용역연구사업 연구결과보고서

관리 번호	25123037602			
사 업 명	2012년 기록보존기술 연구개발 사업			
과 제 명	국문	디지털포렌식 기법을 적용한 전자기록물 관리기술 고도화 연구		
	영문	Research on advanced electronic record management technology using digital forensics		
주관연구기관	기 관 명		소재지	대 표
	아주대학교 산학협력단		경기도 수원시 영통구 산5	유 재 석
주관연구 책임자	성 명		소속 및 부서	전 공
	손 태 식		정보 컴퓨터 공학과	정보보호
총연구기간	2012년 4월 24일 - 2012년 11월 30일(8개월)			
총 연구비	일금 오천삼백사십이만구천원			
연구년차	연구기간		연구비	
1차년도	2012. 04. 24 - 2012. 11. 30		일금 오천삼백사십이만구천원	
총참여연구원	9명 (책임연구원: 1명, 연구보조원: 8명)			

2012년도 기록보존기술 연구개발사업에 의하여 수행중인 연구과제의 연구결과보고서를 붙임과 같이 제출합니다.

붙임 . 연구결과보고서 35부(별첨).

2012년 11월 20일

주관연구책임자 손 태 식 (인 또는 서명)

주관연구기관장 유 재 석 (직인)

국가기록원장 귀하

주 의

1. 이 보고서는 국가기록원에서 시행한 용역연구개발사업의 연구결과보고서입니다.

2. 이 보고서 내용을 발표할 때에는 반드시 국가기록원에서 시행한 용역연구개발사업의 연구결과임을 밝혀야 합니다.

3. 국가과학기술 기밀유지에 필요한 내용은 대외적으로 발표 또는 공개하여서는 아니 됩니다.

제 출 문

국가기록원장 귀 하

이 보고서를 “디지털포렌식 기법을 적용한 전자기록물 관리기술 고도화 연구(아주대학교/손태식) ”과제의 연구결과보고서로 제출합니다.

2012. 11. 20

주관연구기관명 : 아주대학교

주관연구책임자 : 손태식

목 차

연구결과보고서 요약문

연구과제명	디지털포렌식 기법을 적용한 전자기록물 관리기술 고도화 연구		
중심단어	디지털 포렌식, 전자기록관리, 법적 허용성, 증거능력, 기록의 무결성		
주관연구기관	아주대학교 산학협력단	주관연구책임자	손태식
연구기간	2012. 04. 24 - 2012. 11. 30		

디지털 포렌식(Digital Forensics)은 디지털 증거물에 대한 수집, 확인, 식별, 분석, 기록 등에 있어 과학적인 원리에 의해 도출된 기술과 신뢰성 유지를 위한 절차 및 방법 수행을 의미하며, 이는 곧 디지털 증거가 사법적 증거능력을 가질 수 있는 판단 기준이 된다. 한편 기록관리 분야에서도 디지털 방식으로 저장된 기록물이 급증함에 따라 이러한 전자기록들의 수집·보존·관리에 있어 신뢰성과 진본성을 보장하는 것과 이를 통해 사법적 효력이 보장되는지 여부가 주요 이슈가 되었다. 본 연구는 전자기록물 관리에 디지털 포렌식 기법을 적용하여 전자기록의 진본성 및 신뢰성을 보장하고 이를 통해 사법적 효력을 보장하고자 수행되었다. 이러한 목적을 달성하기 위해 크게 아래 5가지 목표를 수립하였고 각각에 대한 세부 연구들을 수행하였다.

○ 국외 전자기록물 보존 처리에 관한 연구 동향 파악
○ 국내 전자기록물의 라이프사이클 분석 및 기록물 처리 관련 제도 분석
○ 국내외 디지털 포렌식 표준 및 특허, 기술 분석
○ 전자기록의 사법적 증거력 및 공·사 영역에서의 효력 조사
○ 디지털 포렌식 기반의 전자기록 수집 및 보존 방안 제시

본 연구는 위 5가지 연구 목표를 연구 제안 시점에서 계획한 바에 따라 진행하였으며, 이를 통해 최종적으로 도출된 주요 성과 및 결론은 다음과 같다.

○ 디지털 포렌식을 적용한 전자기록관리 연구 사례 분석을 통해 디지털 포렌식 접목 연구의 세계적 흐름 파악 및 국가기록원 전자기록 관리에의 접목점 도출
○ 국가기록원에서 관리하는 전자기록들에 대한 민·형사 영역에서의 증거능력 여부에 대한 고찰 및 전자기록이 법적 효력을 가지기 위한 요건 도출
○ 디지털 포렌식 기반의 전자기록 수집 및 보존 방안 제시

이 연구를 통해 도출된 성과들은 향후 디지털 포렌식 기반의 전자기록 수집 도구 개발 및 절차, 정책 수립에 있어 참고 될 수 있을 것이며, 국가 전자기록 관리 시스템 개선 및 고도화의 기반 지식으로 활용될 수 있을 것이다.

Summary

Title of Project	Research on advanced electronic record management technology using digital forensics		
Key Words	Digital Forensics,		
Institute	Ajou industry-academic cooperation foundation	Project Leader	Teashik Shon
Project Period	2012. 04. 24 - 2012. 11. 30		

Digital Forensic is about methodology and procedure for the maintenance of reliability and techniques derived from scientific principles on digital evidence collection, verification, identification, analysis, and recording. This means that such procedure gives the digital evidence legal force. With the rapid growth of digital records, the acceptance of judicial validity and the guarantee of reliability and authenticity in collection, preservation, maintenance of digital records became hot potato in the field of record management. In this research, the Digital Forensic techniques will be applied to management of digital records to guarantee the judicial validity through the assurance of authenticity and reliability of digital records. To fulfill such goal, the following 5 objectives were established and the detail research was carried out.

○ Grasp of the worldwide trend of digital record preservation process

○ Analyzing the domestic life-cycle and management of digital records

○ Analyzing domestic and foreign digital forensic standards, patents, and technologies

○ Investigation of the evidence admissibility of digital records in public and private domains

○ Proposing method of collection and preservation of digital records based on Digital Forensic

This research has proceeded above 5 project goals from the project proposal as planned and produced following results.

○ Grasping global trend of Digital forensic grafting research and applying this trend to National Archives of Korea digital record management, through analyzing the instances of Digital Forensic appliance in digital record management

○ Considering acceptance of digital records preserved by 국가기록원 as the evidence in civil, criminal suit and drawing requirement for digital records to have legal force

○ Proposing the method of collection and preservation of digital records based on Digital Forensic.

The result of this research can be considered in developing tools and establishing procedures and policies for collecting digital record based on Digital Forensic. It can be used in improvement of national digital record management system and can be used as reference data for advancement of technology.

총괄연구개발과제 연구결과

제 1 장 총괄연구개발과제의 최종 연구개발 목표

제 1 총괄연구개발과제의 목표

1. 연구배경

IT 기술의 발전과 급격한 정보화 사회로의 변화는 정보의 디지털화를 가속 시키고, 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 국가 기록원에 저장되고 있다. 이러한 중요 기록물들은 국가기록원에서 자체 디지털화 하기도 하지만 다수의 출처로 부터 생성되어 국가기록원으로 보내어지기도 한다. 국가기록원으로 디지털 기록물을 운반하기 위해 디지털 기록물은 하드디스크, USB 등의 저장매체에 저장되어 물리적으로 운반되어지거나 컴퓨터 네트워크를 통해 전송될 수 있다. 하지만 디지털 데이터의 특성 상 디지털 기록물은 여러 종류의 보안 위협에 노출 될 수 있으며, 이에 따라 기록원, 도서관 등의 기록물을 보관하는 기관들은 이러한 **전자기록에 진본성(authenticity) 및 무결성(integrity)에 대해 보장할 수 있는 방안**이 필요시 되고 있다. 또한 점점 디지털 데이터의 법정 증거능력에 대한 요구사항이 높아지고 있어 **기록원 차원의 전자기록 법정 증거능력을 확보할 수 있도록 제도 개선안 마련이 시급**하다.

해외 일부 기관에서는 이러한 요구사항을 만족하기 위해 디지털 포렌식(Digital Forensic) 기술을 접목하는 시도를 하고 있다. 디지털 포렌식 기술은 다른 말로 '컴퓨터 법의학'이라 불리며, 정보기기에 내장된 디지털 자료를 근거로 삼아 그 정보기기를 매개체로 하여 발생한 어떤 행위의 사실 관계를 규명하고 증명하는 디지털 수사과정을 뜻한다. 이러한 디지털 증거는 무형의 자료로서 훼손 및 위변조가 쉽기 때문에 법정 제출을 위한 디지털 포렌식 기술은 일련의 적법한 절차가 필요하며, 증거가 수집될 당시의 원본 데이터로부터 추출되었음을 보장할 수 있는 조치가 취해져야 한다. 디지

털 정보를 증거로 활용하기 위해 디지털 포렌식은 크게 증거 수집, 증거 분석, 증거 제출의 3단계의 절차로 이루어진다.

- 증거 수집 : 손상되기 쉽고, 사라지기 쉬운 디지털 증거가 저장된 저장매체(컴퓨터 메모리, 하드 디스크, USB 등)에서 데이터의 무결성을 보장하면서 데이터를 읽어 내야 한다. 이 때 무결성이란 원 저장매체에 대한 데이터 변조가 일어나지 않음을 의미한다. 증거 수집에서 유용한 기술로는 무결성을 보장하는 이미징 기술 등이 있다.
- 증거 분석 : 증거 수집으로 얻은 데이터로부터 유용한 정보를 이끌어 내야 한다. 유용한 정보는 보통 저장 매체에 존재하는 파일 시스템의 내부나 외부에 존재할 수 있다. 예를 들면, 범죄자는 저장매체에 존재하는 NTFS와 같은 파일 시스템 내부나, 파일 시스템에서 사용하지 않는 저장매체 구역에 중요 정보를 숨길 수 있다. 증거 분석에서 유용한 기술로는 삭제된 파일 복구 기술이나 암호화된 파일 해독 및 문자열 검색 기술 등을 들 수 있다.
- 증거 제출 : 입수된 디지털 증거가 법적 증거로 채택되기 위해서는 증거자료의 신뢰성이 확보 되어야 한다. 이를 위해 법률적으로 디지털 포렌식에 대한 표준 절차뿐만 아니라 포렌식 툴에 대한 검증 절차 또한 이루어져야한다.

위에서 살펴본 바와 같이 이러한 **디지털 포렌식의 절차 중 증거 수집 및 분석 단계는 기록원, 도서관 등의 정보기록기관의 보안 요구사항과 상충**하는 것을 알 수 있다. 실제로 국외 Stanford, Oxford, King's Kollege 대학을 비롯한 몇몇 대학의 도서관 및 학계 등 **해외 일각에서는 디지털 포렌식 도구를 디지털 데이터의 진본성과 무결성을 보장하는 수단으로써 사용하는 것에 대해 연구를 진행 중**이다.

현재 국가기록원은 처음부터 전자적으로 생산된 전자기록물(born-digital)을 본격적으로 이관 받아 보존·활용한 경험이 많지 않다. 그러나 2015년부터 정부기관이 생산한 전자기록물이 본격적으로 이관될 예정임으로 이에 대비하여 필요한 기반 기술 개발과 인프라 구축을 진행하여야 한다.[1] 이때 무엇보다 전자기록물의 진본성과 무결성이 우선적으로 보장되어야 함은 당연하다. 아직 해외에 비해 국내에서는 전자기록물 관리에 디지털 포렌식 기법을 적용하는 것에 대한 연구는 전무한 실정이다. 전자기록물 관리에 디지털 포렌식 기법을 적용하면 전자기록물의 진본성과 무결성을 보장함과 동시에 법적 증거능력 또한 얻을 수 있으므로 이에 대한 연구는 향후 기록물 보존 및 전자기록의 증거능력 확보에 많은 기여를 할 것이다.

1) 국가기록원 전자기록물 연구개발 현황, 이창영, 2011

2. 연구목표

가. 국외 전자기록물 보존 처리에 관한 연구 동향 파악

(1) 전반적인 국외 전자기록물 관리 동향 조사

(2) 국외 전자기록물 관리에 디지털 포렌식 적용 사례 조사

나. 국내 전자기록물의 라이프사이클 분석 및 기록물 처리 관련 제도 분석

(1) 국가기록원의 전반적인 전자기록관리 프로세스 분석

(2) 국가기록원 전자기록관리 표준 및 기술 문서 분석

(3) 전자기록관리 프로세스에서의 증거능력 관련 이슈 파악

다. 국내외 디지털 포렌식 표준 및 특허 파악

(1) 국내 디지털 포렌식 절차 및 기술 분석

(2) 국외 디지털 포렌식 가이드라인, 표준 및 특허 분석

라. 전자기록의 사법적 증거력 및 공·사 영역에서의 효력 조사

(1) 국내외 전자기록의 증거능력에 관한 법령 및 판례 분석

(2) 국내 포렌식 및 기록물관리의 법적 효력에 대한 종합 분석

마. 디지털 포렌식 기반의 전자기록 수집 및 보존 방안 제시

(1) 국가기록원 전자기록물 관리 절차에 적합한 디지털 포렌식 기반의 전자기록물 관리 방안 제시

3. 연구범위

가. 국외 전자기록물 보존 처리에 관한 국외 연구 동향 파악

(1) 미국, 영국, 호주, 캐나다 등 국외 전자기록관리 주요 동향 조사 및 디지털 포렌식 관련 이슈 파악

(2) Stanford, Oxford, King's College London, University of British Columbia 등 해외 대학 도서관을 중심으로 진행되고 있는 디지털 포렌식 접목 연구 조사

나. 국내 전자기록의 라이프사이클 분석 및 기록물 처리 관련 제도(특허, 표준 등) 분석

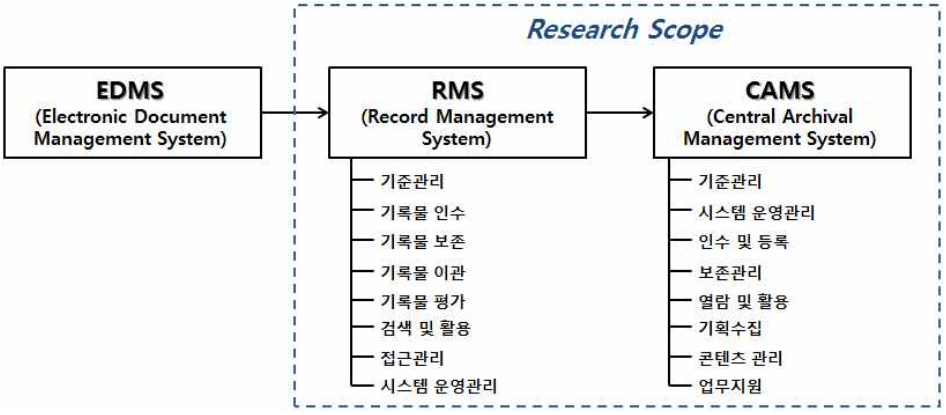
(1) 전자기록 생산 방식에 있어서 증거력 확보 요건 충족도

(2) 전자기록 보존 및 제공 방식에 있어서 증거력 유지 요건 충족도

(3) 국가기록원과 공동으로 전자기록물 Life-cycle(EDMS-RMS-CAMS) 관련 내용을 분석하여 전자기록물의 생산 후 관리, 저장 단계에서의 디지털 포렌식 기술 요구사항 도출

(4) 기존 국가기록원 전자 기록물 관리 프로세스를 파악하여 디지털 포렌식 적용 가능한 부분적인 요소 파악

(5) 기존 국가 기록물 수집 및 이관 절차를 파악하여 전자기록물의 수집 및 이관에 발생가능한 문제점 도출



(그림 1. 전자기록물 life-cycle 및 연구 범위)

다. 국내외 디지털 포렌식 기반 표준 및 특허 파악

(1) 국내 경찰청 디지털증거 처리 표준 가이드라인

(2) 디지털 포렌식 관련 TTA 표준(TTAS.KO-12.0057, TTAS.KO-12.0058)

(3) 미국 NIST, Guide to Integrating Forensic Techniques into Incident Response

(4) 미국 NIST, Computer Forensics Tool Testing Program(CFTT)

(5) RFC 3227 '디지털 증거 수집 및 획득에 대한 가이드라인(Guidelines for Evidence Collection and Archiving)'

라. 전자기록의 사법적 증거력 및 공·사 영역에서의 효력 조사

(1) 공·사 영역에서 전자기록의 효력 인정 범위 파악 및 요건 도출

(2) 재판증거로서 전자기록이 채택된 판례분석 및 요건 도출

(3) 디지털 포렌식 기술을 이용하여 증거력을 획득한 사례 분석 및 요건 도출

(4) 국외 전자기록 수집 및 보존을 위한 관련 법령 및 제도 분석

(5) 전자기록물과 종이기록물과의 차별성에 관한 제도적 측면에 대해서 분석

마. 디지털 포렌식 기반의 전자기록 수집 및 보존 방안 제안

(1) 디지털 포렌식 기술을 분석하여 기록물에 적용가능성이 있는 기술 집중 분석

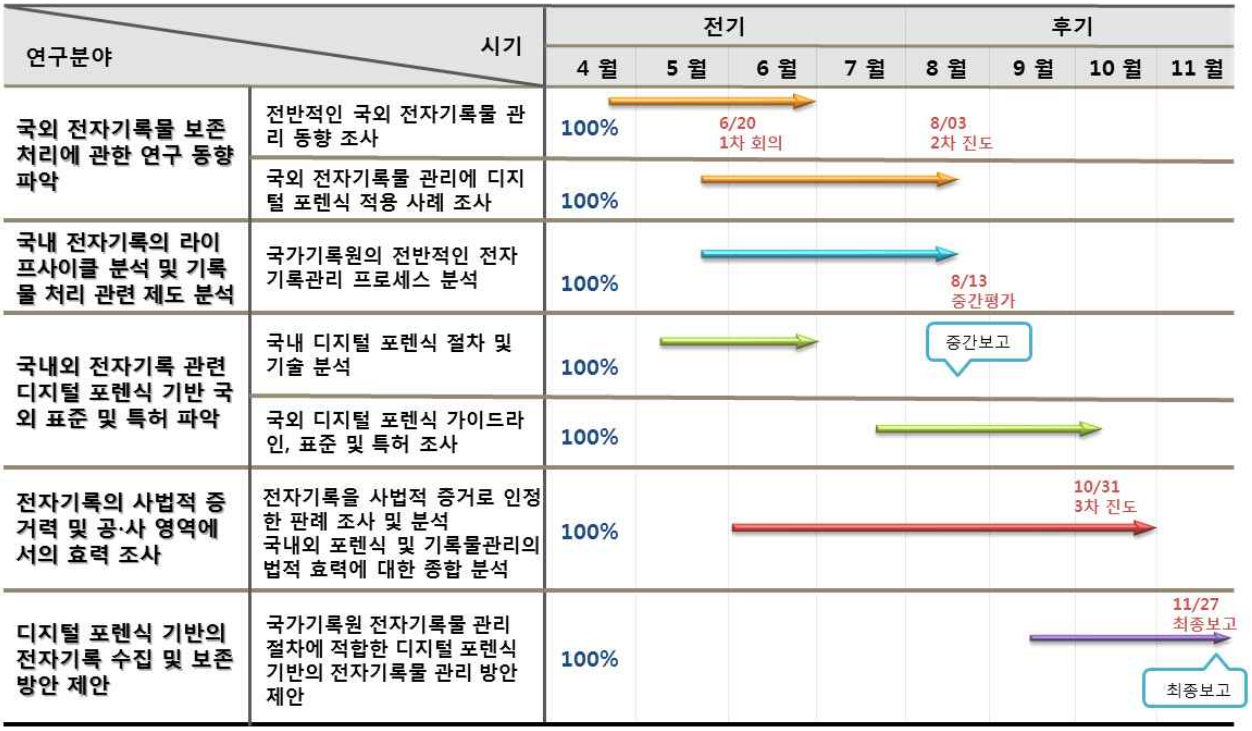
(2) 국내 국가기록물 관리에 필요한 기존 디지털 포렌식 절차의 적용 방안 및 새로운 프로세스 도출

(3) 국외 디지털 포렌식 기법 적용 사례 및 최신 전자기록물 관리 연구 등을 분석하여 국내 실정에 맞는 디지털 포렌식 기반 전자기록물 관리 프로세스 제안

제 2 절 총괄연구개발과제의 목표달성도

1. 연구 계획 대비 목표 달성도

본 연구는 처음 5가지 큰 연구 목표를 설정하고 진행되었다. 아래 (그림 2)는 5가지 큰 연구 목표에 대한 기존 계획 대비 목표 달성도를 나타낸다. 3번의 진도보고와 중간평가를 통해 국가기록원과 연구 방향 및 목표에 대해 논의하였고, 최종적으로 기 계획한 목표를 모두 달성하였다.



(그림 2. 연구 계획 대비 목표 달성도)

2. 관련 분야 연구에의 기여도

국내에서는 아직까지 전자기록 관리에 디지털 포렌식을 접목한 연구 사례가 없기 때문에 본 연구를 통해 도출된 연구 결과물은 향후 디지털 포렌식 기반 전자기록관리 도구 및 세부 가이드라인 또는 표준 개발 등의 연구에 있어 초석이 될 것이다. 또한, 전자기록의 법적 증거능력에 관한 이슈를 제기함으로써 향후 관련 제도 및 법령 개선에 있어 중요하게 고려될 수 있다.

제 3 절 국내·외 기술개발 현황

정보기술의 발달로 인해 디지털 방식으로 생성되는 기록이 늘어남에 따라 이러한 디지털 형태로 생성·저장된 기록물을 장기적으로 안전하게 보존하는 것이 기록관리 분야의 중요 이슈가 되었다. 미국 NARA(National Archives and Records Administration), 영국 NA(National Archives) 등 해외 여러 국가기록원에서는 이러한 이슈에 대응하기 위해 많은 노력을 기울이고 있다. 특히 Stanford, Oxford, King's College London, University of British Columbia 등의 주요 대학 도서관을 중심으로는 디지털 포렌식 절차 및 기술을 전자기록관리 프로세스에 적용하여 전자기록의 무결성 및 진본성을 보존하고자 하는 연구가 활발히 진행되고 있다. 국내에서는 2006년에 표준RMS 개발 사업을 완료하였으며, 2010년에는 장기보존 기록물의 안전한 보존 관리 체계 구축을 위해 WORM 스토리지에 대한 증설을 완료하였다. 그러나 국내에서는 아직까지 디지털 포렌식을 접목하여 디지털 기록의 무결성을 유지하는 연구에 대해서는 알려진 바가 없다.

1. 국외연구동향

가. 미국

- 미국 국가기록청(NARA)는 1998년부터 전자기록물 관리를 위한 준비 작업을 거쳐, 2004년 시스템 개발업체를 선정(Lockheed Martin 社)하여 2011년 9월 전자기록관리 체계인 ERA(Electronic Records Archives)구축을 완료
- 2012년 말까지 모든 연방정부 기관에서 ERA 시스템을 성공적으로 적용할 수 있는 성능 개선에 중점
- Stanford University, North Carolina University, Maryland University, Virginia University 등의 대학을 중심으로 디지털 포렌식 도구 및 절차를 전자기록관리 프로세스에 접목하고자 하는 연구 수행
  - "BitCurator", North Carolina, University of Maryland, 2011~현재
  - "Digital Forensic and Born-Digital Content in Cultural Heritage", Council on Library and Information Resources, 2009~2010
  - "AIMS", Hull University, Stanford University, Virginia University, Yale University, 2009~2011

나. 영국

- 영국 국가기록원(National Archives) 디지털 보존 부서(National Archive Digital Preservation Team)는 현재 디지털 정보를 하나의 데이터 포맷에서 다른 포맷으로 이전(migration)하는 프로세스에 대해 연구
- 2011년 조지아기술연구소(Georgia Tech Research Institute) 및 미국 국립문서보

관기록청(National Archives and Records Administration, NARA)와 협력하여 상당수의 파일 포맷 시그니처를 PRONOM에 추가(현재 v6.2)

- DPC(Digital Preservation Coalition)에서는 디지털 정보의 보존에 관심 있는 여러 단체의 컨소시엄 역할을 수행하고 있으며 최근 까지 디지털 포렌식 접목에 대한 워크샵 개최 등 진행
- Oxford University, British Library, King's College London, Yale University 등의 기관들에서 디지털 포렌식 도구 적용 연구 수행
  - "AIMS", Hull University, Stanford University, Virginia University, Yale University, 2009~2011
  - "FIDO", King's College London, 2011
  - "futureArch", Oxford University, 2008~2012
  - "Digital Lives", British Library, 2009
  - "Paradigm", Oxford University, 2005~2007

다. 캐나다

- 캐나다 국립도서기록청(Library and Archives Canada)은 2007년 캐나다 디지털 정보전략(Canada Digital Information Strategy)을 수립하였으며, 국민의견을 수렴하여 2008년 이에 대한 최종보고서 발표
- Luciana Duranti 교수를 중심으로 InterPARES 연구 수행(1998~2012)
- University of British Columbia 대학에서는 2008년에서 2011년 사이 "Digital Records Forensic"이라는 연구를 통해 디지털 포렌식 분야와 전자기록 관리 분야의 상호 보완 가능성에 대해 시사

라. 호주

- 호주 빅토리아 기록보존소(Public Record Office Victoria, PROV)는 전자기록물을 장기적으로 보존하기 위해 2000년부터 시작된 'The Victorian Electronic Record Strategy(VERS)'라는 장기 전략을 통해 2005년 Digital Archive 시스템 도입
- 호주 국가기록원(National Archive of Australia, NAA)은 2012년 3월 정부기관의 디지털 정보 및 기록관리 체계로의 전환에 관한 디지털 지속성 계획(Digital Continutiy Plan) 발표
- 또한, 2011년부터 check up 2.0 을 통해 공공기관의 전자기록물 관리 평가 실시

마. 덴마크

- 2004년, 덴마크 국가기록원은 2000년 이전에 수집한 전자기록물을 디지털 정보 보존을 위한 표준 방식으로 이전(migration)하는 대규모 프로젝트를 착수하여

2010년 완료

- 해당 이전 프로젝트를 위해 총 135.000 유로 사용

2. 국내연구동향

국내에서는 변화하는 기록물관리 환경에 대처하기 위해 2007년 기록물관리법을 전명 개정하고 기록관리 대상과 범위를 확대하였다. 전자기록물 분야에서 추진된 과제는 2008년부터 2011년 4월까지 총 17개가 수행되었다. 주요 연구 제목은 다음과 같다.

- 전자기록무로간리 재난복구 모델 연구('08)
- 디지털 포맷 및 애플리케이션 기술정보은행(DFR) 개발 ('08~'09)
- 웹(Web) 기록물 아카이빙 기반기술 연구 및 적용 시험('08~'10)
- 전자기록물 장기보존 전략 연구 및 테스트베드 구축 ('08~'09)
- 디지털 기록매체 최적수록 기술 및 도구 개발('08~'11)
- 차세대 전자기록관리 인프라 기술 연구('10~'11)
- 모바일 정부서비스 환경에 맞는 기록물서비스 최적화 모델연구('10~'11)
- 복합 전자기록물 장기보존 아키텍처 연구('11)

국내 전자기록물 기록관리 표준화 현황은 다음과 같다.

(표 1. 국내 전기기록물 기록관리 표준화 현황)

표준 번호	표준명	연도
NAK/S 6:2009	기록관리시스템 기능 요건	2009
NAK/S 7:2010	영구기록관리시스템 기능 요건	2010
NAK/S 8:2012	기록관리 메타데이터 표준	2012
NAK/S 9:2008	영구기록물관리기관 표준운영절차	2012
NAK/S 10:2012	기록관 표준운영절차:일반	2012
NAK/S 13:2008	디지털기록매체 요구기준	2008
NAK/S 16:2008	폐지기관 기록물 관리 및 이관 지침	2008
NAK/TS 1-1:2009	기록관리시스템 데이터연계 기술규격 -제1부: 업무관리시스템과의 연계	2009
NAK/TS 1-2:2008	기록관리시스템과 영구기록관리시스템 간 데이터 연계규격	2008
NAK/TS 1-3:2012	기록관리시스템 데이터연계 기술규격 -제3부: 기능분류시스템과의 연계	2012
NAK/TS 2:2008	전자기록물 문서보존포맷 기술규격	2008
NAK/TS 3:2008	전자기록물 장기보존포맷 기술규격	2008
NAK/TS 4-1:2011	전자기록물 전자서명 인증서 장기검증 기술규격	2011
NAK/TS 4-2:2011	전자서명 장기검증 통합연계 API규격	2011
NAK/TS 5:2010	전자기록물 온라인 전송을 위한 기술규격	2010

제 2 장 총괄연구개발과제의 최종 연구개발 내용 및 방법

본 연구의 5가지 연구 목표에 따라 아래와 같은 방향으로 연구를 수행하였다.

- **연구 목표 1. 국외 전자기록물 보존 처리에 관한 연구 동향 파악**

  연구 목표 1-1. 전반적인 국외 전자기록물 관리 동향 조사

  연구 내용 (1) 미국, 유럽 등 주요 국가기록원의 전자기록물 관리 동향 조사

  연구 내용 (2) 국외 전자기록관리 표준 및 기술 문서 분석

  - 미국, DoD 5015.02-STD
  - 미국, ERA Requirement Document
  - 호주, VERS@DOI
  - 유럽, Moreq

  연구 목표 1-2. 국외 전자기록물 관리에 디지털 포렌식 적용 사례 조사

  연구 내용 (1) 해외 주요 대학 도서관을 중심으로 디지털 포렌식 적용 사례 조사

  - 미국, Stanford University Libraries
  - 영국, Oxfrod University Bodleian Libraries
  - 영국, King's College London

  연구 내용 (2) 전자기록관리에 디지털 포렌식을 접목한 주요 프로젝트 분석

  - 미국, Digital Forensics and Born-Digital Content in Cultural Heritage Collections (2009~2010)
  - 미국, BitCurator (2011~현재)
  - 미국/영국, AIMS(An Inter-Institutional Model for Stewardship) (2009~2011)
  - 영국, Digital Lives (2009)
  - 캐나다, Digital Records Forensics Project (2008~2011)

- **연구 목표 2. 국내 전자기록물의 라이프사이클 분석 및 기록물 처리 관련 제도 분석**

  연구 목표 2-1. 국가기록원의 전반적인 전자기록관리 단계별 프로세스 분석

  연구 내용 (1) EDMS-RMS-CAMS를 거치는 전자기록 life-cycle의 전반적인 분석

  연구 목표 2-2. 전자기록관리 표준 및 기술 문서 분석

  연구 내용 (1) 국가기록원 전자기록관리 주요 표준 문서 분석

  - NAK/TS 1-1:2009 기록관리시스템 데이터연계 기술규격 제1부
  - NAK/TS 1-2:2008 기록관리시스템 데이터연계 기술규격 제2부
  - NAK/TS 5:2010 전자기록물 온라인 전송을 위한 기술규격
  - NAK/TS 2:2008 전자기록물 문서보존포맷 기술규격

- NAK/TS 3:2008 전자기록물 장기보존포맷 기술규격
- NAK/S 8:2012 기록관리 메타데이터 표준(※ 2012. 10 개정)

연구 목표 2-3. 전자기록관리 프로세스에서의 증거능력 관련 이슈 파악

연구 내용 (1) 표준 및 기술 문서 분석 내용을 바탕으로 전자 기록의 무결성 및 신뢰성 관련 이슈 파악

- **연구 목표 3. 국내외 디지털 포렌식 표준 및 특허, 기술 분석**

연구 목표 3-1. 국내 디지털 포렌식 표준 및 특허 분석

연구 내용 (1) 국내 디지털 증거 처리 가이드라인 및 표준 분석

- 경찰청 디지털증거 처리 표준 가이드라인 (2006)
- TTAS.KO-12.0058 컴퓨터 포렌식 가이드라인
- TTAS.KO-12.0057 컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항

연구 내용 (2) 국내 디지털 포렌식 기반 전자기록관리 특허 분석

- 디지털 포렌식 시스템에서 대용량 증거 이미지의 다중 색인 장치 및 방법 (출원번호 : 10-2009-0122959)
- 디지털 증거의 저장 및 분석을 위한 이미지 파일 포맷 구조및 그 구조로 데이터가 기록된 기록 매체 (출원번호 : 10-2007-0132715)
- 디지털 포렌식 시스템을 위한 대용량 데이터 고속 검색시스템 및 방법 (출원번호 : 10-2007-0120759)

연구 목표 3-2. 국외 디지털 포렌식 표준 및 특허 분석

연구 내용 (1) 국외 디지털 증거 처리 가이드라인 및 표준 분석

- NIST Special Publication 800-86, “Guide to Integrating Forensic Techniques into Incident Response”,
- RFC 3227, “Guidelines for Evidence Collection and Archiving”
- NIST Computer Forensics Tool Testing Program(CFTT)

연구 내용 (2) 국외 디지털 포렌식 기반 전자기록관리 특허 분석

- METHOD AND APPARATUS FOR MAINTAINING HIGH DATA INTEGRITY AND FOR PROVIDING A SECURE AUDIT FOR FRAUD PREVENTION AND DETECTION (국가 : 미국, 출원번호 : 12950454)
- Method and apparatus for digital forensics (국가 : 미국, 출원번호 : 12252869)

연구 목표 3-3. 국내외 디지털 포렌식 도구 및 기술 비교

연구 내용 (1) 디지털 포렌식 이미징(Imaging) 도구 비교 분석

- **연구 목표 4. 전자기록의 사법적 증거력 및 공·사 영역에서의 효력 조사**

  연구 목표 4-1. 국내외 전자기록의 증거능력에 관한 법령 및 판례 분석

  연구 내용 (1) 해외 전자문서의 효력·관리 및 사법적 증거력에 관한 법령 분석

  - 미국, Federal Rules of Evidence
  - 미국, Code of Federal Regulation, Subchapter B Records Management
  - 영국, Lord Chancellor's Code of Practice on the Management of Records Under Section 46 of the Freedom of Information Act 2000
  - 영국, A code of practice for legal admissibility and evidential weight of information stored electronically
  - 캐나다, Uniform Electronic Evidence Act
  - 캐나다, Policy on Electronic Authorization and Authentication 1996
  - 호주, Digital Recordkeeping Guidelines for Creating, Managing, and Preserving Digital Records

  연구 내용 (2) 국내 전자문서의 효력·관리 및 사법적 증거력에 관한 법령 분석

  - 전자문서의 증거능력에 관한 법률 분석 (민사소송법, 형사소송법)
  - 전자문서의 효력 및 관리 법령 분석
    (공공기록물 관리에 관한 법률, 전자정부법, 전자거래기본법, 전자서명법)

  연구 내용 (3) 전자기록의 증거능력과 관련한 주요 판례 분석

  - 일심회 사건(대법 2007도7257)
  - 영남위 사건(대법 99도2317)

  연구 목표 4-2. 국내 포렌식 및 기록물관리의 법적 효력에 대한 종합 분석

  연구 내용 (1) 전자기록이 법적 증거능력을 갖추기 위한 요건 분석

  연구 내용 (2) 기록원에서 관리하는 전자기록의 증거능력에 관한 이슈 분석

- **연구 목표 5. 디지털 포렌식 기반의 전자기록 수집 및 보존 방안 제시**

  연구 내용 (1) 전자기록 수집 및 관리 케이스 별 신뢰성 이슈에 관한 디지털 포렌식 관점의 해결방안 제시

  - Case 1. 전자기록관리시스템을 통한 공공기관으로부터의 기록 입수
  - Case 2. 외부로 부터의 매체 이전 방식을 통한 기록 입수

  연구 내용 (2) 디지털 포렌식 기반 전자기록물 관리 전체 프레임워크 제시

  연구 내용 (3) 디지털 포렌식 기반 도구 및 시스템 설계 예제 제시

제 1 절 국외 전자기록물 관리 동향 조사

미국, 호주, 유럽 등 기록관리 분야를 선도하고 있는 나라들의 전자기록관리 동향 및 전자기록관리 표준 문서(DoD 5015.02-STD, VERS@DOI, MoReq)들을 살펴봄으로써 디지털 포렌식 관점의 접근 또는 전자기록의 무결성 및 진본성 이슈에 대해 해외 기록원에서 대응하고 있는 바를 조사하였다.

1. 미국

미국 국립문서보관기록청(National Archives and Records Administration, NARA)는 1998년부터 전자기록물 관리를 위한 사전 준비 작업을 거쳐, 2004년 록히드 마틴(Lockheed Martin 社)를 시스템 개발업체로 선정, 2011년 전자기록관리 체계인 ERA)(Electronic Records Archives) 구축을 완료하고 현재 각 행정기관에 배포 및 업데이트를 계속해나가고 있다. ERA 시스템은 어플리케이션 또는 플랫폼 종류에 독립적으로 데이터를 저장하는 방법으로 전자기록물을 XML 형태[2]로 변환한다.[3] 2012년 말까지 모든 연방정부 기관에서 ERA 시스템을 성공적으로 적용할 수 있는 성능 개선에 중점을 두고 있으며, 2013년부터는 모든 연방기관이 영구보존 전자기록물에 대한 보존기한 책정과 이관을 위해 ERA를 사용하도록 예정이다. ERA 요건서(RD, Requirements)는 이러한 ERA 구축을 위해 필요한 요구사항을 규정한 문서로 2010년 7월에 나온 문서(v4.0)이 가장 최근 버전이다. ERA 요건서에서는 기록 관리(Records Management), 보존(Preservation), 기록관리 저장(Archival Storage), 보안(Security), 기록물 입수(Ingest), 접근(Access), 이용자 인터페이스, 행정관리, 시스템 특성으로 범주를 나누어 각각에서의 요구사항을 서술하고 있다. 한편, NARA는 최근 신뢰할 수 있는 디지털 저장 및 관리에 대해 다음의 두 가지 표준을 개발하고 있다.

- ISO/DIS 16363 : Audit and certification of trustworthy digital repositories
- ISO/DIS 16919 : Requirements for bodies providing audit and certification of candidate trustworthy digital repositories

ISO/DIS 16363 은 Trustworthy Repositories Audit & Certification: Criteria and Checklist(TRAC)에 기반하고 있으며, TRAC는 ISO 14721:2003(OAIS) 요구사항에 대응하여 만들어졌다.[4]

---

2) 디지털 보존에 있어 XML(eXtensible Markup Language)이 갖는 의미는 디지털 문서의 내용과 구조, 그리고 외관을 분리하기 때문에 디지털 정보의 운영체제 또는 어플리케이션 소프트웨어 의존성을 극복할 수 있다는 것이다.

3) http://ip.org.au/migration/

4) http://blogs.archives.gov/

- ISO 14721:2003 - OAIS Reference model

ISO 14721:2003는 기록 정보 시스템의 참조 모델을 명시하고 있다. OAIS 의 목적은 정보를 보존하고, 이를 지정된 커뮤니티에 이용하도록 디지털화된 기록 정보를 위한 시스템을 구축하는 것이다. 이 참조 모델은 정보의 입수, 기록물 저장, 데이터 관리, 접근, 그리고 보급을 포함하여 폭넓은 기록 정보 보존 기능을 설명한다. 이것은 또한 새로운 매체와 포맷, 정보를 나타내기 위한 데이터 모듈, 정보 보존에서의 소프트웨어의 역할, 그리고 기록원 사이의 디지털 정보교환에서의 디지털정보 이전(migration)을 설명한다.

2. 영국

영국 국가기록원 디지털 보존 부서(National Archive Digital Preservation Team)는 현재 디지털 정보를 하나의 데이터 포맷에서 다른 포맷으로 이전(migration)하는 프로세스에 대해 연구하고 있다. 이 연구의 목적은 현재 시대가 남긴 전자 기록물을 미래 세대에서도 계속해서 접근하고 사용할 수 있는 서비스의 개발에 있다. 영국 국가 기록원은 이를 위해 파일 포맷 연구, 디지털 보존에서의 포렌식 컴퓨팅, 비트 보존의 세 가지 특정 영역에 대해 중점을 두고 있다.

