사이버 범죄 수사를 위한 사이버 포렌식 범주 온톨로지

박 흠*

Cyber forensics domain ontology for cyber criminal investigation

Heum park*

요 약

사이버 포렌식은 사이버 공간에서 일어나는 범죄 수사로 디지털 포렌식의 처리 절차와 기술적 방법을 그대로 사용한다. 사이버 범죄에는 사이버 테러와 사이버 공간을 이용한 일반 사이버 범죄로 나눌 수 있는데 대부분 서로 연관되어 있다. 그리고 사이버 테러 수사에는 높은 수준의 조사 기법과 시스템 환경, 분야별 전문가가 필요하며, 일반 사이버 범죄는 사이버 공간에서의 디지털 증거에 의해 일반 범죄와 연결되어 있다. 그래서 관련 범죄 유형 판단이나 증거 수집, 법적 증거 능력 확보에 많은 어려움이 겪고 있다. 따라서 본 논문에서는 사이버 범죄 분류, 사이버 공간에서의 증거 수집, 사이버 범죄 관련 법 적용 등에 초점을 두었고, 효율적인 사이버 범죄 수사를 위한 사이버 범죄에 대한 개념 통합이 필요하여 사이버 범죄 분류, 관련 법률, 증거, 피의자, 사건 정보 등의 개념과 속성과 관련도를 이용한 개념망으로 사이버 포렌식 범주 온톨리지를 구축하였다. 이 온톨로지는 사이버 사건 수사 절차와 범죄 유형, 사건, 증거, 용의자 등의 분류, 클러스터링, 연관 검색, 탐지 등의 데이터마이닝에 활용할 수 있다.

ABSTRACT

Cyber forensics is used the process and technology of digital forensics as a criminal investigation in cyber space. Cyber crime is classified into cyber terror and general cyber crime, and those two classes are connected with each other. The investigation of cyber terror requires high technology, system environment and experts, and general cyber crime is connected with general crime by evidence from digital data in cyber space. Accordingly, it is difficult to determine relational crime types, collect evidence and the legal admissibility of evidence. Therefore, we considered the classifications of cyber crime, the collection of evidence in cyber space and the application of laws to cyber crime. In order to efficiently investigate cyber crime, it is necessary to integrate those concepts for each cyber crime-case. In this paper, we constructed a cyber forensics domain ontology for cyber criminal investigation using the concepts, relations and properties, according to categories of cyber crime, laws, evidence, and information of criminals and crime-cases. This ontology can be used in the process of investigating of cyber crime-cases, and for data mining of cyber crime; classification, clustering, association and detection of crime types, crime cases, evidences and criminals

키워드

온톨로지, 사이버 범죄, 디지털 증거, 범죄 수사, 사이버 포렌식

* 신라대학교 컴퓨터정보공학부

접수일자 2009. 02. 10
심사완료일자 2009. 04. 09

Ⅰ. 서 론

정보기술과 인터넷 서비스, 디지털 장비의 발달로 다양한 디지털 도구와 사이버 공간을 이용한 사이버 범죄자들이 점점 늘어나고 있다. 사이버 범죄는 사이버 테러형 범죄와 일반 사이버 범죄로 나뉜다. 사이버 테러형 범죄에는 사용자 도용, 단순침입, 파일삭제와 자료 유출, 폭탄 메일 등과 같은 해킹과, 트로이목마, 웜, 스파이웨어 등과 같은 악성프로그램 생성 및 유포 범죄가 있다. 또 일반 사이버 범죄에는 전자상거래 사기, 불법 복제, 불법유해 사이트 개설, 사이버 명예훼손, 개인정보 침해, 사이버 스토킹 등이 있다 [6]. 그 외 불법 온라인 도박, 아동 성인물 유통, 사이버 피싱 등 의 사이버 범죄도 있다. 그리고 인터넷 보급과 모바일 기기의 확산으로 다양하고 새로운 사이버 지능 범죄가 생성되고 있고 이런 사이버 범죄 증가로 인해 법 집행기관의 방어와 근절 노력도 계속되고 있다 [1].

