A Framework to Analyze the Relevancy of Electronic Evidence

Zhi-Jun LIU\textsuperscript{1,a,*} and Ning WANG\textsuperscript{2,b}

\textsuperscript{1}Information Technology Department, Hubei University of Police, Wuhan 430034, China
\textsuperscript{2}Hubei Provincial Collaborative Innovation Center for Electronic Data Forensics, Wuhan 430035, China
\textsuperscript{a}seraphtear@163.com, \textsuperscript{b}assemblylp@163.com

*Corresponding author

Keywords: Electronic Evidence, Relevancy of Evidence, digital forensics

Abstract. For electronic evidence, its legal status has been admitted and the electronic evidence as a new form of evidence in law has been specified clearly. Currently relatively little electronic evidence has been adopted in the court because of multiplicity, concealment and fragility of electronic evidence, which is considered by the courts to be of a complexity that is beyond the understanding of general judge and it is usually questionable in the courts because of their relevancy. In this paper, we put forward a framework to analyze the relevancy of electronic evidence, and discussed their analytical methods to guild the judicial practice.

Introduction

The rapid development in computer and network technology has brought forth a tremendous increase in cyber crime. Because electronic evidence can provide a significant link between the perpetrator and the victim, and can prove the motivation and methods used of the suspects. To combat cyber crimes, electronic evidence has played an increasing role, and the role is to provide a clue for solving an involving cyber crime case during the investigation.

In recent years, the types and the quantity of cyber crimes involved are constantly increasing, it appears to trend ascendantly on cybercrime cases. Electronic evidence, as a new kind of proof, is paid close attention to by both the theorists and practical circles. From January 2013, the criminal procedure amendment, civil procedure amendment and administrative procedure amendment in turn came into effect in China, establishing the electronic evidence as an independent category of evidences [1].

The rules of the collection and a small number of adoption of criminal electronic evidence have been built in judicial practice, but currently relatively little electronic evidence has been adopted in the court and the judges usually adopt the transforming evidence of electronic evidence, such as documentary evidence, the defendant confession, testimony of witnesses, etc. In large part because of the multiplicity, concealment and fragility of electronic evidence, it is considered by the court to be of a complexity that is beyond the understanding of the judge.

Whether electronic evidence in a civil or criminal case is admissible depends on the authenticity (integrity, reliability), objectivity and relevancy of electronic evidence [2, 3]. The relevancy checking belongs to the principle of discretionary evidence, and research about this is too little in academia. The rest of this paper is organized as follows. In Section II, the research motivations and backgrounds are discussed. We put forward a generic analytical framework and the corresponding analytical methods to analyze the relevancy of electronic evidence in Section III and IV respectively. The conclusions and future work are covered in Section V.
The Research Motivations and Backgrounds

The issue is raised by introduction into a controversial real case. In a certain month in 2015, the police patrolled and found a few inappropriate posts on the internet. By analyzing the posts reflected the content for the network and tracing back through IP address, the police viewed the managed server IP address and server logs, and found the computer’s IP address. After investigation, this IP address was the computer’s IP address of suspect A, then the police questioned the suspect A and the suspect admitted that he was on the internet at that time. According to the relevant rules of penal clauses on public order administration, the police penalized the suspect A.

The suspect A, as a plaintiff, lodged an appeal against the decision, and then prosecuted the local Public Security Bureau, as the defendant. The plaintiff argued that the IP address was not his computer IP address, and the post was sent by the Trojans because his PC had been infected by the Trojans. The defendant argued that IP address is achieved with the reverse analysis and confessions, and as a senior netizen for many years, the plaintiff has the abilities to safeguard system security. Both sides disputed the case in the court, and the judge was in a dilemma because both explanations were plausible.

In judicial practice, there are many cases like this case. The essence of disputations involves the relevancy judgment of electronic evidence in these cases. In the above given case, the arguments in the court focused on whether the plaintiff used the computer in that time, which involves the relevancy analysis of human and machine. What is the relevancy? The relevancy means the objective connection between the litigation proof and the will-be-proved facts. The relevancy examination indicates the important component, position, and interrelation of a crime.

Compared with the authenticity (integrity, reliability) checking and the objectivity checking of electronic evidence, the relevancy checking belongs to the principle of discretional evidence. The authenticity (integrity, reliability) checking is to prove it has not been modified during evidence-handling process, which can be finished by MD5 or hash algorithm [4]. The exclusionary rules of illegal evidence can be used by the judge for examining the objectivity of electronic evidence. For example, whether the forensics subject is legitimate, or the ways of evidence collection are legitimate, etc.

