情報保護學會論文誌
第 23 卷 第 2 號, 2013. 4

디지털 포렌식 기법을 적용한 전자기록물 관리기술 고도화 연구*

유 형 욱,[1†] 손 태 식[2‡]
[1]아주대학교 컴퓨터공학과, [2]아주대학교 정보컴퓨터공학과

Research on Advanced Electronic Records Management Technology Using Digital Forensics*

Hyunguk Yoo,[1†] Taeshik Shon[2‡]
[1]Division of Computer Engineering, Ajou University
[2]Division of Information Computer Engineering, Ajou University

요 약

디지털 방식으로 생산·저장되는 기록들이 급증함에 따라 이러한 디지털 기록들을 수집·보존·관리하는데 있어 신뢰성 및 무결성을 유지하고 이를 통해 법적 증거로써의 가치를 보장하는 것이 중요한 이슈가 되었다. 본 논문에서는 국내 형사 소송법 및 기록관리 법령을 토대로 현재 국가기록원에서 관리하고 있는 전자기록물의 사법적 증거능력에 대해 고찰하고 이에 대한 문제점을 도출하였다. 또한 본 논문에서 도출된 문제점을 해결하기 위해 디지털 포렌식 (Digital Forensics) 절차 적용 및 해시값 활용 방안을 제시한다.

ABSTRACT

Recently, according with a sudden increase of records produced and stored by digital way, it becomes more important to maintain reliability and authenticity and to ensure legal effect when digital records are collected, preserved and managed. On the basis of domestic legal procedure law and record management-related legislation, this paper considered judicial admissibility of evidence on electronic records managed by National Archives of Korea and drew potential problems when these are submitted to court as a evidence. Also, this paper suggested a plan applying digital forensics technique to electronic records management to ensure admissibility of evidence about electronic records stored in National Archives of Korea.

Keywords: Digital Forensics, Electronic Records Management, National Archives of Korea, Admissibility of Evidence

I. 서 론

IT 기술의 발전과 급격한 정보화 사회로의 변화는 정보의 디지털화를 가속시켰고 그 결과 많은 양의 데이터를 손쉽게 저장하고 관리할 수 있는 능력을 갖추게 되었다. 특히 보존 가치가 높아 국가차원의 기록화가 필요한 중요 정보들 역시 많은 부분 디지털화 되어 국가기록원에 저장되고 있다. 이러한 중요 기록물들은 국가기록원에서 자체 디지털화하기도 하지만 다수의 출처로 부터 생성되어 국가기록원으로 이관되기도 한다. 전자기록물의 생산부터 이관, 보존, 활용 전 단계에 있어 전자기록의 진본성, 무결성, 신뢰성을 보장하고 이에 따라 증거적 가치를 확립하는 것은 기록 관리

접수일(2012년 11월 29일), 수정일(2013년 3월 7일), 게재확정일(2013년 3월 19일)
* 이 논문은 행정안전부 국가기록원 재원으로 2012년 기록보존기술 연구개발사업의 지원을 받아 수행된 연구임
† 주저자, cielo1025@ajou.ac.kr
‡ 교신저자, tsshon@ajou.ac.kr

의 주요 목적 중 하나이다(ISO 15489). 특히 국가기록원은 보존 가치가 높은 기록들을 국가차원에서 보존 및 관리 하고 있기 때문에 이러한 기록의 진본성, 무결성, 신뢰성 확보는 필수적이다.

디지털 포렌식(Digital Forensics)은 전자 증거물을 사법기관에 제출하기 위해 데이터를 수집, 분석, 보고하는 일련의 작업으로 전자 증거물의 무결성과 신뢰성을 확보한다는 측면에서 전자기록 관리에서 앞서 살펴본 목적들과 유사하다. 본 논문에서는 국가기록원에서 관리하고 있는 전자 기록물들의 사법적 효력에 대해 고찰하고, 디지털 포렌식 기법을 적용하여 전자기록물의 무결성 및 신뢰성을 보장하는 방안에 대해 살펴본다. 본 논문의 2장에서는 국내 민·형사 소송법을 토대로 전자기록이 증거능력을 갖추기 위해 필요한 요소를 살펴보고, 3장에서는 국가기록원에서 관리하는 전자기록물에 대한 증거능력 여부를 고찰한다. 4장에서는 디지털 포렌식을 적용한 전자기록 관리 연구 사례를 살펴보고, 5장에서는 국가기록원 전자기록관리 절차에서 디지털 포렌식 기법을 적용하는 방안에 대해 논의한다. 마지막 6장에서는 본 논문에 대한 결론과 향후 연구 방향에 대해 제시하고 논문을 마무리 한다.