그리고 사이버 범죄는 사이버 공간에서의 증거와 일반 디지털 증거물에 의해 일반 범죄와 서로 연계되어 있어 수사하는데 많은 어려움이 있고, 증거 수집 절차와 수집 기술에 관련 전문가가 필요하다. 사이버 범죄 수사에서는 먼저 사이버 증거물과 디지털 증거물을 수집하고 범죄 현장과 환경을 보존해서 법적 증거 능력을 확보해야 한다. 그리고 이런 증거와 범죄 환경을 조사하고 분석해서 관련 범죄 유형 판단, 유사 사건 수집, 관련 법률 적용 등을 고려하게 된다. 또 사건 보고서 작성과 관련 문서를 분류 관리하는 데이터 마이닝 기법이 적용된다.

따라서 범죄 수사에서 데이터마이닝 기법을 이용한 데이터 분석과 데이터 탐지를 위한 강력한 도구가 요구된다 [1]. 또 디지털 범죄에 대한 개념의 정의와 개념간 관련성을 조사하여 통합할 필요가 있다. 최근에는 사이버 범죄 개념 정의와 증거 수집에 대한 데이터 마이닝 기법과 포렌식 온톨로지를 이용한 정보 검색과 지식 표현 시스템에 대한 연구가 많이 일어나고 있다. 하지만 대부분 일반 범죄 수사와 디지털 증거 수집에 대한 데이터베이스 시스템을 이용한 정보검색 시스템에 많이 집중되어 있다. 최근 들어 국외 연구에서 일반 범죄 범주 온톨로지를 기반으로 한 포렌식 지식 기반 정보시스템이 발표되었고, 2007년에는 A. Brinson, A. Robinson, M. Rogers에 의해 최초로 사이버 범죄 포렌식 온톨리지가 발표되었으나, 이 온톨로지는 사이버 범죄 수사 범주에 대한 전문분야 기술, 인증 절차, 교육에 대한 개념망을 정의한 것이었다 [2]. 따라서 실제 사이버 범죄 개념 정의와 사이버 범죄 수사를 위한 사이버 범죄 분류, 사이버 공간에서의 증거 수집, 사이버 범죄 관련 법 적용 등에 대한 개념 정의와 개념간 통합이 필요하다.

본 논문에서는 실제 범죄 수사와 데이터마이닝에 적용 가능한 사이버 범죄 분류, 관련 법률, 증거, 피의자, 사건 정보 등의 개념과 개념간 속성, 관련도를 이용해 사이버 포렌식 범주 온톨리지를 실험적으로 구축하였다. 이 온톨로지는 경찰청 사이버 테러 대응 센터(Korean National Police Agency : KNPA, http://www. netan.go. kr)의 사이버 범죄 분류, 증거, 법률 분류 등과 범죄자 정보, 사건 정보 등을 이용하여 개념을 정의하고, 개념간 속성, 관련도를 기반으로 개념망을 구축하였다. 논문의 2장에는 관련 연구로 온톨로지와 범죄 수사를 위한 정보시스템, 기존에 발표된 사이버 포렌식 온톨리지, 데이터마이닝 기법에 대해 기술하겠다. 3장에서는 사이버 범죄 수사를 위한 사이버 포렌식 범주 온톨리지의 개념 정의, 개념간 속성, 관련도와 그 응용에 대해 소개하겠다. 4장에는 온톨로지를 이용한 정보 지원시스템을 소개하고, 5장에서는 온톨리지 구축에 따른 향후 연구 과제와 결론을 내리겠다.

Ⅱ. 관련 연구

온톨로지는 1992년 Tom Gruber에 의해 "a specification of a conceptualization"로 정의되어 컴퓨터 분야에 최초로 제안되었다. 원래 온톨로지라는 단어는 철학에서 오랫동안 '존재의 실체'라 불리어진 용어인데, 최근 들어 AI 분야에서 활발하게 많은 논쟁거리가 되어 여러 분야에서 연구가 되어 오고 있다. 온톨로지는 개념(클래스)과 속성, 개념 간 관계를 묘사한 것으로 개념 정의와 개념망의 집합으로 표현하고, 일관성 있는 적용을 위해 의미 정보와 제약 조건을 포함한다 [3][4].

