DOI: 10.3745/KIPSTD.2009.16-D.2.265

디지털 포렌식 온톨로지를 이용한 디지털 증거의 증거능력에 대한 검증 방법

조 혁 규[†] · 박 흠[††] · 권 혁 철[†††]

요 약

디지털 장치들의 활발한 사용은 디지털 증거들을 양산하지만, 이들 증거들이 법정에서 범죄사실을 증명하는 증거로 채택되기에는 많은 어려움이 있다. 따라서 이 논문에서는 디지털 포렌식 온톨로지를 이용한 디지털 증거들의 증거능력에 대한 검증 방법을 제안한다. 디지털 증거들의 증거능력을 검증하기 위하여 경찰청에서 정의한 표준 디지털 포렌식 처리절차에 따라 디지털 포렌식 온톨로지를 확장하고, 디지털 포렌식 온톨로지에서 정의한 각 클래스들 간의 property 관계를 설정하였다. 또한 각 클래스간의 property 제한 규칙을 정의하여 활용한다. 이 논문에서 제안된 검증방법과 온톨로지는 디지털 증거 수집을 위한 계획을 수립하거나, 디지털 포렌식의 교육 등에 활용할 수 있다.

키워드 : 디지털 포렌식 온톨로지, 디지털증거, 증거능력의 검증

The Method of Verification for Legal Admissibility of Digital Evidence using the Digital Forensics Ontology

Hyuk-Gyu Cho[†] · Heum Park[††] · Hyuk-Chul Kwon[†††]

ABSTRACT

Although the various crime involved numerous digital evidence, the digital evidence is hard to be acknowledged as a evidence to proof the crime fact in court. We propose the method of verification for the legal admissibility of digital evidence using digital forensics ontology. In order to verify the legal admissibility of digital evidence, we will extend the digital ontology by standard digital forensics process from Digital Forensics Technical Manual defined by KNPA and set up the relation properties and the rule of property constraint to process class in the digital forensics ontology. It is possible for proposed ontology to utilize to plan the criminal investigation and to educate the digital forensics.

Keywords : Digital Forensics Ontology, Digital Evidence, Verification For Legal Admissibility of Digital Evidence

1. 서 론

정보화 사회가 정착되면서 컴퓨터와 인터넷의 사용이 일반인들의 생활에 많은 부분을 차지하고 있어 다양한 디지털 정보가 사용되고 있다. 한국의 경우 2007년도 상반기에 인터넷 사용자가 전체 인구의 75%를 차지하고 있다[1]. 또한 2003년도 버클리 대학의 연구 보고서에 따르면 전 세계적으로 생성되는 정보의 약 92% 이상이 디지털 형태로 나타나고 있다[2]. 따라서 인터넷 상에서 발생하는 사이버 범죄뿐만 아니라 실생활에서 발생하는 일반 범죄에서도 디지털 자료가 범죄사실의 증거로 활용되게 되었고, 소송에 있어서도 디지털 증거(digital evidence)를 배제하고서는 사실입증이 곤란할 만큼 디지털 증거가 중요하게 되었다[3].

디지털 자료가 법적 증거능력(legal admissibility)을 갖게 하기 위한 제반 처리절차와 기술적인 방법을 나타내는 디지털 포렌식(Digital Forensics)은 그 대상에 따라서 디스크 포렌식(Disk Forensics), 네트워크 포렌식(Network Forensics), 전자메일 포렌식(E-mail Forensics), 웹 포렌식(Web Forensics), 모바일 포렌식(Mobile Forensics), 소스코드 포렌식(Source Code Forensics), 멀티미디어 포렌식(Multimedia Forensics), 데이터베이스 포렌식(Database Forensics) 및 회계 포렌식(Account Forensics)으로 분류된다. 또한 디지털 증거는 잠재성, 이진성, 취약성, 다양성, 대량성, 휘발성 및 네트워크성 같은 복합적인 특성을 지니고 있다[2]. 특히 디지털 증거는 복제가 쉽고, 원본과 사본의 구분이 어려우며, 조작, 변경,

※ 이 논문은 2008년 교육과학기술부로부터 지원받아 수행한 연구임 (지역거점연구단 육성사업/차세대물류기술연구단).
† 정 회 원 : 영산대학교 사이버경찰학과 교수
†† 정 회 원 : 부산대학교 인공지능연구실
††† 종신회원 : 부산대학교 전자전기정보컴퓨터공학부 교수
논문접수 : 2009년 2월 5일
수 정 일 : 1차 2009년 2월 23일
심사완료 : 2009년 2월 24일

삭제가 용이하기 때문에 법정에 증거로써 제출되는 경우에 증거로서의 가치를 상실하지 않도록 적법한 절차와 방법을 이용하여 획득, 보관, 처리 및 분석되어야 한다.

디지털 포렌식 분야에서 디지털 증거를 획득하기 위한 기술적인 방법에 대한 다양한 연구가 진행되어 오고 있다[2]. 또한 법정에서 증거능력을 인정받기 위하여 디지털 증거의 처리 절차에 대한 연구 또한 활발하게 진행되어 오고 있으며, 수사 실무를 담당하는 조직에서도 조직의 특성에 맞는 다양한 처리절차를 제정하여 수사실무에서 활용하고 있다[4, 5, 6, 7, 8]. 또한 디지털 증거의 증거능력을 인정받기 위하여 디지털 증거에 관한 법률 체계와 법제에 관한 연구도 진행되고 있다. 한국의 경우 "일심회 사건" 이후 디지털 증거에 대한 논의가 시작되었고[9], 판례연구 등을 통한 디지털 증거의 법제에 관한 연구도 활발하게 진행되고 있다[3, 10, 11].