II. 전자기록물의 특징과 증거능력

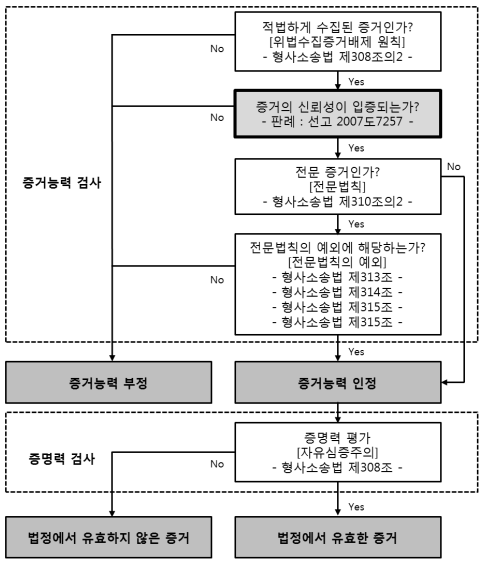
2.1 전자기록물의 특징

전자기록물이라 하면 전자기 신호를 이용하여 매체에 저장된 기록물을 총칭하는데, 이는 다시 아날로그 방식의 기록물(비디오테이프, 녹음테이프 등)과 디지털 방식의 기록물(HDD, Flash Memory, DVD 등)로 구분할 수 있다. 본 논문에서 언급하고 있는 전자기록물은 디지털 매체에 기록된 기록물로 그 범위를 한정 한다.

디지털 방식으로 기록된 전자기록물은 매체독립성, 비가독성, 위·변조 취약성, 대량성, 전문성 등의 특징들을 가지고 있다[1]. 이중에서 위·변조 취약성은 디지털 방식의 전자기록이 손쉽게 삭제·변경됨을 뜻하며 이러한 특징은 전자기록이 법정에 증거로 제시될 때 그 신뢰성을 추정하는데 큰 영향을 미친다.

2.2 전자기록물의 법적 증거능력을 위한 요건

일반적으로 증거라 하면 법적 사실인정의 근거가



〔그림 1〕 형사소송법에서의 증거능력 및 증명력 판단

되는 자료를 뜻하는데, 이 때 제시된 증거가 실질적 효력을 지니기 위해서는 법률상의 형식적·객관적 자격인 증거능력을 기본적으로 갖추어야 한다. 증거능력이 인정된 증거는 이후 자유심증주의 원칙에 따라 증거의 실질적 가치를 의미하는 증명력 여부가 결정 된다. 국내 형사소송법에서는 증거의 증거능력에 대해 〔그림 1〕에서와 같이 엄격한 기준(위법수집증거배제법칙, 전문법칙, 증거의 신뢰성)을 규정하고 있다.

국가기록원에서 관리하고 있는 전자기록의 증거능력에 대해 형사 소송법 상의 기준으로 판단할 때, 무엇보다 증거의 신뢰성 여부가 주요한 문제로 제시될 것이다. 대법원 판례(선고 2007도7257)에 따르면 제시된 전자 증거의 일부를 인정함에 있어 수사기관이 디지털 포렌식 절차를 엄격하게 준수한 것을 근거로 하였다. 따라서 현재 국가기록원에 관리하고 있는 전자기록이 사법적 증거로 제시될 경우, 증거의 신뢰성을 판단하는 기준은 디지털 포렌식에서와 같은 절차적·기술적 신뢰도를 제공했는지 여부가 될 것이다.

III. 전자기록관리에서의 신뢰성 문제 고찰

전자기록물 관리 체계는 생산-준현용-비현용 3단계 전자기록물 라이프 싸이클에 준하여 업무관리시스템, 기록관리시스템, 영구기록물관리시스템으로 구성된다. 생산단계에서 생산된 전자문서는 이후 보존기간 등을 고려하여, 하위 애플리케이션 또는 시스템에 독

립적으로 접근하기 위한 문서보존포맷 및 전자기록물의 진본성·무결성을 보장하고 장기간 안전하게 보존하기 위한 장기보존포맷으로의 변환이 이뤄진다. 장기보존포맷에서는 기록물관리기관 인증서로 생성한 전자서명을 포함함으로써 전자기록의 진본성 및 무결성을 보장하며, 여기에 사용된 전자서명 인증서에 대한 장기 검증체계를 구축하고 있다(NAK/TS 4-1:2011, NAK/TS 4-2:2011). 하지만, 장기보존포맷으로의 변환 이전 단계인 생산·수집 및 활용, 이관 등의 시점에서는 형사 소송법 상의 엄격한 증거능력 기준으로 판단할 때 신뢰성이 확보된다고 판단하기 어렵다. 특히, 기록관리 시스템을 거치지 않고 off-line으로 기록원에 이관되는 경우에 있어서 적합한 이관 도구 및 절차가 적용되지 않아 전자기록의 무결성 또는 신뢰성을 증명하기 어렵다.