온톨로지를 표현하는 도구로 최근에 개발된 온톨로지 표준 언어로 World Wide Web Consortium (W3C)에서 개발한 OWL이 있다. OWL은 개념적 의미와 관계를 형식 묘사에 사용되는데, Protégé OWL은 개념 정의와 편리한 기능을 제공하는 대표적인 도구다 [5]. 본 논문에서는 OWL-DL 언어와 표현 도구 Protégé를 사용하여 온톨

로지를 작성하였다.

2002년 D. Dzemydiene는 범죄 수사 범주의 지원 정보 시스템(Advisory Information System of Crime Investigation Domain)으로 범죄 수사 지식표현에 대해 발표하였고, 이후 범죄 수사학에 도움이 되는 정보시스템을 개발하였다. 그리고 중범죄, 절도, 불법무기 소지 등과 같은 범죄에 대한 개념과 관련성으로 온톨로지를 구축하였고, 범죄 수사를 위한 지능적 과학 수사 처리 방법에 대해 제시하였다 [9]. 또 D. Dzemydiene과 E Kazemikaitiene은 2005년 범죄 수사 처리를 위한 온톨로지-기반 의사 결정 시스템을 제안했다. 여기서 온톨로지는 증거 수집, 자료 수집, 저장, 처리 방법, 전달 방법 등을 일정 형식으로 기틀을 잡는데 도움이 되었고, 이 시스템은 범죄 수사에서 선택적 의사 결정 조건으로 사용되어졌다 [8].

2004년 H. Chen은 일반 범죄에 대한 개체 추출, 클러스터링, 연관도, 편차 탐지, 분류, 문자열 비교, 사회망 분석에 응용할 수 있는 데이터 마이닝 기법을 소개하였다. 또 경험과 다양한 증명 기법을 나타내는 범죄 데이터 마이닝에 대한 일반적인 기틀을 소개하였다 [1].

C. M. Donalds과 K. Osei-Bryson는 2006년에 치안 부대를 지원하기 위해 범죄 수사 활동에서 국내 국외 증거 수집, 저장, 정보 검색과 보고서 작성을 위해 범죄 수사 지식 시스템 (Criminal Investigation Knowledge System :CRIKS) 제안하였다. 그리고 관련 개념의 인증과 정의에 의한 범죄 수사 범주 온톨로지 OntoCRIKS를 구축하였고, 이 온톨로지의 개념간 관련도로 조직 체계에서의 개념과 관련성의 불명확성을 없앴다. 이 온톨로지의 개념과 관련도는 문서-기반, 사건-기반, 시행-기반, 토의-기반, 인지-기반, 시나리오-기반에 의해 만들어졌고 텍스트 마이닝 기술에도 적용되었다 [7]. 2007년 Ashley Brinson에 의해 최초로 사이버 포렌식 온톨로지가 사이버 포렌식 범주에서 전문분야 기술, 인증 절차, 교육 분야에 대한 정확한 계층 구조를 만들기 위한 목적으로 구축되었다. 이 온톨로지는 technology과 profession 등 두 가지의 세부 논제로 구성되었다 [2]. 하지만 이 온톨로지는 사이버 포렌식에서의 전문분야 기술, 인증 절차, 교육 분야에만 디자인되었기 때문에 실제 사이버 범죄 수사에서는 적용하기 어렵다.

