기록보관소 전자기록물의 증거능력 확립을 위한 디지털 포렌식 적용 연구

유형욱*, 손태식*, 박지혜**, 김상국**
*아주대학교 컴퓨터공학과, **국가기록원
e-mail:{cielo1025, tsshon}@ajou.ac.kr, {rosin, southkang}@korea.kr

An Approach for Electronic Records Management using Digital Forensics

Hyunguk Yoo*, Taeshik Shon*, Ji Hye Park**, Sang Kook Kim**
*Dept. of Computer Engineering, Ajou University,
**National Archives of Korea

요 약

이 연구에서는 전자기록물의 일반적인 특징과 법적 증거능력에 대해서 조사하고 이를 통해 국가기록원을 비롯한 기록보존소에서 관리하는 전자기록들의 증거능력에 대해 고찰하였다. 또한 디지털 증거를 수집·분석하여 법정에 제출하기 위한 분야인 디지털 포렌식(Digital Forensics)에서의 절차 및 기술을 통해 전자기록관리 프로세스에서 전자기록의 증거능력을 확보하기 위한 기초적인 방안을 제시한다.

1. 서론

현대는 정보기술의 발달로 인해 매일 엄청난 양의 정보들이 디지털 방식으로 생산·저장되고 있다. 기존 국가기관 및 기업 업무에서 종이문서의 형태로 보존되던 많은 정보들도 업무 효율성 등의 이점에 따라 전자적 형태로 변환이 되고 있으며, 이에 따라 이러한 전자기록의 안전한 보관 및 관리가 기록관리 분야에서의 중요한 이슈가 되었다. 기록 관리의 주요 목적 중 하나는 기록의 진본성 및 무결성 측면에서 처음 생성된 시점의 기록과의 동일성을 증명하고, 추후 그 기록이 법적 증거로 제출될 경우 사법적 구속력을 가질 수 있게 하는 것이다. 그러나 전자문서의 경우 기록의 복제 및 위·변조가 용이하기 때문에 사법적 구속력을 가지기 위한 여건이 중요한 이슈가 되었다. 한편, 디지털 포렌식(Digital Forensic)은 수사 기관에서 수집한 디지털 정보가 법정에 제출되기까지 변경되지 않았음을 증명하기 위해 만들어진 일련의 절차 및 기술들로 과거에는 범죄수사, 민·형사소송, 침해사고 중심으로만 활용되었지만 근래 기업의 산업유출방지 및 보안감사, E-Discovery에 사용되는 등 적용분야가 확대되고 있다.

최근에는 기록관리 분야에서도 전자기록의 진본성, 무결성을 확보하기 위한 디지털 포렌식 기법 적용 연구가 일부 이루어지고 있다[1][2][3][4]. 이 논문의 2장에서는 먼저 전자기록의 특징과 법적 증거능력에 관련된 이슈를 소개하고, 3장에서는 전자기록관리 프로세스에서 증거의 신뢰성과 관련한 취약점을 분석하였다. 이어서 4장에서는 디지털 포렌식 절차 및 기술에 대해 살펴보고, 5장에서 전자기록관리에서 디지털 포렌식 기법을 적용하여 전자 기록물의 신뢰성 및 진본성을 확보하는 방안을 제시한다.

2. 전자기록물의 특징과 법적 증거능력

2.1 전자기록물 특징

전자기록물은 넓은 의미로 전기와 자기신호를 이용하여 매체에 저장된 기록물들을 총칭하며, 이는 아날로그 방식의 매체(비디오테이프, 녹음테이프 등)에 기록된 것과 디지털 방식의 매체(HDD, Flash Memory, DVD 등)에 기록된 것 모두를 포함한다. 하지만 대량 복제 가능성, 용이한 위·변조 취약성 등은 디지털 방식의 기록에 국한되기 때문에 이 논문에서는 디지털 방식으로 저장된 전자기록물에 대해서만 고려한다.

디지털 방식으로 기록된 전자기록물은 기본적으로 매체독립성, 비가독성, 취약성, 대량성, 전문성 등의 특징을 가진다.[1] 이 중에서 취약성은 디지털 증거가 삭제·변경이 용이한 특징을 나타내는데, 예를 들어 특정 워드 파일을 열어보는 것만으로도 파일 속성이 변경되어 원본과 다른 파일이 되기 때문에 여기에서 디지털 증거에 대한 무결성 문제가 대두된다.