이와 같이 디지털 증거 법률체계의 정비 및 법제화를 통하여 디지털 증거의 증거능력에 대한 법적 근거를 마련하고, 디지털 증거의 처리절차를 표준화하여 증거능력을 안정적으로 인정받을 수 있다. 그러나 실제 디지털 증거를 다루는 전문성을 인정받는 수사관의 무의식적인 실수로 인하여 디지털 증거의 증거능력을 상실할 수도 있다. 한국의 일심회 사건의 경우 최초 이미징 작업에서 해쉬 값을 작성하지 않는 실수를 범하여 증거능력에 대한 의구심을 유발하게 되었다. 따라서 디지털 포렌식의 법률적인 근거를 마련하고, 절차를 표준화하는 것과 함께 시스템을 통하여 표준 절차에 맞게 수사 진행을 계획하고, 수사의 진행을 시스템이 검증하여, 적법한 절차에 따라서 수사가 진행되는 것을 확인할 수 있도록 해야 한다.

이 논문에서는 디지털 포렌식 온톨로지(Digital Forensics Ontology)를 이용하여 디지털 증거 수집의 표준 절차에 따른 수사의 진행을 검증하는 방법을 제안한다. 온톨로지를 구축하기 위한 표준 절차는 경찰청에서 발표한 "디지털 증거 분석 전문 매뉴얼(Digital Forensics Technical Manual)"을 활용하고, 프로테제(Protégé)를 도구로 사용하여 온톨로지를 구축한다. 또한 필수적인 처리절차의 존재여부를 검증하기 위한 새로운 규칙을 정의하고, 각 처리절차에 대한 before/after 관계를 설정한다. 사례연구를 통하여 이 논문에서 제안하는 디지털 증거의 증거능력에 대한 검증 방법을 실험한다.

이 논문은 디지털 증거의 증거능력에 대한 연구 동향을 2장에서 소개하고, 3장에서는 이 논문에서 제안하는 증거능력의 검증방법에서 활용하는 온톨로지의 구조를 소개하고, 4장에서는 처리절차의 순서검증을 위한 before/after 관계의 설정과 증거능력 검증을 위하여 정의하는 규칙을 소개한다. 5장에서는 제안된 온톨로지를 활용하여 증거 수집에 대한 증거능력 검증의 사례를 살펴본다. 마지막으로 이 논문의 결론을 말하고, 향후 연구방향 등을 살펴본다.

2. 디지털 증거의 증거능력에 대한 연구 동향

디지털 증거의 증거능력에 대한 연구는 디지털 증거가 법정에서 증거능력을 인정받기 위한 처리절차의 표준화에 대한 연구, 디지털 증거의 증거능력에 대한 법률적인 근거를 마련하기 위한 법률 체계와 법제화에 대한 연구 및 온톨로지를 이용한 디지털 포렌식의 연구 분야가 있다.

디지털 증거의 처리절차 표준화에 대한 연구는 포렌식 절차를 11단계의 처리 절차로 규정하고 있는 CERT(Computer Emergency Response Team)의 표준 처리절차가 있으며[4]. 미국 법무성(DOJ)의 포렌식 프로세스 모델에서는 사전준비, 수집, 범죄현장 보존, 사건현장의 문서화, 증거 수집, 조사, 분석과 보고서작성의 8 단계 처리절차를 규정하고 있다[7], 또한 미국 공군(U.S. Air Force)의 포렌식 프로세스 모델에서는 디지털 포렌식에 대하여 9단계의 처리절차를 규정하고 있다[8]. 국내의 경우 경찰청에서 규정한 포렌식 프로세스 모델에서 사전준비, 증거수집, 조사, 분석의뢰 · 접수 · 운반, 증거분석, 결과보고서와 보존 및 증거관리의 7개의 단계로 처리절차를 규정하고 있다[5, 6].

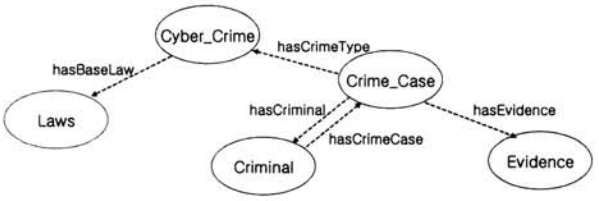
디지털 증거의 법률적인 근거를 위한 법률 체계와 법제화에 대한 연구는 전문증거로서 디지털 증거의 예외적 허용가능성을 중심으로 연구되고 있으며[3, 9-11], 국외의 경우 별도의 전자증거법을 제정하거나 기존의 증거법에 전자증거, 전자문서 또는 디지털 증거에 관한 규정을 신설하여 증거능력에 대한 문제를 해결하고 있다[3].