III. 사이버 포렌식 범주 온톨로지

범죄 수사 절차를 보면, 먼저 수사 계획을 세우고, 범죄 현장과 환경을 보존하고 증거물을 수집 절차에 따라 수집하다. 그리고 증거물을 조사하고 분석한 다음, 사건의 윤곽과 정확한 범죄 유형을 파악하고, 이를 토대로 범인을 체포하고, 적합한 관련 법규를 결정하여 보고서를 작성한다 [8][9]. 경찰청 사이버 테러 대응 센터(KNPA, http:// www.netan.go.kr)의 사이버 범죄수사 처리 지침을 보면, 첫째 현장을 보존하고 증거물(휘발성, 비휘발성 포함)을 수집 절차에 의해 수집한다. 둘째 그 증거물을 조사하고 분석한 다음 안전하게 보관한다. 셋째 기소를 위해 관련 법류를 적용하고 사건 보고서를 작성한다 [6]. 그리고 미국 법무성(DOJ)의 포렌식 프로세스를 보면, 먼저 사전 준비, 수집, 현장 보존, 사건 현장 문서화, 증거 수집, 조사, 분석, 보고서 작성 등의 순으로 이루어진다 [10]. 이와 같이 사이버 범죄 수사 절차는 일반 범죄 수사 절차와 크게 다르지 않다.

사이버 포렌식에서는 일반 범죄 유형와 관련 법규, 사이버 범죄 유형이 서로 연관되어 있기 때문에 증거물 수집 과정에서 관련 범죄 유형과 법규를 쉽게 알 수가 있다. 따라서 사이버 범죄 수사 프로세스를 기반으로 범죄 유형, 증거물 수집, 피의자 정보, 사건 정보, 관련 법규 등으로 개념 정의와 개념간 속성, 관련도를 연결하여 사이버 범죄 수사를 위한 사이버 포렌식 범주 온톨로지를 실험적으로 구축하였다. 이 온톨로지에는 다섯 가지 개념, 즉 Law, Crime_Case, Criminal, Crime_Type, Evidence 클래스로 구성하였다. 그림 1은 사이버 포렌식 온톨로지의 개념과 속성, 개념간 연결도를 다이어그램으로 보여준다.

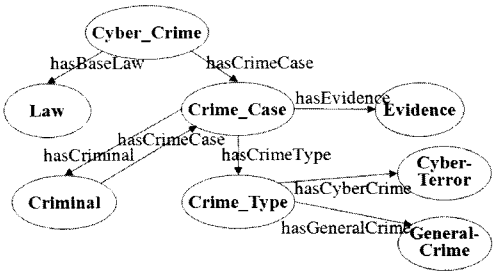

그림 1. 사이버 범죄 수사를 위한 사이버 포렌식 온톨로지 개념도

Fig. 1 Concept diagram of cyber forensics ontology for cyber criminal investigation

'Cyber_Crime' 클래스는 'Crime_Case'와 'Law' 하위 클래스를 가지고 있고, 'Crime_Case' 클래스와 속성 'hasCrimeCase'로 연결되어 있고, 'Law' 클래스와는 속성 'hasBaseLaw'로 연결되어 있다. 'Law' 클래스는 관련 법규의 집합이다. 또 'Crime_Case' 클래스는 'Criminal', 'Evidence', 'Crime_Type' 등의 하위 클래스를 가지고 있고, 'Criminal'와는 속성 'hasCriminal'과 역속성으로 'hasCrimeCase'로 연결되어 있다. 또 'Evidence'와는 속성 'hasEvidence'를, 'Crime_Type'과는 속성 'hasCrime Type'으로 연결되어 있다. 그리고 'Crime_Type' 클래스는 'CyberTerror'와 'GeneralCrime' 하위 클래스를 가지고 있고, 각각 속성 'hasCyberCrime'와 'hasGeneralCrime'으로 연결되어 있다. 'Cyber_Crime' 클래스의 하위 클래스 'Law', 'Crime_Case', 'Criminal', 'Crime_Type', 'Evidence'의 세부 하위 클래스와 관계를 보면 다음과 같다.

'Law' 클래스의 하위 클래스로 'Criminal Act', 'Act on Promotion of Information and Communications Utilization and Information Protection, etc', 'Information Communication Infrastructure Protection Act' 등으로 구성하였다. 즉 '형법', '정보통신망 이용촉진 및 정보보호 등에 관한 법률', '전기통신기본법', '성폭력범죄의 처벌 및 피해자보호등에 관한 법률', '전파법', '신용정보의 이용 및 보호에 관한 법률' 등으로 경찰청 사이버 테러 대응 센터(KNPA, http://www. netan.go.kr)에서 정의한 사이버 범죄 관련법규를 하위 클래스 개념으로 정의하였다. 그리고 각 하위 클래스의 인스턴스에는 표 1과 같이 적용 법조항과 범죄사실을 두었다 [6].

