Journal of The Korea Society of Computer and Information
Vol. 19, No. 12, December 2014
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2014.19.12.161

지능형 범죄수사 시스템을 위한 범용 디지털포렌식 온톨로지

윤 한 국*, 이 상 훈*

Digital Forensics Ontology for Intelligent Crime Investigation System

Han-Kuk Yun *, Sang-Hoon Lee*

요 약

디지털포렌식은 범죄와 관련된 디지털 증거를 수집, 분석하여 범죄혐의를 입증하는 과정으로 범죄수사에서 중요한 역할을 한다. 지금까지의 디지털포렌식 온톨로지에 대한 연구는 디지털포렌식을 사이버 관련 범죄에만 적용하였거나 디지털포렌식 자체의 절차와 기법에 관한 것으로 한정되었다. 본 연구에서는 다양한 유형의 범죄수사에서 디지털포렌식을 효과적으로 활용하기 위해 전반적인 수사절차와 디지털포렌식의 연관성을 분석하여 연계 모델을 설계하고 이를 바탕으로 디지털포렌식 온톨로지를 구축하였다. 온톨로지 구축시 포렌식 분석결과의 구체적인 활용 분야를 도출하여 반영하였고, 디지털포렌식의 절차 검증과 관련된 적법성 규칙, 분석 결과 활용과 관련된 적절성 규칙을 적용하여 의사결정지원이 가능하도록 하였다. 구축된 디지털포렌식 온톨로지는 다양한 범죄 유형에 적용 가능한 지능형 범죄수사 시스템 구축시 중요한 기반을 제공하게 될 것이다.

▸ Keywords : 디지털포렌식, 디지털포렌식 온톨로지, 범죄수사

Abstract

Digital forensics is the process of proving criminal charges by collecting and analyzing digital evidence which is related to the crime in question. Most digital forensic research is focused on digital forensic techniques themselves or cyber crime. In this paper, we designed a digital forensics-criminal investigation linked model in order to effectively apply digital forensics to various types of criminal investigations. Digital forensic ontology was developed based on this model. For more effective application of digital forensics to criminal investigation we derived specific application fields. The ontology has legality rules and adequacy rules, so it can support investigative decision-making. The ontology can be developed into an intelligent criminal investigation system.

▸ Keywords : Digital forensics, Digital forensics Ontology, Crime investigation

•제1저자 : 윤한국 •교신저자 : 이상훈
•투고일 : 2014. 9. 1, 심사일 : 2014. 10. 16, 게재확정일 : 2014. 11. 10.
* 국방대학교 컴퓨터공학과 (Dept. of Computer Science & Engineering, Korea National Defense University)

I. 서 론

범죄 양상의 다양화와 정보기술의 발달, 휴대용 디지털기기 대중화에 따라 범죄 수사에서 디지털 증거의 중요성이 증가하고 있다. 컴퓨터, 스마트폰, 태블릿 PC 등과 같은 디지털 기기에서 증거를 수집하고 분석하여 범죄 혐의를 입증하는데 사용하는 수사 방법을 디지털포렌식(Digital Forensics)이라고 한다[1]. 실제 범죄 수사 과정에서 디지털포렌식은 사이버 범죄 등과 같은 특정 사건뿐만이 아니라 살인, 강도, 사기 등 다양한 범죄에 활용되고 있으며 디지털포렌식을 통해 획득한 정보가 사건 해결에 결정적인 영향을 미치는 경우도 많다. 따라서 다양한 범죄유형에 대해 디지털포렌식을 적시적절하게 활용할 경우 보다 효과적인 수사가 가능하고 수사과정에서 자칫 누락될 수 있는 부분까지 검토할 수 있게 하는 역할을 해줄 것으로 기대된다. 또한 최근 수사환경은 범죄의 지능화와 더불어 인권보장, 적법절차의 준수 등 다양한 문제에 직면해 있으므로, 이러한 문제들을 해소하고 보다 효과적으로 수사를 진행하기 위해서는 다양한 유형의 범죄에 디지털포렌식을 효과적으로 활용하는 과학적인 수사방법이 필수적으로 요구되고 있다.

범죄수사에서 디지털포렌식의 영향은 증가하였으나, 특성상 전문적인 지식과 기술을 필요로 하기 때문에 디지털증거를 전문으로 다루는 분석관에게만 관련된 것으로 인식되어 왔으며, 따라서 수사에 참여하는 일반 수사 담당자들이 다양한 범죄 유형과 현장 상황에 따라 디지털포렌식을 수사 과정의 전반적인 절차와 연계하여 효과적으로 활용하지 못하고 있는 실정이다. 이에 따라, 범죄 현장에서 증거 수집시 다양한 디지털 증거가 누락되거나 적절하지 못한 방법으로 수집되는 경우도 있으며 획득한 디지털정보들이 적시적절하게 활용되지 못하는 경우도 있다. 디지털포렌식에 관한 연구는 다양하게 진행되고 있는데, 주로 특정 시스템이나 파일 조사 기법 등에 관한 연구에 집중되어 있다.

디지털포렌식에 개념적 연관 체계인 온톨로지(Ontology)를 적용시킨 사례를 디지털포렌식 온톨로지라 하는데, 디지털포렌식 온톨로지에 관한 연구는 디지털포렌식의 개념과 절차, 관련법규, 증거능력을 확보하기 위한 절차 등을 온톨로지로 구축하여 활용하는데 중점을 두었으며, 대부분 디지털포렌식 자체의 절차와 방법적인 측면을 주로 다루고 있고, 디지털포렌식의 대상 범죄도 사이버수사에 제한적으로 적용하고 있다[2,3].