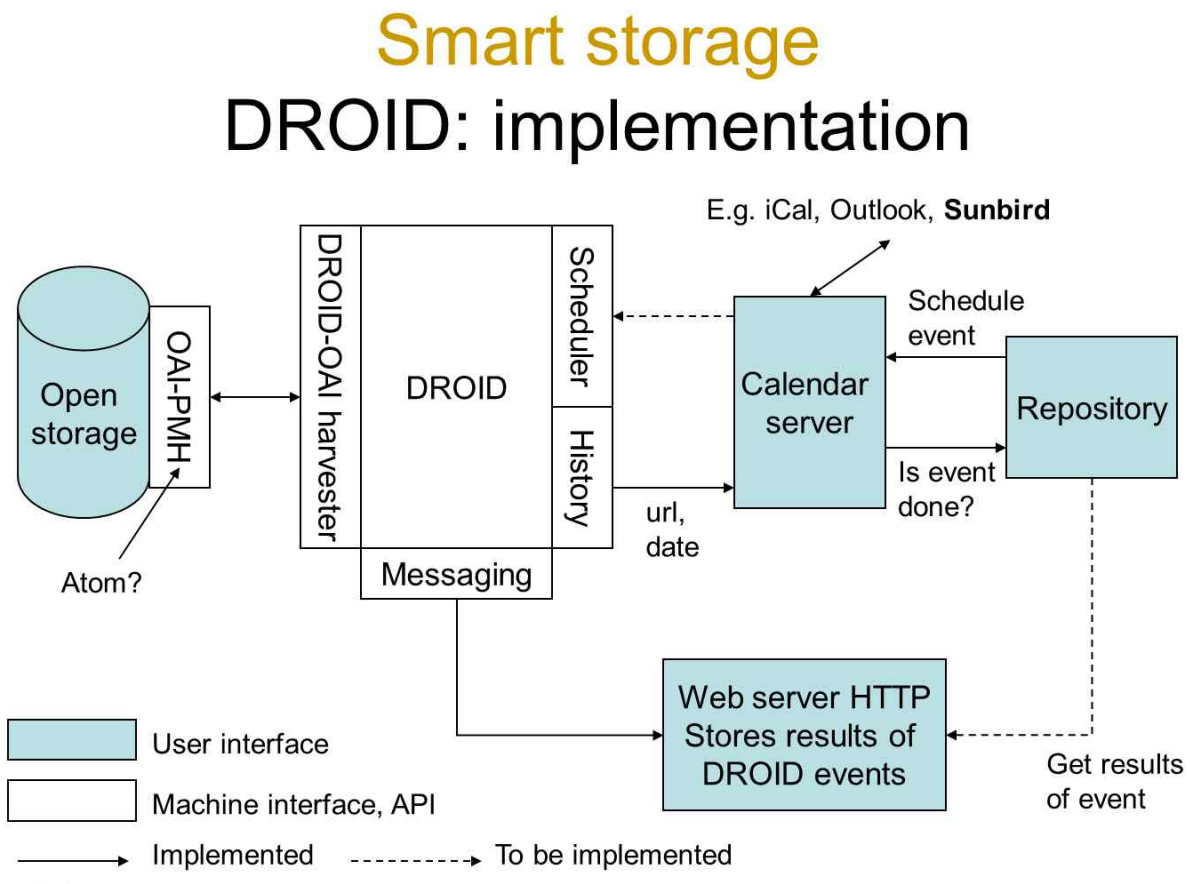
2011년에는 조지아기술연구소(Georgia Tech Research Institute) 및 미국 국립문서보관기록청(National Archives and Records Administration, NARA)와 협력하여 상당수의 파일 포맷 시그니처를 PRONOM[5] 에 추가하였다.

DROID (Digital Record Object Identification)[6]는 파일 포맷 확인을 위해 영국 국가기록원에서 개발한 소프트웨어이다. DROID의 목적은 디지털 저장소가 저장된 파일들의 포맷을 확인하는데 있다. DROID는 파일의 포맷을 확인하기 위해 내부(internal) 또는 외부(external) 시그니처를 사용한다. 이러한 시그니처 정보는 XML 형태로 PRONOM에 저장되어져 있으며, 새로운 시그니처 정보는 정기적으로 PRONOM에 저장되며 DROID는 PRONOM으로부터 자동적으로 시그니처를 다운받을 수 있게 설정가능하다. DROID는 Java로 개발되어 플랫폼에 독립적이며 GUI 또는 Command Line Interface로 구동 가능하며, DROID를 통해 식별(Identification)된 결과를 CSV(Comma-Separated Values)를 포함한 다양한 포맷으로 저장가능하다. 최신 버전은 v6.1(2012년 9월)이다.

---

5) PRONOM 은 영국 국가기록원이 디지털 정보 보존 서비스를 위해 개발한 웹 기반의 technical registry 로 파일 포맷 시그니처 정보들을 저장하고 있다.

6) http://droid.sourceforge.net/



(그림 3. Smart Storage, DROID[7])

한편, 영국의 DPC(Digital Preservation Coalition)는 영국에 기반을 두고 2001년 설립된 비영리 글로벌 회사로 전 세계적에 산재해 있는 전자적 기억(digital memory)과 지식(knowledge)들을 안전하게 보존하는 것을 목적으로 하여 디지털 정보의 보존에 관심 있는 여러 단체의 컨소시엄 역할을 수행하고 있다. DPC에의 참여는 다양한 상업, 문화 유산, 교육, 정보, 연구 등 모든 분야의 구성원들에게 열려 있으며, 주요 멤버는 British Library, Cambridge University Library, Digital Curation Centre, Oxford University Library Services 등이 있다. 최근 DPC는 전자기록 보존 및 관리에 있어 디지털 포렌식 기술을 접목하는 방향에 대해 많은 관심을 가지고 있다. 2011년 6월에 "Digital Preservation for Forensics" 라는 이름으로 워크샵 개최한 바 있으며, 이 워크샵에서는 전자기록물 관리를 위한 디지털 포렌식 분야의 많은 주요 연구자들이 참여하여 수행한 연구를 발표하였다. 또한 DPC는 매년 전자기록 관리의 주요 기술 이슈에 대해 Technology Watch Reports를 발행하는데, 2012년 11월에는 전자기록 관리를 위한 디지털 포렌식 연구 분야의 선구자인 Jeremy Leighton John이 "Digital Forensics for Preservation" 라는 제목으로 보고서 출판한 바 있다.

7) Steve Hitchcock, "Towards smart storage for repository preservation services", 2008

3. 덴마크

덴마크 국가 기록원은 1973년 이후부터 전자기록물을 보관하기 시작하였다. 2004년, 덴마크 국가 기록원은 2000년 이전에 모은 전자기록물을 디지털 정보 보존을 위한 표준방식(preservation standard)[8]으로 이전(migration)하는 대규모 프로젝트를 착수하여 2010년 완료하였다. 이러한 디지털 데이터 이전의 주요 목적은 노후화된 기술로 만들어진 데이터를 보호하고 접근비용을 줄이기 위함에 있다. 이 이전(migration) 프로젝트에는 소프트웨어, 하드웨어, 외부 서비스 등을 합하여 총 135.000 유로가 사용되었다.

4. DoD 5015.02-STD

미국 DoD 표준은 전자기록관리 소프트웨어 어플리케이션을 위한 설계 기준 표준(ELECTRONIC RECORDS MANAGEMENT SOFTWARE APPLICATIONS DESIGN CRITERIA STANDARD)으로 기록의 생산, 분류, 색인, 저장, 검토, 검색, 복사, 이전, 파기 등 9개의 영역으로 나누어 23가지의 기능 요건을 정의하며, 각 요건과 관련된 데이터 요소 제시하고 있다. 이 표준은 2007년 4월 25일에 마지막으로 개정되었다(국가기록원 측에서 분석한 자료는 2002년 버전임). 최근 개정 문서에서 전자기록의 무결성 및 사이버 보안 관련 사항은 아래와 같다.

- Field-level Classification
  - RMAs(Records Management Requirements software)가 승인된 개인이 각각의 메타 데이터 필드를 분류할 수 있는 기능
- Marking Printouts and Displays
  - 출력, 보고, 쿼리, 검토 목록 등을 위한 메타데이터를 조직이 각각의 선택된 메타데이터 필드에 분류 제한 기능을 구현할 때, 현재 분류 필드와 분류 사유, 그리고 downgrading instruction이 필요
  - 집계 결과가 표시 될 때 최상위 분류 레벨이 표시
- Redacted Version Notification
  - RMAs는 수정된 버전이 공개 저장소에서 사용할 수 있는지 사용자에게 알림
- Populating "Reasons for Classification" from the Guide
  - 분류 가이드에 속해있는 주제가 선택 된 경우, RMAs는 분류 사유를 자동으로 채우는 기능 제공해야 함
- 강화된 데이터 보안과 무결성 제공
  - 메타데이터 변경에 대한 경고(alarm) 및 메타데이터 접근 통제 정책 지원

8) ISO 14721:2003 - Open Archival Information System(OAIS).

5. ERA Requirement Document

미국 전자기록관리에서의 무결성 관련 이슈를 파악하기 위해 미국 국립문서기록보관청(NARA: National Archives and Records Administration)의 전자기록 저장관리소(ERA: Electronic Records Archives)의 요건 문서(RD: Requirements Document)를 분석하였다. NARA는 1998년부터 전자기록물 관리를 위한 준비 작업을 거쳐 2011년 9월 미국 전자기록관리 체계인 ERA 구축을 완료하였고, 2012년 말에 각 연방정부 기관으로부터 ERA를 통해 전자기록물의 이관작업을 진행할 예정이다.[9] ERA는 미국 국가기록청의 전자기록물을 보존관리하기 위해 설계된 시스템이다. ERA는 미국 국가기록청이 관리하는 전자기록물의 전체 생애주기와 비전자기록물의 부분적 생애주기를 포함한다. ERA는 평가, 보존기한 책정, 이관, 인수, 접근을 위한 미국 국가기록청의 영구적 기록물처리 전체 과정을 지원한다. ERA는 연방정부, 민간 기증자, 그 외 광범위하고 다양한 원천으로부터 전자기록물을 입수(Ingest)할 수 있을 뿐만 아니라 미국 국가기록청이 소장하고 있는 전자기록물도 입수할 수 있다.

(표 2. ERA 기능 범위)

구분	주요 내용
기록물 관리 수행을 위한 주요기능	• 모든 기록물에 대한 스케줄링 과정(평가, 생산, 스케줄 승인) 조정 • 모든 기록물에 대한 기술사항 저장과 검색 • 전자기록물의 처리 및 저장 • 비전자기록물의 영구보존 처리과정 및 위치는 추적하지 않음 예) 상자의 이동, 서가정리 작업, 재 정리 • 비전자기록물의 전자적 포맷으로 전환하는 기능은 제공하지 않음 • 비전자기록물의 전자적 포맷 변환 결과의 기록물 입수(Ingest) • 이관된 전자기록물에 접근 가능하고 변조(위조)로부터 자유롭도록 함 • 처분합의(계약)에 따라 전자기록물 처분 • 전자기록물의 접근과 배포에 대해 제한을 강제할 수 있음 • 접근제한기록물과 고급 비밀로 분류된 민감한 기록물 저장 가능
전자기록물의 자동화된 영구처리과정을 위한 기능	• ERA로 데이터 입수를 정보통신과 물리적 매체를 통한 기록집합(set)의 물리적 이관 • 기록집합을 위한 설명 정보의 유효성 확인 • 전자기록물의 장기 보존 • 접근성과 진본성을 유지하기 위한 전자기록물의 변형 • 조사, 검색, 제시, 출력

9) 미국 전자기록관리체계 구축 동향 및 시사점, 조이형, 2011

ERA는 (표 2)의 기능을 통해 볼 때 일종의 영구기록관리시스템(AMS)라고 볼 수 있다. 한국은 각급 기관 RMS에서 기록물 이관 요청, 기록물처리일정 관련 업무를 수행하는데 반해 미국의 경우는 각 연방기관 관계자들이 내부 기록관리 업무를 위해서는 RMS를 사용하고, 기록물 이관과 기록물처리일정표 승인과 관련한 업무는 ERA를 통해 수행하고 있다.

(표 3. 한국과 미국 RMS-AMS 역할 비교[10])

구분	세부 내용
한국	• RMS(각급기관) : 기관내 기록물관리 업무 수행, 기록물 처리일정 관련 업무, 기록물 이관(RMS->CAMS) • AMS(국가기록원-CAMS): RMS->CAMS 이관 연계, 이관 이후 국가기록원 내부 프로세스
미국	• RMS(각급기관) : 기관내 기록물 관리 업무수행 • AMS(국가기록청-ERA): (기관담당자 ERA 접속) 기록물 처리일정 관련 업무, 기록물 이관요청 및 패키징 이관 작업, (국가기록청 직원) 이관 이후 단계 국가기록청 내부 프로세스

ERA 요건서(RD, Requirement Documents)는 미국 국가기록청이 ERA 구축을 위해 필요한 요구사항을 규정한 문서이다. ERA RD는 2002년 4월 버전 1.0을 시작으로 2002년 8월에 버전 2.0을 거쳐 2003년 12월 버전 3.0이 만들어졌고, OAIS 모델을 기초로 분류되고 다듬어져 최종적으로 2010년 7월 버전 4.0이 만들어 졌다.

ERA RD에서는 기록 관리(Records Management), 보존(Preservation), 기록관리 저장(Archival Storage), 보안(Security), 기록물 입수(Ingest), 접근(Access), 이용자 인터페이스, 행정관리, 시스템 특성으로 범주를 나누어 각각에서의 요구사항을 서술하고 있다.

- 기록 관리(Records Management)

시스템은 모든 종류의 기록관리 생애주기를 위한 미국 국가기록청의 관리 과정에 대한 의사결정을 지원하게 된다. 여기에는 전자 및 비전자기록물에 적용하는 평가, 보존기한 책정, 기술(description)과 같은 활동을 위한 영구기록절차의 지원이 포함된다. ERA의 기록관리 과정은 처분 합의(disposition agreements) 관리, 기록물의 물리적 이관 관련 문서화와 업무흐름(업무지원 시스템의 한 유형으로서의) 관리, 기록물 생애주기 데이터 관리, 기록물의 법적 보관에 대한 이관 관련 문서화와 업무흐름 관리 등을 포함한다.

10) 미국 전자기록관리체계 구축 동향 및 시사점, 조이형, 2011

- 보존(Preservation)

ERA RD는 전자기록물의 보존 측면에서, 전자기록물을 위변조로부터 보호하며, 생산 시기와 저장·전송·관리 방식에 관계없이 전자기록들이 진본 사본으로 출력될 수 있다는 것을 보장해야 된다고 서술한다. 전자기록 보존 분야에서 다루어져야 할 필수요건은 매체이전 등의 과정에서 전자기록물의 진본성을 보장하는 것과 전자기록의 저장, 통신, 관리 등에 사용되어진 정보기술의 변화에 상관없이 전자기록물의 진본성 사본의 출력을 가능하게 하는 것이다. 보존 프로세스에서는 전자기록의 이전 또는 영구보존 포맷으로의 변환 등도 포함하며, 기록물의 진본성을 증명하기 위해 모든 보존 활동에 대한 감사추적(audit trail)을 생성하고 관리하여야 한다고 서술한다. 여기서의 감사추적은 디지털 포렌식 측면에서의 연계 보관성(Chain of Custody)과 관련이 있다고 추정할 수 있다.

- 기록관리 저장(Archival Storage)

ERA는 전자기록물을 포함하는 신뢰할 수 있는 데이터의 저장을 요구하는데 여기에는 저장 관리 서비스, 모든 저장데이터의 물리적 무결성을 보장하기 위한 매체 관리, 전체 기록물 자산의 확인 및 위치 탐색, 여러 개 기록물 자산의 복제 관리, 매체이전(migration) 등이 포함된다.

- 보안(Security)

ERA 보안은 부당한 접근과 피해로부터 자산을 보호하는 것과 승인된 사용자들에게 자산에 대하여 지속적인 접근을 보장하는 것을 포함한다. ERA는 다양한 위협들(threats)로부터 시스템 자체뿐 아니라 자신이 보유하고 있는 자산을 보호해야 한다. 보안 체계는 시스템 자원 및 서비스, 사용자, 그리고 정보 자산에 대하여 적용되어야 한다.

- 입수(Ingest)

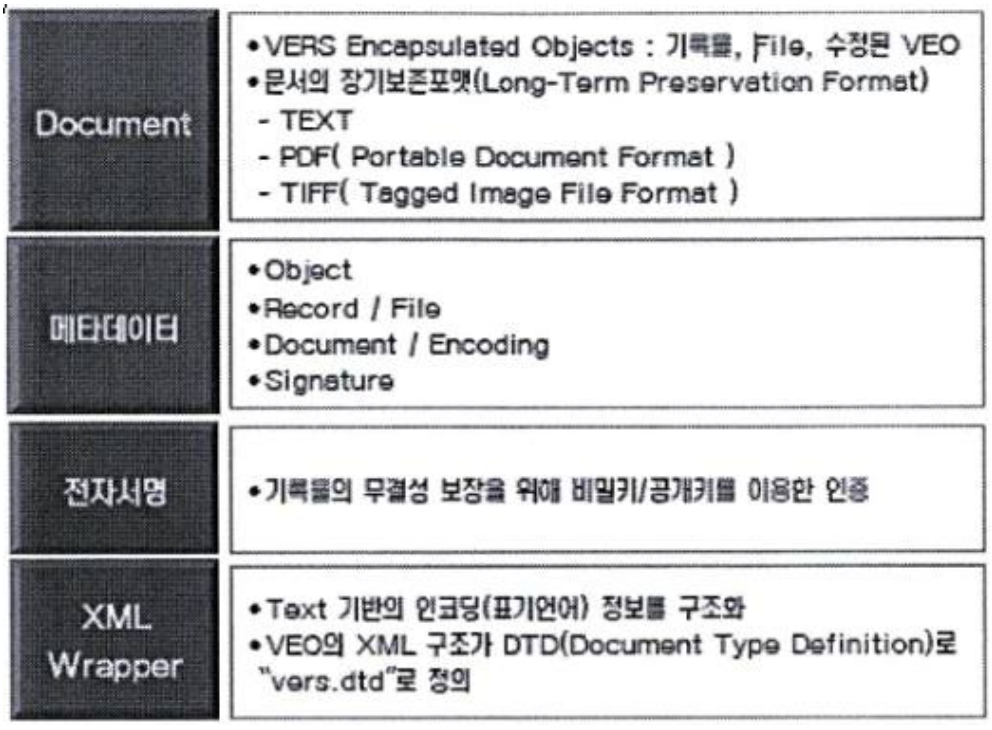
입수는 전자기록물을 ERA로 가져오는 과정으로 전자기록물을 ERA로 물리적으로 이관하는 것과 이관 컨텐츠의 유효성 검증을 포함한다. 이관하는 기관은 지원되는 모든 파일 포맷 유형의 전자기록을 이관할 수 있어야 하며, 각각의 이관 대상에 대하여 무결성(integrity), 정확성(correctness), 그리고 완전성(completeness)을 점검하여야 한다. 또한, 다양하게 정의된 기록관리적·기술적 특성을 확인하기 위해서 ERA는 기록관리 업무 수행자들(archivists)이 이관된 전자기록들에 대한 검증 일과(verification routines)를 가동할 수 있는 툴을 제공해야 한다. 이는 전자기록물이 증거로 인정받기 위한 신뢰성 요건과 밀접한 연관이 있다고 추정할 수 있다.

• 접근(Access)

기록물 자산으로의 접근 제공에 대해서는 시스템 내에 포함된 모든 기록물 자산뿐만 아니라 기록물을 발견하기 위한 검색 성능이 요구되어진다. ERA는 기록물 생산자에 의해 구축된 그룹 내에 전자기록물의 정리된 묶음(Ordered sets)으로 접근을 제공할 수 있어야 하는데 이 접근 제공에는 사용자가 받기를 원한 것에 대한 접근 제공과 제한된 내용에 대한 비인가 접근 제한 두 가지 의미가 포함되어 있다. 이 경우 접 근 제한은 전자기록물 전체 또는 개별 단위로 적용할 수 있다.

6. VERS@DOI

1995년 호주 빅토리아 기록보존소(PROV, Public Record Office Victoria)는 빅토리아 주의 공공기관에서 생산되는 전자기록물을 장기적으로 보존하기 위한 보존 전략을 개발하기 위해 전자기록관리전략 VERS(Victorian Electronic Records Strategy) 프로젝트를 수립하였다. VERS는 이관 및 보존을 위한 XML 기반 포맷으로 VEO(VERS Encapsulated Object)를 정의하고 있으며, VEO는 장기포맷으로 변환된 기록과 기록물 보존 및 관리에 필요한 정보를 포함한 메타데이터, 무결성 보장을 위한 인증정보를 포함한 전자서명, 텍스트 기반의 인코딩 정보를 구조화하는 XML 래퍼로 구성된다[11].

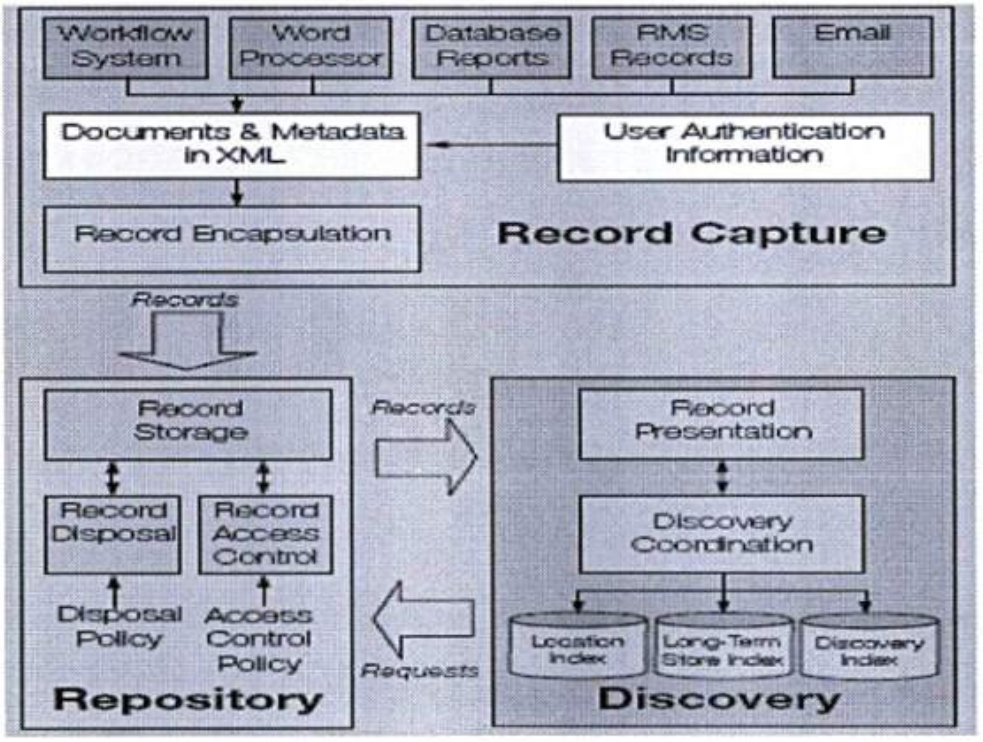


(그림 4. VEO 구성요소[12])

11) 전자기록의 관리와 보존을 위한 국제협력 아젠다 개발, 국가기록원, 2007

12) 디지털 아카이빙 보존 전략에 관한 분석 및 연구, 이경란, 2008

VERS@DOI는 VERS의 표준에 따라 가 부처별로 기록물 관리 시스템을 구축하기 위한 목적을 가진 프로젝트로 전자 기록물의 영구보존 및 장기적으로 기록에 대한 접근이 가능한 시스템에 대한 요구사항을 서술하고 있다. 각 부처에서 만들어지는 모든 형태의 문서는 다양한 소프트웨어를 통해 VERS 기록물 캡쳐 모듈로 전달된다. VERS 기록물 캡쳐 모듈은 기록물 객체 모델인 VEO로 전자 기록물 형태를 변환하여 VERS의 저장소로 보낸다. VERS@DOI의 주요 세가지 기능은 다음과 같다.[13)]



(그림 5. VERS@DOI의 세 가지 기능)

- 기록물 캡쳐(Records Capture)
  - 다양한 포맷으로 생성된 기록물을 XML 포맷으로 변환하고, 내용 정보와 그에 해당하는 메타데이터 추출
  - 내용, 메타데이터, 사용자 인증 정보를 함께 캡슐화하여 VEO 생성

- 저장(Repository)
  - VEO 객체의 장기 보존 및 접근 기능 포함

- 검색(Discovery)
  - 기록 열람 요청자가 정보를 검색하기 위한 사용자 인터페이스 제공

13) 디지털 아카이빙 보존 전략에 관한 분석 및 연구, 이경란, 2008

VERS@DOI는 2003년 7월 31일에 마지막으로 개정되었다(기록원 측에서 분석한 문서의 버전과 같음). 마지막 개정된 버전에서 전자기록의 무결성에 대해 다음과 같이 언급하고 있다.

- 전자기록물은 법적 증거물로써 반드시 인정될 수 있어야 하며(must be admissible as evidence), 또한 법정에서도 이에 대해 마땅히 고려되어야 함

- 기록물이 누구에 의해서 최초 생성되었으며, 이후 허가 없이 변경되지 않았음에 대해 증명할 수 있는 능력이 필요

- 기록의 무결성(integrity)에 대한 증명
  - 문서의 무결성이 지켜져야 함을 원칙으로 하나, 정책에 의해서 변경이 허가되는 경우 법적 증거 능력이 상실되지 않는 범위에서 변경이 가능

7. Moreq

MoReq(Modular Requirements for Records System)는 유럽 전체를 대상으로 하고 있으며, 국제적으로 적용 가능한 전자기록관리 기능요건을 정의하고 있다. 분류표와 편철지침, 접근과 감사, 백업과 시스템 복구, 보유와 처분, 이관 혹은 파기, 기록획득, 고유 식별자 원칙, 검색(디스플레이 및 출력), 시스템 관리, 전자 형태가 아닌 기록의 관리나 하이브리드 기록철, 문서 관리, 전자서명과 암호화 등 기타 기능을 8가지로 제시한다. 이 문서는 2010년 마지막으로 개정되었으며(기록원 측에서 분석한 문서는 2002년 버전), 전자기록에 대한 접근제어를 위해 아래와 같은 요구사항을 정의한다.

- 기록물의 소유권을 토대로 접근 제한
  - 자신이 속한 그룹에 대해서만 기록물을 생성, 열람할 수 있음

- 각 비즈니스 유닛은 유저-기록물의 접근에 대한 레벨을 설정해야 하며 각 레벨 간 접근권한을 설정해 보안을 유지해야 함

제 2 절 전자기록물의 디지털 포렌식 적용 연구 동향

국외 전자기록물 관리에 있어 디지털 포렌식 적용 연구 사례에 있어서는 Luciana Duranti, Matthew G. Kirschenbaum, Christopher A. Lee 등의 기록관리 분야 또는 디지털 포렌식 전문가들이 전자기록관리와 디지털 포렌식을 아우르는 분야에 대해 진행한 연구 결과물들을 위주로 분석하고 있다. 주요 연구 프로젝트로는 『InterPARES Project』, 『Digital Records Forensics Project』, 『Digital Lives』, 『Digital Forensics and Born-Digital Content in Cultural Heritage Collections』, 『AIMS』, 『BitCurator』등이 있으며, 이와 더불어 Stanford University Libraries, Bodleian Libraries, King's College London 등 해외 주요 도서관에서 전자기록 수집 및 분석에 있어 디지털 포렌식 기술을 사용하고 있는 사례들에 대해 개략적으로 조사하였다. 특히, 2010년 Matthew G. Kirschenbaum(Professor of the University of Maryland)에 의해 진행되었던『Digital Forensics and Born-Digital Content in Cultural Heritage Collections』프로젝트는 전자기록관리에 디지털 포렌식을 접목한 기존 사례들에 대해 전반적으로 소개하고, 디지털 포렌식 적용 가능 부분과 이점 등에 대해 구체적으로 기술하고 있어 주의 깊게 살펴볼 필요가 있었다. 또한, 이 프로젝트의 후속으로 『BitCurator』라는 이름으로 2011년부터 Christopher Lee(Professor of the University of North Carolina) 교수와 함께 전자기록수집 및 분석 단계에서 실질적으로 활용할 수 있는 디지털 포렌식 통합 도구를 개발하고 있기에 관련 진행 사항을 계속해서 주의 깊게 살펴볼 필요가 있다.

다음에서는 본 연구에서 조사한 디지털 포렌식 적용 연구 동향들을 개략적으로 살펴보고, 앞서 언급한 『Digital Forensics and Born-Digital Content in Cultural Heritage Collections』프로젝트 및 『BitCurator』프로젝트에 관해서는 좀 더 구체적으로 기술한다.

1. InterPARES Project

InterPARES(International Research on Permanent Authentic Records in Electronic System) 프로젝트는 진본 전자기록의 생애주기 전반에 걸친 장기보존 문제의 해결방안을 모색하기 위한 다국적 연구 프로젝트이며 1998년 1차 프로젝트를 시작한 이래 현재까지 총 3단계에 걸쳐 진행 중에 있다. 이 프로젝트의 연구 책임자는 UBC(University of British Columbia) Dr. Luciana Duranti 교수이다.

- InterPARES 1차 프로젝트(1998~2002)

전자기록의 진본성을 이론적으로 규명하고 진본성을 평가하거나 추정할 기준 요건을 밝히는 것을 목적으로 하며, 보존자 관점에서 진본 전자기록을 장기적으로 보존하는데 필요한 이론적 방법론을 개발하였다.

• InterPARES 2차 프로젝트(2002~2007)

예술, 과학, 전자정부 분야의 복잡한 디지털 환경에서 생산된 기록물을 중심으로 생산부터 영구보존까지 전체 생명주기 관점에서 진본성, 신뢰성, 정확성에 대한 제반 문제 연구를 진행하였다.

• InterPARES 3차 프로젝트(2007~2012)

정부나 기업, 단체, 연구, 예술, 오락, 사회 및 지역사회 활동 등 다양한 영역에서 전자 기록을 생산하고 관리하는 중소 규모의 공공 및 민간기록 생산조직 및 프로그램들이 실무에서 활용할 수 있는 지침을 마련하는 것을 목적으로 한다.

2. Stanford University Libraries

2008년, Stanford University Libraries는 디지털 기록 매체의 정보를 확인하기 위한 연구를 수행하였다. 이 연구의 목적은 디지털 기록 매체의 용량, 나이 그리고 비트 부식(bit rot) 및 포맷 노후화(format obsolescence) 에 따른 정보 손실 위험도를 측정하기 위함이었다. 2009년에는 디지털 포렌식 연구실을 설립하고 FRED 장비 2대와 상용 포렌식 소프트웨어(Access Data's Forensic Toolkit, Guidance Software's EnCase Forensic)를 구입하였다. 하드웨어 장비는 다양한 범위의 레거시 디바이스(legacy device)를 지원하기 위해 부분적으로 수정되었다[14].

(그림 6. 스탠포드 대학이 개발한 하드웨어 기반 포렌식 툴 - FRED[15])

14) 이 수정 사항으로 인해 다양한 종류의 하드드라이버, 광디스크, 플래쉬 메모리, Imoega Zip 디스크 등을 지원할 수 있게 되었다.

15) Digital Forensics and Born-Digital Content in Cultural Heritage Collections, 2010

3. Bodleian Libraries

옥스퍼드 대학교의 Bodleian도서관에서는 기록물들의 보존을 위해서 전자 기록물의 문서화 및 문서의 전자 기록물화 위해 Bodleian Electronic Archives and Manuscripts(BEAM) service를 개발하고 있다. 이 BEAM에서는 Digital forensic tool들은 데이터 출처의 인증 및 대용량의 데이터를 처리하는데 용이하기 때문에 본래의 기능보다는 기록 보관을 위한 도구로 여겨진다. 다음은 BEAM service에서 hybrid archive의 workflow이다.

- Separation : Hybrid archive를 적용할 대상을 선정한다.
- Capture : Digital forensic tool을 이용하여 각 디스크의 내용을 신뢰할 수 있는 사본 및 hash value, 각 개체에 대한 hash 및 메타데이터 형식을 포함하는 디스크의 내용의 목록, 이미징 프로세스에 대한 메타데이터, 그리고 디스크의 사진을 얻어낸다.

4. King's College London

King's colleage of London은 디지털 포렌식 기술을 기록물 저장소(기록원)에 적용하는데 관한 연구 결과를 발표했다. 그 내용은 2011년 6월에 옥스포드 센터에서 발표한 "Digital Forensics in the Archive" 자료에서 확인할 수 있다. 그들은 주제와 관련하여 FIDO(Forensic Investigation of Digital Objects) 프로젝트를 진행하였다. 이 프로젝트는 디지털 미디어와 컴퓨터 시스템에 의한 디지털 정보의 지속과 보존을 제공하기 위한 디지털 포렌식 어플리케이션을 조사하는 것을 목표로 하고 있다. 특히 다음 세 항목이 주 목적이다. 첫째, 이 프로젝트는 HE archives가 디지털 기록을 유지하기 위한 조직의 규약과 법적인 요구사항에 부흥하는 것을 가능케 하는 디지털 포렌식 원리들과 사례들의 적합성을 평가할 것이다. 둘째, 디지털 정보를 획득하고, 식별하고, 분석하기 위한 오픈소스 디지털 포렌식 도구를 사용하여 효율성을 평가한다. 마지막으로 디지털 포렌식 도구 및 기술을 KCL Archives & Information Management(AIM)의 Working Practice에 포함하는 것을 추구하는 것이다.

발표자료에는 기록물 저장소에 포렌식을 적용할 때, 고려해야할 문제들을 제시하고 있다. 첫째로, 데이터가 캡쳐되는 위치나 대상이 되는 하드웨어 및 그 환경에 적합한 하드웨어/소프트웨어 등, 작업환경에 대한 문제점을 제기하였다. 둘째로, "기록자나 수집가가 갖고 있어야 할 지식이나 전문능력이 무엇인가?", "어떤 훈련이 필요한가?"로써 조사 작업을 수행 하는 사람에게 고려해야 될 문제들을 제기하였다. 셋째로, "자료 증여 협정 시, 삭제되거나 조각난 데이터의 검색에 관련한 문제들에 대해서 어떻게 전달할 것인가?"에 대한 문제를 제기하면서, '포렌식 클럽의 첫번째 룰은 포렌식에 대한 언급을 하지 않는 것이다.'라고 한 가지 답변을 제시하기도 하였다.

또한, 기록물을 저장한 파일에 대해서 파일이름, 작성자, 매직넘버와 같은 고정된 값 등, Hashset을 이용하여 파일의 출처나 목적에 대한 판단을 한다고 밝히고 있다. 파일이 운영체제나 어플리케이션의 목적으로 사용되는지, 바이러스, 크래커의 툴, 그외 악성 파일들인지 판단할 수 있다. 이는 NIST의 NSRL(National Software Reference Library)에 기록된 Hashset을 이용해 판별하거나 HashKeeper와 OFSDB(Online File Signature Database) 와 같은 소프트웨어와 데이터베이스를 이용해서 판별할 수 있다고 하였고, 발표 시기에는 알려진 서드파티가 만든 파일인지, 기타 사용자가 만든 파일인지 기록자가 구별하여 식별했다고 하였다.

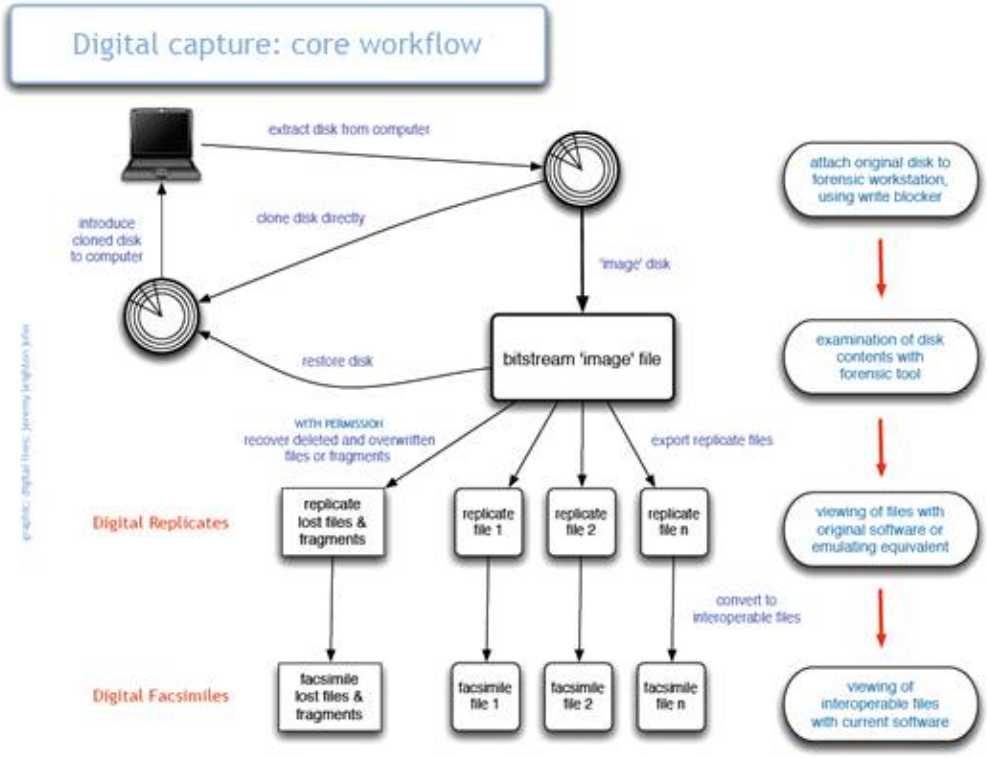
5. Digital Records Forensics Project

University of British Columbia's School of Library, Archival and Information Studies(SLAIS), UBC Faculty of Law, Computer Forensics Division of the Vancouver Police Department의 공동연구로 2008년부터 2011년까지 진행되었으며, UBC(University of British Columbia) Dr. Luciana Duranti 교수가 총괄 책임을 맡았다. 이 연구는 현재의 전자기록관리 분야와 디지털 포렌식 분야 각각의 한계점과 문제점에 대해 논의하였다는데 의의가 있다. 전자기록이 원본 매체에서 이전된 후 그 정보를 정확히 파악하는 것에 대한 문제(원본 시스템의 다양성으로 인한 어려움)와 전자기록 관리에 있어 진본성을 어떻게 보장할 것이며, 법적 증거물로 채택될 수 있는가에 대한 문제 그리고 전자증거물의 보관에 있어, 어떻게 영구보관 할 것인가(공소시효 기간 동안 증거물의 무결성 유지)에 대한 문제를 논의하고, 두 분야의 기술들이 서로에게 도움이 될 수 있음을 나타내었다. 이 연구의 결과로 전통적인 문서학(diplomatic)에 디지털 포렌식(digital forensic)을 접목시킨 새로운 모델인 "Digital Records Forensics" 이라는 개념을 정립하였다.

6. Digital Lives

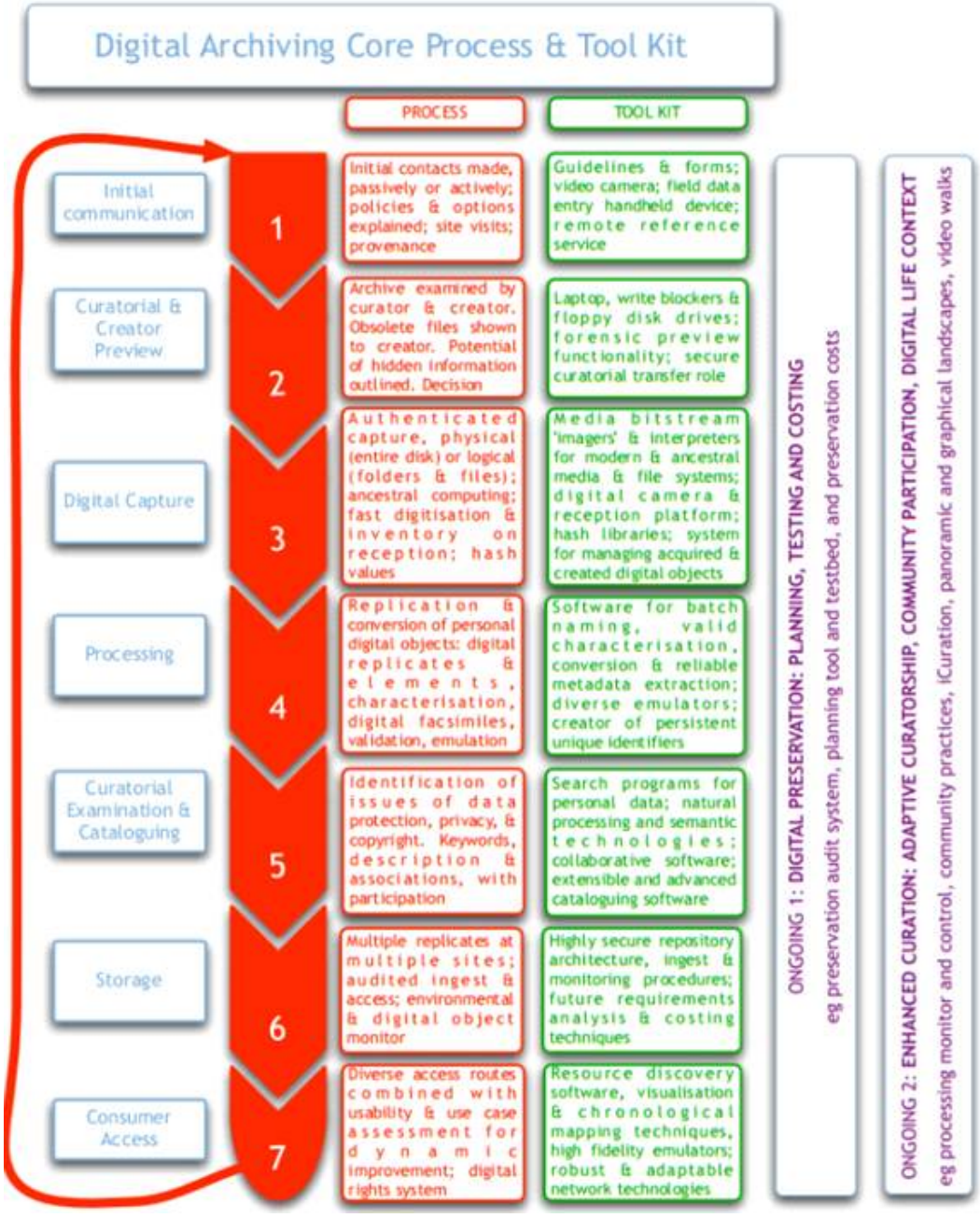
Digtial Lives 프로젝트는 영국국립도서관(British Library)의 큐레이터인 Jeremy Leighton John에 의해 2009년 수행된 프로젝트이다. 이 프로젝트는 전자기록의 보존 및 관리에 있어 디지털 포렌식 기술을 접목을 선구적인 연구로 평가받고 있다. 실제 이 연구 이후 수행된 Digital Forensics and Born-Digital Content in Cultural Heritage Collections(2009~2010), AIMS(2009~2011) 등의 연구는 Digital Lives 프로젝트의 연구결과에 많은 영향을 받았다. Jeremy Leighton John은 최근에도 여러 학회 및 워크샵에서 디지털 포렌시 관련 연구 내용들을 발표하는 등 왕성한 활동을 하고 있다. Digital Lives 프로젝트의 최종 보고서는 2010년 출간되었으며 전자기록의 진본성(authentication) 보장을 위해 매체 이전(migration) 단계에서 디지털 포렌식 도구(FTK Imager 등) 적용하는 방법과 함께 전자기록 관리 work flow에서 디지털 포렌식 기술

및 절차를 접목시키는 방안에 대해 제시하였다(그림 7)(그림 8).