Currently Forensic sciences technical standards include 4 national standards, 22 industry standards of public safety, 9 standards by the Justice Department, and 8 standards by the Supreme People's Procuratorate in China. Most of them are difficult to fit the relevancy judgment of electronic evidence, and very few standards involve technical standards of the relevancy of electronic evidence, but only in the content relevancy [5]. The absence of the generic analytical framework and the corresponding analytical methods affects the law-officers to use electronic evidence to settle juristic events in judicial practice.

To our knowledge, few research focus on the relevancy of electronic evidence. In this paper, we focus on building a framework to analyze the relevancy of electronic evidence, and discussed their analytical methods to guild the judicial practice.

The Generic Analytical Framework of the Relevancy of Electronic Evidence

The Framework Design

For the traditional crimes, the fact that cases occur or not, time of crimes, places of crimes, and subject of crimes, etc., need to be considered. But for the cyber crimes, it involves the digital forensic, which includes the collecting, obtaining, preservation, analysis and representation of electronic evidence. In the digital forensics justice practice, by obtaining the carriers (digital devices) and analyzing the display content of carriers, the investigators hope to demonstrate that who was involved in the case? What have they done? How have they done? Where have they done? When have they done? Why have they done?
Contrary to the traditional crimes, firstly it is mainly the criminal behaviors of utilizing digital devices and network to implement in the cyber crimes. Secondly the carriers (machine or digital devices) and the display content of carriers have the unity and electronic evidence stores the corresponding digital devices. Thirdly the evidence obtained is electronic evidence, which is volatile and changeable, etc. Lastly Digital evidence may lies in different places of cyber crime scene according to Lockard’s exchange principle. Unlike physical crime scene, the boundaries of a cyber crime scene are not clearly outlined and the crime scene area may extend a room, a city.

For a specific cyber crime case in judicial practice, the judge need to examine whether the operators in virtual space is consistent with the suspects in physical space, whether the suspects has operate the machine (digital devices), whether the source of electronic evidence obtained from multiple digital devices is correct, whether the corresponding electronic evidence content can reveal the cyber crime behavior, as well as the legal requirement for the cyber crime behavior, etc., from the perspective of the relevancy of electronic evidence.

Based on the above analysis, the framework of relevancy of the electronic evidence is put forward, as shown in Figure 1. For a cyber crime, the judge can examine the relevancy of electronic evidence, which includes the relevancy between the “Operators” and “Machine”, the relevancy between the “Machine” and “Digital Data”, the relevancy between the “Digital Data” and “Crime Behavior”.

![Figure 1. The framework of the relevancy of electronic evidence.](image)

**The Issues to be Resolved**

In the relevancy between the “Operators” and “Machine” analysis process, with the reform and perfection of China's legal system, it is not suitable to adopt the self-incrimination of suspect’s signature or oral confession to verify the suspect has used machine (digital devices) to commit crimes, which shows the relationships (or bindings) between the “Operators” and “Machine”. Next, the legal defense, such as SODDI (Some Other Dude Did It) in the computer field, has become more common, the suspects often push their crimes to others, for example, without the content, the computer system downloaded automatically some content or the email was send automatically because the malicious code had been injected into the computer system.

Therefore, the pressing problems facing this process are how to verify the machine has the crime ability, whether the Operator operated the machine, whether the Operators in virtual spaces in consistent with the suspects in physical spaces.
In the relevancy between the “Machine” and “Digital Data” analysis process, digital data may lie in different places of cyber crime scene according to Lockard’s exchange principle, which will store different machines (digital devices). Epistemic uncertainty, an unavoidable attribute, will cause poor choices in selection of evidence origin and channels of collecting digital evidence, which will lead to the incompletion of digital evidence collected. Currently collecting the carriers (digital devices) and analyzing the display content of carriers usually depend on the experience and intuition of the investigators, such as the direct method, the weight method, the level of uncertainty judgment method of Casey[6], etc., which will distort the assessment result.

Therefore, in this process the urgent problems are the relevancy of storage location of electronic evidence, the consistency problem of the carriers and the display content of the carriers, and the relevancy of machine and machine, which reveals that how the digital data flows and how the cyber crime implements.

In the relevancy between the “Digital Data” and “Crime Behavior” analysis process, it is an evidence reasoning process, which tries to find causes (events) that result in existence of a certain digital data used, and draws a conclusion. Currently amount of manual and empirical intervention play an important role, the inference conclusion usually will be called into question in the court. Evidence analysis errors may occur because certain digital evidence can have different events as source. As an example, a single line in a firewall log file showing the opening or closing of a connection, will bring out a set of events which can be considered as causes such as browsing the net using different web browser or opening a TCP connection caused by another application.