본 연구에서는 다양한 사건 유형에 대한 범죄수사에 있어서 수사 전반의 과정에 디지털포렌식을 효과적으로 활용할 수 있도록 온톨로지를 구축하였다. 구축시 중점은 다양한 범죄유형에 디지털포렌식을 적용하는데 두었고, 온톨로지에 지식을 부여하기 위해 절차적인 측면과 활용적인 측면을 고려하였다. 절차적인 측면은 디지털포렌식의 전 과정에서 법률에서 규정한 절차가 누락되거나 절차상 오류가 없도록 하는 것이고, 활용적인 측면은 디지털포렌식의 전 과정을 수사절차와 긴밀하게 연계하여 포렌식 결과 획득한 다양한 정보를 범죄수사에 효과적으로 활용하는 것이다.

온톨로지 구축을 위해 위해 관련된 도메인을 범죄 수사 절차, 디지털포렌식, 법률 분야로 정하였다. 도메인 선정 후 다양한 범죄유형에 적용할 수 있는 표준화된 범죄수사절차를 제시하고, 이를 디지털포렌식 모델과 연계하여 상호 연관성을 분석하였다. 연관성 분석결과를 온톨로지에 반영시킴으로써 수사과정에서 체계적인 디지털포렌식 활용이 가능하도록 하였다.

디지털증거는 사건을 해결하기 위한 다양한 정보를 제공하기도 하지만 궁극적으로는 법정에서 증거로 제출되어야 하기 때문에 기술적인 측면 뿐만 아니라 법적으로 유효하게 하는 절차적 측면 역시 중요하다. 따라서 온톨로지 구축시 절차적 측면과 활용적 측면의 필수 조치사항들을 SWRL 규칙[2]으로 반영하여 수사절차의 적법성, 적절성 등을 검토할 수 있도록 하였다. 이러한 규칙은 수사 관계자들이 적절한 수사방향을 검토하고 판단하는데 도움을 줄 것으로 기대된다.

구축된 디지털포렌식 온톨로지는 다양한 방법으로 효용성을 검증하였으며, 이때 검증시 일관성 검사를 통하여 온톨로지 자체의 모순성을 검토하고, 사건 사례 적용을 통하여 온톨로지상에서 절차, 규칙들이 바르게 적용되는지 확인하였다. 디지털포렌식 온톨로지는 향후 다양한 사건 유형, 증거의 형태, 디지털포렌식 기술의 개발 등에 따라 기존 온톨로지에 새로운 온톨로지를 추가하거나 개념구조 수정시 보다 유연하게 대처할 수 있을 것이다. 또한 온톨로지 설계를 통하여 범죄수사간 디지털포렌식 절차나 활용 방법의 모순을 제거하고, 운용 개념을 보다 명확하게 정립할 수 있다.

본 연구의 공헌은 다양한 유형의 범죄에 대해서 디지털포렌식을 효과적으로 활용하기 위한 범죄수사-디지털포렌식 연계 모델을 제안하고 이를 온톨로지로 구축한 것이다. 또한 포렌식 분석결과의 구체적인 활용분야를 유형별로 구분하여 제시하였고, 디지털포렌식 절차 준수, 분석결과 활용의 적절성을 검토할 수 있는 규칙 반영을 통해 의사결정 지원이 가능

1) Semantic Web Rule Language (www.w3.org/Submission/SWRL)

하도록 하였다. 온톨로지는 지능형 범죄수사 시스템의 중요한 기반이 될 것이다.

논몬의 구성은 다음과 같다. 2장에서 디지털포렌식과 디지털포렌식 온톨로지에 대한 관련 연구를 소개하고, 3장에서는 범죄수사-디지털포렌식 연계 모델을 제안하고 이를 온톨로지로 구현하는 과정을 소개한다. 4장에서는 일관성 평가와 사례 적용을 통해 온톨로지의 효용성을 검증하고, 마지막으로 결론과 향후 연구에 대해서 제시하고자 한다.

II. 관련 연구

1. 디지털포렌식

디지털포렌식이란 디지털증거를 수집, 운반, 분석하여 범죄와 관련된 정보를 획득하고 법정에서 유죄의 증거로 사용하기 위한 일련의 과정을 말한다. 디지털포렌식이라는 용어는 1991년 미국 포틀랜드에서 열린 IACIS(International Association of Computer Specialists)에서 처음으로 사용되었다[1]. 디지털포렌식의 영역은 초기에는 사이버 범죄, 시스템 공격 등의 지능형 범죄에 주로 사용되었으나, 지금은 디지털증거와 관련있는 모든 사건 유형으로 그 영역이 확대되었다.

디지털포렌식은 범죄 수사의 일환으로 행하여지는 것이기 때문에 디지털증거를 수집하는 절차는 일반적인 증거물에 적용되는 법률 절차가 그대로 적용되며, 디지털 매체의 특성으로 인한 추가적인 조치가 필수적이다. 디지털포렌식의 대상이 되는 디지털 매체나 데이터는 비가시성, 변조가능성, 복제용이성, 휘발성의 특징이 있기 때문에[1] 최초 증거 수집에서부터 분석 및 보관까지 각 매체별 특징에 맞는 적절한 조치가 취해져야 하고, 이러한 과정과 절차가 준수되었다는 사실을 수사기관이 입증하여야 한다. 특히 디지털 증거는 전문 수사관 이외에도 다양한 사람들에 의해 취급되어질 수 있으므로 수집시 유의하여야 한다.