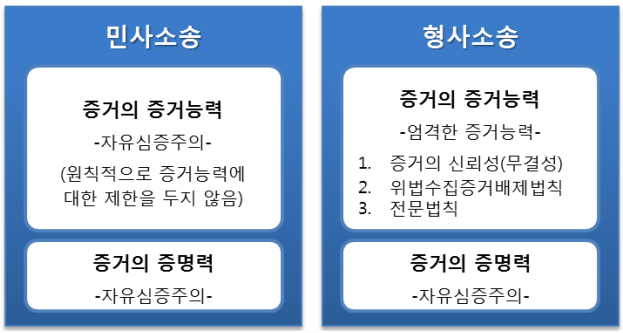
2.2 전자기록물의 법적 증거능력에 관한 이슈

증거란 사실인정의 근거가 되는 자료를 말하는데, 이때 증거가 실질적 증거로 사용되기 위해서는 형식적·객관적인 법률상의 자격을 뜻하는 증거능력과 증거의 실질적 가치를 의미하는 증명력이 있어야 한다. 증명력은 사실상 법관의 자유심증에 의해 판단되지만(자유심증주의), 증거능력은 법률에 의해 규정되어 객관적 구속력을 지닌

· 이 논문은 행정안전부 국가기록원 재원으로 2012년 기록보존기술 연구개발사업의 지원을 받아 수행된 연구임.

1) 장상귀, “디지털증거의 증거능력에 관한 연구”, 2008

다. 민법에서는 증거능력에 대해 원칙적으로 제한을 두고 있지 않지만, 형법에서는 위법수집배제법칙(제308조의2), 전문법칙(형사소송법 제310조의2), 증거의 신뢰성 등 엄격한 증거능력 요건을 요구한다(그림 1). 위법수집배제법칙은 적법한 절차에 따르지 않고 수집한 증거에 대해 증거능력을 인정하지 않는 것으로, 증거 수집 시 형사소송법 제106조(압수)에 위배되지 않아야 함을 의미한다. 정보저장매체의 경우 2011년 7월 개정안에 따라 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 전문법칙은 원진술자가 공판기일에 행한 진술 이외의 진술(전문증거)에 대해 증거능력을 인정하지 않는 것으로, 그 이론적 근거에는 신용성의 결여가 있는데 이는 그 진술 내용의 진정함이 증명되지 않는다고 판단하는 이유이다. 다만, 형사소송법 제313조에서 진술서의 경우 작성자 또는 진술자의 자필이거나 그 서명 또는 날인이 있는 것에 한하여 그 성립의 진정함이 증명된 때에는 증거로 할 수 있다고 규정하고 있는바, 이 규정을 엄격하게 적용하면 전자기록물의 형식적 진정 성립을 인정하기 위해서는 작성자의 서명·날인이 반드시 있어야 한다. 하지만 전자기록물의 경우 일반 종이문서에서와 같은 자필 또는 서명·날인을 기대할 수 없기 때문에, 이와 관련하여 전자서명법 제3조에서 '다른 법령에서 문서 또는 서면에 서명, 서명날인 또는 기명날인을 요하는 경우 전자문서에 공인전자서명이 있는 때에는 이를 충족한 것으로 본다' 규정하고 있다.



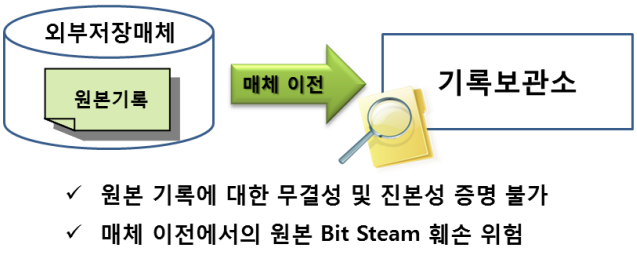
(그림 1) 민·형사 소송에서의 증거능력과 증명력

위법수집증거배제법칙, 전문법칙과 관련하여 증거능력 요건을 확립하였어도, 증거의 신뢰성과 관련하여 조작의 가능성이 있는 경우 증거로 채택될 수 없다. 특히 전자기록물의 경우 위·변조에 취약하기 때문에 일반 종이문서에 비해 신빙성이 낮게 평가될 가능성이 높으며, 일반적으로 증거능력을 가지기 위해 엄격한 잣대가 요구된다.

3. 전자기록관리에서의 취약점 분석

현재 국가기록원을 비롯하여 도서관, 박물관 등 기록보존소에서는 가치 있는 여러 형태의 기록들을 보관하고 있다. 최근에는 IT 기술의 발전에 따라 전자 기록의 수가 급격히 증가하고 있는 추세이기 때문에 이러한 전자기록들이 앞서 살펴본 바와 같은 증거능력을 갖추고 있는지 여부는 기록관리 측면에서 중요한 이슈이다[2].