(그림 7. Digital Capture: Core workflow[16])

16) Digital Lives, 2009



(그림 8. Digital Archiving Core Process & Tool Kit[17])

STEP 1 : Initial Communication

- 이관 자료에 대한 정보 교환

STEP 2a : Examination of Archive, offsite and/or onsite

- 이관 대상 자료가 근래 IT 기술 매체에 기록된 경우, 쓰기방지장치(write blocker) 및 포렌식 렙탑(forensic laptop) 준비
- 이관 대상 자료가 오래된 IT 매체(3.5", 5.25" floppy disk 등)에 기록된 경우, usb

17) Digital Lives, 2009

인터페이스로 연결할 수 있는 reader 준비

STEP 2b : Explain to creator the pros and cons of physical or logical acquisition

- 기록 생산자 및 기증자에게 전자기록에 대한 물리적 수집 및 논리적 수집의 장·단점을 인지시켜주고 수집 방법에 대한 선택 및 허가 권한 획득

STEP 2c : Curatorial report to institution followed by decision and any transfer of media and hardware to repository

STEP 3 : Acquisition with digital capture using forensically sound techniques, retained in holding repository

- 쓰기방지장치를 이용한 포렌식 이미지(hash 값 포함) 수집
- virus, malware 체크

STEP 4a : Digital Replicates

- 이미지 파일로부터 replicate 파일 추출
- replicate 파일들에 대한 속성 파악
- 이미지 파일 및 replicate 파일들에 대한 메타데이타 추출

STEP 4b : Digital Facsimiles

- Replicate 파일들에 대해 상호 운용 가능한 포맷(PDF/A, XML 등)으로 변환한 facsimiles 파일 생성

STEP 4c : Produce access copies (of the replicates and facsimiles) and describe process

STEP 4d : Option for making available media 'image' file

- Replicate 파일 또는 facsimile 파일을 추출하지 않고도 이미지 파일 자체에 대한 접근이 가능한 옵션

STEP 5 : Curatorial examination and cataloguing

- 프라이버시 이슈 및 저작권 이슈 검사

STEP 6 : Digital archival storage system

- 전자 기록 및 메타데이타를 기록보존소에 저장

STEP 7 : Access including use of emulators

- 저장된 기록에 대한 접근제어를 포함한 활용

7. Digital Forensics and Born-Digital Content in Cultural Heritage Collections

이 연구는 Matthew G. Kirschenmaum, Richard Ovendan, Gabriela Redwine가 공동으로 Andrew W. Mellon Foundation로부터 자금을 지원받아 2009년에서 2010년 사이에 진행되었다. 이 연구의 목적은 기록학 분야의 전문가에게 디지털 포렌식 분야를 소개하는 것으로, 전자기록 관리에 있어 디지털 포렌식를 적용할 수 있는 부분들에 대해 다음과 같이 논의하였다.

- Legacy Format

기술의 발전에 따라, 전자기록이 생성되는 환경(물리적 매체, 운영체제, 파일시스템, 파일 포맷, 프로그램 등…)이 변화하기 때문에 legacy format으로 생성된 전자기록을 새로운 매체로 이전할 필요성이 존재하게 된다. 이 때 매체 및 포맷 등의 변화로 인해 전자기록의 무결성이 훼손될 가능성이 존재하게 된다. 예를 들어 FAT32에서는 파일 용량 제한(4GB) 및 파일 이름 길이 제한 등이 있으며, NTFS에서는 /, \, : 와 같은 문자들을 파일 이름으로 사용 못하는 반면 HFS 파일 시스템에서는 : 를 제외한 모든 문자를 허용한다. 이러한 파일 시스템 간의 차이는 서로 다른 파일 시스템 간의 전자기록 이전(migration)에 있어 기록의 무결성을 훼손시킬 수 있다. 이 때 포렌식 기술을 이용한 저장매체 이미징을 통해, 기록 이전 단계에 있어서의 파일 시스템 등의 차이로 인한 의존성 탈피할 수 있다.

- Trustworthiness

디지털 기록이 원본 매체로부터 기록 보존소(repository)까지 이동되기까지 무결성 및 신뢰성을 보장할 수 있어야 한다. 원본 매체에서 처음 디지털 기록을 수집할 때 신뢰성을 인정받은 디지털 포렌식 도구를 이용함으로써 무결성을 보장할 수 있다.

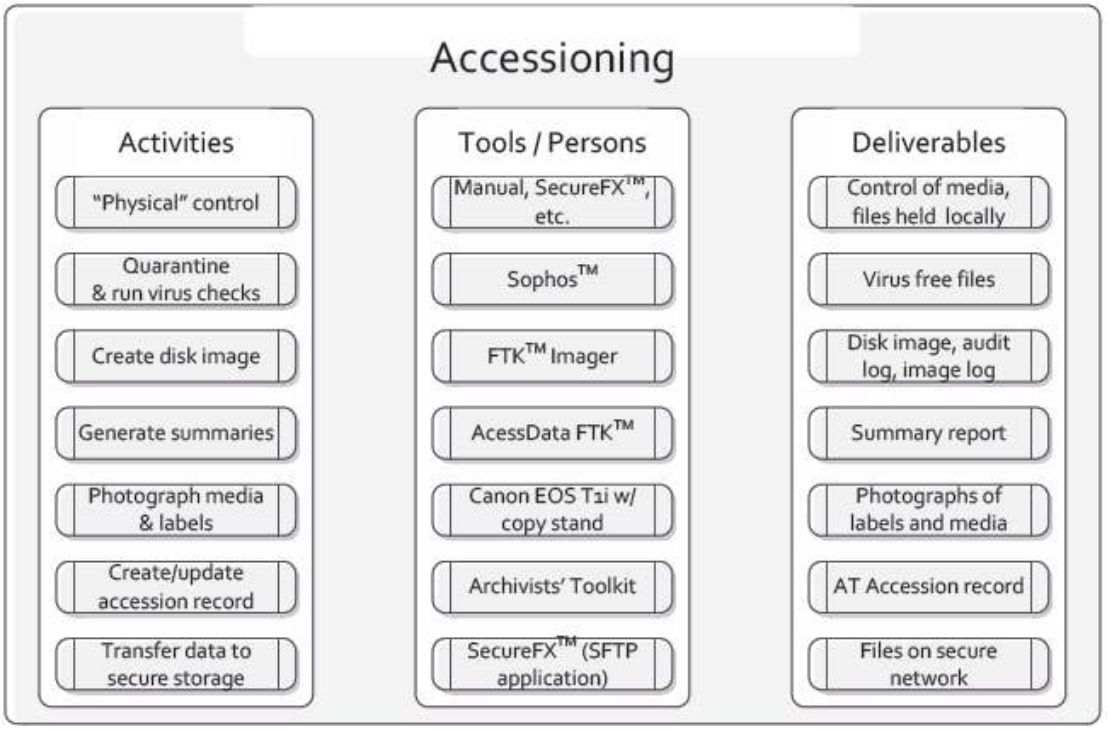
- Data Recovery

디지털 포렌식 기술을 이용해 의도치 않게 지워진 기록의 복구가 가능하다.

이 연구의 책임자 중 한명인 Matthew G. Kirschenmaum는 2011년 12월부터 전자기록 수집 프로세스에 있어 디지털 포렌식 기술을 적용하는 방안에 대한 연구로써 BitCurator 프로젝트를 진행하고 있다.

8. AIMS(An Inter-Institutional Model for Stewardship)

AIMS 프로젝트는 디지털 방식으로 생성된(born-digital) 기록들을 관리하기 위한 방법론 및 지속 가능한 프레임워크(Model for Stewardship)를 제시하기 위해 Andrew W. Mellon 재단의 지원을 받아 University of Virginia Libraries, Stanford University Libraries and Academic Resources, University of Hull Library, Yale Uiversity Library의 공동연구로 진행된 프로젝트이다. 이 프로젝트의 최종 보고서[18]는 2012년 1월에 발표되었으며, 제안하는 전자기록 관리 프레임워크(framework for the stewardship of born-digital materials)에서 기록의 수집(capture), 식별(identification), 보전(preservation)에 있어 기존의 디지털 포렌식 분야에서 사용되는 도구들(AccessData 社 FTK3.3, FTK Imager 3.0)을 활용하였다고 기술하고 있다. FTK Imager 3.0은 매체에 저장된 디지털 기록을 이미징(Imaging)하는데 사용하였고, FTK 3.3을 통해 이미징한 대상에서 의미 있는 정보들을 추출하였다.



(그림 9. Access 단계에서의 activity 및 사용 도구[19])

18) www2.lib.virginia.edu/aims/whitepaper/AIMS_final.pdf

19) AIMS Born-Digital Collections: An Inter-Institutional Model for Stewardship, 2012

9. BitCurator

BitCurator 프로젝트는 기록 수집 기관(collecting institution)의 업무 프로세스(workflow)에서 디지털 포렌식 도구를 적용하여 디지털 기록의 무결성 및 신뢰성을 확보하고, 잠재적으로 가치성 있는 정보(potentially valuable data)를 식별하기 위한 목적으로 시작되었다. 현재 School of Information and Library Science(SILS) at the University of North Carolina와 Maryland Institute for Technology in the Humanities (MITH) at the University of Maryland의 공동연구[20]로 2011년부터 진행되고 있다. AFF(Advanced Forensics Format)을 지원하는 전자기록 수집 도구(Disk Imaging Tool), 이미지 파일에서 특징적인 정보를 추출하는 분석 도구 등을 개발 중에 있으며 이들에 대한 통합 테스트 버전과 소스코드를 공개하고 있다[21]. 2012년 9월 12일 BitCurator 0.1.5 버전이 릴리즈 되었으며, BitCurator 기본 요구사항 문서(Basic Requirement Documents) v0.9가 2012년 9월 11일 발표되었다. BitCurator 프로젝트에 대한 진행 정보는 해당 홈페이지[22]에서 확인 가능하며, 다음에서는 BitCurator 기본 요구사항 문서를 기초로 BitCurator의 범위와 계획 그리고 기술적 사항들을 살펴본다.

가. 범위

BitCurator는 기록 수집 기관(collecting institution)의 업무 프로세스(workflow)에서 디지털 포렌식 도구를 적용하여 전자기록의 수집, 분석, 평가에 있어 활용하는 것을 주요 목적이다. 이 프로젝트의 수행은 2단계로 나누어 진행될 예정이며, 현재는 Andrew W. Mellon Foundation의 재정적 지원을 받아 1단계(2011.09~2013.09) 프로젝트를 수행중이다. 1단계에서의 주요 목적은 1차적인 전자기록관리에서의 디지털 포렌식 시스템 개발에 있으며, 2단계에서는 지속적인 업데이트와 안정성 개선에 있다. 다음은 1단계에서의 주요 목적이다.

- 전자기록물을 수집/분석하기 위해 공개된 오픈소스 기반의 이미징 도구, 디지털 포렌식 도구, 메타데이타 추출도구 식별
- 현재 존재하는 전자기록관리 시스템에서 위에서 식별한 도구들을 사용할 수 있는 통합 환경 제공
- 기 식별한 도구들에 대해 기록 관리 환경에 적합한 형태로의 수정/보완
- 현존하는 전자기록관리 프로세스에서의 문제점 식별 및 BitCurator 적용 가능 케이스 도출

---

20) Christopher A. Lee(Associate Professor at the University of North Carolina)와 Matthew Kirschenbaum(Associate Professor, University of Maryland)가 공동으로 프로젝트 주도

21) http://wiki.bitcurator.net/index.php?title=Software

22) http://www.bitcurator.net/

나. 일반사항

도서관(Library), 기록보존소(Archive), 박물관(Museums)들은 점점 더 디지털 방식으로 기록된(Born-Digital) 매체에 대한 수집/분석/관리/보존 요구가 늘어나고 있는 상황에 맞닥뜨리고 있다. 전자기록의 관리 프로세스에서는 처음 기증자가 제공한 기존의 매체로부터 보존 매체로의 기록 이전(migration)이 일어날 수 있는데, 이러한 상황에서 기록의 무결성 등이 보장되지 않는다.

디지털 포렌식(Digital Forensic) 분야에서는 이러한 매체 이전의 상황에서 디지털 증거의 무결성을 보장하는 도구, 기술 및 절차가 잘 정의되어 있지만 아직까지 기록관리 분야에서 잘 활용되고 있지 않다. BitCurator는 이러한 갭(Gap)을 줄이고자 전자기록관리에서 사용할 수 있는 디지털 포렌식 도구 및 방법을 제공한다. 다음은 BitCurator에서 제공하고자 하는 기능들이다.

- 기록저장매체로부터 디스크 이미징(Imaging)
  - HDD, 광디스크, 플로피 디스크 등으로 부터의 raw data 이미징과 AFF 패키징 기법을 포함하며 Encase 포맷 등 다른 이미징 포맷도 고려
  - 디스크 이미징 하드웨어 사용을 위한 문서 또한 제공할 예정

- 이미지로부터 메타데이타 추출 및 연계(Metadata Association)
  - 포렌식 소프트웨어로부터 생성되는 provenance metadata(시간 정보, 수집 및 분석 과정에 관한 로그)
  - 이미지 내용에 관한 메타데이타
  - 위의 메타데이터 들은 XML 형식(Digital Forensics XML, DFXML)으로 표현되어 기록관리 분야의 메타데이터 표준과 상호 호환될 것

- 이미지 수집/분석 결과에 대한 보고서 생성
  - 유즈케이스에 따라 XML, PDF, 또는 text 파일 형식으로 출력
  - 보고서는 아래와 같은 내용을 포함
    · 파일 트리 구조와 파일 시스템 속성에 관한 정보
    · 파일 타입 종류에 따른 개수
    · 디스크 이미지에 포함되어 있는 잠재적 중요 정보
    · 드라이브 볼륨에 관련된 사용자 계정 정보
    · 특정 볼륨에 설치된 소프트웨어 및 로그 파일
    · 파일 속성 정보에 기반한 파일 생성, 수정, 접근 시간
    · 삭제된 파일
    · File fragments

다. 사용되는 기술 및 도구

아래 그림은 BitCurator에서 사용하는 오픈소스 기반의 포렌식 소프트웨어를 나타낸다.

Forensics software	Current Version	Purpose
Data Processing		
Advanced Forensic Format Library (AFFLIB)	3.7.1	Support for AFF packaging of disk images
fiwalk	0.6.16 (or equivalent functionality in current SleuthKit Release)	Fast file and inode walks, DFXML output
Bulk Extractor	1.3.0	Identification of private/sensitive information
sdhash	2.0	Fuzzy hashing, file similarity
SleuthKit	3.2.3, 4.0 when available	Accessing and processing filesystem data
reg2xml, regXMLParse.py	0.1	Extraction and processing of Windows Registry data (including XML output)
Metadata		
lxml (libxml2, libxslt)	2.3	Python XML library, metadata handling and DFXML reprocessing
User Interface		
wxPython	2.8.12	BitCurator cross-platform interface development
Packaging		
Ubuntu packaging tools – build-essential, devscripts, ubuntu-dev-tools, debhelper, dh_make, diff, patch, cdbs, quilt, gnupg, fakeroot, lintian, pbuilder	Varies (see Ubuntu packaging docs)	Support for apt packaging of BitCurator sources, generation of the BitCurator virtual environment, and construction of a bootable ISO image

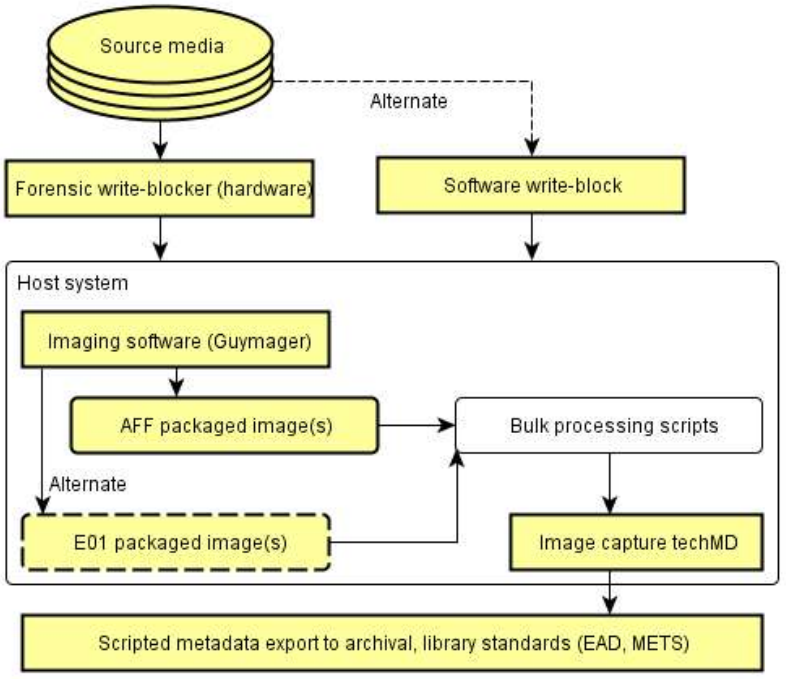
(그림 10. Forensics Software)

BitCurator의 기술영역은 크게 다음 4가지 기본 영역으로 구분된다.

- 디스크 이미징(Disk Imaging)
- 특징 정보 파악(Identification of Private and Sensitive Information)
- 정보 분류(Data Triage)
- 메타 데이터 추출(Metadata Export)

• 디스크 이미징(Disk Imaging)

BitCurator는 다양한 매체로부터 전자 기록을 이미징하기 위해 Guymager[23] 및 aimage[24]와 같은 기존 오픈 소스 이미징 툴을 이용하고 있다. 아래 그림은 BitCurator를 통한 디스크 이미징 기본 절차를 보여준다.



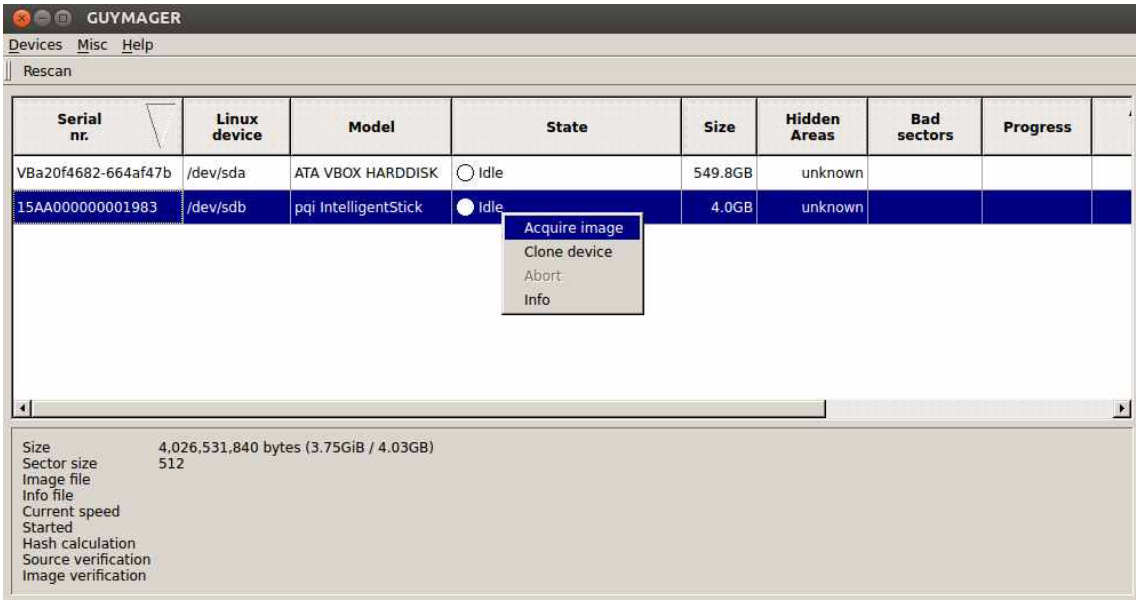
(그림 11. BitCurator Imaging 절차[25])

실제 테스트버전으로 제공하는 BitCurator 패키지를 다운받아 VirtureBox 4.1.18 버전에서 실행해 보았다. (그림 12)는 Gyumager를 통해 USB를 이미징 하는 것을 나타낸다. (그림 13)은 출력 이미지 파일 포맷을 설정하는 화면으로 raw 포맷, AFF(Advanced Forensic Format), E01(Encase 포맷) 중에 선택할 수 있으며, 이미지 파일의 무결성을 입증하기 위해 적용할 해쉬 함수(MD5/SHA-256)를 설정할 수 있다.

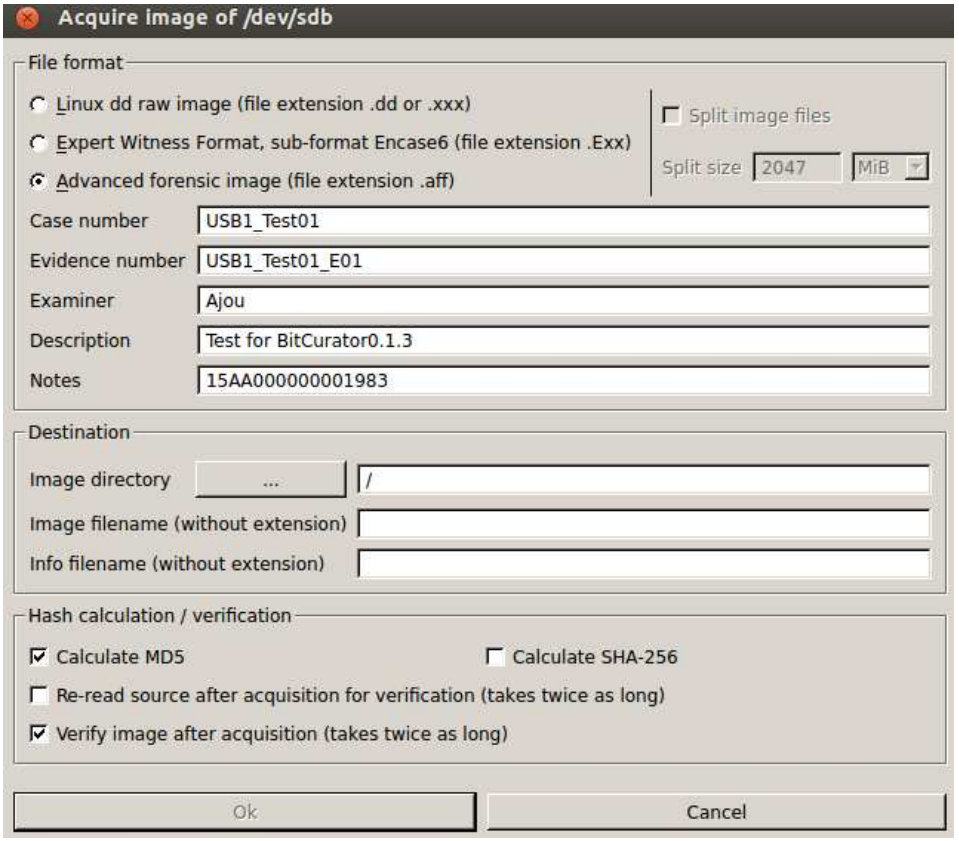
23) http://guymager.sourceforge.net/

24) http://afflib.org/software/aimage-the-advanced-disk-imager

25) http://wiki.bitcurator.net/index.php?title=Description



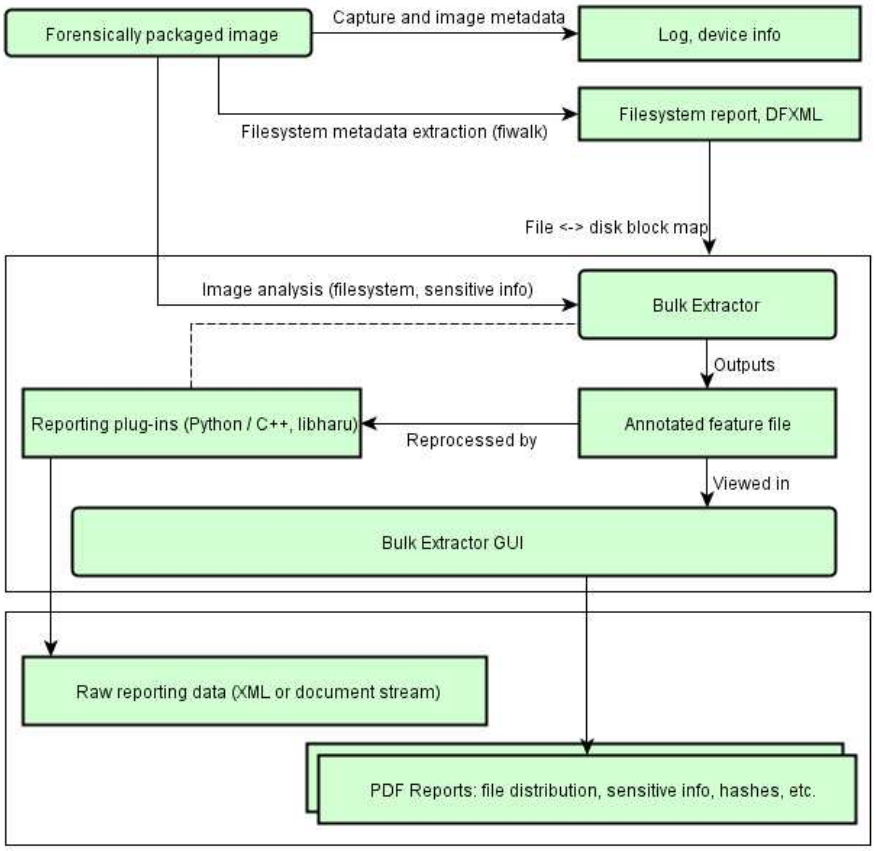
(그림 12. Guymager를 통한 디스크 이미징)



(그림 13. Imaging 포맷 및 해쉬함수 설정)

• 특징 정보 파악(Identification of Private and Sensitive Information)

BitCurator는 이미지 파일에서 특징 정보를 파악하기 위한 파일 시스템 분석 및 스트림 기반 포렌식 분석 기법을 포함하며, 이를 위해 fiwalk[26] 및 Bulk Extractor[27]와 같은 오픈 소스 툴을 사용한다고 설명하고 있다. fiwalk는 이미지 파일을 읽어서 DFXML(Digital Forensic XML)[28] 파일로 출력해주고, Bulk Extractor는 스트림 기반 분석을 통해 e-mail 주소, 지리 위치 메타 정보, TCP 연결 정보, 전화 번호, 신용 카드 정보 등을 추정하여 추출해 준다. 아래 그림은 BitCurator를 통한 정보 파악 단계를 보여준다.



(그림 14. BitCurator Information Identification[29])

다음 (그림 15) 및 (그림 16)는 BitCurator 테스트 패키지에 포함되어 있던 Bless Hex Editor와 Bulk Extractor View를 통해 USB 이미지 파일을 분석한 화면이다.

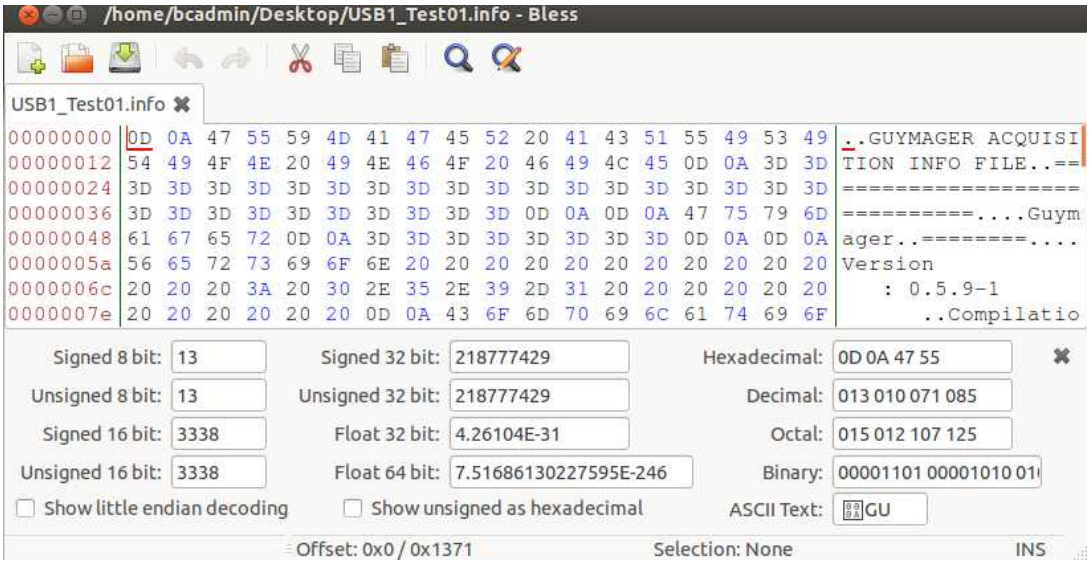
26) https://github.com/kfairbanks/sleuthkit

27) http://afflib.org/software/bulk_extractor

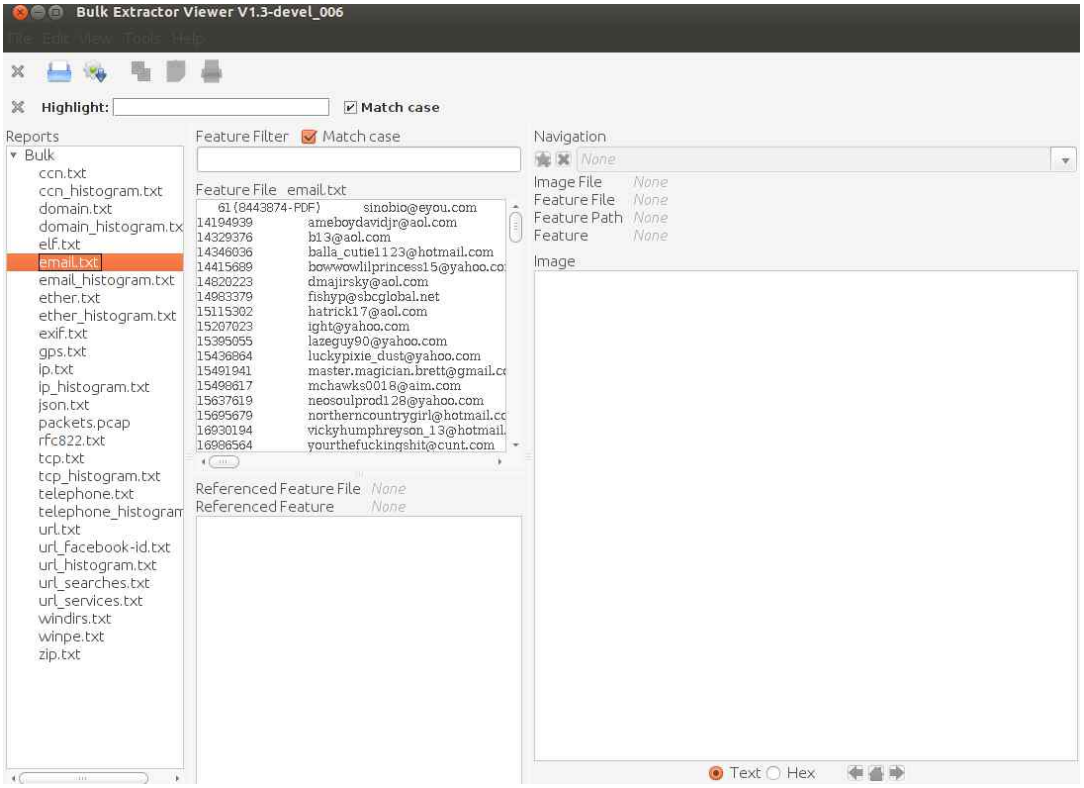
28) Forensic information과 forensic processing results들을 표현하기 위해 설계된 XML 언어로 서로 다른 툴, 조직 간에 정보공유를 가능하게 해줌

29) http://wiki.bitcurator.net/index.php?title=Description

Bulk Extractor 의 경우 그림에서 볼 수 있듯이 이미지 파일에서 추출할 수 있는 특징 정보들(e-mail 주소, 전화번호, ip주소 등)을 미리 설정된 패턴 값과 비교해 찾아내는 것을 알 수 있다.



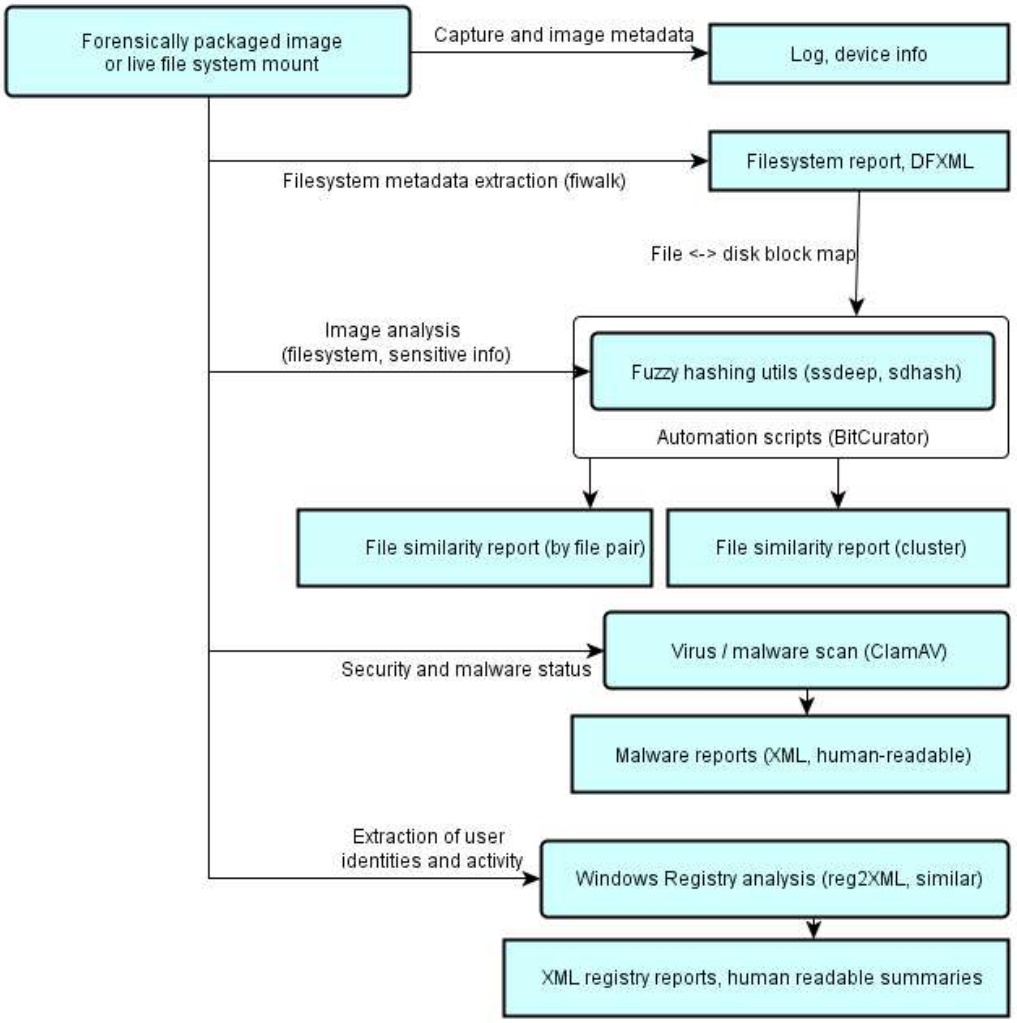
(그림 15. Bless Hex Editor)



(그림 16. Bulk Extractor Viewer)

- 정보 분류(Data Triage)

BitCurator는 정보의 중요성와 유사성 등에 따라 분류하기 위한 도구를 제공하는 것을 목표로 한다. 파일들의 유사성(similarity)를 분석하기 위해 sdhash[30] 도구 등이 사용된다.



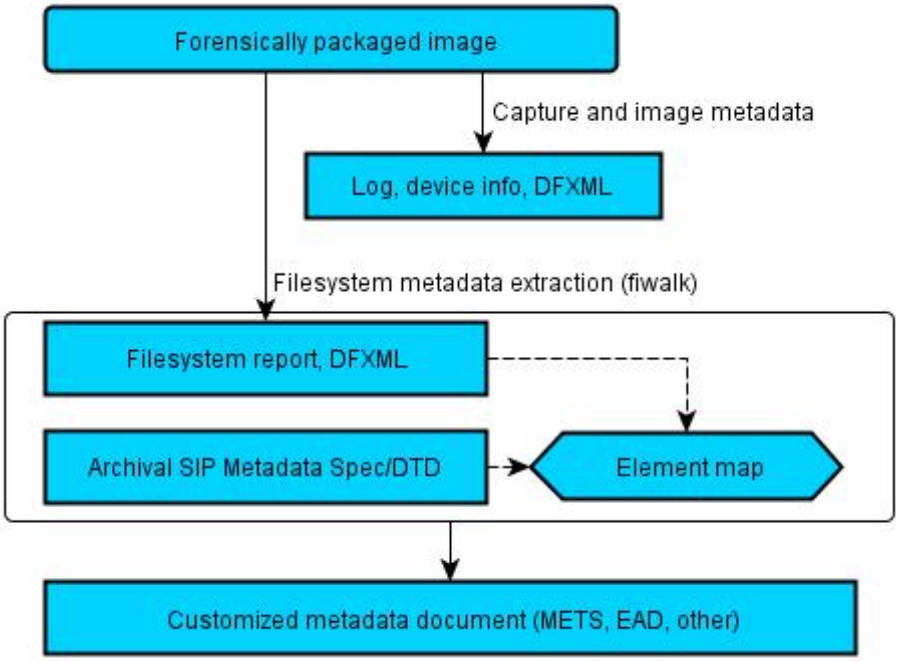
(그림 17. BitCurator Triage Facilities[31])

30) http://roussev.net/sdhash/sdhash.html

31) http://wiki.bitcurator.net/index.php?title=Description

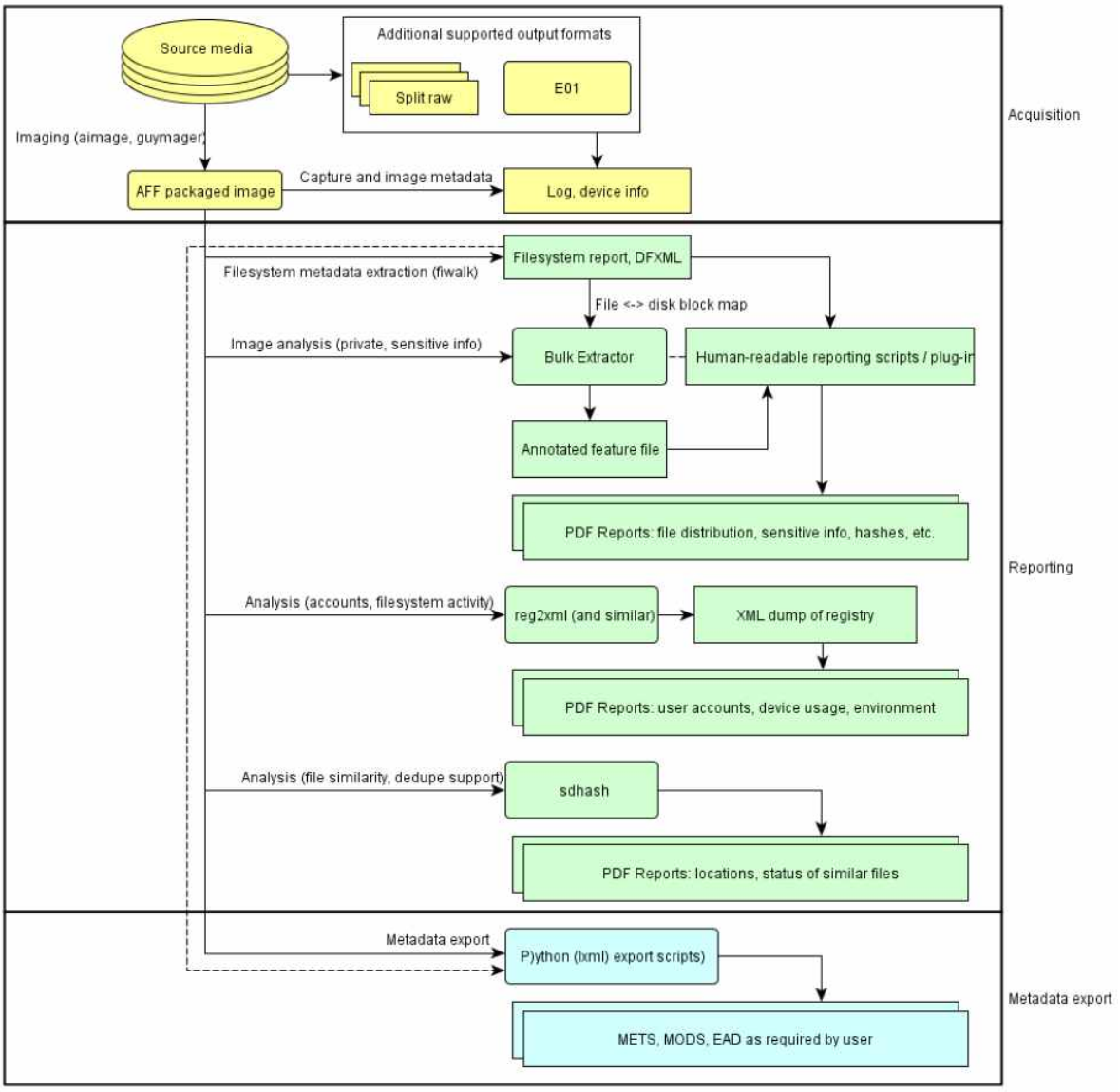
- 메타 데이터 추출(Metadata Export)

BitCurator는 DFXML 메타 데이터, 기록 보존 메타 데이터 등 다양한 형태의 메타 데이터를 METS(Metadata Encoding and Transmission Standard) 및 EAD(Encoded Archival Description) 형태로 출력하는 것을 지원한다.