디지털포렌식에 관련된 연구 분야는 디지털증거수집과 관련된 절차적인 문제에 관한 연구와 다양한 디지털 데이터를 분석하는 기법에 관한 연구가 주류를 이루고 있다[4,5,6]. 디지털 증거를 분석하는 기법은 파일카빙, 키워드 검색, 타임라인 분석, 파일 포맷 분석, 암호 해독 등의 다양한 영역이 존재한다. 특히 최근에는 모바일 기기 등 다양한 저장매체의 대중화와 클라우드, 가상시스템 등의 등장으로 각각의 매체와 데이터의 유형에 따른 조사, 분석 방법에 대한 연구도 활발히 진행되고 있다[7,8,12].

2. 디지털포렌식 온톨로지

디지털포렌식(사이버포렌식) 온톨로지를 도입하여 절차적, 결과적 효용성을 향상 시키고자 하는 다수의 연구가 있다. Ashley Brison[9]는 사이버포렌식 온톨로지라는 개념을 정립하고 이를 통해 사이버포렌식을 연구하는 새로운 접근 방법에 대해서 연구하였다. 이 온톨로지는 포렌식 관련 분야를 6개의 상위 클래스로 구분하고 각각의 클래스에 관련된 분야를 세분화하여 표현하였다. 이 연구는 디지털포렌식의 전반적인 영역을 체계적으로 분류하였지만, 연구의 내용이 디지털포렌식에 대한 개념과 향후 활용 측면에 집중되어 있다. JHM Nogueira[10]은 역동적인 수사 환경에 대응할 수 있는 디지털포렌식 온톨로지를 구축하였고 이를 통해 복잡하고 다양한 디지털포렌식 수사 환경에 맞게 조직구성, 팀 편성, 임무분장 등에 대한 시스템적인 접근을 시도하였다. 그러나 주로 상황별로 포렌식 전문인력을 적절하게 배치하고 활용하는 측면에 중점을 두었다. HG Cho[2,3]은 사이버 범죄 수사 지원을 위한 디지털포렌식 온톨로지를 설계하였다. 온톨로지는 사이버 범죄를 대상으로 하여 사이버 포렌식 관련 용어를 분류하고 관련 영역을 연계하여 설계하였으며 구축된 온톨로지는 디지털 증거의 증거능력에 대한 검증, 사건 정보의 검색 확장 등의 기능을 지원하도록 하였다.

지금까지의 디지털포렌식 온톨로지에 관한 연구는 디지털포렌식의 절차에 관한 것이나 특정매체, 데이터 분석과 관련된 것이었으며, 디지털포렌식을 활용하는 범죄분야도 사이버 범죄, 컴퓨터 관련 범죄를 주로 대상으로 하였다. 본 연구에서는 다양한 범죄에서 디지털포렌식을 효과적으로 적용하고 활용하기 위해서 일반적인 범죄수사 절차와 연계하여 디지털포렌식의 절차적인 측면과 활용적인 측면에 중점을 두고 디지털포렌식 온톨로지를 구축하고자 한다.

III. 디지털포렌식 온톨로지 구축

디지털포렌식 온톨로지 구축은 도메인 분석, 표준절차 분석, 연관성 분석, 연계모델 생성, 규칙 반영, 온톨로지 구축 순으로 진행하였으며, 절차는 그림 1과 같다.

도메인 분석 단계에서는 디지털포렌식을 중심으로 연관관계가 있는 영역을 검토한 후 수사 절차, 법률 분야로 도메인의 범위를 한정하였다. 표준절차 분석단계에서는 표준화된 범죄 수사 절차와 디지털포렌식 절차의 모델을 구성하는 과정이다.

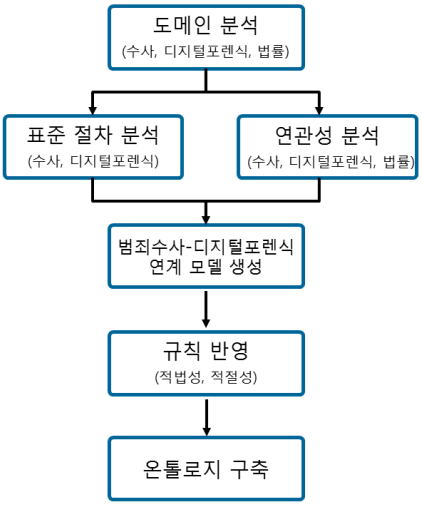

그림 1. 디지털포렌식 온톨로지 구축절차
Fig. 1. Development Process of Digital Forensic Ontology

범죄 수사 모델에서는 사이버 범죄와 관련된 분야 뿐만이 아니라 다양한 범죄에 적용이 가능하도록 일반적인 범죄수사의 절차를 검토하였다. 모델 구성을 위해 관련 법률과 검찰, 경찰 등 주요 수사기관의 범죄수사 매뉴얼을 토대로 표준화된 수사 절차를 도출하고 다양한 실무지식 요소들을 더하여 보완하였다.

디지털포렌식 절차는 경찰청 사이버테러대응센터의 디지털포렌식 가이드라인과 대검찰청 디지털 증거 수집 및 분석규정[11]에 제시되어있는 표준 디지털포렌식 절차를 기본으로 하고 실무에서 사용되는 다양한 규정, 절차 들을 적용하여 검토하였다. 또한 디지털포렌식 관련 판례와 개정된 형사소송법상의 디지털증거수집 관련 절차를 적용하고 실무에서의 경험적 지식을 더하여 모델을 구성하였다. 완성된 모델은 그림 2와 같다.