기록보존소에서 전자기록을 기록 생산자(또는 기증자)로부터 기록을 수집할 때는 필연적으로 원본 매체에로부터 보존 매체로의 매체 이전(migration)이 발생한다. 이때 단순히 파일 또는 디렉토리를 복사(Copy)하는 경우, 사람이 가시적으로 파악할 수 있는 정보는 그대로 복사되지만 눈에 보이지 않는 원본 데이터의 비트 스트림(Bit Stream)은 변화하게 된다. 또한, 이러한 방법으로 매체 이전할 경우 파일의 최근 수정 날짜와 같은 메타 데이터 정보가 변화하게 되고 원본 매체에서의 파일 시스템과 보존 매체의 파일 시스템이 불일치 할 경우 파일 이름 등의 정보도 변경될 수 있다. 또한, 전자기록의 경우 고의적인 기록 위변조 또는 의도치 않은 행동에 의한 비트 변화가 일어나기 쉽기 때문에 기록의 신뢰성과 무결성을 증명할 수 없고, 이에 따라 법적 증거 능력과 관련하여 신뢰성을 기대할 수 없다.



(그림 2) 매체 이전(Migration)에서의 문제점

4. 디지털 포렌식(Digital Forensc)

디지털 포렌식은 디지털 증거에 대해 수집·분석하고 법정에 제출하기까지의 일련의 절차 및 기술들을 포괄하며, 증거의 무결성 및 진본성을 유지하여 증거능력을 인정받기 위함이 주요 목적이다. 소위 일심회 사건으로 유명한 판례[3]에서는 디지털 포렌식 절차를 통해 수집·분석한 일부 증거에 대해 그 증거능력을 인정한 바 있다.

4.1 디지털 포렌식 절차

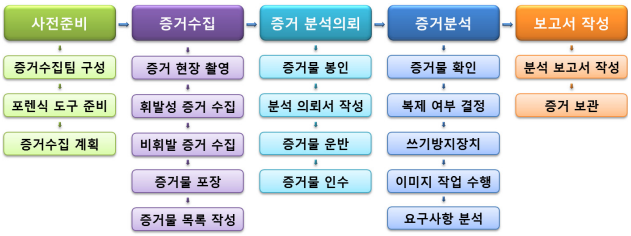
디지털 포렌식 절차는 디지털 증거의 준비·수집·분석·제출까지의 일련의 과정으로 해외 모델로는 DFRWS 모델, Casey 모델 등이 있으며 국내 모델로는 2007년 TTA에서 제정한 가이드라인(TTA.KO-12.0058)과, 대검찰청 및 경찰청에서 사용하는 디지털증거 처리 모델 등이 있다. 아래 (그림 3)은 경찰청 디지털 증거 처리 모델[4]을 도식화 하고 있으며, 기본적으로 사전준비, 증거수집, 증거 분석의뢰, 증거분석, 보고서 작성의 5단계로 나누어진다. 모

2) ISO 15489 (국제기록관리지침)에서는 기록 관리의 중요한 주요 목적은 증거적 가치 보호에 있다고 표명하고, 기록물(또는 전자기록물)이 갖추어야 할 4대 요건으로 진본성, 무결성, 신뢰성, 이용가능성을 제시

3) 대법원 2007.12.13., 선고, 2007도7257

4) 경찰청, "디지털증거 처리 표준 가이드라인", 2006

든 단계에서의 엄격한 절차 수행이 이루어져야 되지만 증거의 신뢰성에 관한 기술적 측면에서 중요하게 고려되는 부분은 증거 수집 단계에서 어떻게 원본 데이터의 무결성을 증명할 것인지와 증거 분석 단계에서 어떻게 비가시적인 디지털 데이터로부터 의미 있는 정보를 도출해 낼 것인지 이다.