(그림 18. BitCurator Metadata Export[32])

32) http://wiki.bitcurator.net/index.php?title=Description



(그림 19. Overview of the BitCurator Architecutre[33])

BitCurator는 기록 수집 기관에서 적용 가능한 디지털 포렌식 도구 및 기술 개발이 목적으로 진행되는 연구로 2013년 까지 1차 프로젝트가 진행된다. BitCurator 프로젝트는 기존 디지털 포렌식 도구를 그대로 사용하지 않고, 기존 오픈소스 기반 도구들을 수정 및 보완하여 전자기록관리 분야에서 응용 가능한 형태로 변환한 점에서 큰 의미가 있다고 볼 수 있다.

33) BitCurator: Requirements Document (version 0.9), 2012

10. 주요 디지털 포렌식(Digital Forensics) 관련 사례 비교·분석

2008년부터 국외 기록학 분야에서는 전자기록의 진본성·무결성 유지 및 특징 정보 분석 등을 목적으로 다양한 디지털 포렌식 적용 연구가 이루어지고 있는 실정이다. AIMS 프로젝트 등 실제 포렌식 도구 적용에 관한 대부분의 연구는 2009년 Jeremy Leighton John(British Library)의 "Digital Lives Project"를 기반으로 하고 있으며, 실제 FRED, FTK, FTK Imager 등의 기존 포렌식 도구 적용에 대해 논의한 바 있다. 한편, 2011년부터 North Carolina 및 University of Maryland 대학에서 수행하고 있는 BitCurator 프로젝트의 경우 기존 연구들과 달리 전자기록관리 프로세스에 특화된 오픈소스 기반의 디지털 포렌식 도구를 자체 제작하고 있다. 종합적으로 국외에서는 주요 대학들을 중심으로 전자기록관리에 디지털 포렌식 도구 및 절차를 접목시키려는 움직임이 활발하지만 아직까지 국내에서는 이와 관련하여 알려진 연구가 없기 때문에 본 연구의 의미가 크다고 할 수 있다.

(표 4. 전자기록관리에서의 디지털 포렌식 적용 사례 비교·분석)

국가	프로젝트	년도	연구기관	연구내용 및 특징
미국	BitCurator	2011~현재	North Carolina, University of Maryland	- 오픈소스 기반의 디지털 포렌식 도구를 통한 전자기록 수집 분석 모델 수립중 - AFF(Advanced Forensics Format)을 지원하는 전자기록 수집 도구(Disk Imaging Tool), 이미지 파일에서 특징 정보를 추출하는 분석 도구 등을 개발 중에 있으며 이에 대한 가상 테스트 환경(Virtualbox)과 소스코드 공개 (2012년 9월 0.1.5 버전 공개)
미국	DF and Born-Digital Content in Cultural Heritage	2009~2010	Council on Library and Information Resources	- 전자기록 관리의 디지털 포렌식 적용 사례에 대한 전반적인 동향 조사/분석 - 디지털 포렌식 적용의 이점 설명(오래된 포맷 이전, 진본성 유지, 데이터 복구) - 디지털 포렌식 기술을 어떻게 적용할지에 대한 구체적 방안은 제시하지 않음
미국	AIMS	2009~2011	Hull, Stanford, Virginia, Yale	- 디지털 기록들을 관리하기 위한 방법론 및 지속 가능한 포괄적 프레임워크 제시 - 기록 수집 및 식별 단계에서 디지털 포렌식 도구(FTK Imager 3.0, FTK3.3) 활용 - 2012년 1월, 연구 최종보고서 발표 - 기존 포렌식 도구를 그대로 사용하였기 때문에 유연성, 확장성 효율성 측면이 부족
미국	Stanford Project	2008~2011	Standford University Libraries	- 2008년부터 오래된 전자매체로부터 기록을 이전하는 방안 연구 - 2009년, Digital Forensic Lab. 개설 및 운영 - 2009년, 매체 이전에 사용하기 위한 포렌식 도구 (FRED, FTK, Encase) 구매 - 2009~2011년, AIMS 프로젝트 참여

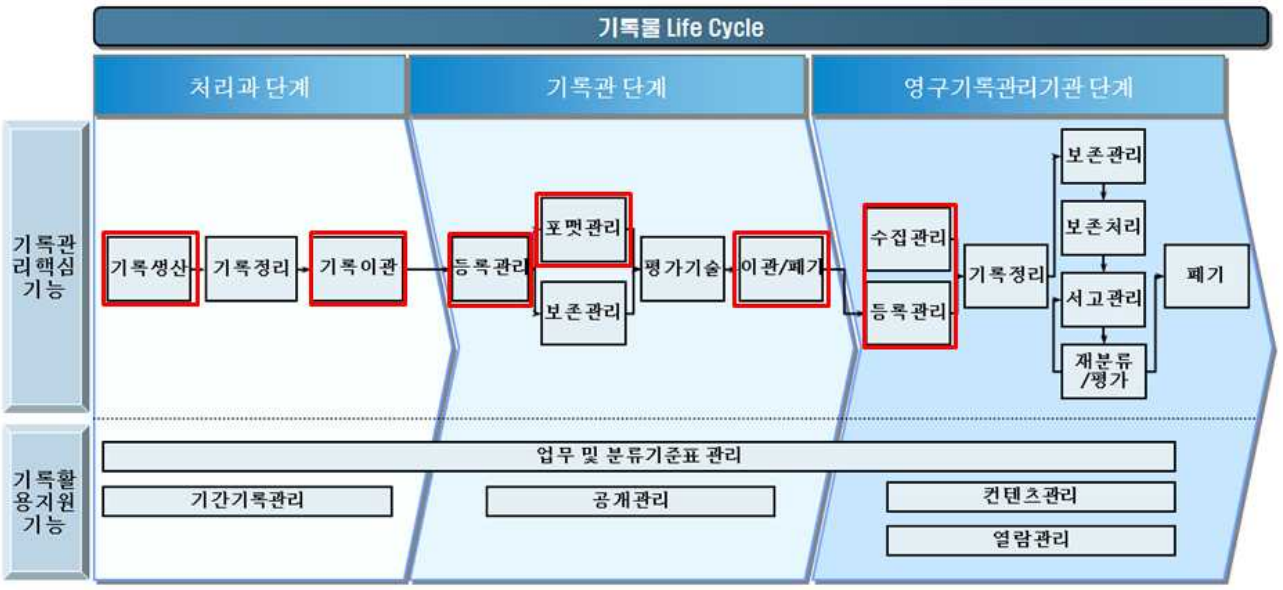
영국	FIDO	2011	King's College London	- 디지털 포렌식 원칙의 적합성 평가 및 디지털 기록 관리를 위한 법적 요구사항 분석 - 기록관리 환경 전자기록 수집, 분석을 위한 다양한 디지털 포렌식 도구 효율성 평가 - 연구 최종보고서 등 참고할 수 있는 구체적 발표 자료가 부족
영국	futureArch	2008~ 2012	Oxford University Boldleian Libraries	- BEAM(Bodleian Electronic Archives and Manuscripts) 서비스를 통해 전자기록의 수집, 보존, 접근 등의 절차를 위한 가이드라인 수립 - 기록 수집단계에서 FRED 장비를 통해 디지털 매체 복제 수행 - 연구 최종보고서 등 참고할 수 있는 구체적 발표 자료가 부족
영국	Digital Lives	2009	British Library	- 디지털 포렌식 도구들을 실제 전자기록 관리 workflow 에 적용한 선구적 연구 - 이후 디지털 포렌식을 적용한 많은 연구는 Digital Lives Project 성과를 바탕으로 함 - 2010년, 연구 최종 보고서 발간
영국	Paradigm	2005~ 2007	Oxford University Boldleian Libraries	- 디지털 기록의 장기 보존을 위해 기록의 생산부터 접근까지의 life-cycle 전반에 걸친 문화적• 법적• 기술적 요소들을 다룸 - 2008년 연구 결과로 workbook 발간 - 디지털 포렌식의 적용에 대해서는 간략히 언급만 하고 깊게 다루지 않음
캐나다	IntrerPARES	1998~ 2012	Social Sciences and Humanities Research Council, University of British Columbia	- 전자기록의 생애주기 전반에 걸친 장기보존 문제의 해결방안을 모색하기 위한 다국적 연구 프로젝트로 1998년 1차 프로젝트를 시작한 이래 총 3단계에 걸쳐 진행 - 대규모 장기 프로젝트로 포괄하는 범위가 매우 광범위하지만 디지털 포렌식 적용에 대한 명시적 언급은 없음
캐나다	Digital Records Forensics	2008~ 2011	University of British Columbia's School of Library	- 디지털 포렌식, 증거법, 문서학 각 분야에서 전자기록에 대한 관점 비교 - 전자기록관리 분야와 디지털 포렌식 분야가 서로 도움을 줄 수 있음을 시사 - 디지털 포렌식을 적용하기 위한 구체적 방안은 제시하지 않음

제 3 절 국가기록원 전자기록관리 프로세스에서의 무결성·신뢰성 문제

전자기록의 진본성, 무결성, 신뢰성 측면에서 국가기록원 전자기록관리 프로세스를 파악하기 위해 기록원 측에서 분석 요청한 문서 및 기록관리 표준 문서들을 토대로 분석하였다.

1. 전자기록관리 단계별 프로세스

전자기록물의 life-cycle은 크게 처리과 단계, 기록관 단계, 영구기록관리기관 단계로 나누어진다.



(그림 20. 전자기록물 Life-Cycle)

처리과의 주요 역할은 기록물의 생산 및 접수로 이러한 기록물들은 전자기록생산시스템으로 등록 및 관리되며, 처리과에서 최대 2년까지 기록물을 보관할 수 있다. 보관기간이 경과하면 기록물 정리 및 이관지침에 따라 해당 기록물을 기록관으로 이관하여야 한다. 처리과 단계에서 전자기록의 진본성 및 무결성과 관련된 주요 이슈는 다음과 같다.

- 전자기록의 생산 및 접수 단계에서 해당 전자기록의 진본성(authenticity)을 판단할 수 있는가?
- 외부에서 전자기록이 접수된 경우, 해당 전자기록에 대한 정보를 정확히 인식(identification)할 수 있는가?
- 전자기록의 이전(migration)에 있어 전자기록의 무결성(integrity)이 보장 되는가?
- 기록관으로 기록물을 온라인으로 이관하는 프로세스에서 전자기록이 위·변조 여부

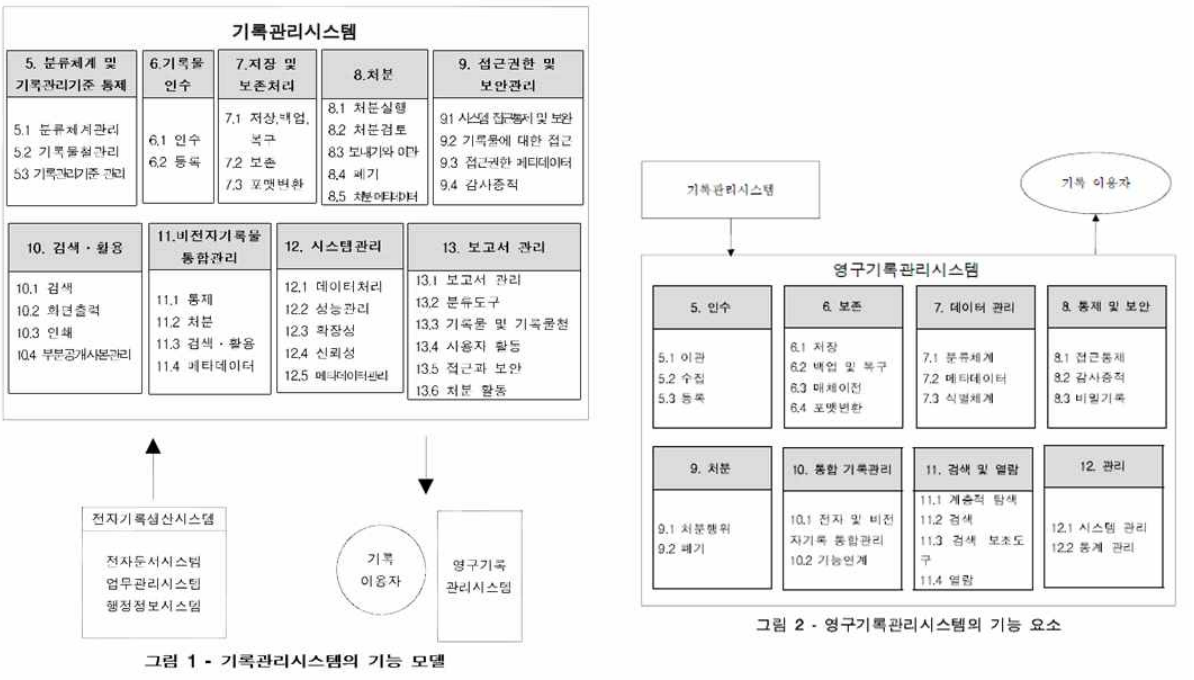
를 판단할 수 있는가?
- 기록물에 대한 접근 및 인수인계에 있어 감시 및 기록(chain of custody)이 이루어지는가?

기록관 단계에서 기록관리시스템은 전자기록이 진본성, 신뢰성, 무결성 및 이용가능성을 확보할 수 있는 형태(영구보존포맷)로 저장하고 관리됨을 보장한다. 이를 위해 전자서명, 암호화와 같은 기술적 보호조치가 이루어진다. 기록관 단계에서 전자기록의 진본성 및 무결성 관련 도출된 이슈는 다음과 같다.

- 전자기록의 등록관리 단계(전자기록 인수, 품질관리 등)에서 무결성이 보장되가?
- 문서보존포맷 변환 단계에서 기록의 원본성이 훼손되는가?

영구기록관리기관은 공공기관으로부터 이관 받은 기록물 및 국가적으로 보존가치가 높은 주요 기록정보를 보존 및 관리한다. 이 경우 제시될 수 있는 진본성 및 무결성 이슈는 기록관 단계에서의 이슈와 유사하다. 한편, 표준 전자기록관리시스템을 통해 공공기관으로부터 이관 받은 전자기록물 외에 외부 기관으로부터 매체 이전 방식을 통해 이관 받는 경우, 처리과 단계에서 제시된 이슈가 비슷하게 제기될 수 있다.

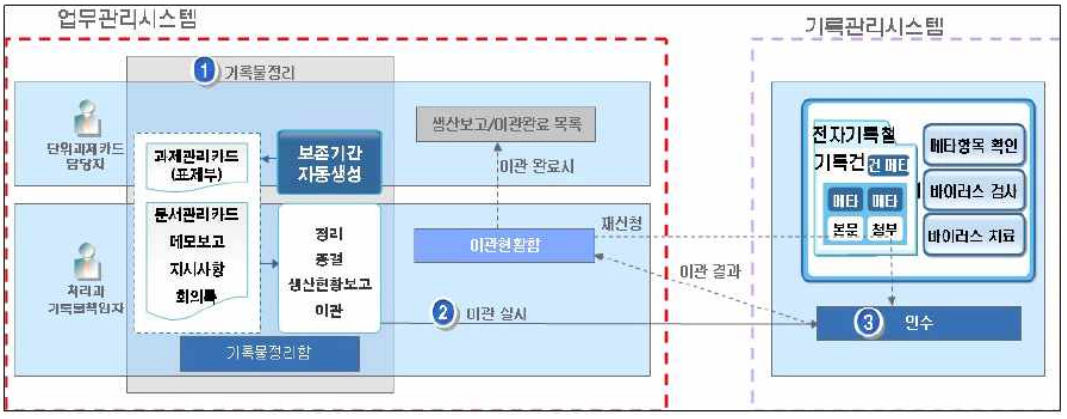
위에서 제시된 진본성·무결성 문제에서 각각 디지털 포렌식 기법의 적용 가능성이 존재한다. 기록 이전 절차에서 증거 수집(이미징) 기술 적용하여 전자기록의 저장매체, 운영체제, 파일시스템 등에 대한 의존성을 줄일 수 있으며, 입증된 수집 도구를 사용함으로써 증거의 무결성 및 신뢰성을 보장할 수 있다. 또한, 전자기록의 진본성 판단 및 정보 인식에 있어 디지털 포렌식 분야에서 사용되는 다양한 증거 분석 기술을 통해 도움을 얻을 수 있다. 디지털 포렌식 기법 적용에 관한 세부적인 사항은 7절에서 자세히 살펴보도록 한다.



(그림 21. 기록관리시스템, 영구기록관리시스템 기능 요소[34])

2. 업무관리시스템과 기록관리시스템간 데이터 연계 기술규격

NAK/TS 1-1:2009(v1.1) 기록관리시스템 데이터연계 기술규격-제1부: 업무관리시스템과의 연계(1.1) 표준은 기록관리시스템과 업무관리시스템의 연계를 위한 데이터 규격을 정의한 것으로, 업무관리시스템에서 생산한 전자기록물을 기록관리시스템으로 연계 이관할 때에 적용한다. 업무관리시스템에서 기록관리시스템으로의 기록물 이관 프로세스는 아래과 같이 나타내고 있다.

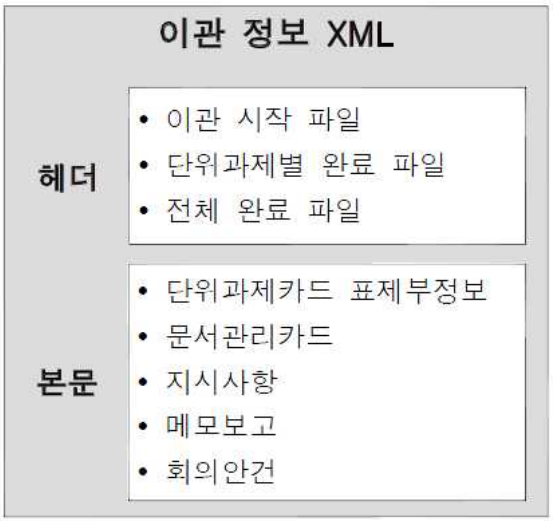


(그림 22. 업무관리시스템에서 기록물 이관 프로세스[35])

34) NAK/S 6:2009(v1.1) 기록관리시스템 기능요건, 국가기록원, 2009
NAK/S 7:2010(v1.1) 영구기록관리시스템 기능요건, 국가기록원, 2010

35) NAK/TS 1-1:2009(v1.1) 기록관리시스템 데이터연계 기술규격-제1부: 업무관리시스템과의 연계(1.1)

업무관리시스템에서 기록관리시스템으로 이관할 때의 데이터는 헤더, 본문으로 구성되며 작성 표준 포맷은 XML(eXtensible Markup Language)로 아래 그림과 같다.



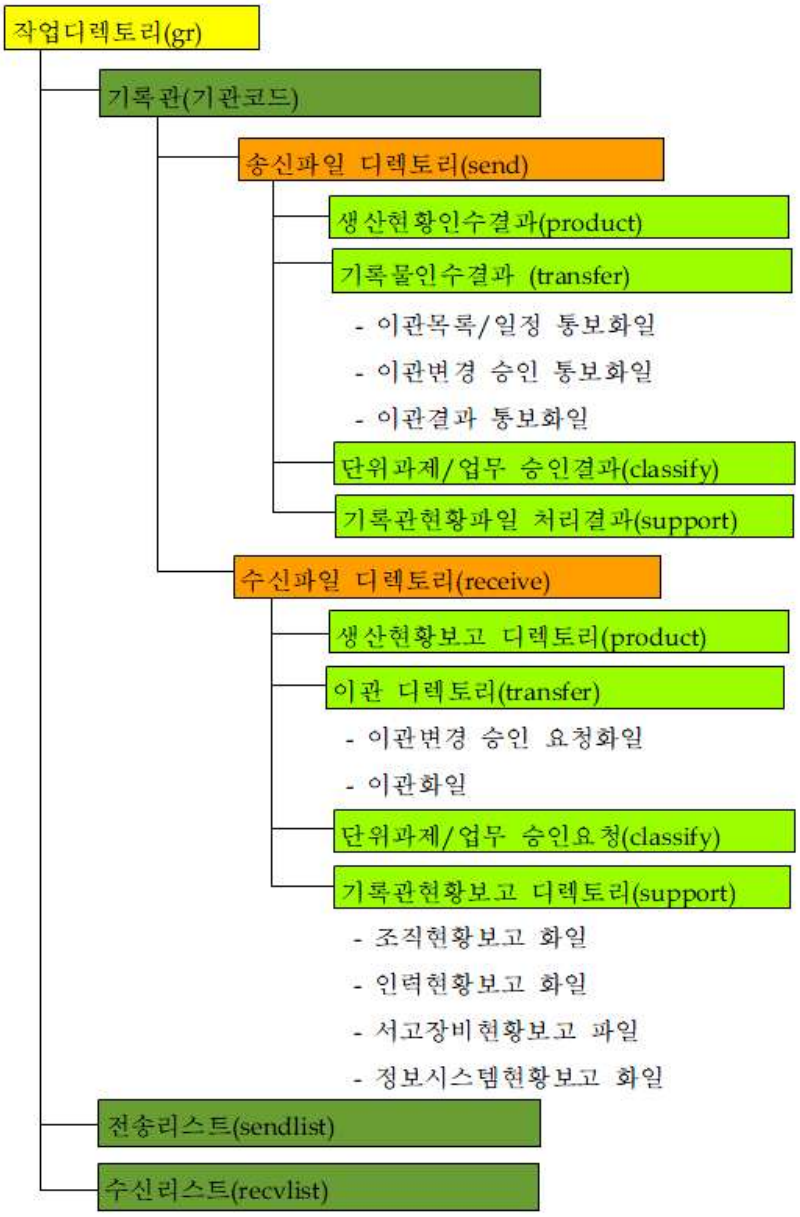
(그림 23. 기록물 이관 연계 포맷[36])

업무관리시스템-기록관리시스템 데이터연계 기술규격에서 기록의 무결성과 관련하여 문제시 될 수 있는 점은 이관 파일 스키마에 원본 파일의 무결성을 입증할 수 있는 XML Signature와 같은 기법의 적용이 전혀 없다는 것이다. 또한 업무관리시스템과 기록관리시스템 사이 통신에서 보안 채널을 구성해야 한다는 것도 명시하지 않는다. 이에 대해 "NAK/TS 5:2010(v1.0) 전자기록물 온라인 전송을 위한 기술 규격"을 따르는지 확인할 필요가 있다.

3. 기록관리시스템과 영구기록관리시스템간 데이터 연계 규격

NAK/TS 1-2:2008(v1.0) 기록관리시스템과 영구기록관리시스템간 데이터 연계규격 표준은 공공기록물 관리에 관한 법률(법률 제11391호)에 따라 설치·운영하는 영구기록물관리기관의 영구기록관리시스템과 각급 공공기관 기록관의 기록관리 시스템간 데이터를 연계할 경우 적용하여야 한다고 나타낸다. 하지만 이 표준에서는 장기보존포맷 기록물과의 연계방안과 메타데이터의 계층 구조의 표현방안은 포함하고 있지 않아 제한적으로만 참조 가능하다고 기술한다.

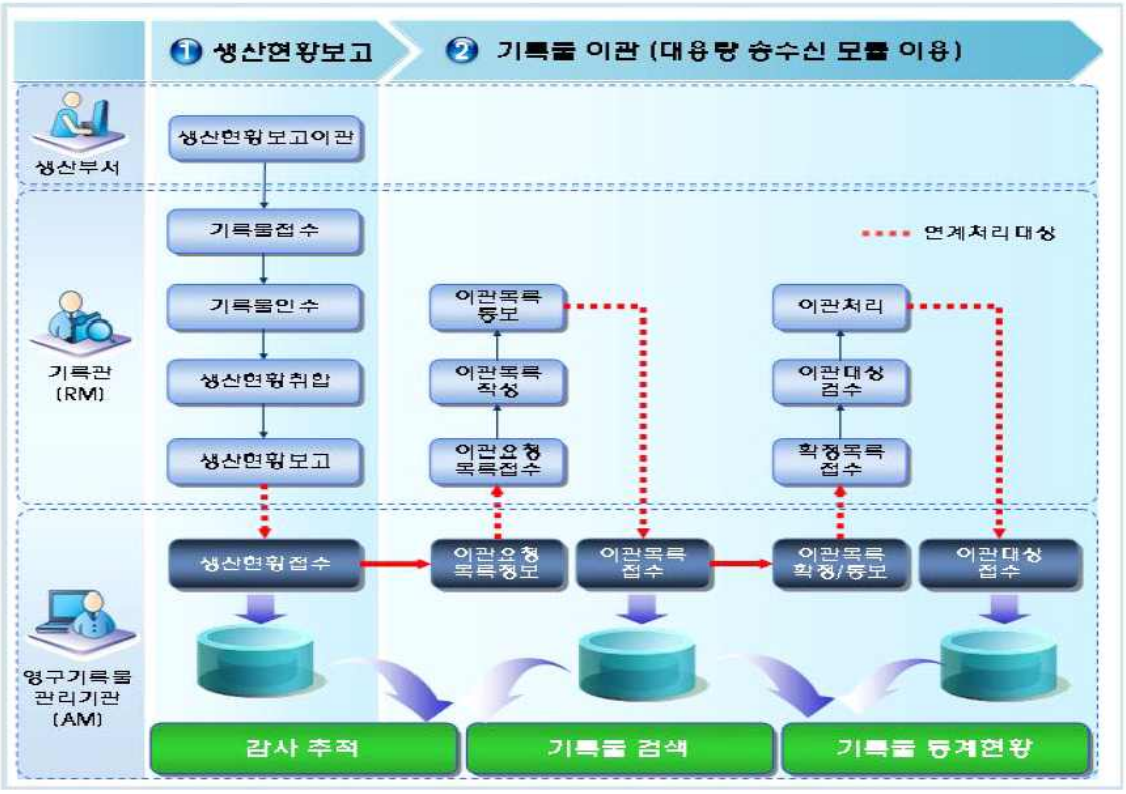
36) NAK/TS 1-1:2009(v1.1) 기록관리시스템 데이터연계 기술규격-제1부: 업무관리시스템과의 연계(1.1)



(그림 24. 기록관리시스템-영구기록관리시스템 연계대상 데이터 구조[37])

기록물 생산기관, 기록관, 영구기록물관리기관 간의 기록물 이관 프로세스는 다음 그림과 같은 단계를 거친다.

37) NAK/TS 1-2:2008 기록관리시스템과 영구기록관리시스템간 데이터 연계규격, 국가기록원, 2008



(그림 25. 연계기능 업무흐름도[38])

(그림 26. 대용량 송수신 서비스 구성도[39])

38) NAK/TS 1-2:2008(v1.0) 기록관리시스템과 영구기록관리시스템간 데이터 연계규격

39) NAK/TS 1-2:2008(v1.0) 기록관리시스템과 영구기록관리시스템간 데이터 연계규격

이 표준에서는 영구기록관리시스템은 다수의 기록관리시스템으로부터 용량의 전자기록물을 특정기간에 집중적으로 전송받을 수 있어야 하기 때문에 성능에 영향을 주지 않으면서 안정적으로 대용량의 데이터를 전송할 수 있는 대용량 송수신 모듈을 활용하여 연계한다고 나타낸다. 이때 네트워크 보안을 제공하기 위해 TLS 보안채널을 구성(GPKI 인증서 및 전자서명키 사용)한다는 점이 업무관리시스템-기록관리시스템 데이터연계 기술규격과의 기록의 무결성 및 보안(security) 측면의 주요 차이점이다. 다음 표는 대용량 송수신 연계모듈에 대한 주요기능을 나타낸다.

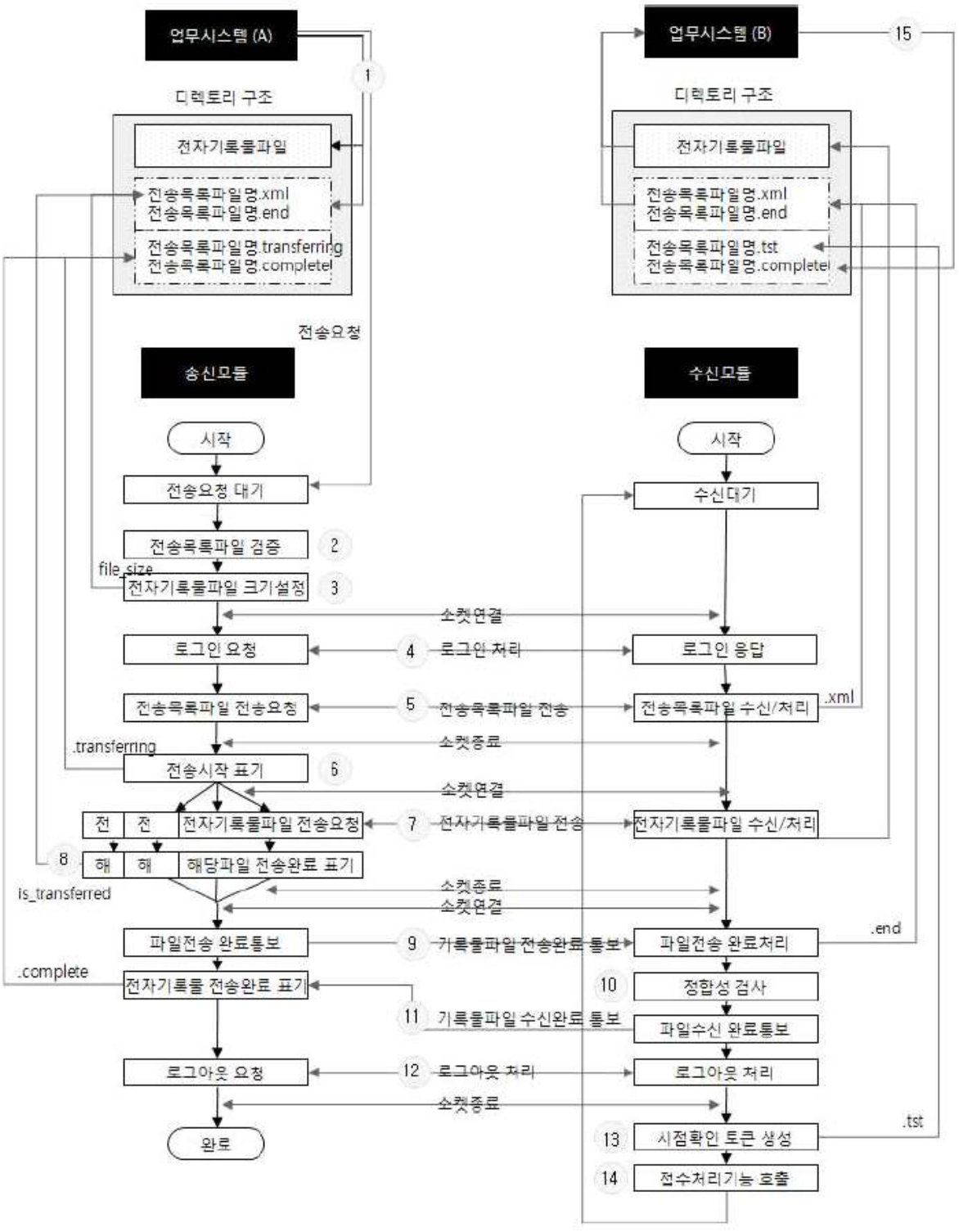
(표 5. 대용량 파일 송수신 연계모듈의 주요기능)

구분	설명
세션 관리	수신측 : 적절한 수의 세션만 접속하도록 관리 송신측 : 전송 가능한 상태인지를 확인 후 접속하여 전송 공 통 : 데이터 이어받기가 가능하도록 세션 관리
이력 및 상태 관리	수신측 : 현재 수신 중인 데이터의 상태 송신측 : 보내는 데이터의 전송 상태 이 력 : 송신/수신 관련
데이터 관리	송신 데이터 관리 : 부하를 줄이기 위해 데이터를 일부만 메모리에 읽어 전송 수신 데이터 관리 : 수신한 데이터만큼 파일로 저장하여 시스템의 부담 감소 이어받기 관리 : 이어 받기가 가능하도록 완전히 전송되지 않은 파일의 상태관리
네트워크 채널 암호화	GPKI 인증서 및 전자서명키를 이용하여 네트워크 채널(터널링 기법)로 암호화하여 전송 TLS 1.0 이용 및 Class3 적용(상호인증)

4. 전자기록물 온라인 전송을 위한 기술규격

이 표준은 업무시스템에서 전자기록물을 온라인으로 전송하기 위한 기술규격으로서 업무시스템의 전송요청 및 접수요청에 관한 인터페이스를 포함한다. 전자기록물의 이관·인수 기능을 수행하는 전자기록생산시스템, 기록관리시스템, 영구기록관리시스템 등 업무시스템은 이 표준의 제5절 업무시스템과의 연계 인터페이스를 준수하여야 하며, 대용량 기록물 파일을 전송하는 대용량 송·수신 소프트웨어는 이 표준을 모두 준수하여야 한다고 명시하고 있다.

전자기록물 송신모듈과 수신모듈 간에 이루어지는 전송 절차의 개요는 다음 그림과 같다.



(그림 27. 전자기록물 온라인 전송절차 개념도[40])

40) NAK/TS 5:2010(v1.0) 전자기록물 온라인 전송을 위한 기술 규격

이 표준에서 전송 소프트웨어의 기록의 무결성 및 보안(security) 관련 주요기능으로 (표 6)에서 기술하는 기능을 필수적으로 갖출 것을 제시한다.

(표 6. 전송 소프트웨어의 보안 관련 주요기능 요구사항)

기능명	기능설명
전송파일 암호화	전송정보를 SSL/TLS기반으로 암호화하는 기능
무결성 정보 생성	전송 대상 메시지에 대한 위변조 여부를 보장하기 위하여 쉬값을 생성, 검증하는 기능
파일 일치성 검사	전송 대상 파일에 대해, 파일명, 파일확장자 그리고 파일크기가 수신한 파일과 일치함을 검사하는 기능
수신이력 시각정보 생성	수신이력에 대한 시점확인 토큰을 생성하는 기능
접속관리	수신모듈로 접속 실패 시 접속 재시도 횟수를 관리하는 기능
사용자 인증	송·수신 모듈간의 상호인증 및 인가절차 기능
로그기능	파일의 전송여부, 전송정보, 시스템 정상작동 여부를 확인 할 수 있는 정보를 파일로 기록하는 기능

- 암호화 처리

전자기록물의 암호화 처리는 SSL/TLS(RFC2246, RFC4345) 네트워크 보안을 이용하여 송·수신모듈 간 기밀성을 보장하여야 한다고 명시하고 있다. 전송소프트웨어는 전자기록물의 암호화 처리를 위해 SSL/TLS와 연계하여 전송한다. SSL/TLS는 클라이언트와 서버 간 handshake 단계를 거친 후에 Cipher Data Transaction을 수행하는데, 전송데이터 암호화 시 사용되는 알고리즘은 SEED[41] 대칭키 블록암호 알고리즘이 지원되어야 하고, SEED 대칭키의 키 정보는 Handshake 단계에서 규격에 의해 생성되어야 한다.

SSL/TLS는 Class2, Class3이 지원되어야 하고, SSL/TLS의 handshake 단계에서는 서버 인증서 검증을 수행하여 신뢰성을 확보하여야 한다. 그리고 전송되는 전자기록물의 암호화 처리여부는 전송목록파일에 명기된 암호화 여부에 따라 선택적으로 적용할

41) SEED는 1999년 2월 한국정보보호진흥원(한국인터넷진흥원의 전신)의 기술진이 개발한 128비트 및 256비트 대칭키 블록 암호 알고리즘으로, 미국에서 수출되는 웹 브라우저 보안 수준이 40비트로 제한됨에 따라 128비트 보안을 위해 별도로 개발된 알고리즘이다.

수 있어야 한다.

• 메시지 무결성 정보 생성

전송 중인 메시지에 대한 위·변조 여부를 확인할 수 있도록 무결성 정보를 포함하여야 하고, 이때 사용되는 무결성 정보는 SHA-1 혹은 SHA-2 해쉬 알고리즘을 이용하여 생성한다. 메시지 무결성 검증을 위해 송신모듈은 해쉬 알고리즘을 이용하여 body 부분의 무결성 정보를 생성하고, 수신모듈은 동일 해쉬 알고리즘을 이용하여 무결성 정보를 검증한다.

(그림 28. 메시지 무결성 정보 생성[42])

• 파일 일치성 보장

기록물 파일 전송 시, 송신한 기록물이 수신한 기록물과 일치함이 반드시 보장되어야 한다. 파일 일치성을 보장하기 위해서는 전송목록파일에 기입된 모든 파일리스트의 파일명, 확장자 및 파일크기가 수신한 파일과 일치하도록 보장되어야 한다.

• 사용자 인증

전자기록물 송·수신 기능 수행 시, 반드시 송·수신 모듈간의 인증절차를 수행하여야 한다. 인증방식은 '인증서 기반' 방식과 'ID/패스워드'방식 둘 중 하나를 반드시 사용하여야 하며, 인증서 기반인 경우 PKCS#7의 SignedData를 이용하여야 한다.

시스템 운영의 편의성을 위해, 송신모듈(이관기관)은 오프라인을 통해 수신모듈(인수기관)에 인증정보를 등록하고, 송신모듈이 수신모듈에 최초 로그인 시 인수기관의 인증정보를 1회 전달하는 방식을 이용한다.

42) NAK/TS 5:2010(v1.0) 전자기록물 온라인 전송을 위한 기술 규격

인증정보는 기관ID, 패스워드, 그리고 인증서DN은 필수항목이고, 관리방안은 구현에 국한된 내용으로 이 규격에서 제약하지 않는다.

(그림 29. 사용자 인증절차도[43])

전자기록물 온라인 전송을 위한 기술규격은 온라인 전송 시 발생할 수 있는 메시지 무결성 문제를 상당부분 고려하고 있으며 이에 대해 적합한 방법(메시지 암호화, 무결성 입증 정보 생성 등)을 통해 보완하고 있다고 판단된다. 따라서 이 표준에서 명시하는 바대로 온라인 이관이 이루어진 경우, 전자기록이 증거로 제시될 때 온라인 이관 자체를 문제 삼을 소지는 없다고 판단된다. 다만, 업무관리시스템-기록관리시스템 데이터연계 기술규격 표준에서는 이관 시 온라인 전송 기술 규격을 따르는지 명시하고 있지 않아 이에 대해 확실히 짚고 넘어갈 필요가 있다.

5. 전자기록물 문서보존포맷 기술규격

이 표준은 기술규격의 적용범위 및 대상으로 기록물관리기관에서 소장하고 있는 전자기록물 중 보존기간 10년 이상의 기록물을 대상으로 한다. 문서보존포맷은 문서가 생산된 당시의 애플리케이션이 없어도 해당문서의 내용과 외형을 그대로 재현하여 내용보기를 가능하게 하는 포맷이다. 이 포맷은 문서의 보존을 위해 필수적인 요소들을 규정하여 문서의 내용과 구조를 보존하며, 또한 문서의 생산, 저장 또는 표현에 사용된 도구와 시스템에 관계없이 시각적 모양을 장기간 지속적으로 유지하도록 전자문서를 표현하며 필요시 정확하게 재현하여 이용자에게 제공한다.