그림 2. 디지털포렌식 모델
Fig. 2. Digital Forensic Model

디지털포렌식 모델 중 포렌식 분석 결과의 활용 측면은 디지털포렌식 전문 수사관과 일반 수사관의 분리된 업무 영역을 연결하는 구심점을 하는 부분으로 디지털포렌식을 통해 획득된 정보가 범죄수사에 효과적으로 활용될 수 있도록 중점적으로 분석하였다.

연관성 분석 단계에서는 범죄수사 절차, 디지털포렌식 절차에 대한 검토와 더불어 각 영역의 상호 연관성을 분석하여 영역별로 수사 진행시 어떠한 연관관계가 있는지 확인하였다. 이를 토대로 범죄수사-디지털포렌식 연계 모델을 생성하였다. 모델 생성후 디지털포렌식 전문 분석관, 수사지휘자, 일선 현장 수사 실무자 등 분야별 전문가들로부터 의견을 수렴하여 모델에 대한 타당성을 검토하고 보완하였다.

연계모델을 설계하고 난 후 온톨로지에 지식을 부여하기 위하여 다양한 규칙들을 적용하였다. 적용규칙은 적법성 규칙과 적절성 규칙이다. 온톨로지에 규칙을 적용함으로서 추론 및 판정이 가능하여 수사활동간 의사결정 지원 역할이 가능하다. 마지막 단계는 온톨로지 구축 단계로 이전 단계에서 완성된 연계 모델과 규칙을 반영하여 온톨로지를 구축한다.

1. 범죄수사-디지털포렌식 연계 모델 생성

모델 구성은 디지털포렌식을 중심으로 하여 범죄수사의 각 단계별 중요 요소와 디지털포렌식 단계들의 연관성을 중점으로 하였으며, 디지털포렌식과 관련된 주요 판례, 실무 수사사례 등 을 이용하여 수사절차와 디지털포렌식 절차가 상호 보완적인 역할을 할 수 있도록 하였다. 완성된 범죄수사-디지털포렌식 연계모델은 그림 3과 같다.

범죄수사-디지털포렌식 연계 모델의 기능은 디지털포렌식의 적법절차 보장의 측면과 범죄수사간 디지털포렌식의 효과적인 활용 측면으로 구분할 수 있다. 적법절차 보장과 관련해서 법률과의 연계성에 중점을 두었고, 활용 측면은 디지털포렌식의 전반적인 과정을 범죄수사 절차와 연계하여 활용하는데 중점을 두었다.

디지털포렌식의 적법절차 보장의 측면은 디지털 증거의 증거능력과 관련된 개념이다. 증거능력은 증거가 엄격한 증명의 자료로 쓰이기 위해 갖추어야 할 자격을 말한다. 증거능력이 없는 증거는 범죄 사실을 인정하는 자료로서 사용할 수 없을 뿐만 아니라, 재판 과정에서 증거로서 제출하는 것도 허용되지 않는다. 증거능력의 유무는 법률의 규정에 따라 제시된 절차와 방법을 거쳐야 한다. 증거능력에 관한 규정은 디지털 증거에도 동일하게 적용된다. 따라서 디지털 증거를 정확하게 분석하여 다양한 정보를 획득하는 것 못지않게 적법한 절차와 방법을 따르는 것이 중요하다. 범죄수사-디지털포렌식 연계 모델에서는 디지털포렌식의 각 단계에서 준수되어야 할 절차

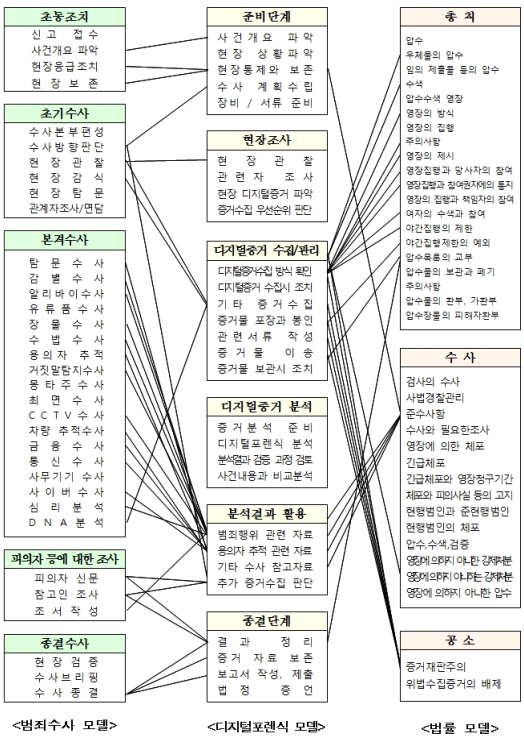

그림 3. 범죄수사-디지털포렌식 연계 모델
Fig. 3. Investigation-Digital Forensic Linked Model

와 조치들을 현행 형사소송법 조문과 연계하여 반영하였다.

디지털포렌식 활용 측면은 범죄수사간 디지털포렌식의 활용효과를 높이기 위한 것이다. 디지털포렌식은 범죄수사의 한 부분으로 실행되는 것이기 때문에 포렌식을 적시적절하게 활용하면 보다 효과적인 범죄수사를 진행할 수 있다. 본 연구에서는 디지털포렌식의 전체 절차 중에서 특히 분석결과 활용 분야를 중점적으로 검토하여 4가지 유형으로 구분하였고 구체적인 상관관계를 온톨로지에 프로퍼티 설정을 통해 반영하였다.

