Chapter 19
A Knowledge Model of Digital Evidence Review Elements Based on Ontology

Ning Wang
Hubei University of Police, Wuhan, China

ABSTRACT

As existing methods cannot express, share, and reuse the digital evidence review information in a unified manner, a solution of digital evidence review elements knowledge base model based on ontology is presented. Firstly, combing with the multi-source heterogeneous characteristic of digital evidence review knowledge, classification and extraction are accomplished. Secondly, according to the principles of ontology construction, the digital evidence review elements knowledge base model which includes domain ontology, application ontology, and atomic ontology is established. Finally, model can effectively acquire digital evidence review knowledge by analyzing review scenario.

INTRODUCTION

Of the criminal cases in China, the public security organization is only in charge of investigation, obtaining evidence. The people's procuratorate is responsible for reviewing the decisions proposed by the public security organization, approving arrests, and initiating public prosecutions. The people's court is responsible for adjudication after strictly examining and reviewing the evidence. Three described above are a kind of parallel relations, perform their respective duties and work in strict accordance with their respective mandates.

For digital evidence, its legal status has been admitted and the digital evidence as a new form of evidence in law has been specified clearly by China's three major procedural laws in 2013. But in judicial practice the digital evidence were not highly applied, most prosecutors and judges would like to adopt traditional evidence, such as physical evidence, documentary evidence, etc., and not to adopt digital evidence in law court.

DOI: 10.4018/978-1-7998-3025-2.ch019

There are multiple reasons accounting for this phenomenon, for example, digital evidence is fragile in that it can be easily modified, duplicated, restored, or destroyed, and the presentation of digital information cannot be well perceived by human senses, there are a large amount of manual interventions in digital forensic analysis, and so on. The chief reason is that there is no common platform can express, share, reuse and review the digital evidence, that is to say, handling digital evidence individually and lacking coordinated operations make it difficult to understand the digital evidence between the public security, the procuratorate and the courts.

Digital evidence review, as a comprehensive concept, involves a large number of multi-source heterogeneous elements, which include, but are not limit to, applicable conditions of law, evidence rule, forensic operation regulations, credible forensic tools, scientific forensic methods, etc. However, many existing research exclusively focus on forensic model, process, tool, methods from a technology perspective, or concerned only the legislative basis, applicable conditions, and legal effect of digital evidence from a legal perspective. The current theoretical research on the digital evidence review elements is also lack of comprehensive and systematic exposition.

Expressing, sharing and reusing the digital evidence review elements in a unified manner between the public securities, the procuratorate and courts can raise the digital evidence utilization in the court, and ontology technology can resolve the multi-source heterogeneous problems of digital evidence review. Therefore, we present a solution of digital evidence review elements knowledge base model based on ontology. In the following Section 2, we discuss related studies concerning this paper. In Section 3, we introduce the digital evidence review elements knowledge base model based on ontology. In Section 4, we analyze review scenario. In Section 5, we draw conclusion.

RELATED WORK

Constructing the unified description knowledge base can effectively solve the problems of data storage and fusion caused by multi-source and heterogeneous data. The familiar knowledge base model includes knowledge base model based on XML, knowledge base model based on IDMEF format, knowledge base model based on first order predicate logic, knowledge base model based on Ontology (Fagerberg, Fosaas & Sapprasert, 2012). XML lacks the ability to express and manage the semantic, and cannot be appropriate to build a semantically-rich knowledge base model. IDMEF is only directed at IDS system and the first order predicate logic cannot support to express uncertainty knowledge. The ontology knowledge base can provide the consistent expression of domain knowledge and be applied to handling the multi-source heterogeneous data.

Tom Gruber defined "ontology" as "a specification of a conceptualization", which is a description of the concepts and relationships that can exist for an agent or a community of agents. The representational primitives are typically classes, attributes, and relationships. The definitions of the representational primitives include information about their meaning and constraints on their logically consistent application (Gruber, 1995).

In recent years, the research and application of ontology is concerned by the extensive application of knowledge engineering, and cyber forensic ontology have been researched for criminal investigation in the knowledge representation systems and information systems. Dzemydiene and Kazemikaitiene (2006) proposed an Ontology-Based Decision Support System, Donalds and Osei-Bryson (2006) proposed ontology OntoCRIKS, and the cybercrime forensics ontology was presented by Brinson et. al (Brinson,