Chapter 13
A Cyber Crime Investigation Model Based on Case Characteristics

Zhi Jun Liu
Hubei University of Police, Hubei, China

ABSTRACT

In the early stages of the digital investigation of cyber crime, digital evidence is inadequate, decentralized and fragmented. Cyber crime investigation model based on case characteristics is presented in this paper, to help determine investigation orientation and reduce investigation area. Firstly, purifying and filtering the digital evidence collected, classification and acquirement of event sets are accomplished. Secondly, a method of imperfect induction is applied to analyze the event sets and construct one or more premises, and combining with the case characteristics extracted from the legal requirements, inference and its reliability are given. Finally, through a case analysis of network pyramid sales, the initial practice shows the model is feasible and has a consulting value with cyber crime investigation.

INTRODUCTION

The rapid development in computer and network technology has brought forth a tremendous increase in cyber crime; digital evidence has played an increasing role in combating cyber crime. Digital evidence performs two major roles. One of the roles of digital evidence is to provide digital evidence accepted by the court after reorganization, protection, extraction, analysis and archiving process. Another role is to provide a clue for solving an involving cyber crime case at the beginning of the investigation.

Digital evidence can provide a significant link between the perpetrator and the victim, and can prove the motivation and methods used of the suspects. But when considering cyber crime case, the facts that the prosecutors or police often face with digital evidence in the initial stage of cyber crime investigation are laid out as follows:

DOI: 10.4018/978-1-7998-3025-2.ch013

- **Digital evidence is inadequate:** The nature of case, investigation direction and investigation range are not clear in this phase. 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;
- **Digital evidence is decentralized:** Unlike physical crime scene, the boundaries of a cyber crime scene are not clearly outlined and the crime scene may extend a room, a city, etc. Digital evidence may lay in different places of cyber crime scene according to Lockard's exchange principle;
- **Digital evidence is fragmented:** The original state of digital data is in the binary form—0 or 1, but its forms are diversified. The digital data stored is massive and disordered which pieces of digital data are mixed and stacked together over time. Maybe little digital data is closely related to the cyber crime case;
- **Digital evidence is fragile:** Digital evidence can be easily modified, duplicated, restored, or destroyed, and the presentation of digital information cannot be well perceived by human senses. That is to say, it is very difficult to prove whether the digital evidence has been changed.

In the face with the above-mentioned facts, during the initial stage of cyber crime investigation, the prosecutors or police have to solve the following questions: firstly, they should determine the nature of such case and the basis of the judgments. The second step is to refer to the previous cases that are similar to the given case to evaluate it. Lastly, if further investigation is needed, the major problem is how to define the focus of the investigation and how to obtain digital evidence.

To our knowledge, few research work is on this area, no adequate operation guidance for cyber crime investigation has been introduced. Moreover, no specific steps for different case categories have been made until now. In this paper, we focus on the application of digital evidence in the initial stage of cyber crime investigation and propose a cyber crime investigation model based on case characteristics, helping to analyze the nature of cyber crime cases, determine investigation orientation and delimit investigation range. In the following Section 2, we discuss related studies concerning investigation technologies, methods and models. In Section 3, we introduce the investigation model. In Section 4, a case study is discussed. In Section 5, we draw conclusions.

RELATED WORK

Most of the related papers presented many digital investigation technologies and methods, which included, but are not limited to, data warehousing, applying Bayesian inference, model checking, data mining, danger theory and attack tree analysis, etc. (Kunari, Noble & Mohapatra, 2016; Waleed et al., 2015; Zhang Guan-Zhu, 2014; Yang, 2012). Some research utilized the OWL and DL to represent and reason the digital evidence obtained from more than one domain (Ha Le & Sun Guo-Zi, 2014; Turnbull, Benjamin, Randhawa et al., 2015). Such technologies and methods are reasonable in theory, but frequently encounter practical difficulties in the initial stage of cyber crime investigation. One of the major reasons is that it is not possible to acquire enough digital evidence in this phase to give strong backing to those technologies and methods, and 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.

To fight against cyber crime, some ethics, guidelines, models, etc. have been proposed. Some of early model like Casey focused on processing and examining digital evidence and comprise of steps