분석결과 활용 분야는 범죄행위 관련 자료, 용의자 추적 관련 자료, 기타 수사 참고자료, 추가 증거수집 판단으로 구분되어 진다. 범죄행위 관련 자료는 발생한 범죄에 대해 범죄사실 자체를 증명할 수 있는 자료를 의미한다. 이 자료는 수사절차의 각 단계 중 감별수사, 알리바이수사, 장물수사, 수법수사, 거짓말탐지 수사, CCTV수사, 심리분석, 조서작성 등과 밀접한 관련이 있다. 용의자 추적 관련 자료는 포렌식 분석결과를 바탕으로 용의자의 소재지나 발견 예상지역을 추측할 수 있는 정보를 의미한다. 용의자 추적 관련 자료는 탐문수사, 용의자추적, 차량추적, 금융수사, 통신수사, 사이버추적수사 등의 수사 단계와 연관되어 있다. 기타 수사 참고자료는 추가 범행에 관련된 자료, 용의자에 대한 공범 또는 조력자 존재여부, 기타 범죄나 용의자와 관련된 정보들을 뜻한다. 이 자료와 관련된 수사 절차 영역은 수사방향 판단, 관계자 조사/면담, 탐문수사 등이 있다. 추가 증거수집 판단은 포렌식 분석을 통해 추가적으로 획득 가능한 증거의 유무를 인지한 경우이다. 추가 증거수집 판단은 수사절차 영역의 수사방향판단, 피의자 신문, 참고인 조사 등의 영역과 관련이 있다. 디지털포렌식 분석결과의 유형에 따라 해당되는 범죄수사 절차의 수사 과정을 누락없이 검토하면 사건을 해결하는데 있어 디지털포렌식의 활용 효과를 증대시킬 수 있을 것이다.

2. 적법성, 적절성 규칙반영

구축된 온톨로지가 수사 활동간 효과적인 의사결정 지원을 할 수 있도록 적법성 규칙과 적절성 규칙을 반영하였다. 적법성 규칙은 디지털 증거의 수집과 분석, 보존의 과정에서 법률에 규정된 절차가 지켜졌는지 확인할 수 있는 규칙으로 법에서 규정된 증거의 증거능력과 관련된 것으로 수사활동간 엄격하게 지켜져야 할 과정이다. 적법성 판정 규칙은 SWRL 규칙을 사용하여 특정 절차를 만족하는 인스턴스들의 집합을 클래스로 생성되도록 하였고, 이를 통해 적법절차 준수 여부를 검증할 수 있도록 하였다. 온톨로지에 반영된 디지털 증거수집 관련 SWRL규칙은 총 16가지이며 예는 그림 4와 같다.

```
DEwarrant(?x)∧hasElaw(?x,?y)
    ∧hasNprocess(?x,?z) ⇒ ValidEvidenceProcess(?x)
DEcollection(?x)∧hasElaw(?x,?y)
    ∧hasNprocess(?x,?z) ⇒ ValidEvidenceProcess(?x)
DEtransfer(?x)∧hasElaw(?x,?y)
    ∧hasNprocess(?x,?z) ⇒ ValidEvidenceProcess(?x)
DEcustody(?x)∧hasElaw(?x,?y)
    ∧hasNprocess(?x,?z) ⇒ ValidEvidenceProcess(?x)
```

그림 4. 적법성 규칙
Fig. 4. Legality Rules

적절성 규칙은 디지털 증거분석을 통해 획득한 다양한 정보를 토대로 수사 절차와 관련된 정보를 적시 적절하게 활용할 수 있는가를 검토하는 것이다. 적법성 절차의 증거능력의 판단과는 다르게 이 절차는 실행 유무가 법률에 제한을 받지는 않으나, 수사 과정에서 적절하게 검토되지 않으면 수사의 효율성이 저해되는 상황이 발생할 수 있다. 따라서 온톨로지에 이러한 검토 과정을 확인할 수 있는 규칙을 적용하면 범죄수사에 활용 가능한 포렌식 정보의 활용여부를 판단할 수 있을 것이다. 적절성 판단을 위한 SWRL규칙은 총 15가지이

며, 예는 그림 5와 같다.

CrimeInfo(?x)∧hasCrimeInfoCheck(?x,?y)
∧hasAprocess(?x,?z) ⇒ AdequacyInveProcess(?x)
ExtraEvidence(?x)∧hasExtraEvidenceCheck(?x,?y)
∧hasAprocess(?x,?z) ⇒ AdequacyInveProcess(?x)
ExtraInfo(?x)∧hasExtraInfoCheck(?x,?y)
∧hasAprocess(?x,?z) ⇒ AdequacyInveProcess(?x)
SuspectInfo(?x)∧SuspectInfoCheck(?x,?y)
∧hasAprocess(?x,?z) ⇒ AdequacyInveProcess(?x)

그림 5. 적절성 규칙
Fig. 5. Adequacy Rules

3. 디지털포렌식 온톨로지 구축

범죄수사-디지털포렌식 연계 모델과 적법성, 적절성 규칙을 토대로 디지털포렌식 온톨로지를 구축하였으며, protege 4.3[1]을 사용하였다. 구축된 디지털포렌식 온톨로지의 클래스 계층도는 그림 6과 같다.

그림 6. 디지털포렌식 온톨로지 클래스 계층도
Fig. 6. Crime Investigation, Digital Forensic Class Hierarchy.