온톨로지를 활용한 디지털 포렌식에 관한 연구는 사이버 포렌식의 개념들을 5단계의 온톨로지로 설계하여 디지털 포렌식에 온톨로지를 활용하는 연구가 소개 되었고[18], 범죄유형, 디지털 증거, 사이버 범죄 관련 법률을 포함하는 온톨로지를 소개한 연구도 진행되고 있다[15-17]. 또한 자연언어처리를 통하여 텍스트 정보에서 사기와 관련된 정보를 TMR (text meaning representation)형태로 온톨로지에 저장하는 연구도 진행되고 있다[19]. 그러나 온톨로지를 활용하여 디지털 증거가 법정에서 증거로 인정받기 위하여 필요한 적법한 처리절차를 검증하는 방법과 관련된 정보를 처리하기 위한 방법에 관한 연구는 아직 이루어지지 않고 있다.

3. 디지털 포렌식 온톨로지

디지털 포렌식 온톨로지는 디지털 증거가 나타날 수 있는 사이버 범죄 및 일반 범죄, 디지털 증거, 관련 법률과 포렌식 표준 절차에 대한 분류를 기반으로 온톨로지를 설계한다. 제안된 디지털 포렌식 온톨로지는 기존의 온톨로지에 대한 연구[12-14]를 참고하고, [H Park(2009)]의 온톨로지[16]를 기반으로 처리절차를 검증하기 위하여 Crime_Case에 디지털 증거의 처리절차에 관한 여러 가지 클래스를 확장하여 사용한다. [H Park(2009)]의 온톨로지에 대한 전체적인 클래스 구조는 (그림 1)과 같다.

이 온톨로지에서 Crime_Case는 발생한 범죄를 나타내는 클래스이며, Cyber_Crime은 온톨로지를 이용하여 처리해야 하는 다양한 범죄의 종류 가운데 Cyber 범죄를 나타내는 클래스이다. Law 클래스는 발생한 범죄가 어떤 법률에 의해



(그림 1) 디지털 포렌식 온톨로지의 구조

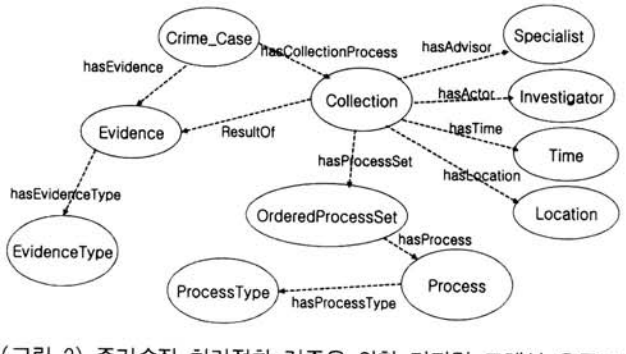
범죄로 성립하는 지를 나타내는 법률에 관한 클래스이다. Evidence 클래스는 범죄에서 수집된 증거들 가운데 디지털 증거에 관한 클래스이며 Criminal 클래스는 발생한 범죄의 피의자를 나타내는 클래스이다. Crime_Case 클래스는 Cyber_Crime 클래스와 hasCrimeType property 관계를 가지고, Criminal 클래스와 hasCriminal 관계를 가지고, Evidence 클래스와는 hasEvidence 관계를 가진다. 또한 Criminal 클래스는 Crime_Case와 hasCriminalCase 관계를 가지며, Cyber_Crime 클래스는 Law 클래스와 hasBaseLaw 관계를 가진다.

3.1 디지털 포렌식 온톨로지의 확장

[H Park(2009)]의 디지털 포렌식 온톨로지에 증거수집에 대한 처리절차를 검증하기 위하여 증거수집 처리절차에 대한 Collection 클래스를 추가한다. 디지털 증거 수집 처리절차를 위한 확장된 클래스 구조는 (그림 2)에서 보여준다.

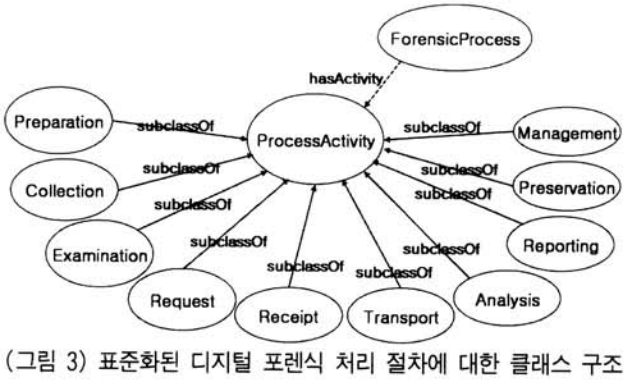
범죄를 나타내는 클래스인 Crime_Case 클래스는 디지털 증거를 나타내는 Evidence 클래스와 hasEvidence property 관계를 가지고 있으며, Evidence 클래스는 디지털 증거의 형태를 구분하기 위하여 EvidenceType 클래스와 hasEvidenceType property 관계를 가진다. EvidenceType 클래스는 (그림 5)에서 그 구조와 등록되는 individual을 소개한다.

증거수집에 대한 절차를 구현하기 위하여 Crime_Case 클래스와 증거수집 절차를 나타내는 Collection 클래스간에 hasCollectionProcess property 관계를 설정한다. Collection 클래스는 증거수집 처리절차에 필요한 일반적인 속성 정보를 나타내기 위하여 SpecialList, Investigator, Time 및 Location 클래스와 property 관계를 설정한다. Collection 클래스는 SpecialList와 hasAdvisor 관계, Investigator 클래스와 hasActor 관계, Time 클래스와 hasTime 관계 및 Location 클래스와 hasLocation 관계를 가진다. 이 논문에서 제안하는 디지털 포렌식 온톨로지에서 실질적인 증거수집 절차는 OrderedProcessSet 클래스와 hasProcessSet 관계를 설정함으로써 구현되며, OrderedProcessSet는 Process 클래스와 hasProcess 관계를 가지며, Process 클래스의 하위 클래스에서 세부적인 증거 수집 절차에 대한 클래스를 정의한다.



