ATLANTIS PRESS
Advances in Social Science, Education and Humanities Research (ASSEHR), volume 130
2nd International Forum on Management, Education and Information Technology Application (IFMEITA 2017)

A Content Framework to the Relevancy Judgement of Electronic Evidence

Zhi-Jun LIU [1, a], Ning WANG [2,b]

[1] Information Technology Department, Hubei University of Police, Wuhan 430034, China

[2] Hubei Provincial Collaborative Innovation Center for Electronic Data Forensics, Wuhan 430035, China

[a]seraphtear@163.com, [b]assemblylp@163.com

Keywords: Electronic Evidence, Relevancy of Evidence, digital forensics

Abstract. The rapid development in computer and network technology has brought forth a tremendous increase in cyber crime. To combat cyber crimes, electronic evidence can provide a clue, and even be the evidence to prove the case, but currently electronic evidence usually have been questioned in the courts because of their relevancy judgement. In this paper, we put forward a relevancy content framework to analyze the relevancy of electronic evidence, and discussed their analytical methods to guild the judicial practice.

Introduction

To combat cyber crimes, electronic evidence has played an increasing role. Electronic evidence performs two major roles, one of the role is to provide a clue for solving an involving cyber crime case 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. The other is to provide forensic evidence accepted by the court after reorganization, protection, extraction, analysis and archiving process.

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]. Whether electronic evidence in a civil or criminal case is admissible depends on the authenticity, objectivity and relevancy of electronic evidence. The authenticity checking is to prove it has not been modified during evidence-handling process, which can be finished by MD5 or hash algorithm. The exclusionary rules of illegally obtained evidence can be used by the judge for examining the objectivity of electronic evidence[2]. The exclusionary rules of illegally obtained evidence, which include forensic subject legitimation judgment rules, the ways of evidence collection legitimation judgment rules,etc., are invalid and can't be adopted in the court.

The relevancy checking belongs to the principle of discretional evidence, and till now, there are not appropriate scientific methods and rules to judege the relevancy of electronic evidence. One reason is that the academia pay too much attention to the authenticity and objectivity of electronic evidence, the other reason is that multiplicity, concealment and frangibility of electronic evidence will bring about the confusion of judgement of the relavancy 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.

The research about relevancy of electronic evidence is too little in academia. The rest of this paper is organized as follows. In Section II, the research works are discussed. We disccus the reseach content of electronic evidence and present the considerations in Section III. In Section IV a case study is discussed. The conclusions and future work are covered In Section V.

Related Works

Most of the related papers presented many correlation analysis technologies and methods, which included, but are not limited to, applying Bayesian inference, data mining, and attack tree analysis,

semantic web technologies, XML-based approach, etc[3,4]. Some research utilized the Forensics for Rich Events architecuter, OWL and SQWRL to represent and reason the correlation of electronic evidence[5].

Such technologies and methods are reasonable in theory, but frequently encounter practical difficulties in analyzing the correlation of the electronic evidence. One of the major reasons is that the research objects focus on the digital evidence in board sense, which can not apply to the court, and not all digital evidence can act as evidence in court. Electronic evidence in narrow sense is that electronic evidence is shown in electronic form, can prove the material facts of the case. The other reason is that each previously suggested technologies and methods seem to be in trial stage and the prosecutors or police cannot get enough help from stated step in those studies.

From a technical standard perspective, operation guidances or technical standard can affects the law-officers to use electronic evidence to settle juristic events in judicial practice. 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 he Supreme People's Procurator ate in china. But most of Forensic sciences technical standards 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 [6].

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

The Framework of Content

The framework design. The relevancy of evidence is important to decide the litigation proof and the will-be-proved facts. For the crimes, the evidence relevancy involves the relevancy about the human, the event, the thing, the time, the space. That is to say, the investigators or judges 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?

But for a cybercrime, firstly the boundaries of a cyber crime scene are not clearly outlined and the crime scene area may extend a room, a city, and electronic evidence is decentralized and may lies in different places of cyber crime scene. Secondly the electronic evidence attach to the carriers (machine or digital devices), and the electronic data stored is massive and disordered which pieces of digital data are mixed and stacked together over time. Thirdly it is mainly the criminal behaviors of utilizing digital devices and network to implement in the cyber crimes, and electronic evidence can be easily modified, duplicated, restored, or destroyed. That is to say, it is very difficult to prove whether the digital evidence has been changed by human senses.

Based on the above analysis, and in accordance with the process of computer forensics in judicial practice, the content framework of relevancy judgement of the electronic evidence is put forward, as shown in Figure.1.