43) NAK/TS 5:2010(v1.0) 전자기록물 온라인 전송을 위한 기술 규격

(그림 30. 문서보존포맷 변환[44])

이 표준에서는 문서보존포맷이 갖춰야할 요건을 충족하는 PDF/A-1(ISO 19005-1:2005 Part 1: Use of PDF 1.4)을 문서보존포맷으로 규정하고 있다. 다만, 문서의 장기보존에 위배될 가능성이 있는 일부 요소(암호화, 내장파일, LZW압축, 투명성, 멀티미디어, 자바스크립트)를 금지하여 사용한다. 장기보존을 위해 필요한 부분(PDF/A를 위한 확장 스키마)을 추가하였다. PDF/A-1의 "A"는 기록물 즉 Archive를 나타내며, "1"은 인쇄가 가능한 모든 매체를 대상으로 하고 있다는 의미이다. 따라서서 동영상, 비디오, 오디오 매체에는 적용이 불가능하다.

전자기록물 문서보존포맷 기술규격에서는 문서보존포맷 자체의 무결성을 입증할 수 있는 항목이 없기 때문에 문서보존포맷이 위·변조 되었을 경우 이를 확인할 수 없다.

6. 전자기록물 장기보존포맷 기술규격

이 표준은 기록물관리기관에서 소장하고 있는 보존기간 10년 이상의 전자기록물과 영구기록물관리기관에서 소장하고 있는 보존기간 30년 이상의 전자 기록물을 대상으로 한다. 장기보존포맷은 전자기록물의 진본성과 무결성을 보장하고 장기간 안전하게 보존하기 위해 전자기록물 원문, 문서보존포맷, 메타데이터, 전자서명을 하나의 패키지로 구성한 포맷이다.

장기보존포맷은 원문, 문서보존포맷, 장기보존포맷 메타데이터, 전자서명으로 구성되며 이 구성요소를 XML을 이용하여 단일한 객체로 패키징한다. 단일한 객체로 패키징하는 이유는 시스템과 기관을 옮겨 다니면서 장기간 보존되는 전자기록물의 관리를 편하게 해주며, 기록물의 유실 및 훼손에 대한 위험성을 줄여주기 때문이다.

- 원문

원문은 생산자가 처음 생산한 기록물을 뜻하며 업무활동의 증거로서 법적 증거로 제시될 수 있다. 그러나 전자기록물의 경우 특성상 다수의 생산자에 의해 시간 및 공간에 제한 없이 여러 개의 복본이 생산가능하기 때문에 위변조가 쉽게 이루어질 수 있으

44) 전자기록 영구보존기술 적용을 위한 테스트베드 구축, 국가기록원, 2006

며, 계속 변화한다. 따라서 진본성 확인을 위해서 적법한 절차에 따라 변화해 온 것인지에 대한 변화과정 등이 메타데이터를 통해 이루어져야 한다. 또한 원래의 기록물이 어떠했는지를 확인할 수 있으려면, 생산 당시의 형상이 있어야 하며 이것이 진본성 확인의 시발점이 된다. 다만, 원문이 장기보존포맷에 포함되기 이전에 위변조 가능성이 있음을 간과해서는 안 된다.

- 문서보존포맷

문서보존포맷은 문서가 생산된 당시의 애플리케이션이 없어도 해당문서의 내용과 외형을 그대로 재현하여 내용보기를 가능하게 하는 포맷이다. 장기보존포맷은 원문파일을 포맷 변환한 문서보존포맷과 메타데이터를 포함하는 캡슐화를 통해 장기보존을 확고히 한다. 비독점적이며 기술 중립적인 문서보존포맷은 원래의 기록물의 내용과 구조를 유지하며, 하드웨어나 소프트웨어의 노후화나 매체의 퇴화 및 기술발전으로 인한 데이터 포맷의 변화에 상관없이 전자기록물을 보존하여 이용자가 접근할 수 있도록 한다.

- 장기보존포맷 메타데이터

전자기록물의 장기보존을 위해 원문과 함께 기록물의 생산부터 관리, 보존에 이르는 전 과정을 기술한 정보를 보존해야한다. 그러므로 장기보존포맷 메타데이터의 확보는 필수적이다. 장기보존포맷 메타데이터는 장기보존포맷이 독립된 객체로서 기능할 수 있도록 메타데이터를 정의한다. 그리고 NAK-P-2007-11 '기록관리 메타데이터표준'을 수용하여 기록관리 메타데이터와 호환성을 유지한다. 또한 KS X ISO 15489-1, KS X ISO 23081-1에서 정의한 메타데이터 요소를 반영한 장기보존포맷 메타데이터는 기록물 생애주기 전 기간에 걸쳐 진본성, 신뢰성, 무결성을 보장하며, 기록물을 관리·보존할 수 있도록 지원한다.

(그림 31. 장기보존포맷 변환)[45]

45) 전자기록 영구보존기술 적용을 위한 테스트베드 구축, 국가기록원, 2006

7. 기록관리 메타데이터 표준(※ 2012.10 개정)

이 표준은 장기간에 걸쳐 기록물의 진본성, 신뢰성, 이용가능성 및 무결성을 보장하기 위해 공공기관이 생산 또는 접수하는 기록물에 대한 맥락과 내용, 구조 및 기록생애주기 동안의 관리사항을 기술하기 위한 기록관리 메타데이터 표준으로 2007년 제정된 'NAK-P-2007-11 기록관리 메타데이터 표준: 현용·준현용 기록물용'의 문제점을 점검하여 현재의 기록관리 관련법규와 현장의 실무, 기록관리 관련 시스템에서의 차질없는 이관·관리에 적합하도록 그 내용이 전면 개정(2012년 10월)되었다. 특히 무결성 이슈와 관련하여 v1.0 버전에서는 전자기록이 장기보존포맷으로 변환되기 전에는 무결성을 입증할 수 있는 메타데이터 항목이 존재하지 않았다. v2.0 문서에서는 전자기록이 훼손·손상·변조 등에 의해 변경되지 않고 완전한 상태를 유지하고 있음을 지칭하는 무결성 유지를 위한 항목을 포함한다. 이에 따라 기록관 또는 영구기록관에서 기록물 인수시 검수지점, 장기보존포맷 변환, 포맷재변환 등의 경우 무결성 체크가 이루어질 수 있도록 하며, 무결성 체크 기법으로는 HSA-256 해쉬 알고리즘을 사용할 것을 명시하고 있다.

(표 7. 메타데이터 요소 : 무결성 체크(Integrity Check)[46])

요소명	무결성 체크 (Integrity Check)
요소 참조번호	23
정의	전자기록물에 위변조 혹은 훼손이 가해지지 않았음을 의미하는 무결성을 점검하기 위한 방법
목적	기록물이 조작되거나 훼손되지 않았음을 증명하여 기록물의 무결성을 보장
적용기록 계층	기록물철, 기록물건
컨테이너 여부	YES
필수 여부	해당시 필수
반복 여부	반복가능
하위요소	요소명
	23.1 무결성체크법(Integrity Check Name)
	23.2 무결성체크값(Integrity Check Value)
작성방법	·자체값은 가지지 않으며, 하위요소에 의해 표현됨 ·기록관, 영구기록물관리기관으로 이관된 이후 검수시점, 장기보존포맷 변환 및 재변환시 등의 경우에 획득됨

46) NAK/S 8:2012(v2.0) 기록관리 메타데이터 표준, 국가기록원, 2012

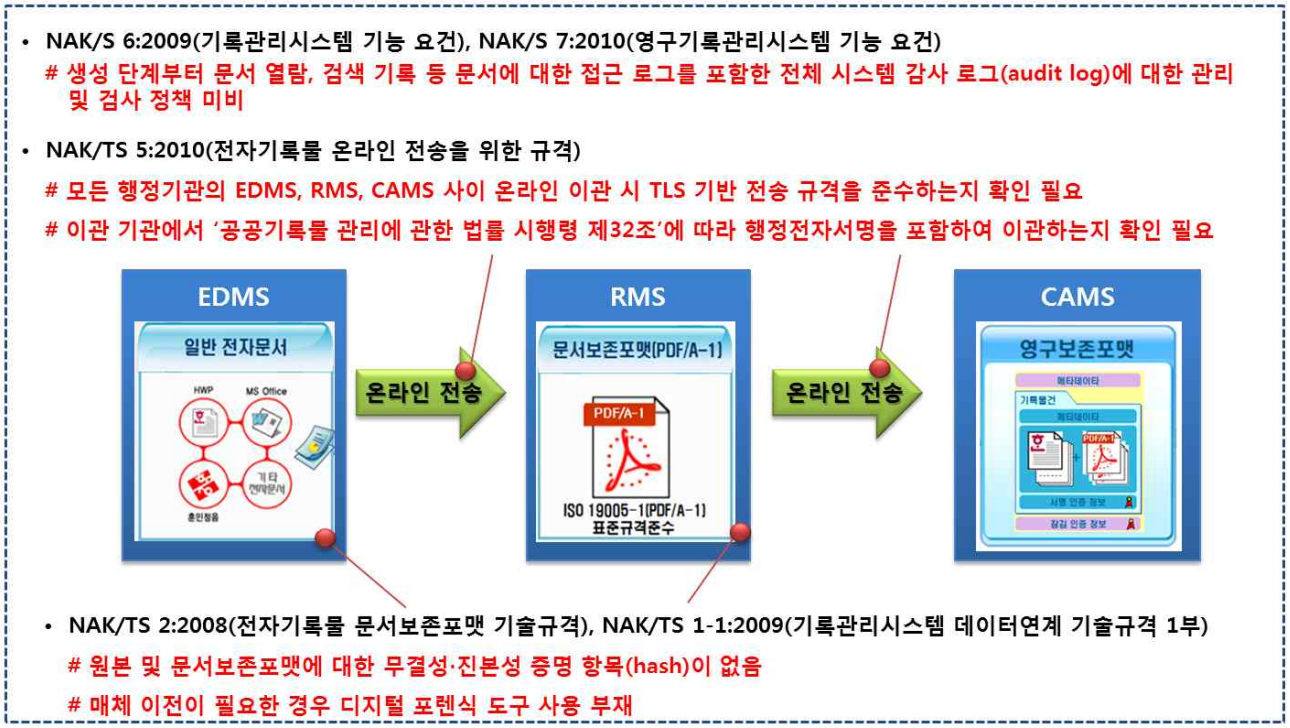
개정된 기록관리 메타데이터 표준에서는 해쉬 값을 통해 전자기록의 무결성을 추정하지만 기록물 인수 단계 등 개별 단계에 국한되어 있으며 기록의 전체 life-cycle에서의 변환 시점 각각에 대한 모든 해쉬 값을 보존하지는 않는다. 또한, 해쉬 알고리즘의 경우 키가 필요하지 않기 때문에 문서 내용과 해쉬값이 모두 변조되는 경우 이를 감지할 수 없기 때문에 별도로 안전하게 해쉬값을 저장·관리할 수 있는 메커니즘이 필요하다.

8. 전자기록관리 프로세스에서의 취약점 분석 결론

앞서 분석한 전자기록관리 표준 및 기술 문서들을 토대로 기록의 무결성·신뢰성과 관련된 이슈 사항을 아래 2가지 경우로 나누어 정리하였다.

- 표준 전자기록관리 시스템을 통해 공공기관으로부터 on-line으로 전자기록을 입수하는 경우
- 폐지 기관 또는 기타 외부 기관으로부터 off-line으로 전자기록을 입수하는 경우

가. 표준 전자기록관리 시스템을 통해 공공기관으로부터 on-line으로 전자기록을 입수하는 경우



(그림 32. 전자기록관리시스템을 통한 on-line 입수 시 무결성 이슈)

(1) 감사 로그(audit log)에 대한 관리 및 검사 기준 미비

추정 근거 : NAK/S 6:2009(기록관리시스템 기능 요건), NAK/S 7:2010(영구기록관리 시스템 기능 요건)

디지털 포렌식 절차에서 디지털 증거는 수집 단계에서부터 최종 법정에 제출되기 까지 모든 과정에서의 연계보관성(chain-of-custody)을 유지하기 위해 모든 과정에서의 소유 변경, 상태 변환, 접근 등의 정보를 기록으로 남겨서 안전하게 관리한다. 한편, 포렌식 준비도(forensic readiness) 관점에서 영국정부의 정보보증 요구사항(CESG, 2010)은 연계보관성의 보존과 더불어 디지털 기록들을 보존하고 있는 시스템 장비들에 대해서도 선제적인 모니터링과 감사로그 관리에 대해 명시하고 있다[47].

국가기록원 NAK/S 6:2009(기록관리시스템 기능 요건), NAK/S 7:2010(영구기록관리 시스템 기능 요건) 기술 문서를 토대로 판단할 때, 이러한 감사로그 관리에 대한 기준이 미비하다. 기록관리시스템 기능 요건문서에서는 감사로그에 대해 언급하고 있지 않으며, 영구기록관리시스템 기능 요건문서에서는 일부 감사증적 정보에 대해 기술하고 있지만 보다 구체적인 시행 규칙 및 기술적 대응 방안 마련이 필요하다.

(2) 모든 행정기관에서 NAK/TS 5:2010 규격을 준수하는지 여부가 불투명

추정 근거 : NAK/TS 5:2010(전자기록물 온라인 전송을 위한 규격)

현재 온라인 전송 시 NAK/TS 5:2010(전자기록물 온라인 전송을 위한 기술규격)에 따라 TLS 기반의 암호채널을 통해 전송하고 있지만, 모든 행정기관에서 실제로 이러한 규격에 따라 전송하고 있는지에 대한 감사가 필요하다. 디지털 포렌식은 모든 케이스에서 동일한 기준의 절차를 요구하기 때문에 기술문서에 명시된 절차적 요구사항이 모든 EDMS-RMS-CAMS 사이의 이관에서 제대로 지켜지고 있는지에 대한 감사가 필요하다.

(3) 원본 기록에 대한 무결성·진본성 증명 불가

추정 근거 : NAK/TS 2:2008(전자기록물 문서보존포맷 기술규격),
NAK/TS 1-1:2009(기록관리시스템 데이터연계 기술규격 1부)

전자기록은 매체 특성상 위변조가 쉽게 일어나기 때문에 처음 원본 기록을 수집 시점부터 원본에 대한 무결성을 증명할 수 있는 메커니즘이 필요하다. 또한, 원본 포맷이 문서보존포맷 또는 장기보존포맷으로 변환되는 각 단계에서 변환된 포맷들에 대한 무결성 검증도 필요하다. 디지털 포렌식 분야에서는 원본 디지털 증거의 무결성을 증명하기 위해 증거 수집 시 기록 전체에 대한 해쉬값을 계산하고 이를 안전하게 보관하여 추후 법정에서 증거의 무결성을 입증하는데 사용된다. 2012년 10월 기록관리 메타데이터 표준이 개정됨에 따라 기록에 대한 무결성을 입증하는 해쉬 값이 메타데이터 항목

47) 백승조, 포렌식 준비도(Forensic Readiness), 한국정보처리학회 디지털 포렌식 실무 단기강좌, 2012

에 포함되었다. 하지만 이는 개별적 이관 단계에서 사용되는 것으로 보이며 전자기록 life-cycle 전체에 걸쳐서 각각의 변환 포맷에 대한 해쉬 값을 보장하지는 않는다. 또한, 지금의 경우 원본 내용과 해쉬 값이 모두 변조되는 경우 위변조 사실을 인지할 수 없게 된다. 즉 전자기록의 특정 부분을 원하는 값으로 위조한 후, 위조한 기록의 해쉬 값을 재계산하여 기존 값과 바꿔치기 하는 경우 보안상 허점이 발생한다. 이러한 취약점을 보완하기 위해서는 해쉬 값을 생성하는 동시에 별도 안전한 저장소를 통해 통합 관리하거나 해쉬 값에 전자서명등을 추가하여 관리하는 방안등을 고려해야 한다.

나. 폐지 기관 또는 기타 외부 기관으로부터 off-line으로 전자기록을 입수하는 경우

기본적으로 행정기관에서 생성된 문서는 온-나라(on-nara) 정부 표준 업무관리시스템을 통해 관리되기 때문에 문서의 생성·수집·분석·관리 등에 있어 형식화되어 관리될 수 있다. 하지만, 외부에서 수집되는 기록에 대해서는 기록원에 보존되기 전에 매체 이전(Migration)의 단계를 필수적으로 거치게 되며, 추가적인 기록에 대한 분석 작업이 필요한 경우도 있을 수 있다. 이것은 고전 기록학에서 출처를 알 수 없는 고대 문서를 발견했을 때 이것에 대한 원본 유지, 시대/작성자/내용/의미 등의 분석, 관리, 보존 등의 작업을 거쳐야 하는 이슈와 비슷하다. 하지만, 현재 기록원에서의 전자기록에 대한 기술 및 프로세스는 고전 기록학에서의 요구사항을 동일한 수준으로 만족시키지 못하고 있다. 전자기록은 저장 매체에 비트 스트림으로 존재하는데 그 비트 스트림 형태는 해당 저장매체에 마운트된 파일시스템 종류에 따라 달라지며 또한 파일 시스템에 따라 서로 다른 메타데이터로 전자 기록의 이름, 수정 날짜, 소유자 등의 관리 정보를 저장하고 있다. 이러한 정보들은 시스템에 조그만 변화가 생겨도 쉽게 바뀔 수 있으며, 기존의 단순 파일 복사를 통한 기록 이전은 파일의 무결성을 완벽하게 훼손시킨다. 이러한 문제점은 전자기록이 법적 증거로 제시될 경우, 증거의 신뢰성 요구사항을 만족시키지 못하는 근거로 제기될 수 있다.

한편, 입수 이후의 정리·보존·활용 등의 관리 단계에서는 앞서 전자기록시시템을 통해 on-line 입수 후 발생할 수 있는 무결성 이슈가 동일하게 대두된다.

(1) 매체 이전(Migration)에서 원본 기록에 대한 정보 손실 위험

추정 근거 : NAK/S 9:2008(영구기록물관리기관 표준운영절차)

국가기록원에서는 전자기록관리 시스템을 통해 on-line 방식으로 문서를 입수하는 경우 외에도, 기획수집과 같이 폐지 기관이나 기타 외부 주체로부터 off-line으로 대량의 전자기록을 수집하는 경우도 있다. NAK/S 9:2008(영구기록물관리기관 표준운영절차) 표준 문서에서는 off-line 수집 시 무결성 및 진본성을 보장하기 위한 디지털 포렌식 도구를 활용한 절차에 대해 고려하고 있지 않다. 단순 복사(copy) 기능을 통해 파일을 이관받는 경우 원본 기록들에 대한 메타데이터가 손실될 수 있으며, 원본 비트스트

림에 대한 무결성 또한 보장할 수 없다.

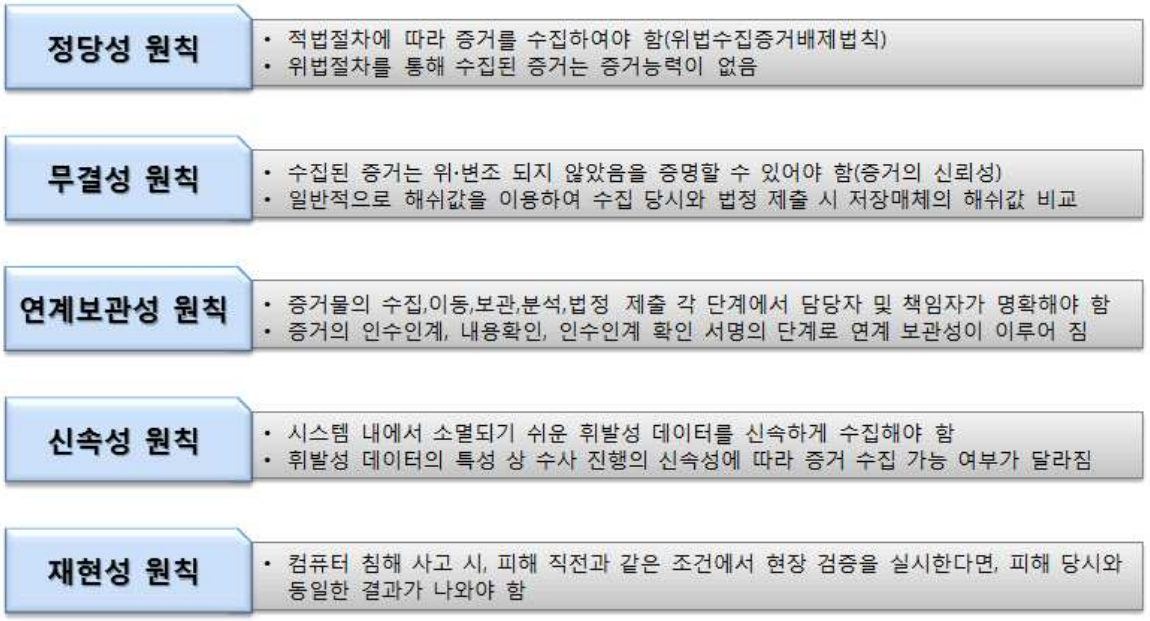
(그림 33. 외부로부터 off-line으로 전자기록 입수 시 무결성 이슈]

제 4 절 국내외 디지털 포렌식 표준 및 특허, 기술 분석

1. 국내 디지털 포렌식 표준 및 특허 분석

가. 경찰청 디지털증거 처리 표준 가이드라인

국내 디지털 포렌식 절차는 경찰청에서 2006년 출간한 『디지털 증거 처리 표준 가이드라인』을 토대로 분석하였다. 원래 검찰청 자료도 함께 분석할 계획이었으나, 현재 검찰청 내부 사정으로 인해 자료 공개 요청이 거절되었다. 디지털 포렌식에 있어 5가지 기본 원칙은 정당성, 무결성, 연계보관성(Chain of Custody), 신속성, 재현성 이다. 특히, 정당성은 위법수집증거배제법칙과, 무결성 및 연계보관성은 증거의 신뢰성 요건과 매우 밀접한 연관성을 가지므로 이에 대해 철저히 지킬 필요가 있다.



(그림 34. 디지털 포렌식 5대 기본 원칙)

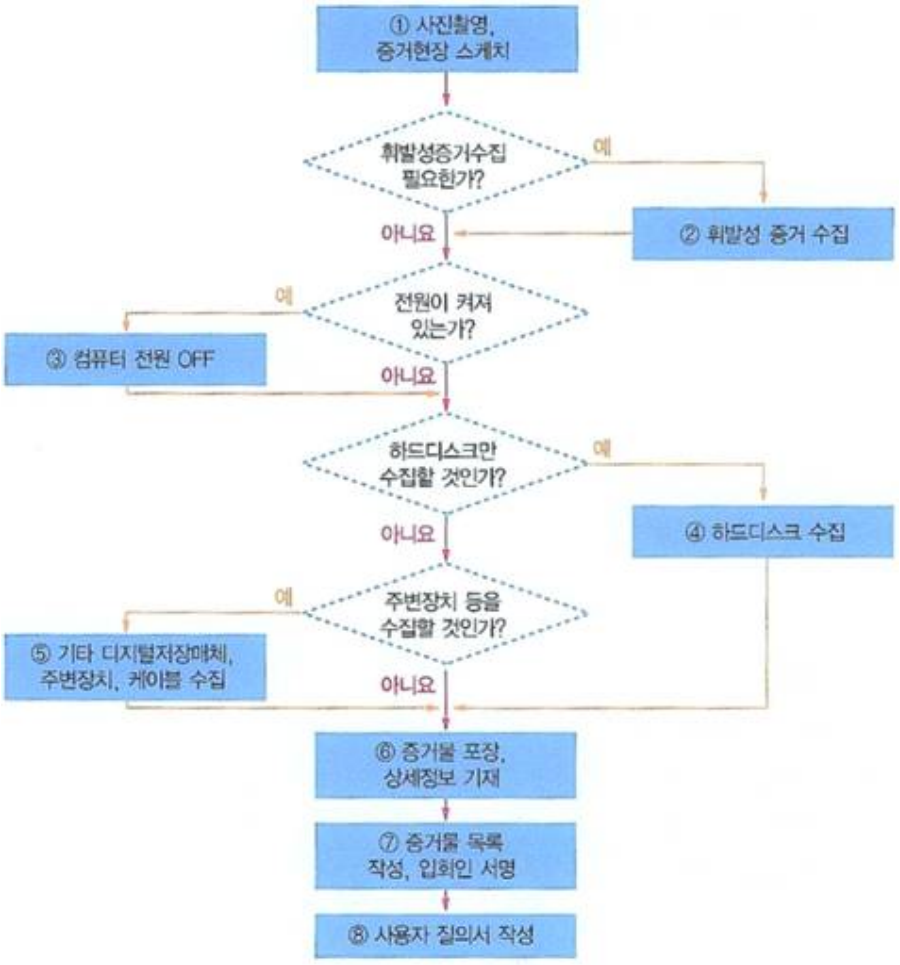
경찰청에서 수행하는 디지털 포렌식 표준 절차는 아래 그림과 같다.

(그림 35. 경찰청 디지털 포렌식 절차 전체 개요)

증거수집에 앞선 사전준비 단계에서는 디지털 증거 수집에 필요한 H/W 및 S/W를 준비하는 것이다. 디지털 포렌식에 사용되는 하드웨어 장비는 증거수집 및 분석용 컴퓨터, 디스크 복제 장비(일선에서는 주로 ICS Image Masster를 사용), 쓰기방지장치(Fastbloc), 증거사본 보관용 대용량 저장 장치 등을 준비하며, 소프트웨어로는 미국 판례법에서 인정받은 Guidance 社의 Encase 및 국내 검찰청에서 개발한 D.E.A.S 등을 사용하여 증거를 이미징하고 분석한다.

(그림 36. 디스크 복제 장비)

증거수집 단계에서는 아래 그림과 같은 절차로 수행한다고 설명되어 있다.



(그림 37. 디지털증거 수집 절차도[48])

① 사진촬영 및 현장 스케치
- 컴퓨터 등 대상물 앞·뒷면 사진, 주변장치, 모니터 등 촬영
- 현장에 있는 수집 대상물의 위치를 상세히 스케치

② 네트워크 정보 등 휘발성 증거 수집

③ 수집 대상물의 전원 확인
- 전원이 꺼진 경우 그대로 수집
- 전원이 켜진 경우, 정상적인 시스템 종료 절차를 수행하면 임시 데이터가 삭제되므로 이를 방지하기 위해 일반 PC의 경우 종료 절차 없이 전원플러그 강제 분리 (단, 서버는 정상 종료 절차 수행)

48) "디지털 증거처리 표준 가이드라인", 경찰청, 2006.12

④ 본체 수집을 원칙으로 하되, 부득이한 경우 하드디스크만 불리하여 수집
- BIOS의 메인 메뉴에서 시스템 시간과 날짜정보 확인

⑤ 외장형 디스크, USB 등 기타 디지털 저장매체 수집

⑥ 증거물 포장 및 상세정보 기재
- 하드디스크는 보호박스를 사용하여 개별 포장함이 원칙
- 상세정보 : 사건번호, 수집자, 입회인, 수집일시, 장소, 물품, 제조번호 등

⑦ 입회인으로부터 압수확인서 및 압수증거물 목록에 서명 날인을 받음

⑧ 사용자 질의서 작성
- 컴퓨터 사용자를 상대로 컴퓨터 용도, 설치된 운영체제, 패스워드 정보 등 질의 후 기재

그러나 2011년 개정된 형사소송법(제106조 제3항)에 의해 하드디스크 등의 저장매체를 통째로 압수하는 것이 원칙상으로 금지되었다. 이에 따라 현장에서 저장매체를 물리적으로 복제하거나 이미징 하는 절차가 추가되어야 한다. 사본 수집 후 원본과 사본에 대한 해쉬값을 생성하여 디지털 증거의 무결성을 증명한다.

증거 분석의뢰 단계에서 수사관 등은 분석관에게 디지털증거 분석에 필요한 모든 정보를 제공하고, 증거의 무결성과 연계보관성(Chain of Custody)를 보장하기 위해 증거의 봉인, 운반, 인수 과정에서의 요구하는 기준을 충족시켜야 한다. 증거물 봉인 과정에서는 물리적 충격 및 전·자기장 영향을 받지 않도록 완충용 보호박스, 정전기 방지용 팩, 하드케이스 등을 사용하여 포장하여야 하며, 밀봉전용 특수 테이프(evidence tape)와 봉인지(sell)를 이용해 증거물 훼손 방지해야 한다. 증거물 운반 과정에서는 증거물 누락 및 도난이 없도록 증거 담당자 목록을 작성하고 유지하여야 한다. 증거물 인수 과정에서는 증거 목록에서 누락된 증거물이 없는지, 증거물의 밀본전용 특수 테이프와 봉인지 상태가 이상 없는지 등을 확인하여야 한다.

디지털 증거 분석 단계에서는 다음의 준비사항이 필요하다.

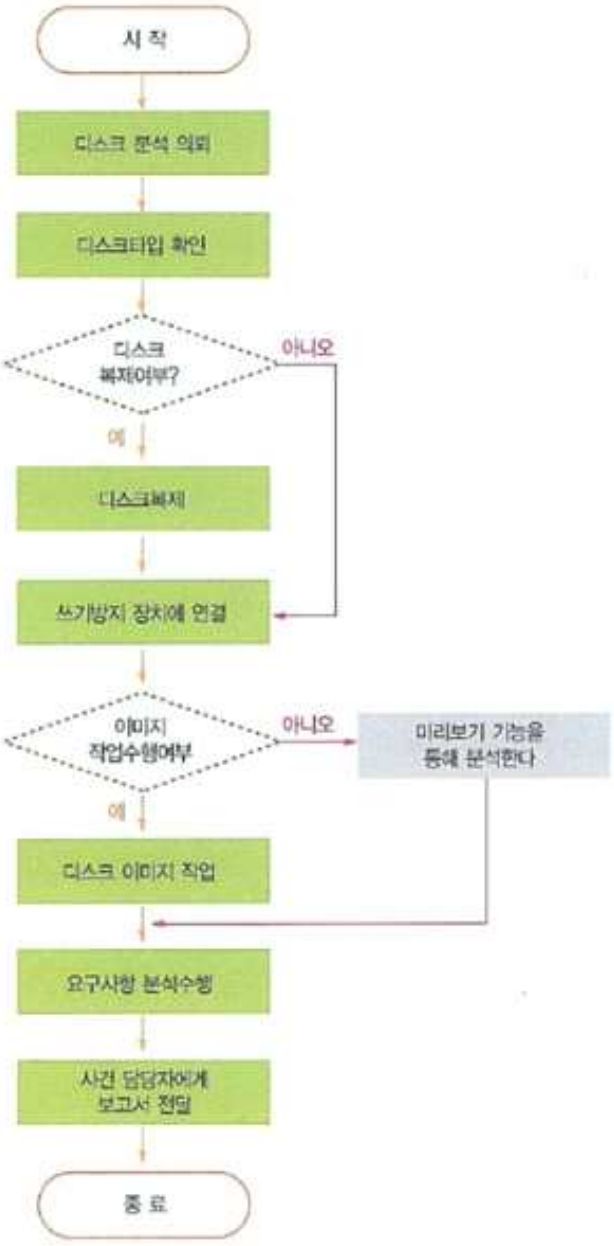
- 분석담당자 지정
  - 증거분석관은 전산•정보통신 분야의 전공자로 디지털증거 분석 전문교육을 이수하고 매년 소정의 보수교육을 수료한 자 중에서 지정
  - 운영체제, 데이터베이스 , 네트워크 등 전문분야에 대한 분석활동이 필요한 경우 전문 영역별로 구분하여 분석

- 복제본 생성
  - 물리적 복제를 수행할 경우 동일한 용량의 하드디스크를 준비하고, 동일한 하드디스크가 없을 경우 원본 디스크보다 대용량의 하드디스크를 준비하여 쓰기방지장치 연결 후 복제본을 생성
  - 이미지 파일을 생성할 경우 원본에 대한 쓰기방지장치를 부착하여 원본의 변경을 방지
  - 복제 후에는 원본과의 동일성 및 무결성 입증을 위해 원본 및 사본의 각 해쉬값을 추출 및 비교

- 분석 대상 및 범위 결정
  - 분석관은 사사관 등과 사전 면담을 실시하여 사건개요, 증거물 수집 과정, 분석의 목적 등을 파악하고 분석 대상 및 범위를 결정
  - 분석관은 증거물의 종류 및 특징에 따라 분석에 필요한 정보 및 기법을 사전에 숙지

일반적인 하드디스크의 경우 아래와 같은 절차로 분석을 진행한다.

① 증거 디스크의 형태(IDE, SATA, SCSI, 플래쉬 메모리) 확인
② 증거 디스크의 복제 여부 결정
③ 증거 디스크를 쓰기방지장치에 연결
④ 증거 디스크의 이미지 작업 수행
⑤ 증거 디스크의 복구가 필요할 경우 복구 수행
⑥ 의뢰서에 작성되어 있는 요구사항을 분석하고 보고서 작성
⑦ 분석이 끝나면 담당자에게 연락하여 상세 설명 후 증거물과 함께 보고서 전달



(그림 38. 디스크 분석 절차[49])

디지털 증거의 분석 기술로는 디스크 브라우징, 데이터 복구, 키워드·해쉬 검색, 암호 해독 및 패스워드 크랙, 타임라인 분석, 통계 분석, 로그 및 히스토리 분석 등이 있다. 이러한 분석 기능을 통합적으로 제공해주는 Encase, FTK 등의 툴이 있으며 특정 기능에 특화되어 분석 기능을 제공하는 Password Recovery Toolkit(암호 해독), Data Rescue(파일 복구), File Extractor Pro(데이터 카빙), Helix3(라이브 시스템 조사) 등의 툴도 존재한다.

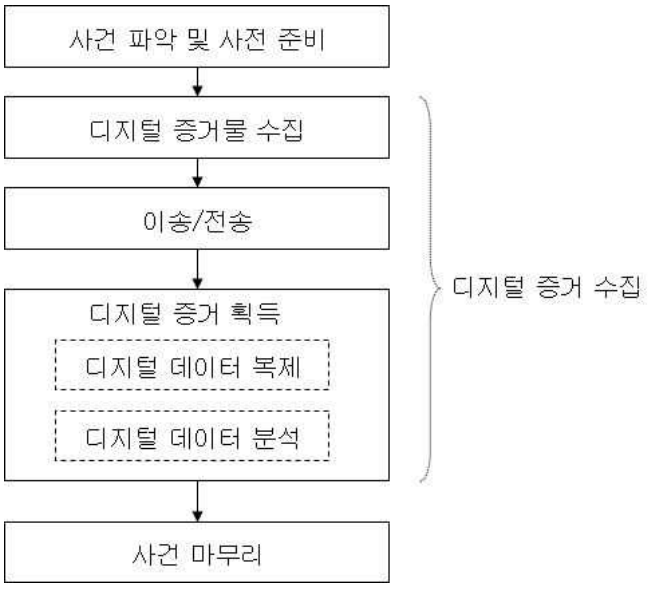
49) "디지털 증거처리 표준 가이드라인", 경찰청, 2006.12

나. TTAS.KO-12.0058 컴퓨터 포렌식 가이드라인

(1) 컴퓨터 포렌식의 절차 및 기본 원칙

(가) 절차

아래 그림과 같이 5단계로 구성된다. 먼저, 사건 파악 및 사전 준비를 하고, 현장에 출동하여 디지털 증거를 포함하고 있다고 판단되는 디지털 증거물을 수집한다. 이후 디지털 증거 분석실로 디지털증거물을 이송하고, 디지털 증거물 내의 디지털 데이터를 분석하여 디지털 증거를 획득한 후, 사건을 마무리한다. 디지털 증거 수집은 디지털 증거물 수집 및 이송, 디지털증거 획득으로 나뉜다.



(그림 39. 컴퓨터 포렌식 절차[50])

- 사건 파악 및 사전 준비 : 범죄의 유형 및 확보하여야 할 정보를 파악하고, 범죄 현장에서 수집 대상을 신속하고 정확하게 효율적으로 획득할 수 있도록 준비하는 과정을 말한다. 증거물 수집 계획 수립, 각 분야의 전문가를 포함한 증거 수집 팀 구성, 필요한 하드웨어 장비 및 소프트웨어 확보 등이 여기에 속한다.
- 디지털 증거물의 수집 : 현장에 도착한 후 현장 상황을 파악하여 디지털 증거가 존재한다고 판단되는 물리적 장치를 확보하는 과정과 해당 증거물을 안전하게 수집하는 과정으로 나뉜다.
- 디지털 증거 획득 : 수집된 디지털 증거물 내의 디지털 데이터를 검색 및 분석하여 사건과 연관된 데이터를 찾아내는 것을 말한다. 디지털 데이터 분석에 앞서 획득된 디지털 증거물 내의 데이터를 보호하기 위해 디지털 데이터 복제가 선행되기도 한다.

50) TTAS.KO-12.0058 컴퓨터 포렌식 가이드라인, 한국정보통신기술협회, 2007

• 사건 마무리 : 분석 결과 및 기타 정보를 포함한 결과 보고서 작성과 증거 자료의 안전한 보관을 포함한다.

(나) 컴퓨터 포렌식 기본원칙

- 관련 법규 및 지침에 규정된 일반적인 원칙과 절차를 준수한다.
- 수사에 필요한 최소한의 증거 수집을 원칙으로 한다.
- 디지털 증거는 기술적, 절차적인 수단을 통해 진정성, 무결성이 보존되어야 한다.
- 신뢰성 있는 디지털 증거를 획득하기 위해 도구의 신뢰성이 뒷받침되어야 한다.
- 최종적으로 법정에 제출되는 디지털 증거의 원본성이 보장되어야 한다.

(2) 디지털 증거물 수집 시 준수사항

(가) 어떤 시스템을 수집할 것인지를 목록에서 확인하여 신속 정확하게 수집한다.

(나) 하드디스크만 수집할 경우 충격 등으로 인해 증거물에 손상이 가지 않도록 주의한다.

(다) 시스템 하드웨어나 네트워크를 파악하고 원본의 손상을 방지한다.

(라) 시스템 전원 차단 여부를 먼저 파악하고, 전원이 꺼져 있다고 판단되더라도 화면보호기 작동 여부, 하드디스크 및 모니터 작동여부 등을 파악하여 전원 유무를 재확인한다.

* 화면보호기에 암호설정이 되어 있는 경우 수사관이 사용자 및 관리자에게 비밀번호 질의한다.

(마) 전원이 켜져 있는 시스템에 수집해야 할 휘발성 자료가 있을 때 시스템에 피해가 가지 않는 최소한의 범위 내에서 작업을 수행한다.

(바) 전원이 켜져 있을 경우 시스템 시간을 확인하는 과정에서 표준시각 정보와 비교해서 정확하게 기록한다.

(사) 전원이 켜져 있을 경우 부주의에 의해 시스템 내의 프로그램을 실행시키지 않도록 주의한다.

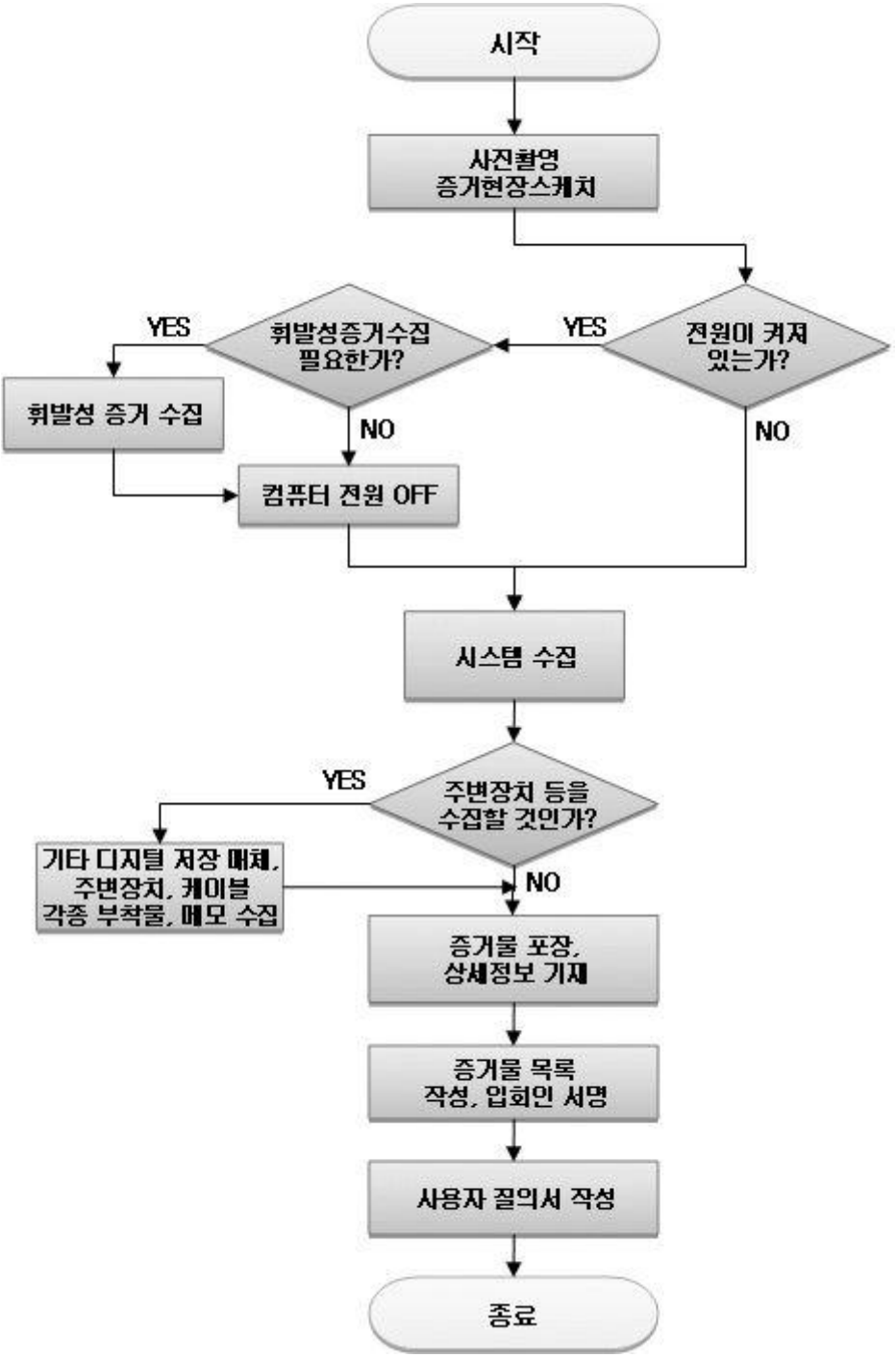
(아) 기타 장치의 종류를 확인하고, 기능이나 용도를 알 수 없는 장치가 있는 경우 사진촬영 등 자료를 확보하고 전문가와 상의한다.

