as finding out unexpected evidences but without legal permission, criminals take extreme actions to destroy or damage evidences, and other unpredictable things, forensic officers could take measures agilely according to current law.
Evidence Analysis	1. Traditional evidence analysis follows current law. 2. Electronic evidence analysis should be taken by qualified organizations, and they should not be delegated by personal people. 3. During electronic evidence analysis, if condition permit, examination and analysis should be under monitor. If there is no video, there should be a complete report on how examination and analysis are going on, 2 or more people should sign their signature. The report should meet the format requirements needed by law.

Table 1. (*continued*)

Evidence Depository	1. The depository should have proper environment to store electronic evidences. 2. During the storage time, there should have complete record for in and out, and the state of electronic evidence for each time.
Evidence Submission	1. Since electronic evidence cannot be perceived directly from the storage medium, in order to make it clear and easy to understand, necessity transformation should be taken. 2. Interface data generated on above phases relevant to proof the integrity of electronic evidences should be demonstrated in court.

Table one gives an overview of the framework of the interface data, if refine them further, there will be a lot of tables and documents need to standardize and define. This paper doesn't intend to regular every rule in every place, but suggests a boundary between law and computer technology. Once the boundary is clear, two sides can devote them to their work. The details and imperfect field can be remedy gradually.

3.2 Supervision

After realizing whole forensic procedure, judges can make up their mind based on fundamental rules, and don't need sink into technique details. According to the logic order in forensic process, judges are mainly concerned on following aspects.

1. Collected evidences should be within legal permission.
Through check the range of legal permission and its valid date, this one can be determined. Investigating the method of obtaining evidences to make sure evidences are legal. For example, judges can check out whether the forensic officers have certificates to proof they are qualified for computer forensic tasks. Before investigation and evidence collection, whether they have applied legal permission or there is any emergency exceptions.

2. Evidences collected on spot should have complete formality.
Traditional evidence collecting has formed a set of formal programs and regulations. As for electronic evidence, the program and regulation are not perfect, some fields are still blank. During the transition, if it refers technique problems, judges can ask technique experts for help. If it refers legal questions, judges have to follow current law. The difficulty is when current law doesn't formulate the solution, what can judges do? Our suggestion is creation. If the situation is never meet before, then it is mainly based on judges' experience and their comprehensive quality, with the help of technique experts, they give a new solution. If this case handles well, the solution can be the reference for other cases. And later, it is a good reference material for making new legislation.

3. Report from evidence analysis should be standardized and regular.
In this phase, tasks are mainly technical. Qualified organizations are delegated to do the evidence analysis. The interface data in this stage are often report. The person who writes the report should have certificate and be authorized, he or she knows the obligation when issued reports to court. Constrains and supervision are mainly on organization audit and assessor audit. Judges are concerned on whether the organization and assessor follow the regulations.

4. Evidence depository should have complete supervision and management records.
Evidence depository runs through the whole forensic procedure. If there is a link loose, or there is a time period is blank, there is a possibility the evidences lose their integrity. Judges should check the records carefully to make sure that the evidences are not damaged or tampered. If there is technique questions, judges can ask technique experts for help.

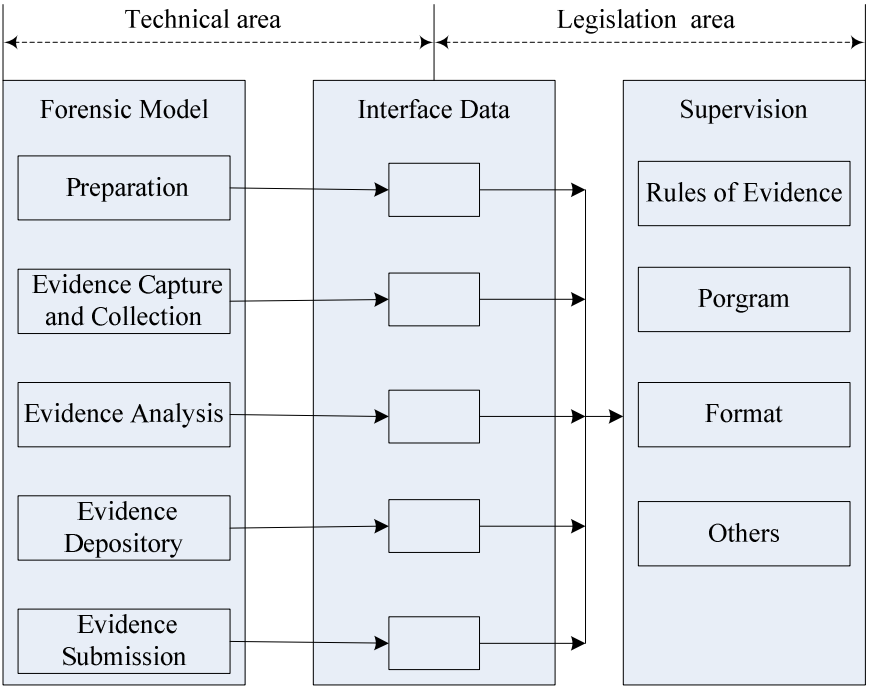

Fig. 1. Border of Technique and Legislation

5. Evidence submission should link above phase and factors together to obtain a chain of custody.
In this phase, valid evidences are displayed in court. Besides the evidences themselves, the chain of custody maintains integrity is also very important. Therefore, two aspects

are concerned in this stage, evidences and proof of integrity of evidences. Lawyers have the duty to arrange these evidences and their relevant proof materials, and let judges to determine the result.

Let's summarize the supervision procedure briefly: first legality examination, next normative examination, then standardization examination, finally integrity overview and check. Figure 1 displays the relationship between technique and legislation, which indicates that the cross field locates on interface data. If two sides define interface data clearly and can operate easily, the problem will be almost solved.

4 Conclusions

Nowadays more and more cases referring to electronic evidences appear. The contradiction between high incidences and inefficient handling gives huge pressure to the society. Both lawful professionals and technique experts are working together to face such challenges. This paper based on previous studies, gives some suggestions on how to reduce the burden of judges' task to determine the integrity of chain of custody to improve the speed of case handling.

References

1. Kruse, W.G., Heiser, J.G.: Computer Forensics: Incident Response Essentials, 1st edn. Pearson Educaiton, London (2003)
2. Baryamureeba, V., Tushabe, F.: The Enhanced Distal Investigation Process Model, http://www.dfrws.org/bios/dayl/Tushabe_EIDIP.pdf
3. Mason, S.: Electronic evidence disclosure, discovery & admissibility, LexisNexis Butterworths (2007)
4. Qi, M., Wang, Y., Xu, R.: Fighting cybercrime: legislation in China. Int. J. Electronic Security and Digital Forensics 2(2), 219–227 (2009)
5. Robbins, J.: An Explanation of Computer Forensics, http://computerforensics.net/forensics.htm
6. See Amendments To Uniform Commercial Code Article 2, by The American Law Institute and the National Conference Of Commissioners On Uniform State Laws (February 19, 2004)
7. Farmer, D., Venema, W.: Computer Forensics Analysis Class Handouts (1999), http://www.fish.com/forensics/class.html
8. Mandia, K., Prosise, C.: Incident Response. Osborne/McGraw-Hill (2001)
9. Robbins J. An Explanation of Computer Forensics [EB/OL], http://computerforensics.net/forensics.htm
10. Gahtan, A.M.: Electronic Evidence, pp. 157–167. The Thomson Professional Publishing (1999)