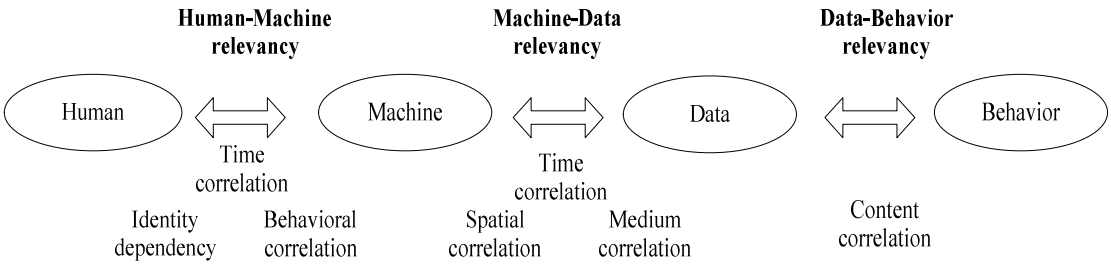

Figure.1. the content framework of the relevancy judgement of electronic evidence

Model definition and structure. In order to explain the content framework more specifically and clearly, we take a specific cyber crime case in judicial practice for example. In the court the judge firstly need to examine whether the operators in virtual space is consistent with the suspects in

physical space, and the suspects has operate the machine (digital devices), then the judge need to examine whether the source of electronic evidence obtained from multiple digital devices is correct. Lastly the judge need to examine whether the corresponding electronic evidence content can reveal the cyber crime behavior, and what is the legal requirement for the cyber crime behavior. Therefore the content framework of the relevancy judgement of electronic evidence can be divided into three periods: Human-Machine relevancy checking, Machine-Data relevancy checking and Data-Behavior relevancy checking.

1.Human-Machine relevancy checking

It includes the identity relevancy ckeching, behavior correlation checking, and the time correlation checking. The identity relevancy ckeching is to verify the consistency of Human between the virtual spaces and the physical space. Behavior correlation checking is to verify whether the Human used machine or digital devices to commit crimes. The time correlation checking is to build the timeline of operation behaviors sets for verifying whether the Human used machine or digital devices to commit crimes at a given point in time.

2.Machine-Data relevancy checking

Firstly the spatial correlation checking is to verify that whether the individual digital device constitutes the implementation process of a crime, one of which is address correlation checking, such as IP address, MAC address, GPS address, the location of Wi-Fi hot spots and cell towers, and files storage locations, the other is time correlation checking, which build the Events-Timeline graph, Time-Activities table, etc. to analyze the flow of digital data between the digital devices. Secondly the medium correlation checking refers to the carriers (machine or digital devices) and the display content of carriers have the unity and electronic evidence stores the corresponding digital devices, which can verify whether the source of electronic evidence obtained from multiple digital devices is correct.

3.Data-Behavior relevancy checking

In this process, it involve the evidence analysis and evidence reasoning, and amount of manual intervention play an import role. 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. Besides, in this process the investigators were used to forming sets of cause events based on their experience and case information.

Therefore, date-behavior relevancy checking includes case characteristic relevancy checking and legal features relevancy checking. Firstly, it need to examine 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? Secondly the crime objective respect, object of crime, crime subjective respect and subject of crime should be in compliance with the items of laws and provisions of judicial explanations.

Case Study

In a certain month in 2015, a lady received an anonymous email, which asked her for immediate remittance of RMB 50,000, otherwise the lady's privacy information would be publicized on the internet. The lady choose to call the police after she thought carefully. The police extracted the email information and parsed the contents of the log file. By tracing back through IP address, the police viewed the managed server IP address and server logs, found fortunately the suspect's computer IP address, and then seized the suspect's laptop computer and other digital devices.

In need of the investigation of the case, the police sought the computer forensics team of Hubei University of Police for technical assistance and evidence analysis. During Human-Machine relevancy checking phase, firstly by an analysis of the content information of account information, computer configuration files, system login logs, application logs, interlinking information,ect, to determine the user identity of suspect's laptop computer. Secondly analyze the system operation logs,

network activities(record files) and memory data,etc., to determine the user behavior. Lastly extract the time information of the corresponding files, such as record time(suspect's laptop computer system), record time(application software logs), record time(files and other stored digital data), etc,. and then, collate them all together into one timeline, which be used to verify whether the suspect used the laptop computer to commit crimes at a given point in time.

In spatial correlation checking, analyze the IP address and MAC address of the suspect's laptop computer from the network configutation files, network activities record files, etc., and analyze IP address information of the transit server by examining the from and to address of email, and analyze the email address information of the victime and IP adrress of victime's computer, which be used to show data flow and detemine the network topology of criminal process.

To simplify this example, the following is the relevancy checking and analytical methods of electronic evidence, as shown in Figure.2.