(자) 수집관의 전문성이 부족하다고 판단되는 경우 증거물을 조작하지 말고 전문가에게 인계한다.

(차) 취급 미숙으로 인해 시스템을 켜는 것 만으로도 데이터를 변경할 수 있으므로 각별히 주의한다.

(3) 디지털 증거물 획득 절차

디지털 증거를 포함하고 있는 증거물을 획득하는 절차는 아래 그림과 같다.



(그림 40. 디지털 증거물 획득 절차[51])

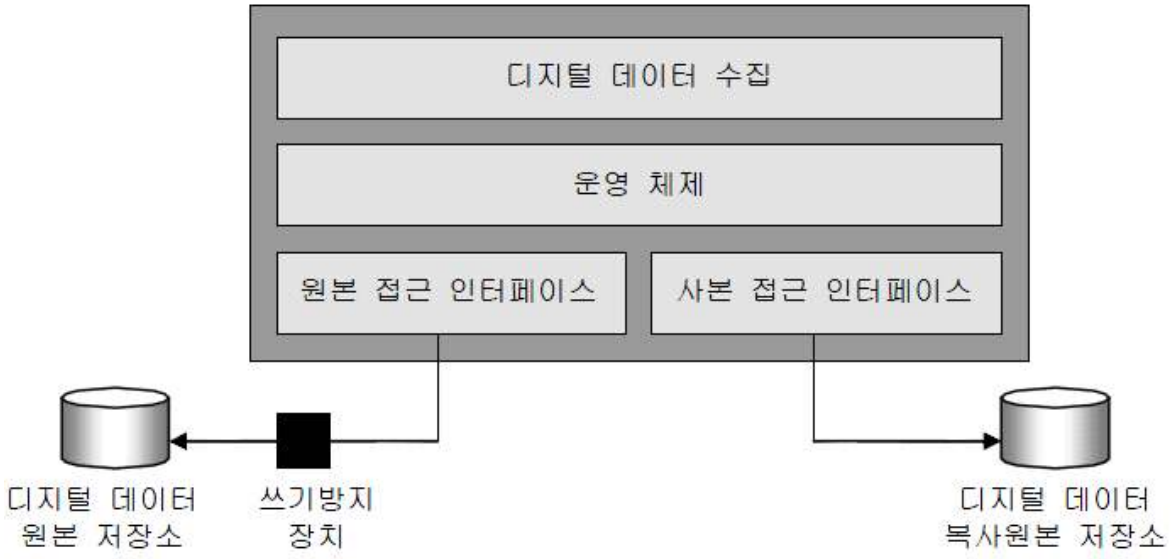
51) TTAS.KO-12.0058 컴퓨터 포렌식 가이드라인, 한국정보통신기술협회, 2007

다. TTAS.KO-12.0057 컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항

(1) 디지털 데이터 수집도구의 필수적인 요구사항

(가) 일반적 요구사항

- 디지털 데이터 수집도구는 획득한 디지털 데이터 원본의 디스크 이미지나 복제 디스크를 생성할 수 있어야 한다.
- 디지털 데이터 수집도구는 디지털 데이터 원본 저장소의 전체 데이터를 수집할 수 있어야 한다.
- 디지털 데이터 수집도구는 디지털 데이터 원본 저장소의 일정 부분 데이터를 수집할 수 있어야 한다.
- 디지털 데이터 수집도구는 디지털 데이터 원본 저장소의 데이터를 완전하게 수집해야 한다.
- 디지털 데이터 수집도구는 디지털 데이터 원본 저장소의 데이터를 정확하게 수집해야 한다.
- 디지털 데이터 수집도구는 디지털 데이터 획득 과정에서 오류가 발생한다면 오류의 유형과 위치를 사용자에게 알려야 한다.
- 디지털 데이터 수집도구는 디지털 데이터 획득 과정에서 해결할 수 없는 오류가 발생한다면 복사 원본 저장소의 해당 위치에 분석 결과에 영향을 주지 않는 값으로 대체해야 한다.
- 디지털 데이터 수집도구는 디지털 데이터 복사 원본 작성시 저장소의 공간 부족을 포함한 기타 오류가 발생한다면 이를 사용자에게 알려야 한다.



(그림 41. 디지털 데이터 수집 시스템 구성[52])

52) TTAS.KO-12.0057 컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항, 한국정보통신기술협회, 2007

(나) 디스크 이미지 작성시 요구사항

- 디지털 데이터 수집도구가 디스크 이미지 생성 기능을 갖는다면, 하나 이상의 디스크 이미지 포맷을 지원해야 한다.
- 디지털 데이터 수집도구가 디스크 이미지 생성 기능을 갖는다면, 디스크 이미지로부터 컴퓨터 파일 시스템으로 접근 가능한 디지털 데이터 원본 저장소와 동일한 형태의 디스크를 복원하는 수단을 제공해야 한다.

(다) 쓰기방지 장치가 없는 환경에서의 요구사항

- 디지털 데이터 수집도구가 쓰기방지 장치 없이 동작한다면, 데이터 수집 과정에서 데지털 데이터 원본의 변경이 발생했는지 확인하는 수단을 제공해야 한다.

(라) 디스크 이미지와 복제 디스크 생성 기능 동시 제공 시 요구사항

- 디지털 데이터 수집도구가 디스크 이미지와 복제 디스크 둘다 생성하는 기능을 제공한다면, 사용자가 디스크 이미지와 복제 디스크 중 선택하여 생성할 수 있는 기능을 제공해야 한다.

(2) 디지털 데이터 수집도구의 선택적 기능 및 각 기능 별 요구사항

(가) 디지털 데이터 수집도구의 선택적 기능

- 디지털 데이터 복사 원본의 보관 과정에서 데이터 변동이 발생했는지 확인하는 기능
- 디지털 데이터 복사 원본의 보관 과정에서 데이터 변동이 발생했을 때 해당 위치를 알리는 기능
- 전체 디지털 데이터 수집 과정을 기록하는 기능
- 디지털 데이터 수집도구가 데이터 수집과정 기록 기능을 제공한다면, 아래와 같은 내용을 포함해야 한다.
  - 데이터 수집 도구에 대한 정보
  - 데이터 획득과 관련해 획득 일자, 획득 시간
  - 데이터 획득과 관련해 디스크 크기, 제조업자, 모델 번호, 시리얼 번호, 파티션 테이블 등 대상 장치의 정보
  - 데이터 획득과 관련해 획득된 데이터의 용량, 획득 결과
  - 획득자의 정보 및 사용자 의견

(나) 디스크 이미지 파일 작성과 관련된 선택적 기능

- 디스크 이미지 생성과 관련된 선택적 기능
  - 디스크 이미지 생성시 디스크 이미지를 분할하여 생성할 수 있는 기능
  - 디스크 이미지 저장소의 공간이 부족할 때 저장소를 전환하여 추가적인 디스크 이미지를 생성하는 기능

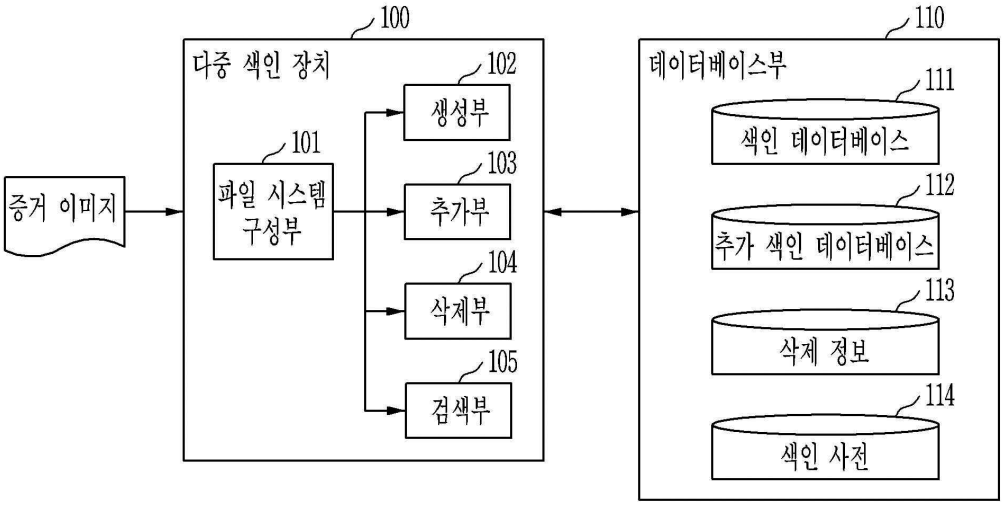
· 특정 포맷의 디스크 이미지를 다른 포맷의 디스크 이미지로 변환하는 기능
· 디스크 이미지의 일부에 대한 복제 디스크를 생성하는 기능
· 디스크 이미지 생성시 생성된 디스크 이미지를 압축하는 기능
· 디스크 이미지 생성시 생성된 디스크 이미지를 암호화하는 기능

- 디스크 이미지 분활 기능과 관련된 요구사항
  · 디지털 데이터 수집도구가 디스크 이미지 분할 기능을 제공한다면, 전체 분할 디스크 이미지 내에 존재하는 데이터는 원본 데이터와 동일하여야 한다.
  · 디지털 데이터 수집도구가 디스크 이미지 분할 기능을 제공한다면, 각 분할 디스크 이미지를 서로 다른 저장소에 저장할 수 있는 기능을 제공해야 한다.
  · 디지털 데이터 수집도구가 디스크 이미지 분할 기능을 제공한다면, 사용자가 분할 디스크 이미지의 크기를 선택할 수 있는 기능을 제공해야 한다.
- 디스크 이미지 저장소 전환 기능과 관련된 요구사항
  · 디지털 데이터 수집도구가 디스크 이미지 저장소 전환 기능을 제공한다면, 전체 분할 디스크 이미지 내에 존재하는 데이터는 획득된 원본 데이터와 동일하여야 한다.
- 디스크 이미지 포맷 변환 기능과 관련된 요구사항
  · 디지털 데이터 수집도구가 디스크 이미지 포맷 변환 기능을 제공한다면, 변환된 디스크 이미지와 원본 디스크 이미지내에 포함된 모든 데이터는 비트 단위로 동일해야 한다.

(다) 복제 디스크 생성과 관련된 선택적 기능
- 복제 디스크 저장소의 공간이 부족할 때 가능한 용량만큼 복제 디스크를 생성하는 기능

라. 주요 관련 특허

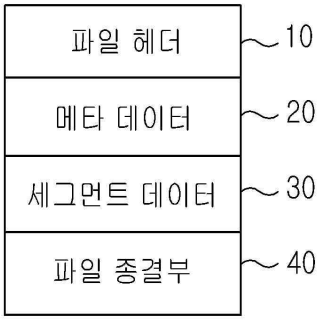
(1) 디지털 포렌식 시스템에서 대용량 증거 이미지의 다중 색인 장치 및 방법
- 출원번호 : 10-2009-0122959
- 출우원일자 : 2009년 12월 11일
- 주요 내용 : 이 발명에 따른 디지털 포렌식 다중 색인 장치는 증거 이미지를 파일 시스템으로 구성하는 파일 시스템 구성부와, 상기 파일 시스템 구성부에 의해 파일 시스템으로 구성된 문서들에 근거하여 적어도 하나의 색인 데이터베이스를 생성하는 생성부와, 상기 적어도 하나의 색인 데이터베이스에 추가되는 색인에 근거하여 추가 색인 데이터베이스를 생성하는 추가부와, 상기 적어도 하나의 색인 데이터베이스 또는 상기 추가 색인 데이터베이스에 대한 삭제 정보를 생성하는 삭제부와, 상기 적어도 하나의 색인 데이터베이스 또는 상기 추가 색인 데이터베이스로부터 단어를 검색하는 검색부를 포함한다.



(그림 42. '대용량 증거 이미지의 다중 색인 장치 및 방법' 대표 도면)

(2) 디지털 증거의 저장 및 분석을 위한 이미지 파일 포맷 구조및 그 구조로 데이터가 기록된 기록 매체

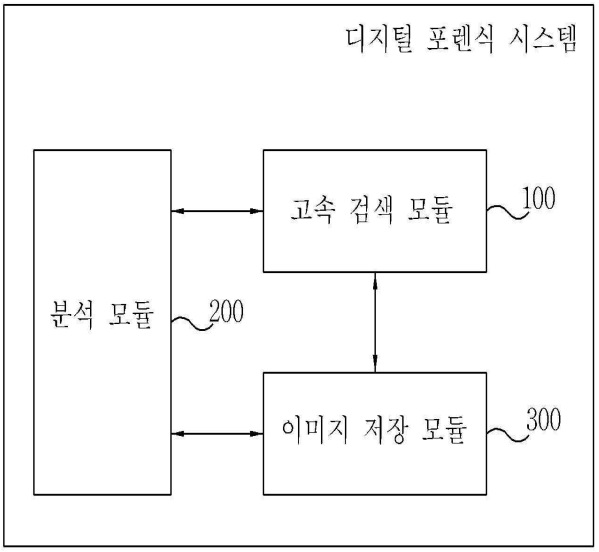
- 출원번호 : 10-2007-0132715
- 출원일자 : 2007년 12월 17일
- 주요 내용 : 이 발명의 디지털 증거의 저장 및 분석을 위한 이미지 파일 포맷은 컴퓨터(Computer) 하드디스크(Hard Disk)나 휴대용 메모리 카드(Memory Card)와 같은 일반적인 디지털(Digital) 저장 장치로부터 획득된 디지털 증거 데이터(Evidence Data)의 저장 포맷(Format) 구조에 관한 것이다. 이 발명에 따르면 압축과 파일 크기에 따른 복수의 이미지 파일 생성에 의해 대용량의 증거 데이터들도 경량화되어 저장될 수 있으며 유한한 저장크기를 가지는 저장매체에 안전하게 저장될 수 있다.



(그림 43. '디지털 증거의 저장 및 분석을 위한 이미지 파일 포맷 구조및 그 구조로 데이터가 기록된 기록 매체' 대표도면)

(3) 디지털 포렌식 시스템을 위한 대용량 데이터 고속 검색시스템 및 방법

- 출원번호 : 10-2007-0120759
- 출원일자 : 2007년 11월 26일
- 주요내용 : 디지털 포렌식 시스템을 위한 대용량 데이터 고속 검색 시스템 및 방법이 개시된다. 디지털 포렌식 시스템을 위한 대용량 데이터 고속 검색 방법은, 이미지 저장 모듈이 검색하고자 하는 디스크 이미지를 입력받는 단계; 분석 모듈에 의해 이미지 저장 모듈로부터 입력된 디스크 이미지를 분석하여 디스크 이미지상에 존재하는 파일 목록을 구성하는 단계, 고속 검색 모듈에 의해 이미지 저장 모듈로부터 입력된 디스크 이미지에 대해 파일별로 클러스터를 재배열하는 단계, 고속 검색 모듈에 의해 텍스트 정보를 가지고 있는 파일로부터 텍스트 정보를 추출하여 저장하는 단계 및 고속 검색 모듈에 의해 비트단위 검색 기법에 의해 키워드 및 통상적인 표현을 검색하는 단계를 포함한다.



(그림 44. '디지털 포렌식 시스템을 위한 대용량 데이터 고속 검색시스템 및 방법' 대표 도면)

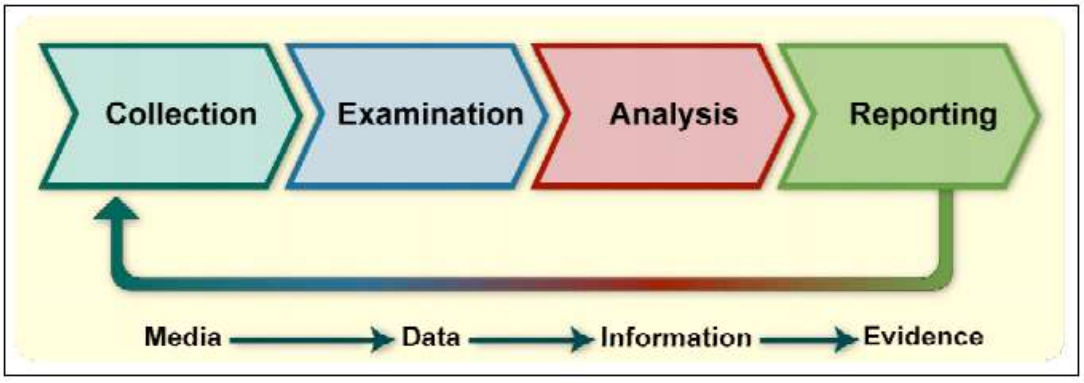
2. 국외 디지털 포렌식 표준 및 특허 분석

가. NIST Special Publication 800-86, "Guide to Integrating Forensic Techniques into Incident Response"

미국 NIST SP 800-86(Guide to Integrating Forensic Techniques into Incident Response)은 2006년 발간된 것으로 보안사고 대응절차에 포렌식 기술을 통합시키는 방법에 대해 제시하고 있다. 이 디지털 증거 표준에서 제시하고 있는 포렌식 프로세스는

아래와 같다.

- Collection
  - Data의 무결성을 유지하며, 다음의 절차에 따라 관련된 data의 가능한 source에서 data를 확인, 식별, 기록, 취득
- Examination
  - 수집된 data의 자동화된 방법과 수동적인 방법의 조합으로 forensically한 처리와 각별히 중요한 data의 판단 및 추출
- Analysis
  - 유용한 정보를 도출하기 위해 법적으로 정당한 방법과 기술을 사용하여 조사된 결과를 분석
- Reporting
  - 이용한 작업에 대한 설명, 어떤 도구와 절차가 선택되었는지에 대한 설명, 다른 작업을 수행할 필요가 있는지에 대한 결정, 정책, 절차, 비용, forensic process의 개선을 위한 권고 등의 기술(記述)을 포함한 분석한 결과를 보고



(그림 45. NIST SP 800-86, Forensic Process[53])

나. RFC 3227, “Guidelines for Evidence Collection and Archiving”

보안사고(Security incident)란 RFC2828(Internet Security Glossary)에 정의되어 있는데로 시스템의 보안정책이 위반되거나 깨어진 보안과 관련된 시스템관련 사고(event)를 말한다. RFC 3227 문서의 목적은 시스템 관리자(administrator)에게 이러한 시스템 보안사고에 관한 증거물수집과 파일보관에 관한 지침을 제공하기 위한 것이다[54].

(1) 디지털 증거 수집 시 피해야할 사항

53) “NIST Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response”, NIST, 2006

54) RFC 3227, “Guidelines for Evidence Collection and Archiving”

- 증거수집이 끝나기 전 시스템을 종료하는 행위
- 원본 시스템 상에 있는 프로그램의 사용
- 접근 시간(access time)을 변경시키는 프로그램의 사용(e.g., tar, xcopy)

(2) 프라이버시 관련 이슈
- 개인정보보호 관련 법률이나 회사의 지침에 위배되지 않도록 주의
- 증거물과 함께 수집된 어떠한 정보도 그 정보에 대한 접근 권한이 없는 다른 사람에게 공개되지 않아야 함
- 합당한 이유가 없는 이상 특별히 접근할 필요 없는 영역에 저장된 정보들에 대해 수집하지 않아야 함
- 사건 현장에서 행하는 증거 수집 행위는 사전에 수립된 절차에 위배되지 않아야 함

(3) 법률적인 고려
- 증거로서의 인정 가능성
- 증거물과 사건과의 연관성
- 증거 수집에서부터 법정 제출까지 전체 단계에 걸쳐 증거의 무결성·신뢰성을 증명할 수 있어야 함
- 법정에서 쉽게 이해할 수 있으며 신뢰가능성에 대해 납득할 수 있어야 함

(4) 수집 절차
- 어떤 시스템으로부터 증거물을 수집할 것인지 기록
- 수집할 증거의 범위를 설정
- 증거의 변경을 초래할 수 있는 외부접근 수단 제거
- 대상 시스템에서 휘발성이 높은 순서로 증거물 수집
- 시스템 clock 편차 기록
- 증거 수집 절차를 문서화
- 증거 수집 시 관련된 사람들 정보 기록

(5) 파일보관 절차(Chain of custody)

증거물이 어떻게 발견되었고 어떻게 다루어졌는지를 비롯한 증거물에 관련된 모든 사항들을 명확하게 기술하여야 한다.
- 어디서, 언제, 누가 증거물을 발견하고 수집하였는가?
- 어디서, 언제, 누가 증거물을 다루었고 검사하였는가?
- 누가 어느 기간에 증거물을 관리했는가, 어떻게 저장되었는가?
- 언제 관리에 대한 변경이 일어났고, 언제 어떻게 이송되었는가?

(6) 필요한 도구들(tools)

- 프로세스를 검사하기 위한 프로그램(e.g., ps)
- 시스템 상태(state)를 검사하기 위한 프로그램(e.g., showrev, ifconfig, netstat, arp)
- bit-to-bit 복사를 할 수 있는 프로그램(e.g., dd, SafeBack)
- 체크섬이나 서명(Signature)을 생성할 수 있는 프로그램 (e.g., sha1sum, checksum-enabled dd, SafeBack, pgp)
- Core image를 생성할 수 있는 프로그램(e.g., gcore, gdb)
- 증거수집을 자동화할 수 있는 스크립트(e.g., Ther Coroner's Toolkit[FAR1999])
- 이 때 사용하는 툴들에 대해 확실성(authenticity)과 진정성(reliability)을 증명할 수 있어야 한다.

다. NIST Computer Forensics Tool Testing Program(CFTT)

미국은 포렌식 도구 기능 검증을 국가적으로 주도함으로써 디지털 포렌식 도구의 검증 및 평가 방안으로써 CFTT(Computer Forensics Tool Testing Program)을 개발하였다. CFTT는 디지털 포렌식 툴의 검증 및 평가 방안을 제시하고, 평가 결과 보고서는 미국의 국가 법무연구소(NIJ)와 함께 공동으로 발간하여 일반인들도 쉽게 열람할 수 있도록 하고 있다. 컴퓨터 범죄 수사관들은 이 보고서를 참조하여 디지털 포렌식 툴의 선정 기준을 확립하며, 변호사와 검사들은 디지털 증거의 객관성을 증명하기 위한 자료로 활용하고 있다.

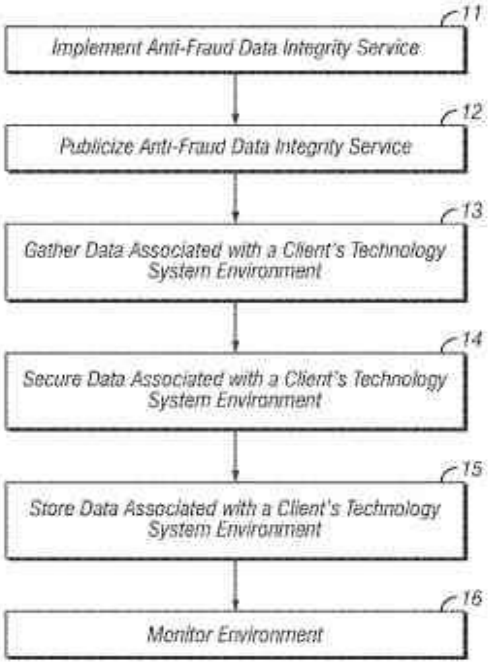
- 포렌식 도구(Tool) 테스트 과정
  - NIST가 테스트 되어야 할 tool을 습득
  - NIST가 tool 설명서를 검토
  - NIST가 tool의 설명서를 통한 특성에 기반해 유사한 테스트 case를 선택
  - NIST가 테스트 계획 발전
  - NIST가 테스트를 실행
  - NIST가 테스트 보고서를 작성
  - 운영 위원회가 테스트 보고서를 검토한다.
  - 해당 tool 생산회사가 테스트 보고서를 검토
  - NIST가 웹사이트에 SW support를 업로드
  - National Institute of Justice(NIJ)가 웹사이트에 테스트 보고서 업로드
- 2011년 CFTT 검사를 통과한 디지털 포렌식 도구 예
  - IMAGE MASSTER SOLO-3 FORENSICS (software version 2.0.10.23F)
  - TABLEAU TD1 FORENSIC DUPLICATOR (firmware version 2.34 FEB 17)
  - TABLEAU IMAGER (TIM) VERSION 1.11

- DC3DD VERSION 7.0.0
- IMAGE MASSTER SOLO-4 FORENSICS (software version 4.2.63.0)
- TABLEAU TDW1 DRIVE TOOL/DRIVE WIPER
- AFLOGICAL 1.4
- MOBILYZE VERSION 1.1

라. 주요 관련 특허

(1) METHOD AND APPARATUS FOR MAINTAINING HIGH DATA INTEGRITY AND FOR PROVIDING A SECURE AUDIT FOR FRAUD PREVENTION AND DETECTION

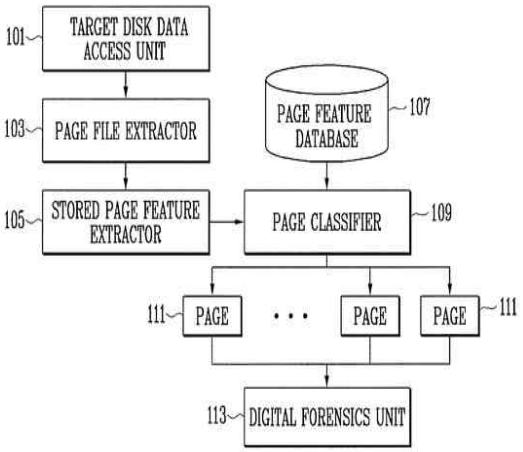
- 출원번호 : (미국) 12950454
- 출원일자 : 2010년 11월 19일
- 주요내용 : 이 발명에서는 서로 다른 시점에서 컴퓨터 폴더에 대한 다양한 비교가 실행된다. 이러한 비교는 분실 되었거나 또는 변경할 필요가 없었을 때 변경된 접근 날짜를 갖는 문서를 탐지하는 기능을 제공하며, 이에 따라 의심되는 오류 또는 그러한 오류에 대한 증거를 찾기 위한 분실 문서의 발견을 허용한다. 특정 기간에 대하여 기간 당 의심스런 행위를 탐지하기 위해 시간적 흐름에 따라 비교된다.



(그림 46. 'METHOD AND APPARATUS FOR MAINTAINING HIGH DATA INTEGRITY AND FOR PROVIDING A SECURE AUDIT FOR FRAUD PREVENTION AND DETECTION' 의 대표도면)

(2) Method and apparatus for digital forensics

- 출원번호 : (미국) 12252869
- 출원일자 : 2008년 10월 16일
- 주요내용 : 이 발명은 디지털 포렌식 기법과 도구에 대한 것으로 저장매체에서 page-file 추출하는 도구, page-file 추출물에 대해 sotred-page feature 추출하는 도구, 추출한 feature로 미리 정해놓은 분류 기준으로 classifier를 찾고 결과 값으로 분류하는 도구, 이러한 방법으로 분류된 페이지들로 디지털 포렌식 분석을 하는 도구로 구성된다.



(그림 47. 'Method and apparatus for digital forensics'의 대표도면)

3. 국내외 디지털 포렌식 도구 및 기술 비교

가. 디지털 포렌식 이미징(Imaging) 도구 비교·분석

디지털 포렌식을 수행할 대상 시스템의 종류가 다양하고, 조사할 디지털 자료의 특성이 다양하기 때문에 디지털 포렌식 도구도 그만큼 다양하게 개발되었다.

(표 8. 디지털 포렌식 도구의 종류별 제품 분류)

종류	제품명
하드 디스크 쓰기 방지 도구 (Hard Ware Protection Tool)	A-Card, FastBlock, NoWrite
하드 디스크 이미징 도구 (Imaging Tool)	DD(Linux), Safe Back, SnapBackDatArrest, FreeBSD, Mares imaging tool
검색 도구 (Searching Tool)	Grep(linux), dtSearch, Text Search Plus(NTI) AfindHfindSfind(Forensic Toolkit)
각종 문서/파일 보기 도구 (Browsing, Viewer)	Conversions Plus, Quick View Plus, ThumbsPlus WinHex, Ultra Edit
분석 및 복구 도구 (Analysis / Recovery Tool)	Hash Keeper, TCT, EasyRecoveryFileRepair Final data, Advanced Password Recovery
통합 도구 (Integration Tool)	EnCase, iLook, Forensix, Forensic Toolkit Autopsy, F.I.R.E, Final Forensic

- 소프트웨어 방식을 이용한 저장매체 이미징

저장매체를 이미징 하는 방식은 크게 소프트웨어 방식과 하드웨어 방식으로 나눌 수 있다. 소프트웨어 방식은 소프트웨어를 이용해 원본 저장매체의 모든 물리적인 섹터를 사본으로 이미징하는 것으로 그 종류가 다양하지만 주로 사용되는 소프트웨어는 (표 9)와 같다.

(표 9. 저장매체 이미징 - 소프트웨어 방식)

이름	인터페이스	플랫폼	제조사	라이선스
FTK Imager	GUI	윈도우	AccessData	무료
Tableau Imager	GUI	윈도우	TABLEAU	무료
EnCase winacq	CLI	윈도우	Guidance Software	상용/무료
dd-like	CLI	리눅스/윈도우	-	무료

소프트웨어 방식으로 이미징을 할 때 주의할 점은 원본 저장매체를 이미징 하는 동안 무결성이 훼손되지 않아야 한다는 점이다. 이를 위해 원본 저장매체를 읽기 전용으로 마운트하거나 또는 쓰기 방지 장치(write blocker)를 사용한다. 쓰기 방지 방식도 소프트웨어/하드웨어 방식이 존재하지만 성능이나 안전성의 이유로 경·검찰청 디지털 포렌식 현장에서는 하드웨어 방식을 권장하고 있다. 대표적인 하드웨어 쓰기 방지 장치는 (표 10]와 같다.

(표 10. 하드웨어 쓰기 방지 장치)

이름	제조사	지원 인터페이스	라이선스
Forensic Bridge	TABLEAU	PATA, SATA, SCSI, SAS, USB, FireWire	상용
FastBloc	Guidance Software	PATA, SATA, SCSI, SAS, USB, FireWire	상용
UltraDock	WiebeTech	PATA, SATA, USB, FireWire	상용
Drive Lock	ICS	PATA, SATA, SCSI, USB, FireWire	상용

쓰기 방지 장치는 원본 저장매체로 전달되는 쓰기 신호를 차단하여 원본의 무결성을 유지시켜주는 장비이다. 원본 저장매체와 이미징 소프트웨어를 동작시키는 호스트 사이에 브릿지(Bridge) 형태로 연결한다[55].

- 하드웨어 방식을 이용한 저장매체 이미징

이미징을 위해 특수 제작된 하드웨어 장비를 사용할 수도 있다. 소프트웨어 방식에서는 원본 저장매체의 마운트와 데이터 전송이 호스트 시스템에 의해 이루어졌다. 하지만, 하드웨어 방식에서는 이러한 작업이 독립된 하드웨어 장비를 통해 이루어진다.

55) http://forensic-proof.com/archives/3613

(표 11. 저장매체 이미징 - 하드웨어 방식)

이름	제조사	특징	라이선스
Image MASSter Solo-4	ICS	동시에 최대 2개의 이미징/복제가 가능한 대용 이미징/복제 장비	상용
Road MASSter	ICS	휴대성이 강화된 올인원 1:1 이미징/복제 장비	상용
Rapid Image	ICS	동시에 최대 20개의 이미징/복제가 가능한 대용량 장비	상용
Forensic Quest	Logicube	휴대성이 강화된 제품으로 1:1 이미징/복제 장비	상용
Forensic Dossier	Logicube	동시에 최대 2개의 이미징/복제가 가능한 휴대용 이미징/복제 장비	상용
OmniClone	Logicube	동시에 최대 10개의 이미징/복제가 가능한 대용량 장비	상용

하드웨어 이미징 장비는 고가이기 때문에 도입이 어려울 수 있다. 따라서 쓰기 방지 장치를 구입하고 무료 소프트웨어를 사용해 이미징하는 방안이 적합할 것으로 판단된다. 반면, 예산에 문제가 없는 경우 하드웨어 이미징 장비를 구입해 사용하는 것도 좋은 선택이 될 수 있다. 하드웨어 장비는 모델에 따라 다르지만 하나의 원본 저장매체를 동시에 여러 개로 복제하거나 이미징하는 것이 가능하고, 대부분의 하드웨어 이미징 장비는 와이핑(wiping) 기능도 포함하고 있기 때문에 저장 매체를 초기화 하는 경우 유용하게 사용할 수 있다[56].

56) http://forensic-proof.com/archives/3613

제 5 절 전자기록의 사법적 증거력 및 공·사 영역에서의 효력 조사

1. 국내외 전자기록의 증거능력에 관한 법령 및 판례 분석

가. 미국

(1) 연방증거법(Federal Rules of Evidence)

미국의 증거법은 1975년부터 시행되고 있는 연방증거법(Federal Rules of Evidence)를 토대로 하고 있기 때문에 이를 토대로 전자문서의 증거능력과 관련된 사항을 조사하였다.

연방증거법은 증거의 증거능력에 관하여 크게 관련성 원칙(Relevance Rule)과 적격성 원칙(Competence Rule)으로 구분하고, 후자를 다시 신뢰성(Reliability)에 근거한 원칙과 특별정책에 근거한 원칙으로 구분한다. 이를 토대로 미국의 증거법을 본다면, 증거를 관련성(Relevance), 신빙성(Reliability), 특별정책(Policy), 증명력(Probative value)이 순차적인 증거능력 판단기준으로서 작용한다고 할 수 있다.

(가) 관련성(Relevance)

주장사실 혹은 공소사실과 논리적으로 관련성이 없는 증거는 배제되며, 관련성이 있음이 확인된 경우는 다른 증거원칙에 부합되는지 여부를 심사하게 된다. 연방증거법 제401조[57]와 제402조[58]는 관련성에 관한 일반원칙을 규정하고 있다.

(나) 신빙성(Reliability)

일단 판사로서는 자료가 주장사실 또는 공소사실과 관련성이 있다고 판단하게 되면, 그 자료가 신빙성이 있는지 판단해야 하는 단계로 넘어가게 된다. 신빙성을 판단하는 기준으로는 서증의 경우 원본이 제출되었는지 여부(best evidence rule), 증거의 진정성 및 동일성 여부, 전문법칙(hearsay rule) 적용 여부 등이 있다.

- 최량증거원칙(Best Evidence Rule)

미국 연방증거법 제1002조는 서류, 기록물 또는 사진의 내용을 증명하기 위하여 문서, 기록물, 사진의 원본이 요구된다고 규정하고 있다. 또한 연방증거법 제1001조 제1호에 의하면 디지털 증거는 자기적 혹은 전기적 방식에 의한 기록물로서 제1002조의 서류, 기록물 등에 포함된다. 따라서 디지털 증거도 당연히 원본으로 제출될 것을 요구

---

57) **Rule 401. Test for Relevant Evidence**
Evidence is relevant if:
(a) it has any tendency to make a fact more or less probable than it would be without the evidence; and
(b) the fact is of consequence in determining the action.

58) **Rule 402. General Admissibility of Relevant Evidence**
Relevant evidence is admissible unless any of the following provides otherwise: the United States Constitution; a federal statute; these rules; or other rules prescribed by the Supreme Court.
Irrelevant evidence is not admissible.

받는다[59]. 그러나 디지털 증거의 경우 보통 원본 매체에 있는 증거를 다른 저장매체에 복사하여 수집하고 가시성·가독성 있는 형태로 변환시켜 제출되기 때문에 이를 원본으로 인정할 수 있는가가 문제된다. 이에 대해 동법 제1001조 제3호에서는 "데이터가 컴퓨터 또는 동종의 기억장치에 축적되어 있는 경우에는 가시성을 가지도록 작출한 출력인쇄물 또는 산출물로서 데이터의 내용을 정확히 반영하고 있다고 인정되는 것은 원본으로 본다"고 규정하고 있어 디지털증거를 출력한 인쇄물의 원본성을 법적으로 인정하고 있다[60].

• 증거의 진정성 및 동일성 여부

미국 연방증거규칙 제901조a항은 '증거허용에 대한 선행조건으로서 진정성과 동일성의 요구조건은 의문시 되는 사안에 대해 청구인이 주장하는 결론을 뒷받침하기에 충분한 증거에 의해 충족되어야 한다'고 규정하고 있으며, 동법 제901조b항에서 진정성을 입증할 수 있는 방법을 예시하고 있다[61]. 미국 법정에서 과학적 증거의 신빙성에 영향을 미치는 요소는 과학적 증거에 근거하는 이론(scientific theory)이 유효할 것, 그 이론을 적용하는 기술(technique)이 유효할 것, 그 기술을 특정 사건에 적절하게 사용(proper application)할 것 등이다[62]. 과학적 이론의 유효성과 원리를 적용하는 기술의 유효성은 아래 네 가지 경우에 의해 인정될 수 있다.

- 법원의 확지
- 입법에 의한 승인
- 상대방의 동의 또는 당사자 간의 합의
- 조사관 또는 전문가의 증언에 의한 입증

새로운 과학기술을 이용한 증거의 경우 법원의 확지나 입법에 의한 승인 및 당사자 간의 동의나 합의를 기대하기 힘들기 때문에 기술의 타당성에 대한 조사관 또는 전문가의 증언에 의한 입증이 필요한데 그러한 증언에 의할 경우 어느 정도의 기준을 요구하는지에 대하여 명확하지 않다. 미 법정에서는 이 기준에 대해 크게 Frye Test, Daubert Test(또는 Relevancy Approach)로 양분된다. 'Frye Test'는 1923년 D.C. 연방항소법원이 살인피고사건에 대하여 심리한 Frye v. United States 사건에서 처음 채택한 데서 유래한 것으로 '대상 과학 기술이 속하는 특정분야에 있어서 일반적인 승인을 얻은 충분히 확증된 것이어야 한다'는 기준을 제시한다. 그러나 이러한 Frye Test는

59) 정교일, "디지털증거의 압수와 공판정에서의 제출방안", 2010

60) 장상귀, "디지털증거의 증거능력에 관한 연구", 2008

61) 정교일, 전게 논문

62) 임경수, 이상진, "디지털 포렌식 관점에서 디지털 증거를 국내법에 일반적으로 수용하기 위한 연구", 2009

일반적 승인기준에 대해 명확하지 않고, 너무 엄격하다는 지적이 있어 왔다. 미 법원은 도버트 판결(Daubert v. Merrell Dow Pharmaceuticals, Inc.)사건에서 이러한 Frye 기준을 어느 정도 완화하여 과학적 증거의 타당성 판단과 당면 문제와의 관련성을 추정하는 완화된 기준으로 Daubert Test를 제시하였다. 이 기준에 따르면 과학적 이론이나 기법이 관련 과학계(Relevant Scientific Community) 내에서 일반적으로 인정받았는지가 과학적 도구와 정당성을 입증하는 가장 중요한 요소가 되었다. 즉, 이것은 전문가들의 증언(expert testimony)에 의해 지지되는 어떠한 관련 결론도 그것을 배제해야 할 특별한 이유가 없는 한 증거로서 채택되어야 함을 뜻한다. 전자적 정보와 관련하여 Daubert 기준이 적용된 사건으로 아동 학대행위의 증거 복원을 위해 디지털 포렌식 도구인 Guidance Software 社의 Encase를 사용한 State of Nerbraska v. Nhouthakith 사건이 있다. 이 사건에서 법원은 "Encase 소프트웨어는 증거를 이해하고 사실을 인정하는데 관련이 있고, 해당 소프트웨어에 사용된 기술이 관련된 과학계 내에서 일반적으로 인정받았기 때문에 정당하다"고 판결한 바 있다.

한편, 과학적 기술의 특정사건에 대한 적절한 사용 여부와 관련해서는 기술에 사용된 검사 도구의 상태, 적절한 절차의 이행, 기술을 실행한 사람의 자격과 그 결과를 해석한 사람의 자격 등의 항목이 문제시 된다. 기술을 실행한 사람의 전문성에 대해 연방증거법 제702조에서 "그 전문가는 관련된 주제에 대한 지식, 기술, 경험, 훈련, 교육을 갖추고 있음을 보여주면 된다"고 규정하고 있다[63].