표 1. 'Law'의 하위 클래스 '정보통신망 이용촉진 및 정보보호등에 관한 법률'의 인스턴스들
Table. 1 Instances of subclass 'Act on Promotion of Information and Communications Utilization and Information Protection, etc' for class 'Law'

법조항	범죄 사실
제70조제1항	사이버 명예훼손 (사실 유포)
제70조제2항	사이버 명예훼손 (허위사실 유포)
제71조제1항	개인정보 목적외 이용 및 제3자 제공
제71조제3항	이용자 개인정보 훼손 · 침해 · 누설
제71조제4항	악성프로그램 (바이러스) 유포
...	...

'Crime_Case' 클래스의 하위 클래스는 그림 1과 같이 'Crime_Type', 'Evidence', 'Criminal' 등이 있다. 그리고 'Law' 클래스와도 'Cyber_Crime' 클래스에 의해 연결되어 있다. 'Crime_Case' 클래스의 인스턴스에는 개개 사건번호와 사건명으로 이루어져 있다. 'Criminal' 클래스에는 'Crime_case' 클래스를 통해 'Evidence', 'Crime_Type', 'Laws' 클래스와 연결되어 있다. 또 연결된 클래스의 인스턴스는 증거물 정보, 범죄 유형 정보, 관련 법규 정보 등 피의자 범죄 정보를 인스턴스로 갖는다.

'Crime_Type' 클래스에는 사이버 범죄 유형을 나열하였다. 하위 클래스로 'Cyber Terror', 'General Cyber Crime'가 있고, 'Cyber Terror' 클래스에는 'Hacking', 'Distribution Virus', 'Distribution Spam' 등의 하위 클래스로 구성되어 있다. 'Hacking' 클래스에는 'Intrusion', 'Dos', 'Information Theft', 'Logical bomb' 등이 있고, 'Distribution Virus'의 하위 클래스에는 'Worm', 'Virus', 'Spyware', 'Adware' 등이, 'Distribution Spam' 클래스에는 'Mail', 'Message', 'Call' 등의 하위 클래스가 있다. 'General Cyber Crime' 클래스에는 9개의 하위 클래스, 'Fraud', 'Illegal Site', 'Illegal Reproduction', 'Defamation', 'Infringement of Private', 'Stalking', 'Sexual Violence', 'Threatment', 'CopyRights' 등이 있다. 각각의 하위 클래스의 인스턴스에는 구체적인 범죄 내용이 포함되어 있다.

'Evidence' 클래스는 증거물 유형과 증거물 수집 절차의 집합으로 되어 있다. 그림 2는 'Evidence' 클래스의 하위 클래스 'Collection'와 'EvidenceType', 속성을 나타낸 다이어그램이다.

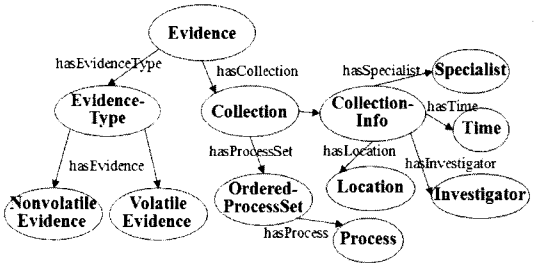

그림 2. 증거물과 증거물 수집 절차에 대한 하위 클래스와 관련도
Fig. 2 Subclasses and Relations among Evidence and Process of Collection

'EvidenceType' 클래스의 하위 클래스에는 'Nonvolatile Evidence'와 'Volatile Evidence'가 있고, 'Nonvolatile Evidence'의 하위 클래스에는 'H/W'와 'S/W'가 있다. 'H/W' 클래스에는 'Computer', 'Scanner', 'Disk', 'CD', 'Memory stick', 'Printer' 등의 하위 클래스와 'S/W' 클래스에는 'Illegal S/W', 'Application Program', 'Hacking Tool' 등의 하위 클래스가 있다.