최상위 클래스는 디지털포렌식, 범죄수사, 법률, 발생사건 등 4개로 구성하였다. 디지털포렌식, 범죄수사 클래스는 각각의 단계별 조치사항들을 74개의 서브클래스로 구성하였다. 법률 클래스는 형사소송법의 조문 중에서 수사의 개시 및 진행, 증거수집과 관련된 내용을 중심으로 25개의 서브 클래스를 구성하였다.

프로퍼티 설정은 범죄수사-디지털포렌식 연계 모델의 상호 관련성을 바탕으로 연관된 클래스가 속성을 통해 연결되도록 하였으며 총 75가지의 연결이 존재한다. 표 1은 온톨로지에 반영된 속성의 일부를 나타내는 것으로 관련된 클래스와 속성의 성격에 따라 각각을 분류하였다.

표 1. 온톨로지에 반영된 속성 유형
Table 1. Property types of Digital Forensic Ontology

구 분	Domain	Range	Property
디지털 증거 수집/분석 절차 (적법성) (Nprocess)	디지털증거 수집방식 (DLmethod)	임의 제출물 등의 압수	hasLDmethod_1
		압수수색 영장	hasLDmethod_2
		영장에 의하지 아니한 압수	hasLDmethod_3
		위법수집증거의 배제	hasLDmethod_4
	디지털증거 수집시 조치 (DLprocess)	영장의 집행	hasLDprocess_1
		영장의 제시	hasLDprocess_2
		영장집행과 당사자의 참여	hasLDprocess_3
분석결과 활용 (적절성) (Aprocess)	범죄행위 관련 자료 (DlcrimeInfo)	감별수사	hasIDcrimeInfo_1
		알리바이수사	hasIDcrimeInfo_2
		장물수사	hasIDcrimeInfo_3
		수법수사	hasIDcrimeInfo_4
		거짓말탐지수사	hasIDcrimeInfo_5
		CCTV수사	hasIDcrimeInfo_6
		심리분석	hasIDcrimeInfo_7
	용의자 추적 관련 자료 (DlsuspInfo)	차량 추적수사	hasIDsuspInfo_1
		금융수사	hasIDsuspInfo_2
		통신수사	hasIDsuspInfo_3
		사이버수사	hasIDsuspInfo_4
		용의자 추적	hasIDsuspInfo_5
		탐문수사	hasIDsuspInfo_6

디지털 증거수집 및 분석절차와 관련된 속성은 디지털포렌식 클래스와 법률 클래스를 연결하는 것으로 적법성 규칙과 연계하여 증거수집 및 분석절차에 대한 제약조건으로 작용한다. 이를 통해 디지털포렌식의 필수 절차를 준수하도록 하는 기능을 한다. 분석결과 활용과 관련된 속성은 디지털포렌식 클래스와 수사절차 클래스를 연결하는 것으로 적절성 규칙을 통해 포렌식 결과를 수사절차에 효과적으로 반영할 수 있도록 하는 기능을 한다. 이외에도 다양한 속성을 반영하여 온톨로지가 디지털포렌식의 적법하고 효과적인 활용에 도움이 될 수 있도록 하였다. 그림 7은 온토롤지를 구성하는 모든 클래스가 각각의 특성에 해당하는 프로퍼티 설정을 통해 상호 연계되어 있는 관계성을 보여준다.

2) http://protege.stanford.edu/

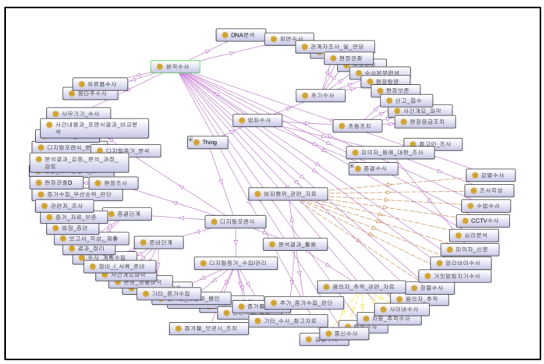

그림 7. 온톨로지 관계성 표현
Fig. 7. Ontology Relationship Representation

온톨로지에서 적법성, 적절성 판단 규칙은 Protege의 Rules을 이용하였다. SWRL규칙의 입력결과는 그림 8과 같다.

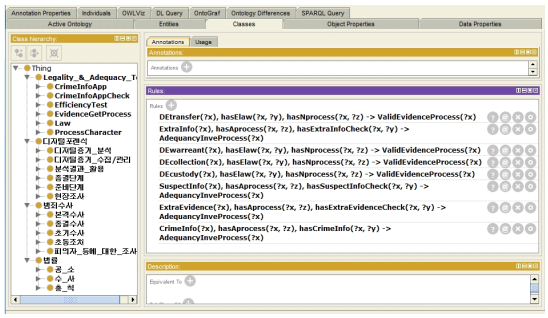

그림 8. SWRL 규칙 입력
Fig. 8. SWRL Rules Implementation

IV. 온톨로지 평가

1. 온톨로지 일관성 평가

구축된 온톨로지의 일관성을 검사하기 위해 OWL 추론 도구인 FaCT++[2]와 HermiT 1.3.7[3]을 사용하였다. 일관성 검사는 구축한 온톨로지의 클래스의 포함관계, 속성 연결의 모순성 등을 검사하게 되는데 이를 통해 온톨로지에 대한 공리적인 유효성을 확인할 수 있다. 검사결과는 그림 9와 같으며 클래스, 속성 구성에 모순이 없고 일관성있게 구축된 것을 확인할 수 있다.