- 전문법칙 적용 여부

'전문증거'는 사실인정의 기초가 되는 사실을 경험한 사람 자신이 법원에 그 경험내용을 직접 보고하지 않고, 다른 매체를 통해 간접적으로 보고하는 경우에 그러한 매체를 말한다. 연방증거법 제801조는 전문증거에 관한 정의규정을 두고 있고, 제802조에서 원칙적으로 이러한 전문증거의 증거능력을 부인하는 이른바 '전문법칙(hearsay rule)'을 규정하고 있다[64]. 그리고, 전문법칙의 예외규정(exception)을 3개 조문(동법 제803조, 제804조, 제807조)으로 나누어 규정하고 있으며, 제803조는 원진술자의 진술가능 여부와 무관하게 인정되는 23개의 예외규정을 담고 있으며, 제804조는 원진술자의 진술이 불가능한 것을 요건으로 하는 5개의 예외규정을 두고 있으며, 제807조는 이와는 다른 특별한 이유에 근거한 예외규정을 포함하고 있다. 특히 동법 제803조 제6항에서는 통상의 업무활동으로서의 기록을 전문법칙의 예외로 인정하고 있는데, United States v. Cestnik 판결에서 컴퓨터에 저장된 업무기록의 증거능력 인정 여부에 대한 구체적 기준을 제시하고 있다. 즉, "① 업무기록이 정확성을 보장하기 위하여 계획된 일상적인 절차를 따랐고, ② 업무기록이 (소송준비 이외의) 정확성을 보장하려는 동기로 인해 창

63) 노명선, "전자적 증거의 수집과 증거능력에 관한 몇 가지 검토", 2008

64) 권순철, "미국 증거법상 증거능력 체계", 2006

출된 것이고, 그리고 ③ 업무기록이 단지 전문 진술들의 축적에 불과한 것이 아니라면 증거능력이 인정될 수 있다"고 설시하였다. 증거의 허용성에 대하여는 법원의 재량판단에 맡겨져 있지만 컴퓨터에 의하여 출력된 업무활동 기록의 허용성은 대부분 문제가 되지 않는다고 한다[65].

(라) 정책

판사가 해당 자료가 논리적 관련성과 신빙성 원칙을 따르고 있다고 판단하면 그 다음으로는 그 자료가 정책상 증거에서 배제되는 경우에 해당되는지 여부를 검토해야 한다. 예컨대, 변호인과 의뢰인 사이에 법률조언을 하면서 이루어진 대화내용은 의뢰인의 의사에 반하여 증거로 제출될 수 없다. 이를 attorney-client privilege라고 하는데, 이는 수정헌법 제6조 규정 내용과 같은 변호인의 조력을 받을 권리를 보호한다는 정책적인 목적에 따른 것이다.

(마) 증명력

자료가 논리적 관련성, 신빙성, 정책 부합성 등의 검증과정을 거치게 되면, 판사는 연방증거법 제403조 규정에 따라 그 자료의 증명력과 다른 요소를 비교형량하는 절차를 거쳐야 한다. 비교요소는 그 자료가가 증거로 제출될 경우 야기될 수 있는 반대 당사자에 대한 편견, 쟁점의 혼동, 소송지연 가능성 등이다[66].

(2) Code of Federal Regulation, Subchapter B - Records Management(Parts 1220-1238)

- Part 1234 : Electronic Records Management
  - 2006년 2월 21일 최종 개정
- 제1234.1조 : 범위
  - 전자기록물의 생산, 관리, 활용 및 처분과 관련된 기본 요건 규정
- 제1234.2조 : 용어 정의
  - 데이터 파일(Data File) : 엄격하게 규정된 양식 및 형식으로 구성된 숫자, 문자 및 그래픽 관련 정보
  - 텍스트 문서(Text Documents) : 자유로이 규정된 양식과 형식으로 된 서신, 메모 및 보고서 등의 서술식 문서
- 제1234.10조 : 행정기관의 책임
  - 관리프로그램 개발의 책임, 통합적 전자기록 관리 책임, 전자기록관리 목적 및 의무에 관한 지도 책임 등

65) 노명선, 전게 논문

66) 권순철, 전게 논문

- 제1234.20조 : 데이터파일의 생산 및 사용
- 제1234.22조 : 텍스트 문서의 생산 및 사용
- 제1234.24조 : 전자메일기록물의 관리 표준
- 제1234.26조 : 전자기록물의 사법적 이용
  - 기록관리시스템 운영과 이에 대한 통제활동이 철저한 문서화를 통하여 신뢰성이 구축된 경우에는 해당 전자기록물은 연방법원에 증거로 인정되어 소송 절차에 사용될 수 있다(증거에 대한 연방규칙 803(8)). 각 기관은 전자기록물이 법적 증거로 인정될 수 있는 가능성을 확대하기 위하여 다음의 절차를 이행하여야 한다.
    · 전자적으로 생산되고 저장되는 유사한 종류의 기록물을 항상 동일한 과정에 따라 생산하며 표준화된 검색 접근 방법을 보유함을 문서화한다.
    · 보안 절차에 의해 기록물의 불법 추가, 수정 및 삭제가 방지되고 정전 등의 문제에 대한 시스템 보호 장치가 확보되어 있음을 입증한다.
    · 기록물이 전체 생애주기에 걸쳐 저장될 전자매체, 기록물이 각 저장매체에 보관되는 최대 기간, 모든 기록물에 대하여 국가기록관리청이 승인한 처분계획을 확인한다.
    · 위의 모든 사항을 법률 자문, IRM의 정보권한관리 담당 고위직원, 기록물관리 담당 직원과 공조하여 조정한다.
- 제1234.28조 : 전자기록물의 보안
  - 각 기관은 다음의 사항이 포함된 효과적인 기록물보안 프로그램을 실행하고 유지하여야 한다.
    · 인가된 직원만이 전자기록물에 접근할 수 있도록 한다.
    · 정보 손실 위험으로부터 정보를 보호하기 위하여 기록물의 백업 및 복구 기능을 제공한다.
    · 기관 내 적합한 직원에게 민감한 전자기록물이나 기밀 전자기록물의 보호에 대한 교육이 제공되도록 한다.
    · 전자기록물에 대한 불법 수정 또는 삭제의 위험을 최소화한다.
    · 전자기록물 보안이 1987년 컴퓨터보안법(Computer Security Act of 1987)에 따라 마련된 컴퓨터 시스템 보안 계획에 포함되도록 한다.
- 제1234.30조 : 전자기록물 보관매체의 선택 및 보존
- 제1234.32조 : 전자기록물의 보존 및 처분
- 제1234.34조 : 전자기록물의 폐기

나. 영국

(1) Lord Chancellor's Code of Practice on the Management of Records Under Section 46 of the Freedom of Information Act 2000

- 제10조(전자기록물의 관리)
- 제10조의1
  - 전자기록물 관리에 있어서의 주요한 이슈(진본성, 무결성, 신뢰성, 이용가능성)는 일반 기록물 관리와 다르지 않음
  - 그러나, 전자적 환경(electronic environment)에서 이러한 이슈들을 다루는 방법들은 다를 것
- 제10조의2
  - 효과적인 전자기록물 관리에 요구되는 7가지 요건 기술
    · 전자기록물의 성질에 대한 명확한 이해
    · 기록물관리시스템의 일부로서 업무처리과정을 문서화하는데 필요한 기록물 및 메타데이터의 생산
    · 기록물이 논리적으로 분류될 수 있는 폴더의 구조유지
    · 전자기록물의 무결성의 안전한 보존
    · 필요한 기간 동안 전자기록물에 대한 접근 및 그 이용(시스템과 교차하여 기록물이 이동한 경우 포함)
    · 보존절차를 포함한 적합한 처리절차의 적용
    · 다양한 환경에서 참조용 전자기록물을 그에 대응하는 문서기록물에 교차시키는 능력
- 제10조의3
  - 전자기록물관리시스템 구축에 필요한 요건 확립은 1999 공공기록물관리법(Public Record Office statement)의 “Functional Requirements and Testing of Electronic Records Management Systems” 에 기초하도록 권고
- 제10조의4
  - 모든 전자정보와 문서 및 기록에 대한 감시(audit trail)이 이루어져야 한다고 명시
  - 이에 대한 절차는 “Principles of Good Practice for Information Management(PD0010)”을 참조하도록 권고
- 제10조의5
  - 기록관리기관은 전자적으로 저장된 정보로서 특히 증거로 요구될 수 있는 기록물들에 대해 “BSI DISC PD0008 - A Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically (2nd ed.)”를 참조하도록 권고

영국에서의 전자기록물 관리 규정은 법령으로 명시된 것이 아니라 영국 표준(British Standards)과 PRO(Public Records Office) 기준을 따르도록 하고 있다.

(2) A code of practice for legal admissibility and evidential weight of information stored electronically(BSI BIP 0008)

BSI(British Standards Institution) BIP 0008은 전자적으로 저장된 정보의 신뢰성, 무결성 및 가용성을 보장함으로써 조직에서 요구하는 정보의 확실성을 만족하기 위해 제정되었다. 이 표준에서 요구하는 방식으로 관리된 전자 기록은 법률 시스템에서도 유효한 능력을 가질 수 있음을 명시하고 있다. 법적 허용성(Legal Admissibility)의 문제는 기록 관리 원칙의 핵심이라고 할 수 있다. 따라서 기록 관리 기관은 전자기록관리 시스템에서 생산 또는 저장, 관리되고 있는 전자기록들이 처음 수집 된 이래 변경되지 않았음을 증명할 책임이 있다. 기록 관리 기관은 이 표준에서 제시하는 정보 관리의 다섯 가지 원칙을 준수하는지 입증해야 한다.

- Representation of Information (i.e. an information management policy)
- A Duty of Care
- Business Procedures and Processes
- Enabling Technologies
- Audit Trails

(가) Representation of Information

기록관리 정책에 대한 문서가 제작·관리되어야 한다. 이것은 기록관리 기관에서 관리하고 있는 정보의 서로 다른 유형에 따라 아래의 사항들이 지정되고 설명되어야 한다.

- the level of security
- appropriate storage media
- formats and version control
- information management standards, e.g. quality
- retention and destruction policy
- responsibilities and roles for information management functions
- responsibilities for compliance with the code BIP0008

또한, 전자기록관리시스템은 기관의 기록관리 정책에 명시된 요구사항을 유연하게 적용 가능해야 한다.

(나) Duty of Care

Duty of Care 원칙을 준수하기 위해 기관은 다음 사항에 대해 준비되어 있어야 한다.

- 관련 법령 및 규제 인지
- 책임에 대한 연계성(chain of accountability)과 전자기록관리 모든 단계에서의 관련된 행위에 대한 책임 정의
- 기록관리 이론과 실행 사항을 최신으로 유지하는 시스템
- 정보보안 정책에 관한 문서화

Duty of Care 원칙에 따라 시스템은 역할의 분리를 허용할 수 있는 기능이 있어야 한다. 즉, 데이터를 입력하는 주체는 품질 검사를 수행하는 주체와 구분되어야 한다. 이러한 역할의 분리는 EDMS(Electronic Documents Management System) 안에서 논리적 접근 제어에 반영 할 수 있어야 한다.

(다) Business Procedures and Processes

기록관리 기관은 기록관리 시스템 운영 절차에 대한 사항을 문서화하여 관리해야 한다. 이러한 문서는 일반적으로 아래와 같은 사항을 정의한다.

- Document types
- Preparation of documents prior to scanning
- Photocopies
- Batch control
- Scanning processes
- Scanning specific documents
- Image Processing
- Compression Techniques
- How information is indexed
- Quality control
- Procedures for producing authenticated output
- procedures for authenticating copies of documents
- how information is transmitted within the system
- Procedures for document retention and destruction
- System maintenance schedules
- Security and protection, including encryption and the use of digital certificates
- Backup and system recovery procedures
- Use of bureau services
- workflow
- date/time stamping
- version control

이 표준은 기록관리 절차 및 프로세스가 매년 감사되거나, 혹은 법적으로 민감한 아카이브에 대해서는 더 자주 감사될 것을 요구한다.

(라) Enabling Technologies

일반적으로 기록관리 시스템은 수많은 기술들로 구성된다. 이러한 각 기술들은 BIP 0008 표준을 준수해야 한다. 이 표준은 기록관리 시스템에서 사용될 수 있는 기술들에 대해 표준에 따라 어떻게 활용되고 제어되어야 하는지 설명하고 있다. 표준에서 설명하고 있는 기술들은 아래와 같다.

- storage media
- access control mechanisms
- system and data integrity
- image processing
- compression techniques
- compound documents
- data migration
- document deletion

(마) Audit Trails

이 표준은 기록관리 시스템이 전체 감사 기능을 가져야 한다고 요구한다. 기록의 전체 life-cycle 히스토리에 대한 감사 추적(audit trail) 없이는 법적 허용성을 만족시키지 못할 수 있다. 감사 추적은 최소한 문서의 life-cycle에서 발생한 이벤트들에 대해 기록으로 남겨야 한다. 감사 추적은 아래 사항을 만족해야 한다.

- 시스템에 의해 자동적으로 수행되어야 함
- 각 이벤트들에 대한 날짜/시간 정보를 포함해야 함
- 로그 기록은 변경 불가능해야 함
- 기관의 기록관리 정책과 일치해야 함
- 적합한 접근제어 수행
- 각 로그들은 안전하게 저장되어야 하며 백업되어야 함

국내에서는 아직까지 전자기록의 법적 허용성에 대해 구체적으로 명시하고 있는 표준이나 법령이 전무하다. 영국의 BIP 0008에서 기술하고 있는 부분들은 향후 전자기록의 증거능력에 대한 표준 마련 및 제도 개선에 있어 많은 참고가 가능할 것이다.

다. 캐나다

(1) Uniform Electronic Evidence Act

캐나다에서는 컴퓨터 기록이 법정에서 적절하게 사용될 수 있도록 하기 위해 캐나다 통일법률 회의(Uniform Law Conference of Canada)가 제안하여 1997년 통일 전자적 증거법(Uniform Electronic Evidence Act)이 제정되었다. 동법은 총9개의 조문으로 되어 있으며 특히 제6조에서는 전자기록의 진정성과 무결성의 입증방법으로 전자적 기록에 대해 기록 내지 저장방법에 관한 표준을 고려하도록 하고 있다. 나아가 동법의 규정들은 2000년 개인정보보호 및 전자적기록법(Personal Information and Electronic Document Act)의 일환으로 캐나다 증거법(Canada Evidence Act)을 개정할 때에 대부분 반영되었는데 제31.1조 내지 제31.8조에 전자적 기록에 관련한 부분이 규정되었다.

캐나다 표준이사회는 2002년 전자적 기록의 무결성, 진정성, 신뢰성을 부여하기 위한 표준인 'e-Evidence Standard'를 제정하였다. 캐나다 증거법이 이 표준에 의해 법원이 증거를 허용하도록 의무지우는 것은 아니지만 증거허용과 관련한 문제들에 대한 적절한 판단 기준을 제공한다. 이 표준안에서는 '허용될 수 있는 전자적 기록'이라는 주제로 법적 절차에 있어서 전자적 기록을 증거로 허용할 수 있는 요건에 관한 지침을 제공하고 있다. 이 지침은 법적 절차에서 증거로 전자적 기록을 제출하고자 하는 조직이나 사람은 세 가지를 입증해야 하는데 첫째 그 기록이 기록되거나 저장된 전자적 기록 시스템의 무결성, 둘째 그 기록의 진정성, 셋째 전자적 기록을 작성하는 것과 관련한 통상적이고 일반적인 업무 절차이다[67].

67) 정교일, 전게 논문

(표 12. 캐나다 증거법에서 전자적 기록과 관련된 주요 조항 및 내용)

조항	주요 내용
제31.1조(1)	전자적 기록을 증거로 제출하는 사람은 제출된 전자적 증거의 진정성을 입증하는 책임을 져야 함
제31.2조(1)	전자기록에 있어서도 최량증거법칙이 적용되어야 하며 이는 전자적 기록이 기록되거나 저장되어 있는 기록시스템의 무결성 입증을 통해서 입증됨
제31.2조(2)	출력된 인쇄물에 있어서, 반대 측의 증거가 없을 경우 출력 인쇄물의 형태로 된 전자적 기록은 그 출력인쇄물이 출력 인쇄물에 기록되거나 저장된 정보의 기록으로서 명백하고 일관되게 기능을 해왔고, 신뢰할만하며 이용되어 왔을 경우에는 최량증거의 법칙을 충족한 것으로 판단함
제31.3조	반대의 증거가 없는 경우에 전자적 기록이 기록되거나 저장되었거나 만들어진 전자적 기록 시스템의 무결성은 다음과 같은 경우에 입증됨 - 전자적 기록 시스템에 사용된 컴퓨터 시스템이나 다른 유사장치가 모든 물질적 시간대에 적정하게 동작되고 있다고 하는 것 혹은 만약 적정하게 작동되지 않고 있다면 적정하게 작동되지 않는 것이 전자적 기록의 무결성에 영향을 미치지 않으며 전자적 기록 시스템의 무결성을 의심할만한 다른 합리적인 바탕이 없다는 것을 입증할 만한 충분한 증거에 의해서 성립된 경우 - 만약 전자적 증거가 증거를 제출하는 당사자의 이익에 반대되는 당사자에 의해 기록되었거나 저장되었다는 것이 성립된 경우 - 전자적 기록이 당사자가 아닌 사람에 의해 통상적인 업무과정에서 기록되거나 저장된 것이며 증거를 제출한 당사자의 조정 아래에서 기록되거나 저장 되지 않은 경우
제31.4조	정부가 보안서명이 된 전자적 기록에 대한 무결성을 추정할 수 있도록 하는 규정을 제정할 수 있는 제도를 규정

(2) Policy on Electronic Authorization and Authentication 1996

- 전자 공인과 인증(Electronic Authorization and Authentication)에 대한 지침
  - 전자적 업무처리의 무결성이 항상 유지되어야 함
  - 전자서명은 전자적 업무처리를 공인하는데 사용되어야 함
  - 전자서명을 사용하는 시스템에 대한 위험분석이 수행되어야 함
  - 전자인증을 공인한 자를 효과적으로 파악할 수 있어야 함

- 전자적 공인 및 인증의 무결성과 기밀성은 항상 유지 및 관리되어야 함
- 업무의 기밀성은 데이터의 암호화 작업으로 이울어지도록 함
- 각 부서는 전자적 업무처리 시스템이 지닌 잠재적 위협을 평가함으로써 전자공인 및 전자인증의 위험평가를 수행해야 함
- 각 부서는 전자공인 및 인증 작업을 포함한 모든 전자적 업무처리에 적절한 통제와 관리를 수행하기 위해서 이에 대한 원칙과 절차를 수립해야 함

한편, “도서 및 기록관리청법(Library and Archives of Canada)” 제2조 8호에서는 “기록물(record)이라 함은 매체 또는 형태에 관계없이 간행물 이외의 문서자료를 말한다”고 기술함으로써 전자기록과 일반 기록물을 구분하지 않고 있다.

라. 호주

(1) Digital Record keeping Guidelines for Creating, Managing, and Preserving Digital Records

- 호주 정부기관이 디지털 형태의 모든 기록물의 생성, 관리, 보존 업무를 수행하기 위한 지표 및 절차 제시
  - 전자기록의 중요성 : 정의, 관리의 필요성, 국립기록원의 역할, 정부기관의 역할
  - 전자기록관리 기반요소: 법규 및 표준, 정책/절차/지침, 역할/책임, 시스템설계, 교육
  - 전자기록의 생성 : 전자기록의 생성과 식별, 획득, 기록관리시스템
  - 전자기록에 대한 정보생성 : 메타데이터, 메타데이터 획득 및 유지관리
  - 전자기록 보유기간 : 전자기록의 처리/이관, 처리승인 절차
  - 전자기록 저장 : 저장방법, 보존방법, 매체 변환, 손실데이터 회복
  - 전자기록 보안 : 보안절차, 보안방법, 전자 기록 인증
  - 전자기록 연속성 유지를 위한 계획 : 필요성, 연속성 계획, 위험관리, 보존가치 평가
  - 전자기록의 장기보존 : 필요성, 정보기술의 노화, 보존기술, 보존정책
  - 전자기록의 접근허용 : 기록원에서의 접근, 정부기관에서의 접근
  - 전자기록의 처리 : 처리방법, 국립기록원으로의 이관, 기관간의 이관, 폐기, 영구보존
  - 외부 전자기록 관리 : 전자우편문서, 웹 기반 전자기록, 다른 정보시스템내의 기록

마. 한국

(1) 전자문서의 효력

국내 민·형사 소송법에서는 전자문서에 대해 따로 명시하고 있지 않다. 그러나 전자정부법(법률 제10580호) 제26조 제3항에서 전자문서 및 전자화문서는 종이문서와 동일한 효력을 갖는다고 명시하고 있으며, 전자거래기본법(법률 제10629호) 제4조 제1항에서도 전자적 형태로 되어 있다는 이유로 문서로서의 효력이 부인되지 않는다고 나타내고 있다.

또한, 전자서명법(법률 제10465호) 제3조에서 다른 법령에서 문서 또는 서면에 서명, 서명날인 또는 기명날인을 요하는 경우 전자문서에 공인전자서명이 있는 때에는 이를 충족한 것으로 본다고 하여 전자문서에 대한 전자서명의 효력을 인정하였다.

(표 13. 전자문서 관련 법률상 용어정의)

용 어	개념 내용
기록물관리기관	**(공공기록물 관리에 관한 법률 제3조 제4호)** 일정한 시설 및 장비와 이를 운영하기 위한 전문인력을 갖추고 기록물관리 업무를 수행하는 기관을 말하며, 영구기록물관리기관, 기록관 및 특수기록관으로 구분
공인전자서명	**(전자정부법 제2조 제3호)** 다음 각목의 요건을 갖추고 공인인증서에 기초한 전자서명을 말한다. 가. 전자서명생성정보가 가입자에게 유일하게 속할 것 나. 서명 당시 가입자가 전자서명생성정보를 지배·관리하고 있을 것 다. 전자서명이 있은 후에 당해 전자서명에 대한 변경여부를 확인할 수 있을 것 라. 전자서명이 있은 후에 당해 전자문서의 변경여부를 확인할 수 있을 것
전자문서	**(전자정부법 제2조 제7호)** 컴퓨터 등 정보처리능력을 지닌 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 저장되는 표준화된 정보
전자화문서	**(전자정부법 제2조 제8호)** 종이문서와 그 밖에 전자적 형태로 작성되지 아니한 문서를 정보시스템이 처리할 수 있는 형태로 변환한 문서
행정전자서명	**(전자정부법 제2조 제9호)** 행정기관(보조·보좌기관 포함), “행정기관과 전자문서를 유통하거나 행정정보를 공동 이용하는 기관” 또는 그 기관에서 “직접 업무를 담당하는 사람”이 신원과 전자문서의 변경 여부를 확인할 수 있는 정보로서 그 문서에 고유한 것

(표 14. 전자문서의 효력에 대한 법률)

법률	조항 및 내용
전자정부법	**제26조(전자문서 등의 성립 및 효력 등)** ① 행정기관등이 작성하는 전자문서는 그 문서에 대하여 결재(국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 대통령령으로 정하는 전자적인 수단에 의한 결재를 말한다)를 받음으로써 성립한다. ② 행정기관등의 보조기관 또는 보좌기관이 위임전결하거나 대결(代決)한 전자문서는 그 보조기관 또는 보좌기관의 제29조에 따른 행정전자서명으로 발송할 수 있다. ③ 이 법에 따른 전자문서 및 전자화문서는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 종이문서와 동일한 효력을 갖는다.
전자거래기본법	**제4조(전자문서의 효력)** ① 전자문서는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 전자적 형태로 되어 있다는 이유로 문서로서의 효력이 부인되지 아니한다. ② 별표에서 정하고 있는 법률에 따른 기록·보고·보관·비치 또는 작성 등의 행위가 전자문서로 행하여진 경우 해당 법률에 따른 행위가 이루어진 것으로 본다.
전자서명법	**제3조(전자서명의 효력 등)** ① 다른 법령에서 문서 또는 서면에 서명, 서명날인 또는 기명날인을 요하는 경우 전자문서에 공인전자서명이 있는 때에는 이를 충족한 것으로 본다. <개정 2001.12.31.> ② 공인전자서명이 있는 경우에는 당해 전자서명이 서명자의 서명, 서명날인 또는 기명날인이고, 당해 전자문서가 전자서명된 후 그 내용이 변경되지 아니하였다고 추정한다. <개정 2001.12.31.> ③ 공인전자서명외의 전자서명은 당사자간의 약정에 따른 서명, 서명날인 또는 기명날인으로서의 효력을 가진다. <신설 2001.12.31>

(2) 전자문서의 증거능력

민사소송법에서는 원칙적으로 증거능력에 대한 제한이 없고, 서증의 사본도 증거능력이 부인되지 않으므로 전자문서는 증거능력이 있다고 보는 것이 타당하다[68]. 그러나 전자문서가 실질적 증거로 인정받기 위해서는 증명력에 있어 진정성을 갖추어야 한다. 공문서의 경우 민사소송법(법률 제10859호) 제356조에 의해 진정성이 추정되나, 사문서의 경우 동법 제357조 내지 제358조에 의해 문성성립의 진정성을 증명하여야 한다. 한편, 민사소송 등에서의 전자문서 이용 등에 관한 법률(법률 제10183호)에 따라 민사소송에서는 법원에 제출할 서류를 전자문서로도 제출 가능하다.

반면, 형사소송법(법률 제10864호)에서는 피고인의 인권 문제와 오판 방지를 위해 증거의 증거능력에 대해 엄격한 기준(증거의 신뢰성, 위법수집증거배제법칙, 전문법칙)을 적용하고 있다. 형사소송법 제310조의2에서 전문증거의 증거능력 제한에 대해 명시하고 있으며, 동법 제313조 제1항에서는 “피고인 또는 피고인이 아닌 자가 작성한 진술서나 그 진술을 기재한 서류로서 그 작성자 또는 진술자의 자필이거나 그 서명 또는 날인이 있는 것은 공판준비나 공판기일에서의 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에는 증거로 할 수 있다”고 규정하고 있는바, 위 규정을 엄격하게 적용하게 된다면 전자문서의 증거능력을 인정하기 위해서는 작성자의 서명·날인이 반드시 있어야 한다[69]. 앞서 전자서명법(법률 제10465호) 제3조에서는 다른 법령에서 문서 또는 서면에 서명, 서명날인 또는 기명날인을 요하는 경우 전자문서에 공인전자서명이 있는 때에는 이를 충족한 것으로 본다고 명시하고 있기에 공인전자서명이 있는 경우에 한하여 전자문서의 증거능력을 인정받을 수 있다. 한편 형사소송법 제315조는 당연히 증거능력이 있는 서류를 규정하고 있다. 여기에 규정된 서류는 진술서에 해당하나 진술서라 할지라도 특히 신용성이 높고 그 작성자를 증인으로 신문하는 것이 부적당하거나 실익이 없기 때문에 필요성이 인정되는 경우에 증거능력을 인정하도록 하였다[70]. 행정기관에서 작성한 공문서의 경우, 형사소송법 제315조에 의해 증거능력을 인정할 수 있을 것이다.

68) 김현경, “전자문서를 둘러싼 법적쟁점과 과제”, 2011

69) 장상귀, 전게 논문

70) 이재상, “형사소송법”, 2003

(표 15. 전자문서의 증거능력에 관한 법률)

법률	조항 및 내용
민사소송법	**제356조(공문서의 진정의 추정)** ① 문서의 작성방식과 취지에 의하여 공무원이 직무상 작성한 것으로 인정한 때에는 이를 진정한 공문서로 추정한다. ②공문서가 진정한지 의심스러운 때에는 법원은 직권으로 해당 공공기관에 조회할 수 있다. ③외국의 공공기관이 작성한 것으로 인정한 문서에는 제1항 및 제2항의 규정을 준용한다
	제357조(사문서의 진정의 증명) 사문서는 그것이 진정한 것임을 증명하여야 한다.
	제358조(사문서의 진정의 추정) 사문서는 본인 또는 대리인의 서명이나 날인 또는 무인(拇印)이 있는 때에는 진정한 것으로 추정한다.
형사소송법	**제310조의2(전문증거와 증거능력의 제한)** 제311조 내지 제316조에 규정한 것 이외에는 공판준비 또는 공판기일에서의 진술에 대신하여 진술을 기재한 서류나 공판준비 또는 공판기일외에서의 타인의 진술을 내용으로 하는 진술은 이를 증거로 할 수 없다.
	제313조(진술서등) ① 전2조의 규정 이외에 피고인 또는 피고인이 아닌 자가 작성한 진술서나 그 진술을 기재한 서류로서 그 작성자 또는 진술자의 자필이거나 그 서명 또는 날인이 있는 것은 공판준비나 공판기일에서의 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에는 증거로 할 수 있다. 단, 피고인의 진술을 기재한 서류는 공판준비 또는 공판기일에서의 그 작성자의 진술에 의하여 그 성립의진정함이 증명되고 그 진술이 특히 신빙할 수 있는 상태하에서 행하여 진 때에 한하여 피고인의 공판준비 또는 공판기일에서의 진술에 불구하고 증거로 할 수 있다. ②감정의 경과와 결과를 기재한 서류도 전항과 같다.
	제315조(당연히 증거능력이 있는 서류) 다음에 게기한 서류는 증거로 할 수 있다. <개정 2007.5.17> 1. 가족관계기록사항에 관한 증명서, 공정증서등본 기타 공무원 또는 외국공무원의 직무상 증명할 수 있는 사항에 관하여 작성한 문서 2. 상업장부, 항해일지 기타 업무상 필요로 작성한 통상문서 3. 기타 특히 신용할 만한 정황에 의하여 작성된 문서

라. 주요 판례

(1) 영남위 사건(대법 99도2317)

영남위 사건은 디지털 매체에서 북한을 찬양한 문서 파일이 발견됨에 따라 이를 국가 보안법 위반 등의 혐의로 기소한 사건이다. 이 사건에 대한 대법원 판례는 컴퓨터 디스켓의 증거능력에 관한 최초의 판례를 중요한 의미가 있다. 컴퓨터 디스켓에 저장된 증거에 관련하여 판례의 요지는 다음과 같다.

"컴퓨터 디스켓에 들어 있는 문건이 증거로 사용되는 경우 그 컴퓨터 디스켓은 그 기재의 매체가 다를 뿐 실질에 있어서는 피고인 또는 피고인 아닌 자의 진술을 기재한 서류와 크게 다를 바 없고, 압수 후의 보관 및 출력과정에 조작의 가능성이 있으며, 기본적으로 반대신문의 기회가 보장되지 않는 점 등에 비추어 그 기재내용의 진실성에 관하여는 전문법칙이 적용된다고 할 것이고, 따라서 형사소송법 제313조 제1항에 의하여 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여 이를 증거로 사용할 수 있다."

(2) 일심회 사건(대법 2007도7257)

일심회 사건 또한 국가보안법 위반에 관련된 사건으로 디지털 매체에 기록된 내용이 형사소송에서 핵심 증거로 제시된바 전자기록의 증거능력에 관련된 최신 판례로 중요한 의미를 가진다고 할 수 있다. 검찰은 플로피 디스크, USB, 노트북 PC, CD, e-mail 출력물 등을 압수하여 증거로 제시하였다. 디지털 저장매체로부터 출력한 문건의 증거능력에 관한 판결 요지는 다음과 같다.

"압수물인 디지털 저장매체로부터 출력한 문건을 증거로 사용하기 위해서는 디지털 저장매체 원본에 저장된 내용과 출력한 문건의 동일성이 인정되어야 하고, 이를 위해서는 디지털 저장매체 원본이 압수시부터 문건 출력시까지 변경되지 않았음이 담보되어야 한다. 특히 디지털 저장매체 원본을 대신하여 저장매체에 저장된 자료를 '하드카피' 또는 '이미징'한 매체로부터 출력한 문건의 경우에는 디지털 저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이에 자료의 동일성도 인정되어야 할 뿐만 아니라, 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다. 그리고 압수된 디지털 저장매체로부터 출력한 문건을 진술증거로 사용하는 경우, 그 기재 내용의 진실성에 관하여는 전문법칙이 적용되므로 형사소송법 제313조 제1항에 따라 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여 이를 증거로 사용할 수 있다."

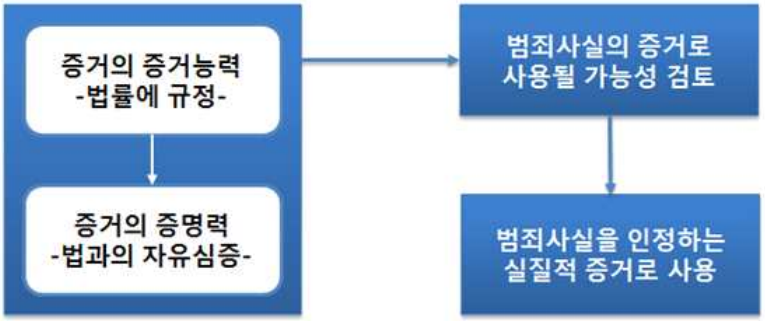
(3) 판례 분석 결론

디지털 증거의 증거능력에 관한 유명한 사건 중 하나인 일심회 사건의 1심 판례(서울중앙법원 2006고합1365)에서는 디지털 포렌식 절차를 통해 수집·분석한 증거에 대해 그 증거능력을 인정받은 바 있다. 그러나 이 사건의 항소심(서울고등법원 2007노929) 및 선고(대법원 2007도7257)에서 보듯이 엄격한 디지털 포렌식 절차를 통해 수집한 증거능력일지라도 전문법칙의 적용에 있어 예외 사유에 해당하지 않는다면 증거능력이 인정되지 않을 수도 있다. 디지털 증거가 전문법칙의 적용을 받느냐의 문제는 복잡한 사안으로 디지털 증거에 적합한 개정안이 필요하다는 의견이 법조인들 사이에서 논의되고 있다. 한편, 기록원 관점에서의 전자기록이 증거능력을 인정받기 위해서는 앞서 살펴본 3가지 요건(증거의 신뢰성, 위법수집배제법칙, 전문법칙)을 충족하는지 살펴보아야 한다. 위법수집배제법칙의 경우 전자기록관리 프로세스 측면에서 고려할 사항은 아니며, 전문법칙의 적용 여부에 있어서는 형사소송법 제315조(전문법칙 예외 사항)의 적용이 가능한지, 형사소송법 제313조 제1항에 의거해 서명·날인의 대체 방안이 존재하는지(전자서명법 제3조 제1항), 원작성자의 증거에 대한 진정성립이 용이한지 등을 판단해야 한다. 증거의 신뢰성 문제는 현재까지 국내에서 전자기록관리 프로세스를 통해 관리된 전자기록이 형사소송에서의 증거로 제출된 판례를 찾지 못하였기 때문에 이에 대한 조사가 더 필요하다.

2. 국내 기록물관리의 법적 효력에 대한 종합 평가

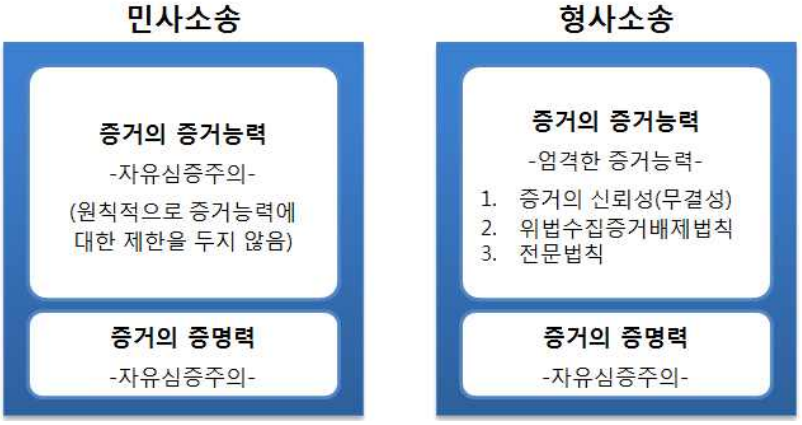
가. 전자기록이 법적 증거능력을 갖추기 위한 요건

증거란 사실인정의 근거가 되는 자료를 말하는데, 이 때 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 미리 법률에 규정되어 있다. 해당 증거가 가치 있는 증거라 할지라도 증거능력이 인정되지 않으면 사실인정을 할 수 없다. 이러한 증거능력의 판단은 증명력 판단 이전의 문제라고 할 수 있다.



(그림 48. 증거가 범죄사실의 인정증거로 사용되는 절차)

민법에서는 증거능력에 대해 원칙적으로 제한을 두지 않고 있지만, 형사소송에서는 증거의 신뢰성, 위법수집배제법칙, 전문법칙 등 엄격한 증거능력 요건을 요구한다.



(그림 49. 민사·형사 소송에서의 증거능력과 증명력)

디지털증거 또한 형사소송에서 증거능력으로 인정받기 위해서는 위에서 언급한 조건을 갖추어야 한다. 하지만 디지털 증거는 위·변조에 취약한 특성으로 인해 증거의 신뢰성 및 무결성 측면에서 의심받기 쉽다. 따라서 디지털 증거가 증거로써 능력을 인정받기 위해서는 엄격한 절차(디지털 포렌식)를 따라야 한다.

나. 기록원에서 관리하는 전자기록의 증거능력에 관한 판단

공공기록물관리에 관한 법률(법률 제11391호)에서는 “공공기관 및 기록물관리기관의 장은 기록물의 생산부터 활용까지의 모든 과정에 걸쳐 진본성(眞本性), 무결성(無缺性), 신뢰성 및 이용가능성이 보장될 수 있도록 관리하여야 한다”고 명시하고 있다. 이에 따라 전자기록물의 진본성, 무결성, 신뢰성을 보장하기 위해서는 먼저 전자기록물을 생산하고 관리하는 시스템의 신뢰성이 요구된다. 현재까지 분석한 기록원 전자기록 관리 표준을 볼 때, 기록을 외부에서 수집하는 경우에 있어 무결성 훼손 가능, 원본 파일 및 문서저장포맷에 있어 해쉬 값과 같은 무결성을 입증할 수 있는 장치 부재, 업무관리시스템-기록관리시스템 연계 시 전자기록물 온라인 전송 규격을 따르는지 여부 등의 문제점을 도출할 수 있었다. 현재는 장기보존포맷으로 변환된 후에 기록의 진본성, 무결성, 신뢰성이 보장되지만, 전자기록의 생성·수집 단계에서부터 진본성, 무결성, 신뢰성을 보장할 필요가 있다. 이러한 문제점이 해결된 경우에 있어서는, 기록원에서 관리하는 전자기록들에 있어 형사소송법 제315조(전문법칙의 예외) 적용이 가능한지 여부를 따져볼 필요가 있다.

다. 국가기록원에서 관리하는 전자기록의 법적 허용성에 관한 법률 자문

(1) A 법학전문대학원 교수님 의견

민사의 경우 증거능력에 관하여 특별하게 문제되는 것이 없기에, 국가기록원에서의 기록물 관리절차 정도라면 그에 따라 작성된 국가기록원 기록물의 증거능력의 인정에는 아무런 문제가 없을 것으로 보임.

그러나 형사절차의 경우 전문법칙, 위법수집증거 배제 등과 같은 복잡한 형사법상의 요구조건들이 있고 이 중 어느 하나만 문제가 되더라도 증거능력이 부정됨.

그래서 그 문서 자체가 증거가 되는 것이 아니라 문서에 적힌 사람의 진술이 증거가 되는 경우라면 그것은 전문증거가 되기에 단순히 국가기록원 기록물의 무오성을 만족하고 있다고 하여서 곧바로 증거능력을 가진다고 하기는 어렵고 다시 전문법칙 등 형사소송법이 요구하는 증거능력 부여를 위한 조건을 따져볼 필요가 있음.

결론적으로 민사의 경우 큰 문제가 되지 않겠지만, 형사의 경우 "경우에 따라" 국가기록원에서의 기록물 관리절차에 의하였다는 것만으로는 증거능력이 부여되지 않고 다시 전문법칙 등 형사소송법이 요구하는 별도의 증거능력 인정을 위한 요건이 추가로 필요할 수 있음.

(2) B 법학전문대학원 교수님 의견

현재 공공기록물 관리에 관한 법률과 그 시행령에 따라서 적법 절차로 보관된 자료에 대해서는 그 정당성, 신뢰성을 인정 할 수 있음.

단, 그 보관된 자료의 최초 수집 시점에서 단순 전자 매체물의 파일 복사와 같은 형태가 아닌 매체 전체의 이미징 형태의 수집이 전제가 되야 함. 따라서 이러한 부분에

대한 포렌식 관점의 시행령 제정이 필요함.

또한 적법 포렌식 절차(최초 이미징 및 이후 진본성, 무결성, 신뢰성, 이용가능성 보장)에 의해 보관되고 있는 국가기록물의 법정 증거물 채택 시 예를 들어 출력물 형태로 그 기록물을 제출하는 경우 보관된 기록물 상태에서 출력하여 제출하는 과정에 대한 적법 포렌식 절차를 통해 제출물의 동일성, 재현성 등이 보장되어야함.