또 'Volatile Evidence' 클래스에는 'Memory Dump', 'CPU Log', 'Routing History', 'Disk Imaging', 'Blog Board' 등의 하위 클래스가 있다. 그리고 각 하위 클래스의 인스턴스로 구체적인 증거물 정보가 저장되어 있다. 사이버 증거물에는 대부분 'Volatile Evidence'의 인스턴스들로 사이버 공간에서의 데이터와 히스토리 정보들이지만 디지털 장비나 부품으로 'Nonvolatile Evidence'의 인스턴스들도 포함한다. 'Collection' 클래스에는 'OrderedProcessSet'와 'CollectionInfo'가 있고, 'CollectionInfo'에는 증거물 수집 정보에 해당하는 'Specialist', 'Investigator', 'Time', 'Location' 등이, 'OrderedProcessSet' 클래스에는 증거물 수집 절차에 해당하는 하위 클래스로 'TakePicture', 'RecordVideo', 'DrawSketch', 'GetCache', 'GetRouting', 'Getmemory Dump' 등이 있다.

Ⅳ. 온톨로지를 이용한 정보 지원시스템

이 온톨로지를 이용해 사이버 범죄 수사에서 사건별 증거 정보, 증거 수집 절차 정보, 피의자 정보, 범죄 유형 정보, 관련 법규 정보 등을 사건 인스턴스로 저장하고 검색할 수 있다. 또 사건 데이터베이스와 연계해 보고서 작성과 증거물 분석, 범죄 유형과 사건 분석, 관련 범죄 유형, 용의자, 유사 범죄, 증거물 수집 절차 정보 등을 얻을 수 있다. 그림 3은 사이버 범죄 수사에서 온톨로지와 데이터베이스를 이용한 정보지원 시스템의 개념도를 나타낸다. KNPA의 포렌식 모델 중 증거수집, 조사 및 분석 단계에서 온톨로지를 이용했을 때, 증거유형, 범죄유형, 증거수집유형 등의 하위 클래스와 인스턴스, 인스턴스 간 관련도와 속성을 참조하여 증거 수집과 조사, 증거 분석을 할 수 있다. 그 결과는 증거 데이터베이스에 저장한다. 또 보고서 작성, 증거보존 등의 절차에서도 위 3가지 하위 클래스와 인스턴스와 속성을 참조하여 보고서 작성과 증거 보전/관리에 적용할 수 있다. 수사 중 관련법 적용 역시, 'Law'의 하위 클래스의 법조항의 인스턴스를 참조하여 처리할 수 있다.

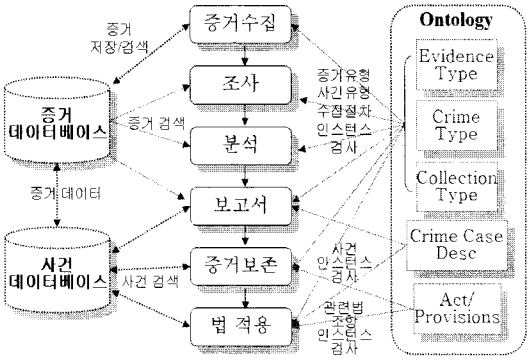

그림 3. 사이버 범죄 수사에서 온톨로지와 데이터베이스를 이용한 정보 지원시스템 개념도
Fig. 3 Diagram of information support system using ontology and database system in cyber forensics

하지만 모든 증거와 사건 정보는 종결 후 증거 데이터베이스와 사건 데이터베이스에 저장되고, 이후 이와 관련된 사건정보 검색은 이 데이터베이스를 이용한다. 여기서 온톨로지의 역할은 증거, 사건, 관련법 등 사이버 수사에 필요한 모든 인스턴스와 속성을 구조적으로 분류하고 연결하여 관련도를 제공하여, 사이버 범죄수사 준비단계부터 종결까지 정보 수집과 처리에 참조함으로써 범죄 수사에서의 일관성을 준다. 현재 일선 경찰에서의 사이버 범죄 수사는 증거 수집과 보존, 법적 효력을 위한 증거 수집/분석 매뉴얼과 증거 수집 유형에 따라 하드웨어/소프트웨어 도구를 사용하고 있다. 이를 온톨로지의 인스턴스로 분류하고 처리 절차를 온톨로지에 넣어 범죄 수사에 사용한다면, 지속적으로 늘어나는 증거 유형과 범죄 유형에 유연하게 대처할 수 있다. 또 이 온톨로지를 이용하면 사건별 증거별 개체 추출, 분류, 연관도 검색, 편차 탐지, 클러스터링, 문자열 비교, 사회망 분석 등과 같은 데이터 마이닝에도 응용할 수 있다.