Therefore, in this process such problems below should be considered, which include: whether or not digital data content can effectively reveal the crime behavior, whether electronic evidence is relevant to the facts of a case, what are the theoretical foundation and technical means for analyzing the relevance of the data and behavior?

The Analytical Methods of the Relevancy of Electronic Evidence

The Relevancy between the “Operators” and “Machine”

The relevancy between the “Operators” and “Machine” includes the relevancy between the virtual spaces and the physical space, the relevancy between the “Operators” and “Machine”. The former refers to the identity relevancy, which is to verify the consistency of Operators between the virtual spaces and the physical space. The latter refers to the behavior relevancy, which is to verify whether the suspect used machine (digital devices) to commit crimes.

1. Functionality checking
Examine the external environment of electronic evidence and decide whether or not it has the crime ability.
Examine the external environment of electronic evidence and decide whether or not it is infected with viruses and Trojans.
2. Identity relevancy checking
Examine the time and status information of system files and stored digital data, which includes system login logs, computer configuration files, account information, application logs etc.
Combine physical investigation, adopt the inference method, not oral evidence to verify the identify consistence.
3. Behavior relevancy checking
Examine the operation records of files and stored digital data, and their corresponding time information. These files include record files about network activities, memory data, system operation logs, etc.
Build the timeline of operation behaviors sets for verifying whether the suspect used machine (digital devices) to commit crimes at a given point in time.
The Relevancy between the “Machine” and “Digital Data”

The relevancy between the “Machine” and “Digital Data” includes the relevancy between the “Machine” and “Machine”, and the relevancy between the “Machine” and “Digital Data”. The former refers to the carrier relevancy, which is to verify that whether the individual digital device constitutes the implementation process of a crime. The latter refers to the content relevancy, which is to verify whether the different machine (digital devices) stores the corresponding electronic evidence, because each forensic cyber case has its own characteristics and shows the corresponding sets of events that result in existence of digital evidence.

1. IP address relevancy checking
   Examine each machine or digital device has the IP address in a certain cyber crime.
   Examine the source and destination IP address of sessions of digital device, etc., and decide whether or not the digital devices involved are interconnected.

2. Location relevancy checking
   Examine the storage location of files involved in the digital devices, pay particular attention to the original source of deleted files, recovery files in the carriers.
   Examine the location information of single digital device and spatial relationships with other digital devices.

3. Time relevancy checking
   Examine the time information of files involved.
   Build the Events-Timeline graph, Time-Activities table, etc. to analyze the flow of digital data between the digital devices.

4. Content relevancy checking
   According to Locard exchange principle, we can access different digital evidence from many sources. Extract the files content or the display content of the carriers.
   Examine and compare the similarity or consistence of the files content or the display content of the carriers, to analyze the relevancy of related carriers.

The Relevancy between the “Digital Data” and “Crime Behavior”

The relevancy between “Digital Data” and “Crime Behavior” includes the relevancy between the “Digital Data” and the “Case Characteristic”, and the relevancy between the “Legal Features” and “Crime Behavior”. The former refers to the characteristic relevancy, which is to verify that whether the display content of carriers reveal the case characteristic. The latter refers to the law features relevancy, which is to verify whether the case characteristics are line with the legal features.

1. Case characteristic relevancy
   Examine the display content of the carriers and the cause events from one or more digital devices. Different events may result in existence of digital evidence.
   Use induction to extract its case characteristic set. For example, in virus transmission case, case characteristic set includes: transmission subject characteristics, transmission means and ways, the extent of damage, etc.

2. Legal features relevancy
   Examine items of laws and provisions of judicial explanations, and then the crime objective respect, object of crime, crime subjective respect and subject of crime are acquired.
   Establish the relationships between the Legal features and case characteristics, and then build the corresponding mapping table.

Conclusions

The relevancy of electronic evidence is important to decide the litigation proof and the will-be-proved facts, and the technical features of electronic evidence makes it difficult for the rule of relevancy of
electronic evidence. The framework and analysis methods of relevancy of electronic evidence presented in this paper will guide judicial practice, but they are still relatively abstract. As future work and extension to this research, we hope to construct the minimal set of relevancy of electronic evidence of each type of cyber crime and build the corresponding mapping table, and then, develop guidelines or a tool that can serve the judicial practice.

Acknowledgement

This work is supported by Social Public Security of the key research base for Humanities and social science in Hubei Province Universities project (2015-12), Teaching and research project of Hubei University of Police (JYXM2016002), the Project of Humanities and Social Sciences, the Ministry of Education in China (17YJCZH172), the National Social Science Fund Project (12CFX053). The authors would like to thank the computer forensics team of Hubei University of Police for their collaborations and contributions. Finally, the authors would like to thank the anonymous reviewers for their time and valuable suggestions that contributed to the overall quality of this paper.

References