3.1 기록 수집 단계에서의 신뢰성 입증 부족

국가기록원을 비롯한 기록보존소에서 전자기록을 수집하는 경우, 필연적으로 원본 기록이 담긴 매체로부터 보존 매체로의 매체 이전(migration)이 발생한다. 이러한 기록 수집 단계에서의 신뢰성 보장 문제는 디지털 포렌식 절차에서의 증거 수집 단계와 대조하여 고려해 볼 수 있다. 디지털 포렌식 절차에서는 증거 수집 시 신뢰성 및 무결성을 확보하기 위해 쓰기방지장치 및 이미징 도구를 사용하며, 수집과 동시에 원본 증거에 대한 해시값을 계산하여 추후 법정에서 무결성을 증명하는데 사용한다. 하지만 영구기록물관리기관 표준운영절차(NAK/S 9:2008)에서는 기록물 인수 절차에 있어서 기록물의 무결성을 입증하기 위한 구체적인 방법을 명시하고 있지 않다. 기록 수집 대상 파일들에 대한 매체 이전에서 단순히 복사(copy)기능을 사용하는 경우 파일의 메타데이터 정보 및 원본 bit-stream이 훼손될 수 있으며 파일의 위·변조가 일어나지 않았음을 증명할 수 없다.

3.2 해시(Hash)값에 대한 체계적 관리 시스템 부재

기록관리 메타데이터 표준(NAK/S 8:2012)에서는 현용, 준현용, 비현용 기록물을 대상으로 한 메타데이터 항목에 SHA-256 알고리즘을 사용한 해시값을 포함하고 있다. 하지만 이러한 해시값의 생성 시점에 대해 구체적으로 명시하지 않으며, 생성된 해시값의 유효성을 보장하기 위한 관리 체계가 미비하다. 디지털 포렌식 절차에서는 증거 수집 시 생성한 해시값을 출력하고 용의자 및 입회인의 서명·날인을 받아 확인함으로써 법정 제출 시 해시값의 유효성을 입증한다. 기록보존소에서 관리하는 전자기록은 방대하기 때문에 이러한 방법을 그대로 적용할 수는 없지만 이와 유사한 정도의 신뢰성을 보장할 수 있는 체계가 필요하다.

IV. 디지털 포렌식 적용 연구 사례

해외에서는 2008년부터 대학 도서관을 중심으로 전자 기록물 관리에 디지털 포렌식을 적용하는 방안을 연구하고 있다〔표 1〕. 특히, 기록 수집 단계에서 FTK, FRED 등 기존 디지털 포렌식 도구를 활용하

〔표 1〕 디지털 포렌식 적용 연구 시례

연구제목 (국가)	년도	주요 내용
BitCurator (미국)	2011 ~ 2013	·오픈소스 기반의 디지털 포렌식 도구들을 통한 전자기록 수집 방안 연구 ·포렌식 기반 전자기록 수집 도구들을 사용할 수 있는 가상 환경 및 소스코드 제공
DF and Born-Digital Content in Cultural Heritage (미국)	2009 ~ 2010	·전자기록 관리에 디지털 포렌식을 적용한 사례 논의 ·디지털 포렌식 적용 이점 제시(포맷 독립성, 무결성 유지, 데이터 복구)
AIMS (미국)	2009 ~ 2011	·전자 기록들을 관리하기 위한 방법론 및 지속 가능한 포괄적 프레임워크 제시 ·기록 수집 및 식별 단계에서 디지털 포렌식 도구 활용
futureArch (영국)	2008 ~ 2012	·BEAM 서비스를 통해 전자기록의 수집, 보존, 접근 등의 절차를 위한 가이드라인 수립 ·FRED 장비를 통해 디지털 매체 복제 수행
Digital Lives (영국)	2009	·전자기록 관리에 있어 디지털 포렌식 적용의 이점 논의 ·전자 기록 수집 시점에서 FTK 등 디지털 포렌식 도구 활용 방안 제시
Digital Records Forensics (캐나다)	2008 ~ 2011	·디지털 포렌식, 증거법, 문서학 각 분야에서 전자기록에 대한 관점 비교

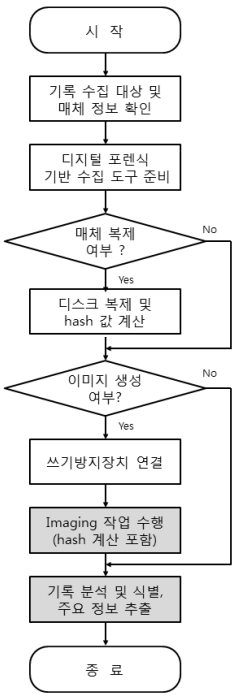
는 방안을 주로 논의하였다.