(그림 2) 증거수집 처리절차 검증을 위한 디지털 포렌식 온톨로지의 확장

경찰청의 포렌식 프로세스 모델에 따르면 디지털 포렌식의 처리절차는 예비단계인 사전준비단계, 증거수집 단계, 조사단계, 분석의뢰·접수·운반 단계, 증거분석 단계, 결과보고서 작성 단계와 증거보존·관리 단계로 구분된다[6]. 이들 각 단계에 대한 온톨로지 상의 클래스 구조는 (그림 3)과 같은 구조를 가진다.



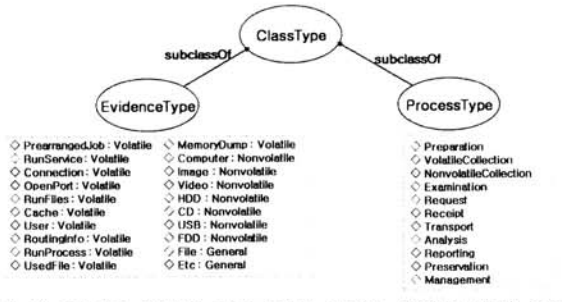
(그림 3) 표준화된 디지털 포렌식 처리 절차에 대한 클래스 구조

(그림 2)의 Crime_Case 클래스와의 연계구조는 각 단계의 클래스 이름과 property 관계(hasCollectionProcess, hasAnalysisProcess)를 가지게 구성되나, 프로테제의 클래스 구조의 명확성을 위하여 최상위에 ForensicProcess 클래스를 두고, 하위에 ProcessActivity 클래스를 둔다. 각 단계에 대한 클래스는 ProcessActivity의 하위 클래스로 구조화 한다. 즉 ProcessActivity 클래스와 각 단계를 나타내는 클래스 가운데 하나인 Collection 클래스는 subclassOf 관계를 가진다.

실제 증거 수집 프로세스가 진행되면 증거수집절차와 함께 다양한 정보가 필요하며, 이들 정보에 대한 클래스로 디지털 포렌식 온톨로지에서는 ProcessProperty 클래스를 두며, 이 클래스의 세부적인 구조는 (그림 4)에서 보여준다. 이 클래스는 언제 누가 어디에서 디지털 증거를 수집했는지에 대한 정보를 저장할 수 있는 클래스로 구성되어 있다. 따라서 ProcessProperty 클래스는 자문을 위한 전문가를 나타내는 SpecialList 클래스, 수사관을 나타내는 Investigator 클래스, 시간을 나타내는 Time 클래스 및 증거수집 장소를 나타내는 Location 클래스와 subclassOf 관계를 가진다.

(그림 4) 증거수집 표준 절차의 속성을 나타내는 클래스

Evidence 클래스와 Process 클래스는 다양한 형태로 나타나기 때문에 각 클래스에 적절한 형태 정보를 추가해야 하는데 이를 위하여 ClassType 클래스를 둔다. ClassType 클래스는 하위 클래스로 EvidenceClass와 ProcessType 클래스를 두고, 이들 클래스와 subclassOf 관계를 가진다. EvidenceClass 클래스는 이 온톨로지에서 다루는 디지털 증거의 타입을 individual로 등록하며, 등록된 각 individual은 (그림 5)에서 나열된 디지털 증거 모두를 설정한다. 또한 ProcessType 클래스는 경찰청의 프로세스 모델에서 정의된 절차들을 individual로 등록하되, 증거수집에 대해서는 휘발성(VolatileCollection)과 비휘발성(NonvolatileCollection)으로 구분하여 등록한다.



(그림 5) 디지털 증거와 처리 절차 클래스 타입을 위한 클래스와 individual 리스트

3.2 증거수집 처리절차 클래스

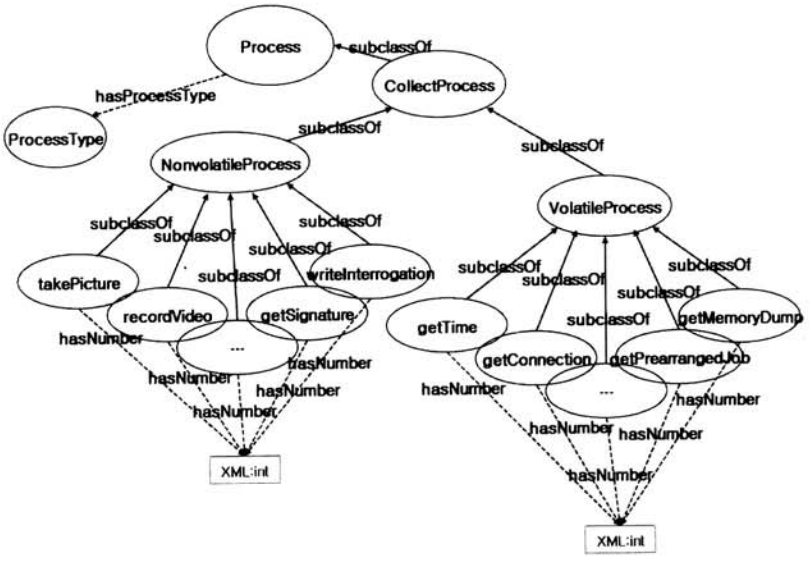
디지털 증거 처리를 위한 처리절차는 Process 클래스에서 정의하며, 증거수집에 대한 처리절차를 정의하기 위해서 CollectionProcess 클래스와 subclassOf 관계를 설정한다. 세부적인 클래스의 구조와 내용은 (그림 6)에서 보여준다. CollectionProcess 클래스는 하위클래스로 휘발성 증거수집 절차를 위하여 VolatileProcess 클래스를 정의하고 subclassOf 관계를 설정한다. 비휘발성 증거수집절차를 위하여 NonvolatileProcess 클래스를 정의하고 subclassOf 관계를 설정한다.