V. 결 론

지금까지 사이버 범죄 수사에서 사이버 범죄와 관련된 개념들, 즉 증거, 범죄 유형, 피의자 정보, 관련 법률 등과 속성, 개념간 연결도를 작성한 사이버 포렌식 범주 온톨로지를 소개하였다. 또 이 온톨로지를 이용하면 증거 수집/분석, 보고서 검색은 물론, 범죄 유형 분석, 증거물 법적 증거 능력검증 등에도 사용할 수 있다. 이런 정보들의 개념간 연결은 데이터베이스 시스템으로도 구축할 수 있으나 온톨로지로 구축했을 때 더 많은 장점이 있다. 데이터베이스 시스템에서는 개념들간의 관계를 필드간의 연결로만 가능하지만, 온톨로지로 구축했을 때는 상위 클래스, 형제 클래스, 하위 클래스와 관계와 인스턴스간 관계, 다양한 속성을 정의할 수 있고, 이미 구축된 온톨로지에서도 하위 클래스나 제약조건을 아주 쉽게 추가할 수 있다. 하지만 이 온톨로지 구성에는 전체 포렌식 절차에서 수사 계획과 증거물 수집단계에만 국한된 것이기 때문에 조사, 분석, 보고서 작성 단계에는 더 확장해야 한다. 또 일반 범죄에까지 적용하려면 더 많은 시간과 노력이 필요할 것으로 보인다.

참고문헌

[1] H. Chen, W. Chung, J.J Xu, G. Qin, M. Chau, "Crime Data Mining: A General Framework and Some Examples". Computer. Vol. 37, No. 4, pp. 50-56, 2004

[2] A. Brinson, A. Robinson, M. Rogers. "A cyber forensics ontology: Creating a new approach to studying cyber forensics". Digital Investigation. 3S, S37-S43, 2006

[3] Gruber, T. R., A, "Translation Approach to Portable Ontology Specifications. Knowledge Acquisition", 5(2): pp. 199-220, 1993

[4] Tom Gruber. http://tomgruber.org/writing/ontol ogy-definition-2007.htm

[5] M. Horridge, H. Knublauch, A. Rector, C. Wroe, "A Practical Guide To Building OWL Ontologies Using The Prot´eg´e-OWL Plugin and CO-ODE Tools". Univ Manchester. 2007

[6] The Cyber Terror Response Center (CTRC) of the Korean National Police Agency (KNPA), http://www.netan.go.kr/eng/index.jsp

[7] C. M. Donalds, K. Osei-Bryson, "Criminal Investigation Knowledge System", CRIKS, the 39th Annual Hawaii International Conference on System Sciences, V-07, pp152-160, 2006

[8] D. Dzemydiene, E. Kazemikaitiene, "Ontology-Based Decision Support System for Crime Investigation Processes, Information Systems Development", Springer, pp427-438, 2005

[9] D. Dzemydiene, "Knowledge Representation in Advisory Information System of Crime Investigation Domain, Databases and Information Systems II". Springer, pp 135-146, 2002

[10] Electronic Crime Scene Investigation Guides, U.S. Department of Justice (DOJ), http://www.ncjrs.org/dffiles1/nij/187736.pdf

저자소개

박흠(Heum park)

부산대학교 계산통계학과 졸업
부산대학교 인지과학 이학석사
부산대학교 정보시스템 공학박사
신라대학교 컴퓨터정보공학부

※관심분야 : 데이터마이닝, 정보처리, 온톨로지