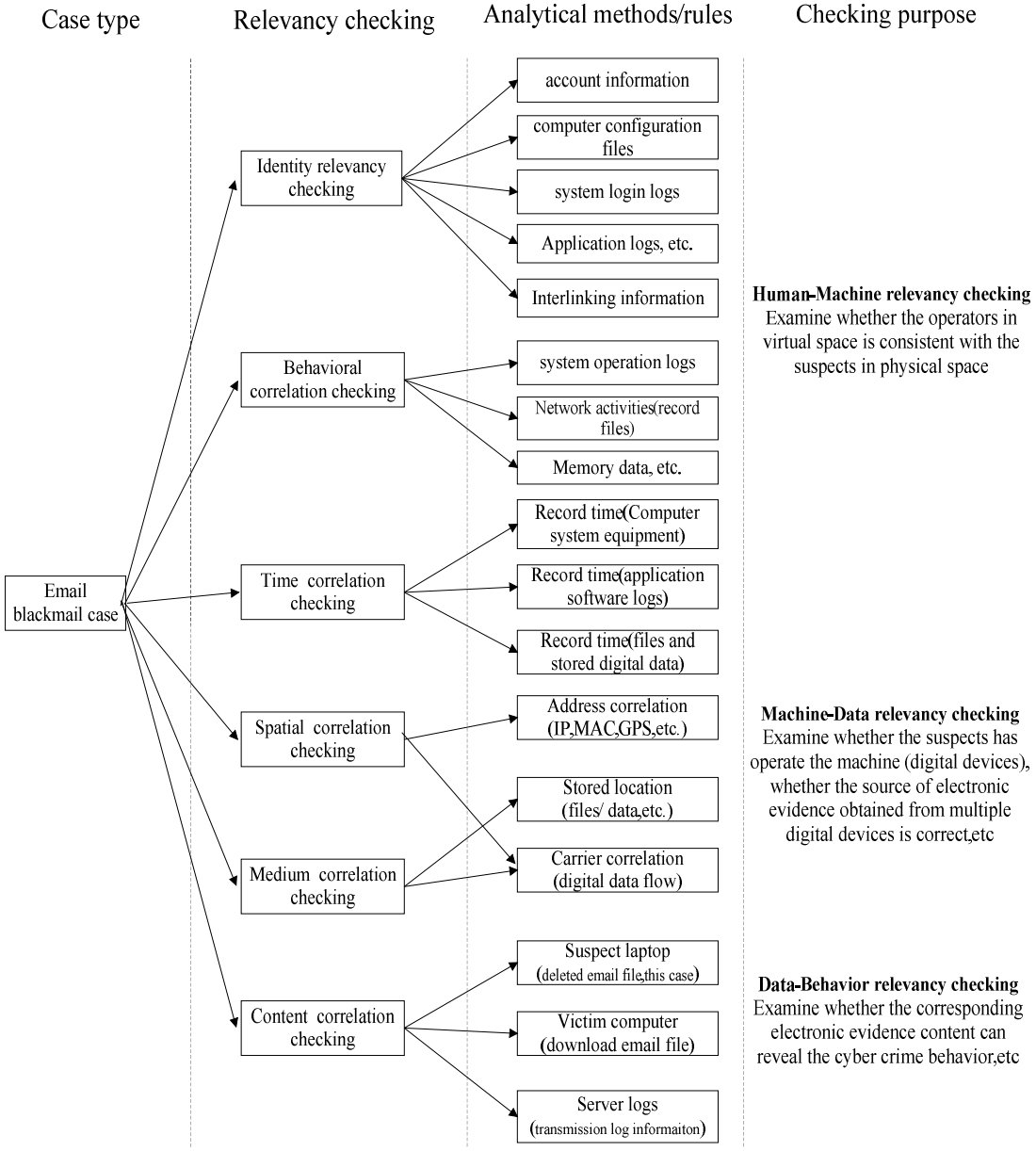

Figure.2. the relevancy checking and analytical methods of electronic evidence

Conclusions

The absence of the generic content framework of the relevancy of electronic evidence and the corresponding analytical methods affects the law-officers to use electronic evidence to settle juristic

events in judicial practice. In this paper we discuss the content framework and analytical methods, 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.

Acknowledgements

This work is supported by Science and Technology research project of Hubei Provincial Department of Education(D20174201), Teaching research project of Hubei University of Police (JYXM2016002). 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

[1] Ning Wang, A Knowledge Model of Digital Evidence Review Elements Based on Ontology. International Journal of Digital Crime and Forensics. Volume 9, Issue 3, 2017, pp. 49-57.

[2]Yang Xinlin, Analyzing the Proof Qualifications and Validity of Proof of Electronic Evidences, Journal of knowledge economy, vol. 11, 2015, pp .76-78.

[3]S. L. Garfinkel, "Automating disk forensic processing with sleuthkit, xml and python," in Systematic Approaches to Digital Forensic Engineering, 2009. SADFE'09. Fourth International IEEE Workshop on IEEE, 2009, pp .73–84.

[4] G. Giova, Improving chain of custody in forensic investigation of electronic digital systems, International Journal of Computer Science and Network Security, vol. 11, no. 1, 2011, pp.1–9.

[5]Flora Amato, Giovanni Cozzolino, Antonino Mazzeo, Nicola Mazzocca, Correlation of Digital evidences in forensic investigation through semantic Technologies, 2017 31st International Conference on Advanced Information Networking and Applications Workshops(WAINA), 2017, pp. 668-673.

[6] Liu Pingxing. The Relevancy of Electronic Evidence .Chinese Journal of Law, No.6, 2016, pp.175-190.