휘발성 증거수집절차는 경찰청의 포렌식 프로세스 모델에서 정의한 절차에 따르며, getTime 클래스부터 getMemoryDump 클래스까지 정의한다. VolatileProcess 클래스는 이들 각 클래스와 subclassOf 관계를 설정하여 하위클래스로 정의한다. 비휘발성 증거수집절차는 경찰청의 포렌식 프로세스 모델에서 정의한 절차에 따라서 showWarrent 클래스부터 writeInterrogation 클래스까지 정의한다. NonvolatileProcess 클래스는 이들 각 클래스와 subclassOf 관계를 설정하여 하위클래스로 정의한다. 비휘발성 증거 수집을 위한 모든 하위 클래스는 처리절차에 대한 각 클래스 간의 순서를 보여주는 (그림 7)에서 나타난다. 비휘발성 처리절차를 나타내는 각 클래스는 처리순서를 나타내기 위하여 XML:int 클래스와 hasNumber 관계를 설정하는데 이 수치는 각 절차가 처리된 순서를 정수로 나타내고, 이 값에 의하여 증거 수집 절차가 표준절차에 따라서 이루어졌는지를 검증한다.

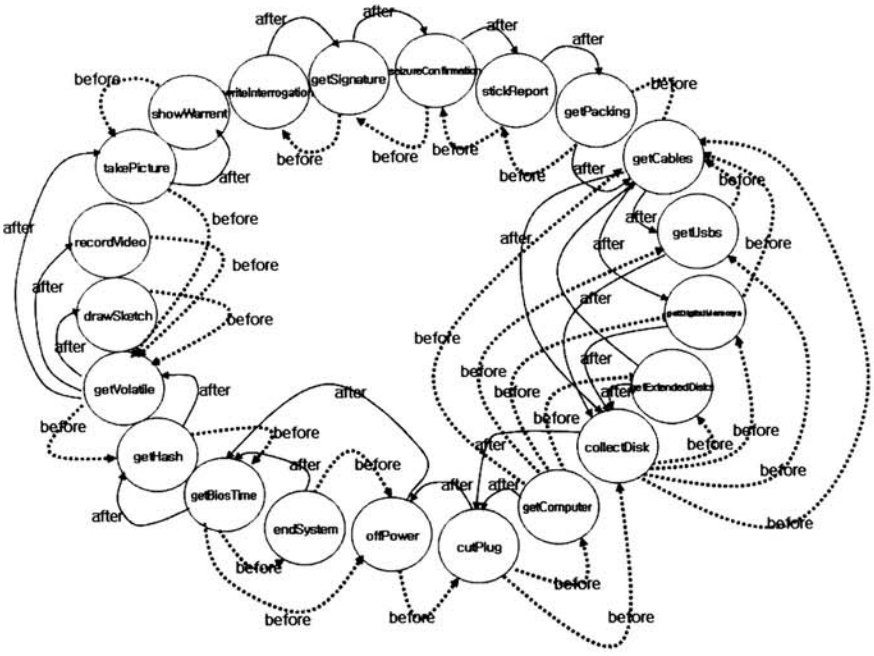
3.3 처리절차에 대한 순서검증과 검증규칙

증거수집 처리절차의 순서 검증은 각각의 처리절차 클래스간의 before/after 관계를 설정하여 구현한다. 증거 수집을 위한 처리절차는 (그림 7)과 같이 처리절차에 대한 각 클래스 간의 순서를 가진다.

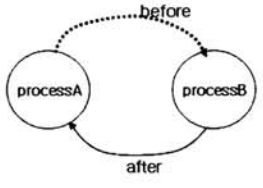
(그림 7)에 나타난 모든 처리절차 클래스는 경찰청에서 규정한 "디지털 증거분석 전문 매뉴얼"의 COL004 절차에 정의된 처리절차이며 이들 처리절차들은 필수적으로 나타나는 처리절차와 선택적으로 나타나는 처리절차로 구분된다. 필수적인 처리절차는 수집된 증거가 법적 증거능력을 갖추기 위하여 반드시 처리과정이 이루어져야 하는 절차이며, 만약 이를 생략할 경우 증거능력의 검증에 문제가 발생하는 처리절차이다. 선택적 처리절차는 해당 처리절차를 생략하여도 법적 증거능력의 검증에 문제가 되지 않는 처리절차를 말한다.