(그림 3) 경찰청 디지털증거 처리 표준 절차

4.2 디지털 증거 수집 기술

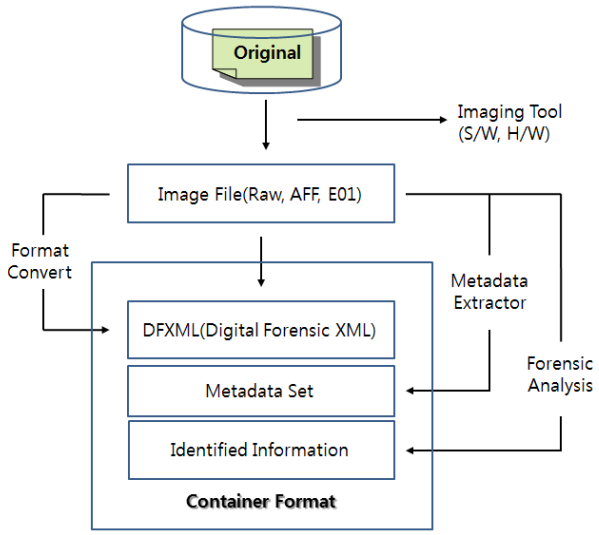
디지털 증거의 수집은 휘발성 증거의 수집과 비휘발성 증거의 수집으로 나눌 수 있다. 휘발성 증거의 수집은 활성 시스템을 조사할 경우 필요할 수 있는데, 물리 메모리(RAM)로부터 네트워크 연결 정보, 실행 중인 프로세스 정보 등을 수집하는 것을 의미한다. 비휘발성 증거의 수집은 HDD, SSD, Flash Memory, ODD와 같은 비휘발성 매체로부터 이미징(Imaging) 도구를 통해 비트 스트림을 그대로 가져오는 것이다. 이미징 작업을 수행하기 전에 쓰기 방지장치(writeblock)를 연결하여 수집 매체의 정보 변화를 방지한다. 이미징에 사용되는 도구는 크게 하드웨어 방식(Image MASSter Solo-4, Rapid Image , Road MASSte) 또는 소프트웨어 방식(FTK Imager, Tableau Imager, Encase, linux-dd)으로 구분할 수 있다. 이러한 도구들은 이미징 작업 시 이미지 파일에 대한 해쉬값(Hash Value)을 선택적으로 생성할 수 있기 때문에 추후 법정에 제출될 시 무결성을 증명할 수 있다.

4.3 디지털 증거 분석 기술

디지털 증거 분석은 수집한 이미지 파일로부터 의미 있는 정보를 도출해내는 작업이다. 기본적으로 디스크 브라우징, 파일 검색, 타임라인 분석, 통계 분석, 시각화, 로그 분석, 파일 복구[5] 등의 기술이 사용되며 시중에 Encase v7(Guidance 社), FTK v4.0(Access Data 社) 등의 상용 분석 도구가 많다.

5. 전자기록관리 프로세스에서 DF 적용 방안

디지털 포렌식 분야에서 사용하는 이미징(Imaging) 기술, 데이터 분석 기술 등은 전자기록관리 프로세스에 발생하는 무결성 문제를 해결하는데 적용될 수 있다. 이 논문에서는 이에 대한 적용 방안으로 디지털 포렌식에서의 디스크 이미징(Imaging) 기법을 통해 원본 비트스트림의 진본성을 유지하며, 원본 비트스트림의 변화가 생겼을 때 이를 감지하거나 또는 복구할 수 있는 정보를 추가함으로써 원본 기록의 무결성을 보장한다. 또한, 추출한 이미지 파일로부터 디지털 포렌식 분석 도구를 통해 분석하고 의미 있는 정보를 도출하여 이미지 메타데이터 집합(Metadata Set)과 함께 하나의 컨테이너(Container)로 관리한다. 그리고 기존 기록관리 프로세스에서 사용되는 문서보존포맷 또는 장기보존포맷 등과의 호환성을 위해 컨테이너 안의 정보를 XML 형태로 관리함을 요구한다. 다음 그림은 제안하는 방법에 대한 개략적인 구조를 나타낸다.



(그림 4) 매체 이전(Migration)에서의 디지털 포렌식 적용

6. 결론

이 논문에서는 기록보존소에서 관리되는 전자기록들의 증거능력 여부에 대해 살펴보고, 증거의 신뢰성과 관련된 문제점을 살펴보았다. 또한 디지털 포렌식 기법을 통해 전자기록의 무결성을 유지할 수 있는 기초적인 방안을 제시하였다. 추후 이를 확장하여 실제 국가기록원 등의 기록관리소의 전자기록관리 프로세스에 적용할 수 있는 구체적 방안에 대한 연구가 필요하다.

참고문헌

[1] Matthew G. Kirschenmaum, “Digital Forensics and Born-Digital Content in Cultural Heritage Collections”, 2010

[2] Kam Woods, “Extending Digital Repository Architectures to Support Disk Image Preservation and Access”, 2011

[3] 장상귀, “디지털증거의 증거능력에 관한 연구”, 2008

[4] 대법원 판례, 2007도7257, 2007

[5] 경찰청, “디지털증거 처리 표준 가이드라인”, 2006

[6] 이상진, “디지털 포렌식 개론”, 2010

[7] 이광열 외 5인, “현행 증거법에 적합한 디지털 포렌식 절차”, 정보보호학회지, 2008

5) 이상진, “디지털 포렌식 개론”, 2010