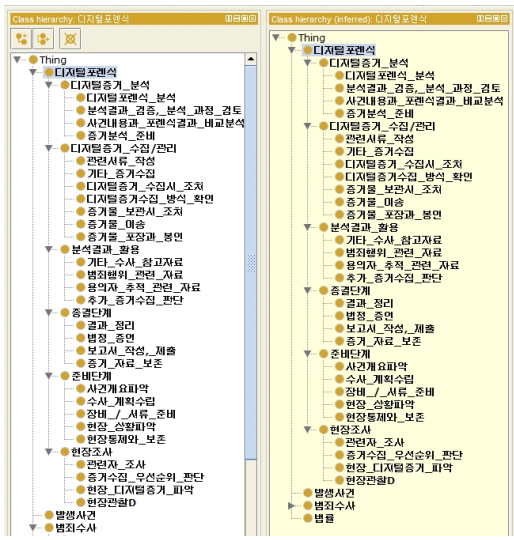

그림 9. 일관성 검사 결과
Fig. 9. Ontology Consistency Test Result

2. 사례적용을 통한 평가

구축된 디지털 포렌식 온톨로지를의 적법성, 적절성 규칙이 올바르게 적용되어 수사 의사결정 지원이 가능한지 확인하기 위하여 사례를 적용하여 온톨로지의 유효성을 검증하였다. 적용 사례는 실무에서 취급한 사건 사례 중 디지털포렌식을 활용한 대표적인 사건들을 일반화하여 구성하였다. 추론기는 Pallet 2.4.14[4]을 사용하여 SWRL기반 규칙들의 유효성을 검증하였다. 사례 적용은 증거수집 사례와 분석 사례를 적용하여 적법성 규칙과 적절성 규칙을 확인하였다.

사례1 : 증거수집

"20XX년 7월 12일 13:00에 수사관 A, B는 살인 사건에 대한 증거물 압수수색을 실시하였다. 압수수색 장소는 경기도 고양시 덕양구 소재 대성 아파트 102-203호이다. 증거수집을 위한 사전 준비단계를 거쳐 압수수색의 형태는 사전 영장에 의한 압수로 진행하였고 압수물을 용의자의 PC와 외장형 HDD 등의 디지털 증거였다. 수사관은 증거수집시 영장을 제시하고 기기의 작동상태 등을 확인하여 휘발성 증거수집, 일반 증거 수집 절차에 따라 증거를 수집하였다. 증거수집시 디지털증거수집 전용 용기를 이용하여 포장하였다. 증거수집의 모든 절차는 사진 촬영 및 동영상 촬영을 하였으며, 관련절차에 대해 문서로 기록을 하였다. 압수 후에는 압수목록을 교부하고 입회자의 확인과 함께 봉인을 하였고 증거물을 개봉할

3) http://owl.man.ac.uk/factplusplus/
4) http://hermit-reasoner.com/
5) http://clarkparsia.com/pellet/

때 입회할 수 있다는 사실을 고지하였다. 이 후 증거의 이송과 분석과정에서 연계보관성의 원칙과 무결성 유지를 위하여 담당관을 명시하여 증거의 훼손, 멸실을 방지하였고, 수집 이후 분석단계에서는 원본의 훼손을 방지하기 위하여 증거에 대하여 이미징 작업을 실시한 후 해쉬값을 생성하여 원본, 사본 동일여부를 확인하고 사본에 대해 분석을 하였다. 또한 증거의 수집부터 분석단계까지의 모든 단계에 대한 조치 과정을 기록하였다."

사건 사례를 통해 디지털증거수집/관리 클래스에는 증거수집 각 절차에 대한 individual이 생성된다. 디지털 증거수집 절차는 법률에 따라 엄격하게 적용되어야 하는 적법성 규칙에 해당되므로 적법성 규칙을 적용하여 증거 수집 절차의 각 단계가 적법성 규칙을 만족하는 ValidEvidenceProcess 클래스에 포함되는지 확인하면 디지털 증거수집 절차의 적법성을 판단 할 수 있다. 그림 10은 온톨로지 추론을 통해 사건사례에서 생성된 모든 수집절차 individual이 적법성 조건을 만족하는 ValidEvidenceProcess 클래스에 포함되는 것을 보여준다. 즉 사례에서 있었던 증거수집절차가 적법한 절차로 이루어졌음을 온톨로지 추론을 통해서 확인 가능함을 보여준다.

다음은 디지털증거 분석결과 활용과 관련된 적절성 검토를 위한 사례이다.

사례2 : 분석결과 활용

"사건 사례에서 수집한 디지털 증거에 대해 포렌식 분석을 한 결과 용의자의 PC에서 범행에 사용된 것으로 추정되는 도구들의 검색 결과가 확인되었으며, 용의자가 주로 접속하는 사이트의 목록을 확인할 수 있었다. 용의자는 주로 포털사이트와 게임 사이트에 자주 접속하였던 것으로 확인되었다. 포렌식 분석팀은 분석결과를 수사팀에게 전달하였고 수사팀에서는 디지털포렌식팀의 분석결과를 토대로 수사방향을 판단한 결과 PC내 검색결과를 참고로 용의자의 범행도구에 대한 범죄현장 추가 수색 및 구입장소 등에 대한 수사를 실시하고 범행현장 주변으로 탐문수사를 확대하였다."