(그림 6) 증거수집의 처리절차의 클래스 구조



(그림 7) 증거수집 절차의 순서 검증을 위한 클래스의 property관계



(그림 8) 처리절차들 간의 전형적인 before/after 관계

필수적 처리절차와 선택적 처리절차를 포함하는 클래스들 간의 순서를 나타내는 전형적인 before/after 관계는 (그림 8)에서와 같이 나타나고, 이 관계에서 필수적인 process 클래스가 처리절차에서 나타나는 지를 검증하는 프로테제의 property에 대한 제약 규칙은 다음과 같이 정의한다.

[규칙 1]만약 processA가 선택적이고, processB가 선택적인 경우
before max n processB
after max n processA
[규칙 2]만약 processA가 필수적이고, processB가 선택적인 경우
before max n processB
after min n processA
[규칙 3]만약 processA가 선택적이고, processB가 필수적인 경우
before min n processB
after max n processA
[규칙 4]만약 processA가 필수적이고, processB가 필수적인 경우
before min n processB
after min n processA
각각의 규칙에서 숫자를 나타내는 n(≥1)은 처리 절차가 발생할 수 있는 최대 개수를 나타내며, 만약 하나만 발생해야 하는 경우는 exactly 1로 표기

이들 제약 규칙은 필수적인 처리절차에 대한 individual들이 나타나지 않는 경우 디지털 증거 수집 과정에 대한 individual들을 등록할 때 검증하게 된다.

4. 사례 연구

구축된 디지털 포렌식 온톨로지를 활용하여 증거수집 절차에 관한 법정에서의 증거능력을 검증하는 과정을 사례를 통하여 살펴보면 다음과 같다.

사례1 :

"2008년 11월 25일 13:00에 수사관 A, B는 사건번호 ○○○-A 사건의 증거물을 압수하기 위하여 부산광역시 해운대구 우1동 120번지 소재 ○○빌딩 3층의 312호실 (주)포렌식의 사무실에 도착하여, 영장을 제시한 후, 사무실 및 설치된 컴퓨터에 대하여 사진을 촬영하고 전원이 꺼져 있는 C 컴퓨터에 대하여 하드디스크를 안전하게 분리하여 보호박스에 개별 포장하여 돌아왔다."

사례1에 대하여 생성되는 각 클래스의 individual의 정보는 다음과 같다.

- showWarrent의 individual : 1001/NonvolatileCollection/1(Evidence:NONE)

이 individual은 "영장을 제시한 후"로부터 생성된 클래스 individual이며, 필수적인 처리절차이다.

- takePicture의 individual : 1002/NonvolatileCollection/2(Evidence:Image)

이 individual은 "사무실 및 설치된 컴퓨터에 대하여 사진을 촬영하고"로부터 생성된 클래스 individual이며, 필수적인 처리절차이다.

- collectDisk의 individual : 1003/NonvolatileCollection/3(Evidence:HDD)

이 individual은 "전원이 꺼져 있는 C 컴퓨터에 대하여

하드디스크를 안전하게 분리하여"로부터 생성된 클래스 individual이며, 필수적인 처리절차이다.

• getPacking의 individual : 1004/NonvolatileCollection/4 (Evidence:NONE)

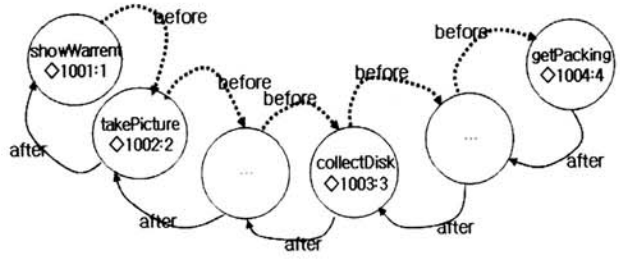
이 individual은 "보호박스에 개별 포장하여 돌아왔다"로부터 생성된 클래스 individual이며, 필수적인 처리절차이다.

이때 각 individual의 마지막 숫자 정보는 순서를 나타내는 정보이며, Evidence 정보는 이 처리과정을 통하여 생성되는 Evidence 클래스 individual의 EvidenceType 정보를 나타낸다. 이 예제의 처리절차에 대한 올바른 순서의 검증은 (그림 9)에서 나타난다. 각 처리절차에 대한 클래스에 생성된 individual의 순서정보와 before/after property의 transitive한 성질에 의하여 올바른 순서에 대하여 검증할 수 있다.

showWarrent 클래스 individual(1001)과 takePicture 클래스 individual(1002)은 [규칙 4]의 before exactly 1 takePicture와 after exactly 1 showWarrent가 적용되어 정상적으로 처리되고, 각 individual의 순서정보인 1과 2에 의해 before/after 관계가 성립한다. takePicture 클래스 individual(1002)과 collectDick 클래스의 individual(1003)은 [규칙 4]의 before min 1 collectDisk와 after exactly 1 takePicture가 적용되어 정상적으로 처리되고, 각 individual의 순서정보인 2와 3에 의하여 before/after 관계가 성립한다. (그림 7)의 before/after 관계에서 중간에 생략된 클래스의 individual은 before/after의 transitive한 성질에 의해서 성립한다. 마지막으로 collectDick 클래스의 individual(1003)과 getPacking 클래스의 individual(1004)은 [규칙 4]의 before exactly 1 getPacking과 after min 1 collectDisk가 적용되어 정상적으로 처리되고, 각 individual의 순서정보인 3과 4에 의하여 before/after 관계가 성립한다. 따라서 모든 처리절차에 대한 individual들의 before/after 관계가 정상적으로 성립하므로 증거능력을 검증할 수 있다.

