Digital Investigation 10 (2013) 175–192

Contents lists available at SciVerse ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

A new triage model conforming to the needs of selective search and seizure of electronic evidence

Ilyoung Hong [a,b], Hyeon Yu [a,c], Sangjin Lee [a], Kyungho Lee [a,*]

[a] Center for Information Security Technologies (CIST), Korea University, Anam-Dong, Seongbuk-Gu, Seoul 136-713, Republic of Korea
[b] Supreme Prosecutors' Office, Seocho-dong, Seocho-gu, Seoul, Republic of Korea
[c] Korea Police Investigation Academy, Hwykung-dong, Dongdaemun-gu, Seoul, Republic of Korea

ARTICLE INFO

Article history:
Received 30 October 2012
Received in revised form 14 January 2013
Accepted 17 January 2013

Keywords:
Digital forensics
Electronic evidence
Search and seizure
Triage
Privacy

ABSTRACT

Recently, digital evidence has been playing an increasingly important role in criminal cases. The seizure of Hard Disk Drives (HDDs) and creation of images of entire disk drives have become a best practice by law enforcement agencies. In most criminal cases, however, the incriminatory information found on an HDD is only a small portion of the entire HDD and the remaining information is not relevant to the case. For this reason, demands for the regulation of excessive search and seizure of defendants' innocuous information have been increasing and gaining strength. Some courts have even ruled out inadmissible digital evidence gathered from sites where the scope of a warrant has been exceeded, considering it to be a violation of due process. In order to protect the privacy of suspects, a standard should be made restricting excessive search and seizure. There are, however, many difficulties in selectively identifying and collecting digital evidence at a crime scene, and it is not realistic to expect law enforcement officers to search and collect completely only case-relevant evidence. Too much restriction can cause severe problems in investigations and may result in law enforcement authorities missing crucial evidence. Therefore, a model needs to be established that can assess and regulate excessive search and seizure of digital evidence in accordance with a reasonable standard that considers practical limitations.

Consequently, we propose a new approach that balances two conflicting values: human rights protection versus the achievement of effective investigations. In this new approach, a triage model is derived from an assessment of the limiting factors of on-site search and seizure. For the assessment, a survey that provides information about the level of law enforcement, such as the available labor, equipment supply, technical limitations, and time constraints, was conducted using current field officers. A triage model that can meet the legal system's demand for privacy protection and which supports decision making by field officers that can have legal effects was implemented. Since the demands of each legal system and situation of law enforcement vary from country to country, the triage model should be established individually for each legal system. Along with experiment of our proposed approach, this paper presents a new triage model that is designed to meet the recent requirements of the Korean legal system for privacy protection from, specifically, a Korean perspective.

1. Introduction

People use digital media to store tons of information about their daily lives. With the proliferation of digital

* Corresponding author. Tel.: +82 1050025099; fax: +82 2 928 9109.
E-mail addresses: kevinlee@korea.ac.kr, klee@secubase.com (K. Lee).

1742-2876/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.diin.2013.01.003

devices, law enforcement officers are often confronted with crime scenes where incriminatory files coexist with hundreds of thousands of innocuous files. For a very long time, the standard digital forensics procedure has been to seize all the physical media to analyze images acquired from the media. This practice, however, has been criticized because it is thought that a defendant's privacy could be excessively infringed and seizing of all physical media can disrupt corporate business activities. It is the right of a defendant to be secure from indiscreet search and seizure by governmental authorities. Owing to the high risk of privacy infringement and business disruption, restrictions on the search and seizure of digital evidence have been increasingly tightened. The invisible characteristic of digital information, unlike any tangible object, results in law enforcement officers reviewing the contents of files on any digital media during the search and seizure process, inevitably resulting in privacy infringement against defendants. The reality is also that, owing to limitations in terms of labor, technology, and the equipment being utilized during the search and seizure process, strict limitations are imposed to directly select only incriminating data at the crime scene. Therefore, it is regarded as reasonable for the law enforcement officers that excessive restrictions on the search and seizure of digital information could downgrade the efficiency of investigations and may hinder the finding of important evidence. Therefore, a most reasonable method that can balance the two contradicting values—protection of human rights and achievement of an effective investigation—is urgently needed. Up to the present time, few research efforts have dealt with on-site procedures focusing on this problem in the digital forensics field.