분석 사례와 관련된 행위들은 individual 형태로 분석결과 활용 클래스에 생성된다. 분석결과 활용은 포렌식 분석결과를 수사절차에 효과적으로 활용하기 위한 것으로 법적으로 필수적인 절차는 아니지만 수사의 효율성을 위해서는 관련된 절차를 누락없이 검토하는 것이 바람직하다. 적절성 규칙을 만족하는 절차는 추론을 통해 AdequacyInveProcess 클래스의 individual 로 생성된다. 사례에서는 범죄행위 관련 자료와 기타 수사 참고자료가 있으므로 수사절차의 단계 중 관련된 모든 절차를 검토하는 것이 적절하지만 AdequacyInveProcess 클래스에는 탐문수사와 추가 증거수집관련 인스턴스만 등록되었다. 즉 장물수사, 수법수사, 통신수사, 용의자 추적 등과 같은 추가적인 수사절차 들이 누락되어 있음을 온톨로지 추론 결과 확인 할 수 있었다.

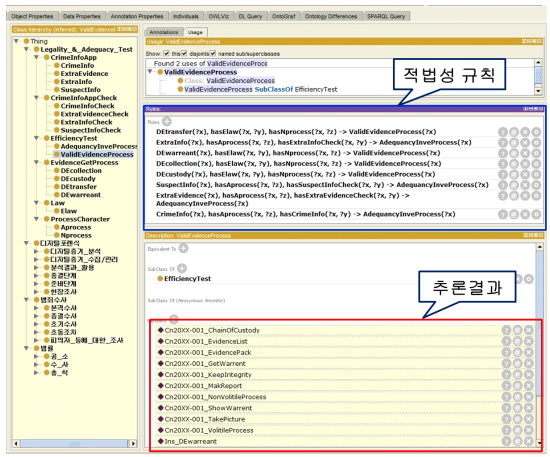

그림 10. 적법성 검사 결과
Fig. 10. Legality Test Result

V. 결 론

본 논문에서는 다양한 유형의 범죄 수사 과정에서 디지털포렌식을 효과적으로 활용하기 위한 디지털포렌식 온톨로지를 구축하였다. 온톨로지를 구축하기 위하여 도메인을 법률, 수사, 디지털포렌식으로 한정하였고 각 영역의 상호 연관성을 바탕으로 연계모델을 생성한 후 온톨로지에 속성과 규칙으로 반영하였다. 특히 범죄수사시 디지털포렌식의 활용성을 높이기 위해 포렌식 분석결과의 구체적인 활용분야를 유형별로 구분하여 제시하였고, 디지털포렌식 절차 준수, 분석결과 활용의 적절성을 검토할 수 있는 규칙 반영을 통해 수사활동간 수사관계자들이 의사결정을 하는데 도움을 줄 수 있도록 하였다.

구축된 온톨로지는 구축절차 및 단계별 모델에 대해 각 영역별 전문가가 검증하였으며, 구체적인 사례를 통하여 효용성을 검증하였다. 향후 범죄수사, 디지털포렌식 기법 발전에 따른 유연한 모델 보완과 구축된 온톨로지를 실무에 적용하기 위한 시스템 구현에 대한 추가적인 연구가 필요하다.

참고문헌

〔1〕 SJ Lee, "Introduction to Digital forensics", Iroon, 2010.

〔2〕 HG Cho, "Design of forensics domain ontology for knowledge based cyber criminal investigation", Pusan University, 2009

〔3〕 HG Cho, H Park, HC Kwon, "The Method of Verification for Legal Admissibility of Digital Evidence using the Digital Forensics Ontology", journal of korea information processing society, v.16-D, no.2, 2009

〔4〕 KH Cho, "Improvement of the Issues in Search and Confiscation of Digital Evidence", Seoul Law Review, V.21, No.3, 2014

〔5〕 YH Kim, "The problem point and improvement program of the scene search and seizure of digital evidence at practical affairs", Journal of the Korea Institute of Information and Communication Engineering, V.17, No.11, 2013

〔6〕 BS Kwack, "A study on Problems and improvements of digital forensic investigation", Law Review, V.42, 2011

〔7〕 SH Jang, "Digital Forensic Investigation of Virtual Desktop Infrastructure", Journal of the Korea Institute of Information Security and Cryptology, v.23 no.2, 2013

〔8〕 SH Park, "Technology Trend on Image File Carving", Journal of the Institute of Electronics and Information Engineers, v.37 no.1, 2014

〔9〕 Ashley Brison. "A cyber forensics ontology: Creating a new approach to studying cyber forensics", Digital Investigation. 3S, 37-43, 2006.

〔10〕 JHM Nogueira, "Ontology for Complex Mission Scenarios in Forensic Computing", In proceedings of the 2nd International Conference of Forensic Computer Science, Guarujá: Brazil, 2007

〔11〕 Confiscation and analysis rules for digital evidence, SPO, 2012. 11.

〔12〕 IS Kim, "Implementation of an Android Smart phone Forensic Tool Based on Logical Analysis", Journal of The Korea Society of Computer and Information Vol. 16, No. 4, April 2011

저 자 소 개

윤 한 국

2003: 육군사관학교
영어과 문학사
현 재: 국방대학교
컴퓨터공학과 석사과정
관심분야: 디지털포렌식, 온톨로지, 데이터마이닝
Email : korea6459@gmail.com

이 상 훈

1978: 성균관대학교
정보통신공학과 공학사.
1989: 연세대학교
산업대학원 전산학과 공학석사.
1997: 일본 교토대학교
정보공학과 공학박사
현 재: 국방대학교
컴퓨터공학과 교수
관심분야: 정보검색, 멀티미디어, DB, 빅데이터
Email : hoony@kndu.ac.kr