사례2 :

"2008년 10월 16일 10:00에 수사관 ○○○은 사건번호 ○○○-B 사건의 증거물을 압수하기 위하여 부산광역시 동래구 온천2동 120번지 소재 ○○빌딩 203호실 (주)○○○○ 사무실에 도착하여, 영장을 제시한 후, 사무실 책상 서랍에 보관되어 있는 USB 메모리 스틱을 압수하여 보호박스에 개별 포장하여 돌아왔다."



(그림 9) 사례1에 대한 Process 클래스와 각 클래스의 individual과 순서 정보

사례2에 대하여 생성되는 각 클래스의 individual의 정보는 다음과 같다.

• showWarrent의 individual : 1005/NonvolatileCollection/1 (Evidence:NONE)

이 individual은 "영장을 제시한 후"로부터 생성된 클래스 individual이며, 필수적인 처리절차이다.

• getUsbs의 individual : 1006/NonvolatileCollection/2 (Evidence:USB)

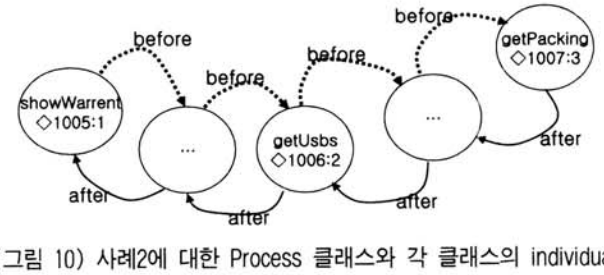
이 individual은 "USB 메모리 스틱을 압수하여"로부터 생성된 클래스 individual이며, 선택적인 처리절차이다.

• getPacking의 individual : 1007/NonvolatileCollection/3 (Evidence:NONE)

이 individual은 "보호박스에 개별 포장하여 돌아왔다"로부터 생성된 클래스 individual이며, 필수적인 처리절차이다.

사례2에 대한 Process 클래스와 각 클래스의 individual과 순서 정보는 (그림 10)과 같이 나타난다.

이 경우 증거수집 처리절차에 대한 증거능력의 검증을 위해 필수적인 showWarrent 클래스 individual(1005)과 필수적인 처리절차인 takePicture 클래스 individual 사이에 [규칙 4]의 before exactly 1 takePicture와 after exactly 1 showWarrent가 적용되어야 한다. before exactly 1 takePicture 규칙은 individual(1005)이 1개 존재하여 만족하나, after exactly 1 showWarrent 규칙은 takePicture individual이 존재하지 않아 규칙을 만족하지 않는다. 따라서 이 증거수집 절차는 takePicture 처리절차의 누락으로 인하여 증거능력을 검증받을 수 없다.



(그림 10) 사례2에 대한 Process 클래스와 각 클래스의 individual과 순서 정보

5. 결 론

정보화 기기의 활용과 인터넷 보급률의 급격한 증가로 인하여 사이버 범죄뿐만 아니라 일반 범죄에서도 디지털 증거를 통하여 범죄사실을 증명해야 하는 필요성이 증대되고 있다. 그러나 재판에서 디지털 증거는 그 증거능력에 대한 인증은 아직 논란의 대상이 되고 있다.

이미 디지털 증거에 대한 법률적인 체계와 법제에 관한

연구가 활발하게 이루어지고 있고, 디지털 포렌식의 표준절차에 대한 연구의 결과로 경찰청의 사이버 테러 대응 센터에서 디지털 증거분석을 위한 전문 매뉴얼이 발표되어 실제 디지털 증거 분석에 활용되고 있다. 이와 함께 디지털 증거의 증거 능력을 보증받기 위한 시스템적인 보완이 필요하다.

이 논문에서는 사이버 테러 대응 센터의 "디지털 증거분석 전문 매뉴얼"에 정의된 표준 처리절차를 이용하여 디지털 포렌식 온톨로지를 구축하고, 구축된 온톨로지를 이용하여 수집된 디지털 증거가 법정에서 증거능력을 획득하는데 하자가 없음을 검증하는 방법을 제안하였다. 이를 위하여 디지털 증거수집의 모든 절차에 대한 처리절차의 클래스를 정의하고, 이들 클래스들 간의 before/after 관계를 설정하고, 필수적인 처리절차를 검증하기 위한 제약규칙을 정의하였다. 또한 사례연구를 통하여 표준절차에 따른 디지털 증거가 제안된 방법에 의하여 적법한 절차를 거쳐 획득된 증거임을 검증함을 보였다.

향후 제안된 증거능력 검증방법에 활용된 디지털 포렌식 온톨로지는 디지털 증거의 증거능력에 대한 검증뿐만 아니라, 디지털증거에 대한 수사 계획의 수립 및 디지털 증거 수집에 대한 교육에 활용할 수 있다. 또한 경찰청의 "디지털 증거분석 전문 매뉴얼"에 정의된 모든 포렌식 절차를 온톨로지에 확장하는 것이 필요하다.

참 고 문 헌

[1] 2007년 상반기 정보화 실태조사, 한국인터넷진흥회, 2007.

[2] 이성진, "디지털 포렌식 기술발전방향," 디지털 포렌식 연구, 제1권, 제1호, 2007.