V. 디지털 포렌식을 적용한 전자기록관리 방안

앞서 3장에서 살펴본 전자기록 관리에서의 문제점을 해결하기 위해 기록 수집 단계에서의 디지털 포렌식 절차 및 도구 활용 방안과 기록물 포맷에 대한 해시값 생성 및 검증 체계를 제안한다.

5.1 기록 수집 시 디지털 포렌식 절차 및 도구 사용

외부로부터 기록 수집 시 〔그림 2〕와 같은 디지털 포렌식 절차적 신뢰성이 보장된 수집 프로세스를 준수하며, 이를 위해 쓰기방지장치, 매체 복제 도구, 이미징 도구 등과 같은 디지털 포렌식 도구를 사용할 수 있다.

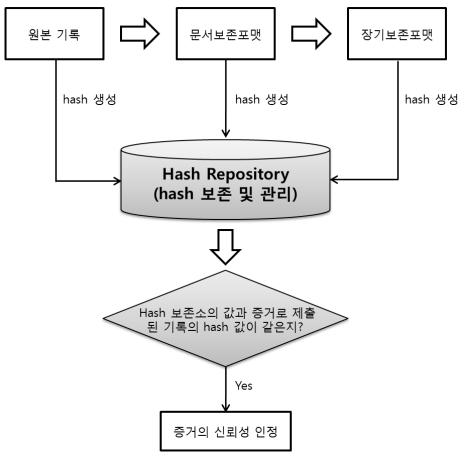


〔그림 2〕 기록 수집 시 디지털 포렌식 도구 및 절차 적용

한편 이미징 및 기록 분석에 있어서 기존 디지털 포렌식 도구를 사용하지 않고 각 기록보관소의 요구 사항에 적합한 도구를 자체 개발하여 사용할 수도 있을 것이다.

5.2 기록 포맷에 대한 해시값 생성·관리

원본 기록 수집 단계, 문서보존포맷 변환 단계, 또는 장기보존포맷 변환 단계에서 각 문서 포맷에 대해 시점정보를 포함하여 해시값을 생성하고 별도 해시 저장소(hash repository)에 보관·관리함으로써 추후 법적 증거능력을 판단할 때 이를 통해 증거의 신뢰성 및 무결성을 증명할 수 있다.



〔그림 3〕 해시값 생성 및 검증 체계

VI. 결 론

이 논문에서는 국가기록원에서 관리하는 전자기록들의 증거능력에 관한 이슈를 살펴보고, 기록의 무결성 및 신뢰성 확보를 위한 디지털 포렌식 활용 방안을 개략적으로 살펴보았다. 2015년 정부 전자 기록물의 본격적인 이관을 앞두고 전자 기록물 관리에서의 무결성 및 신뢰성 보장은 더욱 중요지고 있다. 향후에는 전자기록 수집 및 보존 요구사항에 적합한 디지털 포렌식 기반 기록 수집 도구 개발 및 기존 시스템에 해시값 관리 체계를 적용하기 위한 구체적 연구가 이루어져야 할 것이다.

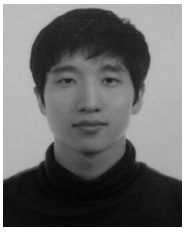
참고문헌

〔1〕 양근원, “형사절차상 디지털증거의 수집과 증거능력에 관한 연구,” 경희대학교 대학원 박사학위논문, pp. 20, 2006년

〔2〕 (준)현용 기록관리 메타데이터 표준화 추진단, 기록관리 메타데이터 표준, NAK/S 8:2012, 2012

년 10월
〔3〕 국가기록원 표준협력과, 영구기록물관리기관 표준 운영절차, NAK/S 9:2008, 2008년 12월
〔4〕 김동명, 전자기록물 문서보존포맷 기술규격, NAK/TS 2:2008, 2008년 11월
〔5〕 김동명, 전자기록물 장기보존포맷 기술규격 NAK/TS 3:2008, 2008년 12월

〈著者紹介〉



유 형 욱 (Hyunguk Yoo) 학생회원
2011년 8월: 아주대학교 정보 및 컴퓨터공학부 졸업
2011년 9월~현재: 아주대학교 컴퓨터공학과 석사과정
〈관심분야〉 스마트그리드 보안, 디지털 포렌식, 이상탐지, 리눅스 및 안드로이드 보안

손 태 식 (Taeshik Shon) 종신회원
2000년 2월: 아주대학교 정보 및 컴퓨터공학부 졸업
2002년 2월: 아주대학교 컴퓨터공학과 공학석사
2005년 8월: 고려대학교 정보보호대학원 공학박사
2004년 2월~2005년 2월: University of Minnesota, Research Scholar
2005년 8월~2011년 2월: 삼성전자 DMC 연구소 책임연구원
2011년 3월~현재: 아주대학교 정보컴퓨터공학과 조교수
〈관심분야〉 스마트그리드 보안, 디지털 포렌식, 이상탐지, 시스템 및 네트워크 보안