Although many triage models have been widely developed to discover timely probative information and utilize it in investigations, most of them simply focus on the necessity to quickly find information to provide investigative leads in a relatively short time (Rogers et al., 2006) or the need for useful intelligence in order to prioritize among the huge amount of digital evidence for backlog reduction (Cantrell et al., 2012; GOMEZ, 2012; Mislan et al., 2010); however, they do not deal with legal requirements such as the demand for privacy protection. Erin et al. (Kenneally and Brown, 2005) dealt with selective search and seizure from the legal perspective. They proposed a risk sensitive digital evidence collection model to collect digital information selectively from live systems, and emphasized the need for selective search and seizure following the 4th Amendment protection. In the same vein, Turner (Turner, 2006) proposed the Digital Evidence Bag (DEB) methodology to effectively manage selectively chosen data by imaging it. Even though these research efforts propose various ideas and techniques, more discussions are needed to help law enforcement officers solve problems they could face at crime scenes during the selective search and seizure process. Decisions made by law enforcement officers at a crime scene include those as to what extent of any data encountered are related with the criminal activity as well as various measures for ruling out irrelevant data. The problem is that if the decisions are deemed unreasonable, the admissibility of the evidence can be denied by the criminal courts. Therefore, objective standards are required to determine whether the decisions are reasonable, and those standards should be established with full understanding of the situation. Standards that lack a holistic consideration of the crime scene are merely meaningless and unrealistic demands.

Hence, we believe that a new approach is needed to establish a triage model using the assessment of on-site search and seizure condition. The result of the assessment could provide valuable information such as the human resources required, technical limitations, expected technical measures, and other useful information. The main contribution of this paper is the establishment of realistic standards for selective search and seizure of digital information by which law enforcement officers can make objective decisions that abide by the legal system's demands for privacy protection when warrants impose limitations on the search and seizure of digital evidence. Thus, anybody who desires to assess the adequacy of the law enforcement officer's decision—conceivably the parties subject to the search and seizure or the judge—can utilize this standard. In addition, the triage model can provide guidelines about the minimum level of competence for law enforcement agencies to satisfy the demand for selective search and seizure.

The remainder of this paper is organized as follows: In Section 2, we present the recent change made to the Korean legal system requiring the use of the selective search and seizure principle for digital information. In Section 3, we deal with the practical difficulties of selective search and seizure and the need for a new approach. In Section 4, we propose a theoretical framework for the new approach. In Section 5, we report on an experiment conducted to show how a new triage model can be established using our proposed framework, we also propose a triage model established based on an assessment of the current Korean law enforcement situation specifically from a Korean perspective. Finally, we conclude this paper in Section 6.

2. Background: legal severity in Korea

The Criminal Procedure Act in Korea (Act No. 10864) was revised on July 18, 2011, and it came into force from January 1, 2012. The amendment includes new requirements for search and seizure of electronic evidence. Prior to this amendment, there was a momentous ruling (2009 MO 1190, decision dated May 26, 2011) that ensures that the target of search and seizure warrants against electronic information is the electronic information itself instead of the actual storage media containing the digital evidence. The court stated that, "Relevant electronic information pertaining to the suspicion on which the issue of the search and seizure warrant is based should be obtained in the manner of collecting the printed documents or duplicating the files to a storage medium carried by a law enforcement officer on the crime scene. When it is not possible, however, for the aforementioned method to be applied, by way of exception, transferring the original electronic media or corresponding image files of the media to an off-site law enforcement office can be admitted, and the process taken at the off-site law enforcement office such as collecting the