[3] 탁희성, "법정에서 디지털 증거의 허용가능성," 디지털 포렌식 연구, 제1권, 제1호, 2007.

[4] Prosise Mandia, Incident Response : Investigating Computer Crime, McGrawHill Osborne Media, 2001.

[5] 디지털 증거처리 표준 가이드라인, 경찰청, 2006. 12.

[6] 변정수, "한국형 디지털 증거분석 표준화:경찰청 디지털 증거처리 표준 가이드라인 및 증거분석 전문매뉴얼의 고찰," 디지털 포렌식 연구, 제1권, 제1호, 2007.

[7] Electronic Crime Scene Investigation: A Guide for First Responders, U.S. Department of Justice(DOJ) <http://www.ncjrs.org/pdffiles1/nij/187736.pdf>

[8] Mark Reith, Client Carr, and Gregg Gunsch, "An Examination of Digital Forensics Models," International Journal of Digital Evidence, Fall, 2002.

[9] 김정옥, "디지털 증거의 증거능력 인정요건-일심회 판결을 중심으로-," 디지털 포렌식 연구, 제1권, 제1호, 2007.

[10] 백승조, 심미나, 임종인, "국가 디지털 포렌식 법률 체계와 국내외 디지털 포렌식 법제 현황," 정보보호학회지, 2008. 2

[11] 이광열, 최윤성, 최해랑, 김승주, 원동호, "현행 증거법에 적합한 디지털 포렌식 절차," 정보보호학회지, 2008. 6.

[12] 양형정; 김경윤; 김수형 , "협업적 제품 설계를 위한 온톨로지 기반 시맨틱 조립체 모델링," 정보처리학회논문지B, Vol.13-B, No.2, pp.139-148, 2006. 4.

[13] 김종우, 김형도, 윤정희, 정현철, "기업간 비즈니스 프로세스 등록저장소를 위한 메타데이터 온톨로지 설계," 정보처리학회논문지D, 제14-D권, 제4호, 6월, 2007년, pp.435-446.

[14] 이신목, 장두성, 신지애, "자질별 관계 패턴의 다변화를 통한 온톨로지 확장," 정보처리학회논문지B, 제15-B권 제4호, 2008.

[15] M. Horridge, H. Knublauch, A. Rector, R. Stevens, C. Wroe. "A Practical Guide To Building OWL Ontologies Using The Building OWL Ontologies Using The Protégé-OWL Plugin and CO-ODE Tools," The Univ Of Manchester, 2007

[16] Heum Park, Hyuk-Chul Kwon, "Cyber forensics Ontology for the Cyber Crimal Investigation," Proceeding of E-FORENSICS 2009 - Int Conf on e-Forensic Applications and Techniques, 2009. 1.

[17] Hyuk-Gyu Cho, Heum Park, Hyuk-Chul Kwon, "Verification and Collection of Digital Evidence using Digital Forensics Ontology in Criminal Investigations," Proceeding of The 8th Application and Principles of Information Sciences, 2009. 1.

[18] A. Brinson. "A cyber forensics ontology: Creating a new approach to studying cyber forensics". Digital Investigation. 3S, 37-43, 2006.

[19] Victor Raskin, et al, "Semantic forensics: An application of ontological semantics to information assurance," 2nd Workshop on TEXT MEANING and INTERPRETATION, 2004. 7.

조 혁 규

e-mail : hgcho3@ysu.ac.kr

1988년 부산대학교 전자계산학과(학사)

1990년 부산대학교 전자계산학과(이학석사)

2009년 부산대학교 전자계산학과(박사과정)

1991년~1997년 창신대학 전산정보처리과 조교수

1997년~2003년 성심외국어대학 정보통신학부 교수

2003년~현 재 영산대학교 사이버경찰학과 교수

관심분야 : 온톨로지, 한국어정보처리, 디지털포렌식

박 흠

e-mail : parkheum2@empal.com

1988년 부산대학교 계산통계학과(이학학사)

1998년 부산대학교 인지과학협동과정(이학석사)

2005년 부산대학교 정보시스템공학(공학박사)

1988년~1990년 코닉시스템㈜

1990년~1998년 부산일보

현 재 부산대학교 인공지능연구실

관심분야 : 한국어정보처리, 정보검색, 유비쿼터스, 텔레메틱스

권 혁 철

e-mail : hckwon@pusan.ac.kr

1982년 서울대학교 전산학(학사)

1984년 서울대학교 전산학(석사)

1987년 서울대학교 전산학(박사)

1988년~현 재 부산대학교 전자전기정보 컴퓨터공학부 교수

1988년~현 재 한국정보과학회 프로그래밍언어 연구회 운영위원

1990년~현 재 한국정보과학회 한국어정보처리 연구회 운영위원

1992년~1993년 미국 Stanford 대학 CSLI연구소 연구원

1992년~1993년 Xerox Palo Alto Research Center 자문위원

2003년~2006년 2월 BK21 산업자동화 및 정보통신분야 인력양성사업단 단장

2004년~2007년 12월 한국정보과학회 이사

2004년~현 재 한국인지과학회 부회장

2007년~현 재 부산대학교 컴퓨터 및 정보통신연구소 소장

2008년~현 재 한국정보처리학회 영남지부장

관심분야 : 한국어정보처리, 정보검색, 프로그래밍언어, 인공지능, 시맨틱웹