즉, 기록원에 보관된 전자기록매체의 법정 증거 채택을 위한 제출 과정에 포렌식 관점의 절차가 제공되어야 하지만 현재는 이런 부분에 대한 고려가 전혀 없음.

제 6 절 전자기록관리 프로세스에서의 디지털 포렌식 적용 방안 제시

본 연구에서는 앞서 3절에서 도출된 전자기록관리 프로세스에서의 신뢰성 이슈에 대해 디지털 포렌식 관점의 접근을 통한 해결 방안을 제시하고자 한다.

1. 전자기록 수집 및 관리 케이스 별 신뢰성 이슈에 관한 디지털 포렌식 관점의 해결 방안

Case 1. 전자기록관리 시스템을 통해 공공기관으로부터 on-line으로 전자기록을 입수하는 경우

문제점 1. 감사 로그(audit log)에 대한 관리 및 검사 정책 미비

(해결방안)

⇒ 기록의 생성부터 전 life-cycle 에서의 변환, 전송, 복사, 접근 등의 모든 이벤트들을 기록 (chain of custody 보장)

⇒ EDBS, RMS, CAMS 등 전체 시스템에서 주요 보안 이벤트들에 대한 감사 로그(audit log) 관리

(Action Item)

⇒ 전자기록의 생산부터 모든 life-cycle에서 법적 신뢰성 보장할 수 있는 감사 추적(audit trail) 정책 수립

⇒ 감사 추적 정책에 따른 구체적인 전자기록 관리 시스템 개선 방안 도출

⇒ 주요 서버와 경계선 보안 장비들에 대한 모니터링 및 보안 로그 기록

문제점 2. 원본 및 문서보존포맷에 대한 무결성·진본성 증명 불가

(해결방안)

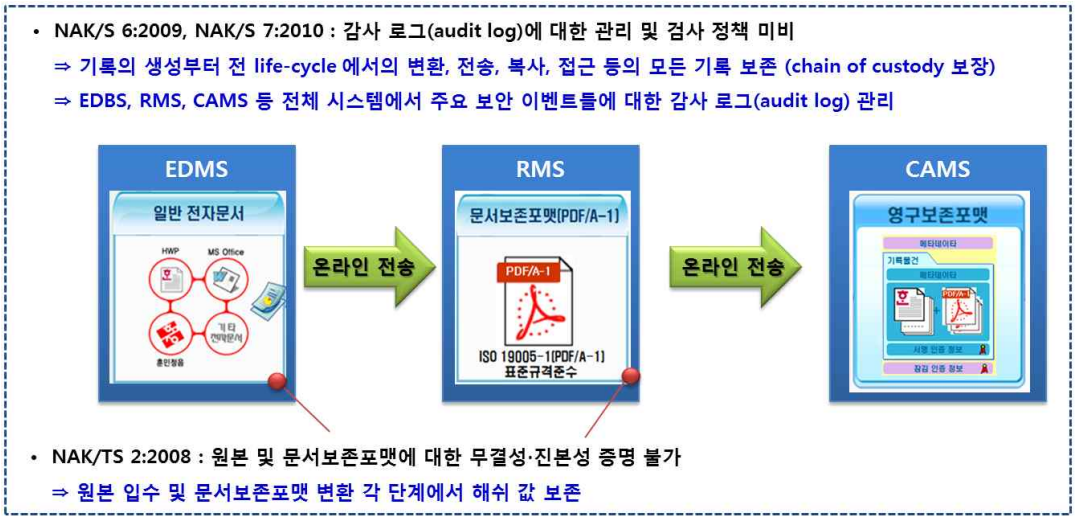
⇒ 원본 입수 및 문서보존포맷 변환 각 단계에서 해쉬 값 보존

(Action Item)

⇒ 원본 입수 단계 및 문서보존포맷 변환 단계, 필요한 경우 장기보존포맷 변환 단계에서 각 문서 포맷에 대한 해쉬 값을 자동으로 계산하여 별도 해쉬 저장소에 보관하고, 기록의 무결성에 대해 검증할 수 있는 시스템 개발

(※ NAK/S 8:2012(v2.0) 기록관리 메타데이터 표준 개정안에 제시된 무결성 체크 항목이 유효한 경우, 이 값을 해쉬 보존소에서 보존·관리)

⇒ 기존 전자기록 관리 시스템과의 호환성 및 기존 시스템 개선을 위한 설계 변경 사항 분석



(그림 50. 전자기록관리 시스템을 통해 on-line으로 전자기록을 입수하는 경우)

Case 2. 폐지 기관 또는 기타 외부 기관으로부터 off-line으로 전자기록을 입수하는 경우

문제점 1. 원본 Bit Steam 훼손 위험 존재, 무결성 증명 불가

(해결방안)

⇒ 매체 이전 시 디지털 포렌식 기술이 적용된 기록 수집 도구 사용

⇒ 디지털 포렌식 절차적 신뢰성이 보장된 수집 프로세스 준수

(Action Item)

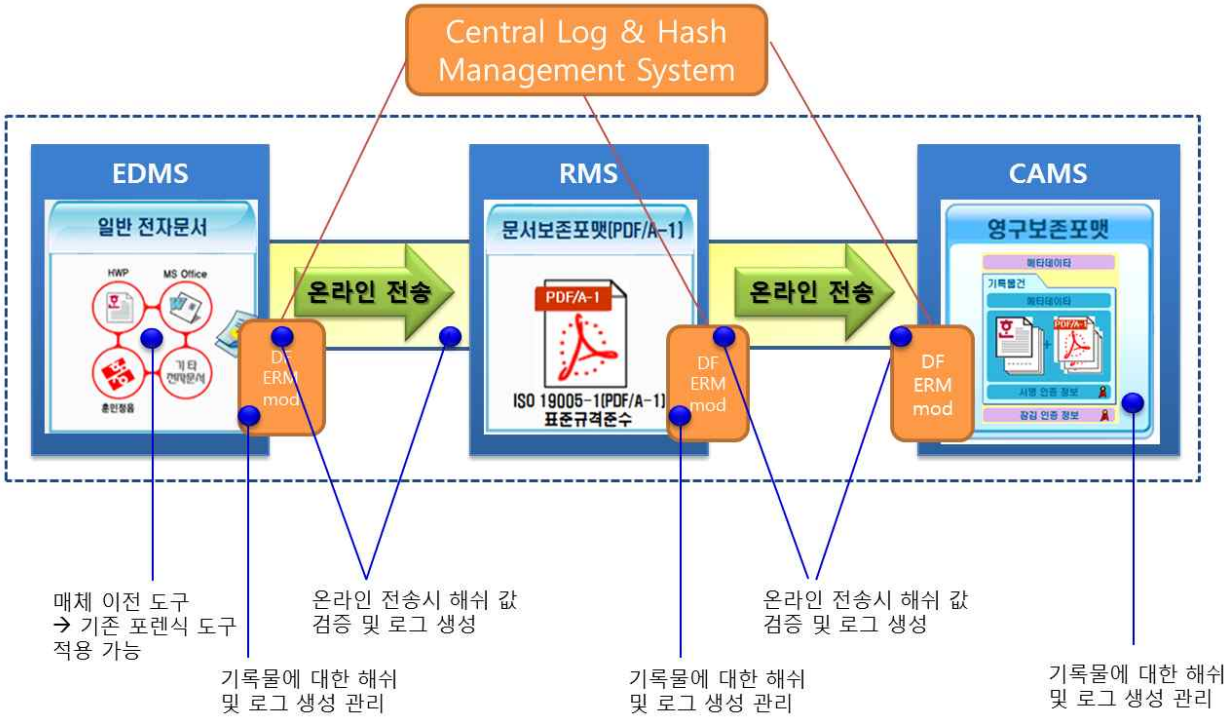
⇒ 디지털 포렌식 비 전문가도 쉽게 사용할 수 있는 국가기록원 전자기록관리 프로세스에 적합한 디지털 포렌식 도구 개발

⇒ off-line 전자기록 수집 시 기록 수집자가 준수해야할 디지털 포렌식 관점의 절차 수립

(그림 51. 외부 기관으로부터 off-line으로 전자기록을 입수하는 경우)

2. 디지털 포렌식 기반 전자기록물 관리 통합 프레임워크

아래 (그림 52)는 본 과제에서 앞서 제안한 디지털 포렌식 기반 전자기록물 관리 방안들을 통합한 프레임워크를 간략히 나타내고 있다.

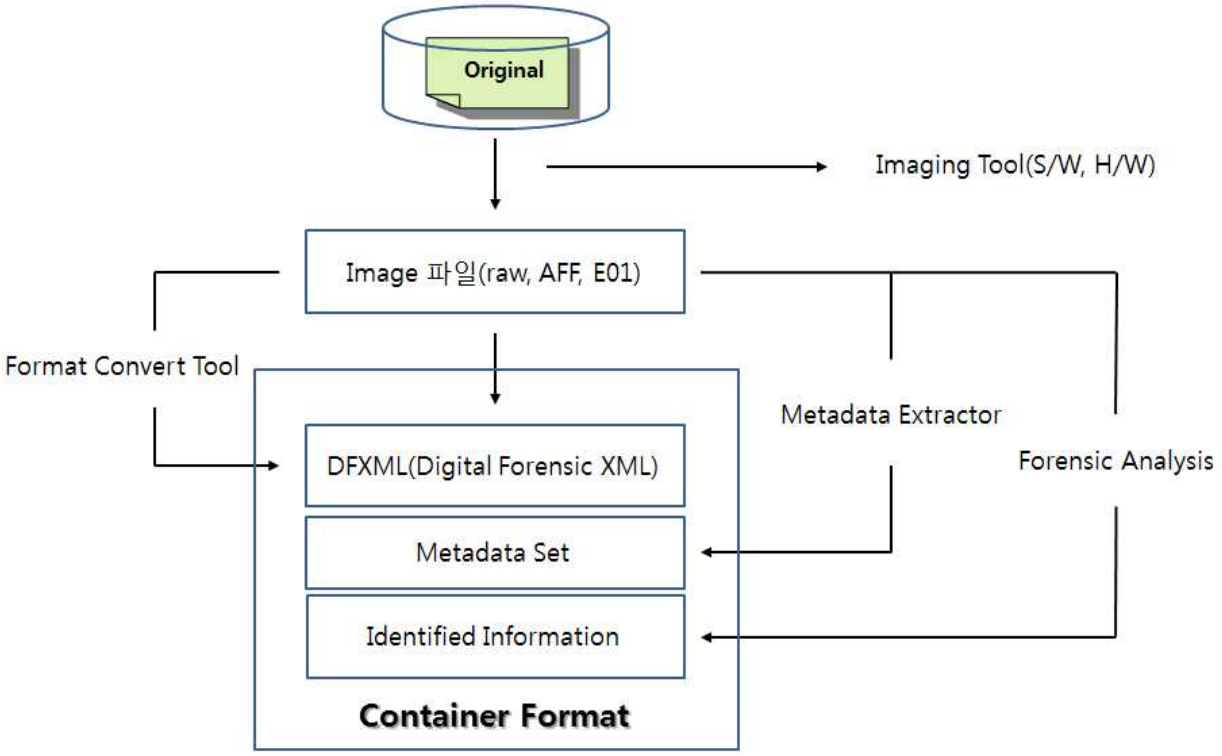


(그림 52. 디지털 포렌식 기반 전자기록물 관리 통합 프레임워크)

3. 매체 이전 시 디지털 포렌식 도구 및 절차 적용 방안 예시

가. (예시1) 외부 기록 수집 시 디지털 포렌식 도구 및 절차 적용

기존의 전자기록관리 프로세스에서의 근본적인 문제점은 기록 수집 및 매체 이전 단계에서의 원본 기록의 무결성 증명 메커니즘의 부재이다. 이를 해결하기 위해 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 Metadata Set과 함께 하나의 컨테이너로 관리한다. 그리고 기존의 문서보존포맷, 장기보존포맷 등과의 호환성을 위해 컨테이너 안의 정보를 XML 형태로 관리함을 요구한다. 아래 그림은 제안하는 기록 파일 포맷에 대한 개략적인 구조를 나타낸다.



(그림 53. 디지털 포렌식 전자 기록 파일 포맷 예)

(1) Imaging

이미징(Imaging)에서는 원본 저장매체로부터 비트 스트림(Bit Stream)을 추출하여 이미지 파일에 대한 무결성을 보장할 수 있는 해쉬값을 포함한 이미지 포맷으로 구성한다. 이미지 포맷으로는 AFF(Advanced Forensics Format)을 제안하며, 그 외 raw 포맷과 E01(Encase) 포맷도 선택적으로 구성할 수 있다. 한 가지 고려할 점은 기존의

이미지 파일 형식은 이미지 파일에 대한 무결성을 보장하는 해쉬값을 추가하지만 이에 대한 전자서명은 포함하고 있지 않다. 형사소송법 상의 전문법칙과 관련하여 만약 전자기록이 진술증거로 사용될 경우, 현재의 형사소송법에서는 서명·날인을 대체할 수 있는 전자서명을 요구할 수 있기 때문에 전자서명을 사용하는 새로운 이미지 포맷에 대해도 고려할 수 있다.

(2) Format Convert

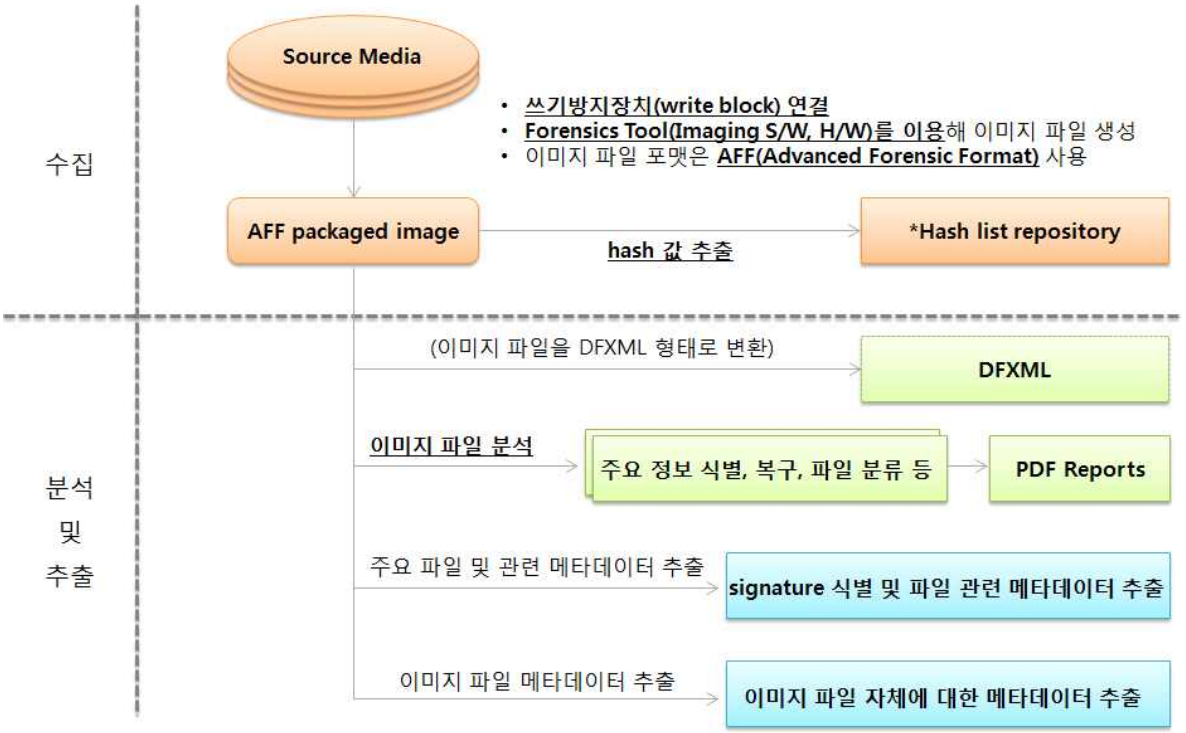
최근 이미지 포맷에 대한 표준 형식으로 DFXML(Digital Forensic XML)에 대한 개발이 진행되고 있다. DFXML은 디지털 포렌식 도구에 대한 의존성을 탈피하기 위해 제안된 것으로 기록관리에서의 파일 포맷 형식과도 호환이 가능할 것으로 사료된다.

(3) Metadata Extract

이미지 파일로부터 파일 시스템 관련 정보, 파일 속성, 사용자 등 중요 메타데이타를 자동으로 추출하여 컨테이너에 넣어주는 것으로 기록 분석관이 이미지 파일을 분석하는데 도움을 줄 수 있다.

(4) Forensic Analysis

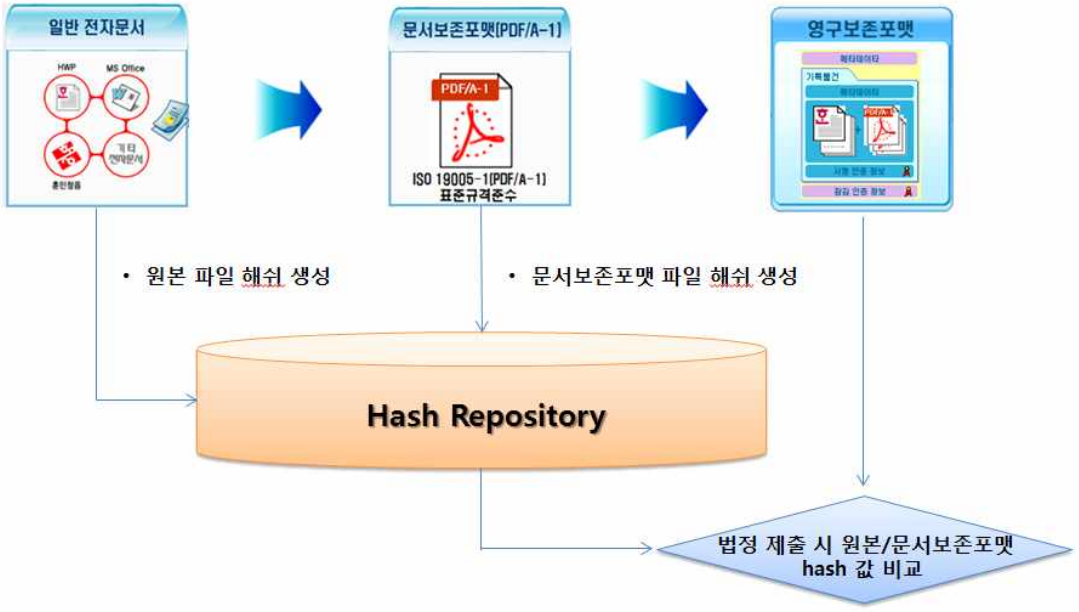
포렌식 분석단계는 이미지 파일로부터 의미 있는 정보를 도출하고자 하는 단계로 기존의 정통 디지털 포렌식 분야에서 사용하는 Encase, FTK 등을 활용할 수도 있지만, 윈도우 환경에서 유닉스, 리눅스 등에서 사용되는 다양한 파일시스템을 view/recovery 할 수 있는 기능 및 인터페이스가 부족하기 때문에 기록관리 분야에서 특화된 기능을 제공할 수 있는 분석도구의 개발이 요구될 수 있다.



(그림 54. 디지털 포렌식 전자 기록 수집 및 분석 예(1) - 포렌식 수집/분석 도구)

나. (예시2) 기록 포맷에 대한 Hash 값 유지/관리

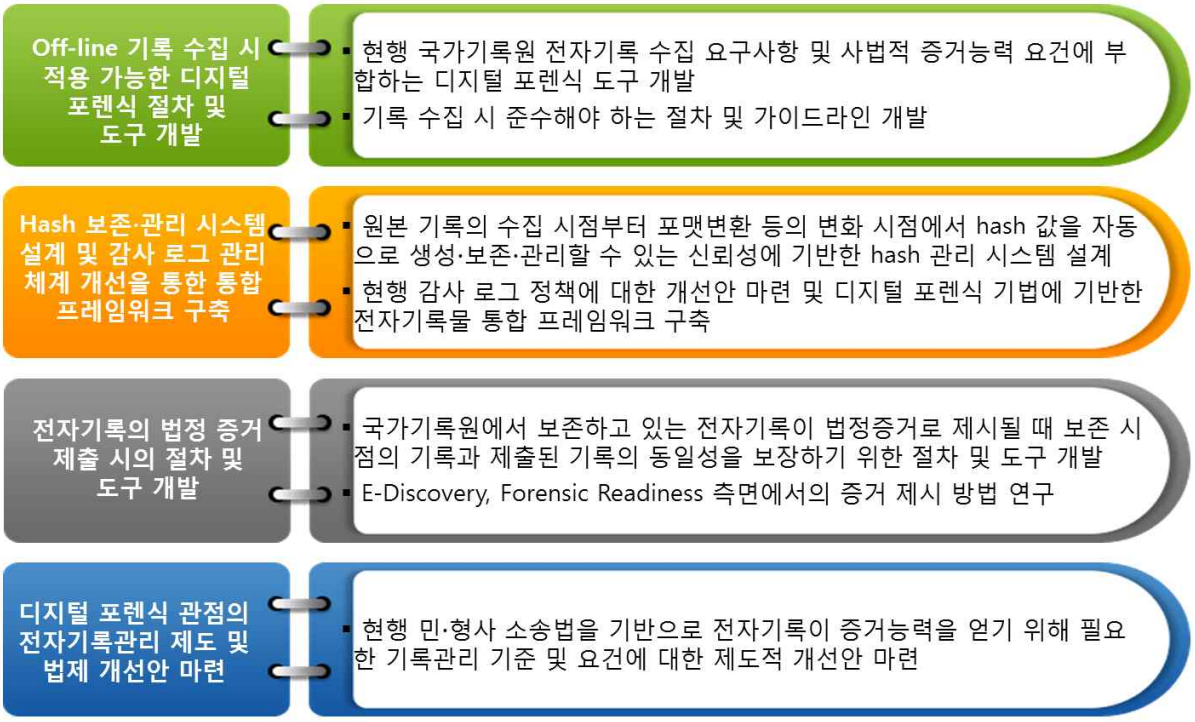
원본 기록이 수집된 시점부터 문서보존포맷 등으로 변환될 때 각각의 포맷에 대한 무결성을 입증할 수 있는 해쉬 값을 별도의 안전한 저장 공간에 보관하고, 추후 법적 증거 능력을 판단할 때 이를 통해 증거의 무결성 및 신뢰성을 증명할 수 있다.



(그림 55. 디지털 포렌식 전자 기록 수집 및 분석 예(2) - 해쉬 보존·비교 방안)

제 7 절 향후 연구 방향 및 로드맵

본 연구에서는 국가기록원 전자기록관리 프로세스에서 디지털 포렌식 기법을 적용하여 전자기록의 신뢰성을 보장하기 위한 기초적인 방법론을 제시하였다. 향후 연구에서는 본 연구 결과를 기반으로 전자기록 수집 절차에서 활용할 수 있는 도구, 절차 개발 및 hash 보존·관리 시스템 설계, 감사 로그 관리 정책 개발, 법정 증거 제출 시의 절차 및 도구 개발, 관련 제도 및 법제 개선안 마련의 방향으로 확장해 나가야 할 것이다. 다음의 (그림 56)은 향후 연구 과제들을 대해 나타내고 있으며, (그림 57)에서는 이러한 연구 과제들에 대한 로드맵을 제시함으로써 앞으로의 방향에 대해 제시한다. Off-line에서의 디지털 포렌식 적용 연구는 기존 전자기록관리 시스템에 어느 정도 투명하게 적용할 수 있는 부분이기 때문에 단기 연구로써 수행이 가능할 것이라 판단된다. 하지만 hash 보존·관리 시스템 및 감사 로그의 개선에 대해서는 기존 시스템에 대한 수정이 불가피 하기 때문에 장기적으로 수행되어야 할 연구 과제이다. 이와 더불어 중기적으로는 전자기록이 법정 증거로 제출될 시의 절차 및 도구 개발 연구와 관련 법제 연구를 통한 전자기록관리 제도 및 법제 개선안을 마련하는 연구가 진행되어야 할 것이다.



(그림 56. 향후 전자기록관리에서의 디지털 포렌식 적용 연구 방향)

(그림 57. 디지털 포렌식 적용 연구 로드맵)

제 3 장 총괄연구개발과제의 최종 연구개발 결과

본 연구과제의 최종 연구개발 결과는 연구 목표에 따라 크게 5가지로 도출되었다.

- 연구 결과 1. 국외 전자기록물 보존 처리에 관한 연구 동향 파악 및 국가기록원에서 접목 가능한 부분과 시사점 도출

(주요 접목 가능 연구 사례 도출)

- 미국, BitCurator (2009~2010)
- 미국/영국, AIMS(An Inter-Institutional Model for Stewardship) (2009~2011)
- 영국, Digital Lives (2009)

(주요 시사점 도출)

- 해외에서는 이미 Stanford, Oxford, King's College London, University of British Columbia 등 주요 대학 도서관을 중심으로 디지털 포렌식 적용과 관련하여 많은 연구가 이루어지고 있으나, 국내에서는 아직까지 관련하여 공개된 연구 사례가 없음.

- 연구 결과 2. 국내외 전자기록 관련 디지털 포렌식 기반 표준 및 특허 조사를 통해 최근 디지털 포렌식 기술 동향 파악 및 시사점 도출

(주요 표준 및 가이드라인 분석)

- (국내) 경찰청 디지털증거 처리 표준 가이드라인 (2006)
- (국내) TTAS.KO-12.0058 컴퓨터 포렌식 가이드라인
- (국내) TTAS.KO-12.0057 컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항
- (미국) NIST Special Publication 800-86, "Guide to Integrating Forensic Techniques into Incident Response",
- (미국) RFC 3227, "Guidelines for Evidence Collection and Archiving"
- (미국) NIST Computer Forensics Tool Testing Program(CFTT)

(특허 조사)

- (국내) 출원 번호 : 10-2009-0122959
- (국내) 출원 번호 : 10-2007-0132715
- (국내) 출원 번호 : 10-2007-0120759
- (미국) 출원 번호 : 12950454
- (미국) 출원 번호 : 12252869

(주요 시사점 도출)

- 국내외 디지털 포렌식 기술 및 특허는 현재 많이 개발되었다. 하지만 전자기록관리를 위한 디지털 포렌식 기술 및 특허는 아직까지 표준 또는 특허로 개발되거나 상용화된 바 없다. 따라서 현재의 디지털 포렌식 기술들을 전자기록관리 프로세스에 적합한 형태로 수정 및 보완할 필요가 있다.

- 연구 결과 3. 전자기록의 증거능력에 관한 국내외 증거법과 기록관리 법령을 분석하여 국가기록원에서 관리하는 전자기록의 사법적 허용성에 관한 결론 도출

(해외 관련 주요 법령 분석)

- 미국, Federal Rules of Evidence
- 미국, Code of Federal Regulation, Subchapter B Records Management
- 영국, A code of practice for legal admissibility and evidential weight of information stored electronically
- 캐나다, Uniform Electronic Evidence Act
- 호주, Digital Recordkeeping Guidelines for Creating, Managing, and Preserving Digital Records

(국내 관련 주요 법령 분석)

- 민사소송법(법률 제10629호)
- 형사소송법(법률 제11002호)
- 공공기록물 관리에 관한 법률(법률 제11391호)
- 전자정부법(법률 제11461호)
- 전자서명법(법률 제10465호)

(법률 자문 주요 결론)

- 형사소송의 경우 현재의 국가기록원에서의 기록물 관리절차에 의하였다는 것만으로는 증거능력이 부여된다고 판단할 수 없음
- 기록원에서 보관된 자료의 최초 수집 시점에서 전자 매체물의 파일 복사와 같은 형태가 아닌 매체 전체의 이미징 형태의 수집이 전제 되어야 하며, 이에 따라 필요한 부분에 대한 포렌식 관점의 시행령 제정이 필요함
- 기록원에 보관된 전자기록매체의 법정 증거 채택을 위한 제출 과정에서 포렌식 관점의 절차가 제공되어야 하지만 현재는 이런 부분에 대한 고려가 없음

- 연구 결과 4. 국내 전자기록의 life-cycle 분석 및 기록물 처리 관련 제도 및 표준 분석을 통해 기록의 무결성 및 신뢰성 관련 이슈사항 도출

(전자기록 관리 주요 표준 분석)

- NAK/TS 1-1:2009 기록관리시스템 데이터연계 기술규격 제1부
- NAK/TS 1-2:2008 기록관리시스템 데이터연계 기술규격 제2부
- NAK/TS 5:2010 전자기록물 온라인 전송을 위한 기술규격
- NAK/TS 2:2008 전자기록물 문서보존포맷 기술규격
- NAK/TS 3:2008 전자기록물 장기보존포맷 기술규격
- NAK/S 8:2012 기록관리 메타데이터 표준

(무결성 및 신뢰성 이슈 사항 도출)

- 감사 로그(audit log)에 대한 관리 및 검사 기준 미비
- 모든 행정기관에서 NAK/TS 5:2010 규격을 준수하는지 여부가 불투명
- 원본 기록에 대한 무결성·진본성 증명을 위한 해쉬 보존 등의 메커니즘 미비
- 매체 이전(migration) 단계에서 원본 기록에 대한 정보 손실 위험 존재

- 연구 결과 5. 디지털 포렌식 기반의 전자기록 수집 및 보존 방안 제안

(제안 방안의 주요 내용)

- 원본 입수 및 문서보존포맷 변환 각 단계에서 해쉬 값 보존
- 매체 이전 시 디지털 포렌식 기술이 적용된 기록 수집 도구 사용
- 디지털 포렌식 절차적 신뢰성이 보장된 수집 프로세스 준수

제 4 장 총괄연구개발과제의 연구결과 고찰 및 결론

근래 국외 기록학 분야에서는 전자기록의 진본성·무결성 유지 및 특징 정보 분석 등을 목적으로 다양한 디지털 포렌식 적용 연구가 활발히 이루어지고 있다. 특히, Stanford, Oxford, King's College London, University of British Columbia, North Carolina, University of Maryland 등의 해외 주요 대학 도서관을 중심으로 진행되었던, 혹은 현재까지 진행되고 있는 일부 연구들은 FRED, FTK 등의 기존 디지털 포렌식 도구를 사용하거나 기존 도구를 수정 또는 직접 제작하여 실제 전자기록 수집 등의 프로세스에 활용하는 것을 목적으로 진행되었다. 해외에서는 이와 같이 기록한 분야에서 디지털 포렌식 도구 및 절차를 활용하고자 하는 연구가 진행되고 있지만, 국내에서는 아직까지 이와 관련하여 알려진 연구 결과가 없는 바 본 연구는 국내 디지털 포렌식 기반의 전자기록관리 연구의 시발점이라 판단된다. 또한, 전자기록의 증거능력에 관한 국내외 증거법과 기록관리 법령 분석을 통해 도출된 국가기록원에서 관리하는 전자기록의 사법적 허용성에 관한 고찰은 향후 국내 기록관리 법령 및 제도 개선안 마련에 있어 활용될 수 있을 것이다. 본 연구에서는 이와 더불어 기존 국가기록원의 전자기록관리 프로세스 분석을 통해 전자기록의 무결성·신뢰성 측면의 이슈들을 도출하였으며, 이에 대한 디지털 포렌식 기반의 해결방안을 제시하였다. 연구에서 제시한 해결방안 중에서 EDMS-RMS-CAMS 전체 시스템에서의 디지털 포렌식 기반 전자기록물 관리 통합 프레임워크를 구축하기 위해서는 기존 시스템의 수정 및 보완이 불가피하며 이는 많은 시간과 노력, 재정적 지원이 필요할 것이다. 한편, off-line 이관에 있어서 매체 이전(migration) 단계에서 발생할 수 있는 신뢰성 문제를 해결하기 위해 제시한 디지털 포렌식 도구 및 절차의 적용은 어느 정도 현재 전자기록관리 시스템 구성에 투명하게 적용할 수 있는 부분이다. 따라서 추후 연구 개발 우선순위에 있어서는 먼저 off-line 이관에서의 포렌식 도구 및 절차 개발을 진행함이 합당하며 이후 감사 로그(audit trail) 및 해쉬 관리 메커니즘을 기존 시스템 추가·보완함으로써 전자기록물 관리 통합 프레임워크를 구축할 수 있을 것이다.

종합적으로 본 연구는 국내 디지털 포렌식 기반의 전자기록물 관리기술 연구의 시초로써 국내외 관련 연구 동향을 조사하고 국가기록원 전자기록관리 프로세스에서의 신뢰성 이슈를 분석하고 이에 대항 대응방안을 제시한 데에 큰 의미가 있으며, 향후 실제 도구 개발 및 현재 시스템을 보완·개선한 통합 프레임워크 구축에 있어서의 기초 연구로 활용될 것을 기대한다.

제 5 장 총괄연구과제의 연구성과

제1절 활용성과

1. 활용성과

총괄과제명	디지털포렌식 기법을 적용한 전자기록물 관리기술 고도화 연구
총괄과제책임자	손태식 / 아주대학교 / 정보보호

가. 연구논문

번호	논문제목	저자명	저널명	집(권)	페이지	Impact factor	국내/국외	SCI여부
1	디지털포렌식 기법을 적용한 전자기록물 관리기술 고도화 연구 (제출예정)	유형욱	정보보호학회 논문지					
2								

나. 학술발표

번호	발표제목	발표형태	발표자	학회명	연월일	발표지	국내/국제
1	기록보관소 전자기록물의 증거능력 확립을 위한 디지털 포렌식 적용 연구	포스트	유형욱	2012 정보처리학회 추계학술대회	2012.11.21	학술대회 논문집	국내
2	Digital Forensics Approach in Electronic Record Management	구두	Sekie Amanuel Majore	2012 IT 서비스 학회 추계학술대회	212.11.07	학술대회 논문집	국내

다. 지적재산권

번호	출원/등록	특허명	출원(등록)인	출원(등록)국	출원(등록)번호	IPC분류
1						
2						

라. 정책활용

본 연구에서 국내 증거법 및 기록관리 법령 분석을 통해 도출된 결론은 향후 전자기록의 증거능력에 있어서의 제도적 개선안을 마련하는데 큰 보탬이 될 것이다. 또한, 국가기록원에서 디지털 포렌식 기반의 전자기록관리 정책 및 표준안을 개발하는데 있이 기초 자료로 활용될 것을 기대한다.

마. 타연구/차기연구에 활용

향후 off-line 전자기록 수집에 있어서 적용 가능한 실제 디지털 포렌식 도구 개발 및 절차 마련 연구가 필요할 것이며, 최종적으로 디지털 포렌식 기반 전자기록관리 통합 프레임워크를 구축하기 위해 기존 전자기록관리 시스템을 개선·보완하는 작업이 수반될 것이다. 이러한 차기 연구 개발 과제에 있어서 본 연구가 활용될 수 있을 것을 기대한다.

바. 언론홍보 및 대국민교육

※ 언론홍보 및 대국민교육 내용, 일자 등을 간략히 기술함.

사. 기타

※ 임상시험 , 관련 DB구축, 워크샵 또는 심포지움 개최 등의 경우 구체적으로 기술함.

2. 활용계획

가. 법·제도 개선안 마련

- 민·형사 소송법 상에서 전자기록의 증거능력에 관한 구체적 기준을 제시할 수 있는 개정안 마련에 활용
- 증거법 상에서 제시한 기준 및 절차를 충족시키기 위한 기록관리 법령 개정에 활용

나. 디지털 포렌식 기반의 도구 및 절차, 통합 프레임워크 개발

- 전자기록의 off-line 이관 시 디지털 포렌식 기반의 절차 및 도구 개발에 활용
- 디지털 포렌식 기반 전자기록관리 통합 프레임 워크 개발에 활용

제 6 장 참고문헌

[1] Luciana Duranti, “Digital Records Forensics: A New Science and Academic Program for Forensic Readiness”, JDFSL Volume 5. No.2, 2010

[2] Luciana Duranti, “From Digital Diplomatics to Digital Records Forensics”, Archivaria, 2010

[3] Kam Woods, Christopher A.Lee, Simson Garfinekel, “Extending Digital Repository Architectures to Support Disk Image Preservation and Access”, JCDL, 2011.06

[4] “AIMS Born-Digital Collections: An Inter-Institutional Model for Stewardship”, 2012, 01

[5] Matthew G.Kirschenbaum, Richard Ovenden, Gabriela Redwine, “Digital Forensics and Born-Digital Content in Cultural Heritage Collections”, 2010

[6] Christopher A.Lee, Matthew G.Kirschenbaum, Alexandra Chassanoff, Porter Olsen, Kam Woods, “BitCurator: Tools and Techniques for Digital Forensics in Collecting Institutions”, D-Lib Magazine Volume 18, 2012.05

[7] Christopher A.Lee, Helen Tibbo, “Where’s the Archivist in Digital Curation? Exploring the Possibilities through a Matrix of Knowledge and Skills”, Archivaria, 2011

[8] Jeremy Leighton John, Ian Rowlands, Peter Williams, Katrina Dean, “Digital Lives”, British Library, 2010

[9] Jeremy Leighton John, “Adapting Existing Technologies for Digitally Archiving Personal Lives Digital Forensics, Ancestral Computing, and Evolutionary Perspectives and Tools”, iPRES 2008, 2008.09

[10] “RFC 3227 Guidelines for Evidence Collection and Archiving”, IETF, 2002

[11] “NIST Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response”, NIST, 2006

[12] “DoD 5015.02-STD ELECTRONIC RECORDS MANAGEMENT SOFTWARE APPLICATIONS DESIGN CRITERIA STANDARD”, Department of Defense, 2007

[13] “ELECTRONIC RECORDS ARCHIVES REQUIREMENTS DOCUMENT (v4.0)”, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, 2010

[14] “Modular Requirements for Records Systems 2010(v1.1)”, DLM Forum, 2010

[15] “Canadian Digital Information Strategy”, Library and Archives Canada, 2007

[16] “Management of Electronic Records PROS 99/007(Version 2)”, Public Record Office Victoria, 2003
[17] “NAK/S 6:2009(v1.1) 기록관리시스템 기능요건”, 국가기록원, 2009
[18] “NAK/S 7:2010(v1.1) 영구기록관리시스템 기능요건”, 국가기록원, 2010
[19] “NAK/TS 5:2010(v1.0) 전자기록물 온라인 전송을 위한 기술규격”, 국가기록원, 2010
[20] “NAK/S 8:2012(v2.0) 기록관리 메타데이터 표준”, 국가기록원, 2012
[21] “NAK/S 10:2012(v1.1) 기록관 표준운영절차 일반”, 국가기록원, 2012
[22] “NAK/S 9:2008(v1.0) 영구기록물관리기관 표준운영절차”, 국가기록원, 2008
[23] “NAK/TS 1-2:2008(v1.00) 기록관리시스템과 영구기록관리시스템간 데이터 연계 규격, 국가기록원, 2008
[24] “NAK/TS 1-3:2009(v1.0) 기록관리시스템 데이터연계 기술규격-제3부:기능분류시스템과의 연계”, 2009
[25] “NAK/TS 2:2008(v1.0) 전자기록물 문서보존포맷 기술규격”, 2008
[26] “NAK/TS 3:2008(v1.0) 전자기록물 장기보존포맷 기술규격”, 2008
[27] 조이형, 김영주, “미국 전자기록관리체계 구축 동향 및 시사점”, 한국기록관리학회지, 제11권 제2호, 2011
[28] “디지털 증거처리 표준 가이드라인”, 경찰청, 2006.12
[29] “TTAS.KO-12.0057 컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항”, 한국정보통신기술협회, 2007
[30] “TTAS.KO-12.0058 컴퓨터 포렌식 가이드라인”, 한국정보통신기술협회, 2007
[31] 길연희, 홍도원, “디지털 포렌식 기술과 표준화 동향”, TTA Journal No.118, 2008
[32] 조상수, 신용태, “디지털 증거의 무결성 보장 절차에 대한 개선”, 정보과학회논문지: 정보통신 제39권 제2호, 2012
[33] 탁희성, 이상진, “디지털 증거분석도구에 의한 증거수집절차 및 증거능력확보방안”, 한국형사정책연구원 연구총서 06-21, 2006
[34] 백승조, 임종인, “개인정보보호 강화를 위한 포렌식 준비도 모델 및 도입방안 연구”, Internet and Information Security 제3권 제2호, 2012
[35] 서혜란, 서은경, 이소연, 오경주, 정원식, “신뢰성 있는 전자기록관리를 위한 법적 기반에 관한 연구”, 한국문헌정보학회지 제38권 제4호, 2004
[36] 이광열, 최윤성, 최해랑, 김승주, 원동호, “현행 증거법에 적합한 디지털 포렌식 절차”, 정보보호학회지 제18권 제3호, 2008.06
[37] 탁희성, “전자증거개시제도(E-Discovery)에 관한 연구”, 형사정책연구원 연구총서 11-13, 2011
[38] 노명선, “전자적 증거의 수집과 증거능력에 관한 몇 가지 검토”, 형사법의 신동향

통권 제16호, 2008.10
[39] 양근원, “디지털 포렌식과 법적 문제 고찰”, 형사정책연구 제17권 제2호, 2006
[40] 전명길, “디지털증거의 수집과 증거능력”, 법학연구 제41집, 2011
[41] 임경수, 이상진, “디지털 포렌식 관점의 디지털 증거를 국내법에 일반적으로 수용하기 위한 연구”, 정보기술융합연구 제1권 제1호, 2009.06
[42] 박혁수, “개정 형사소송법 상 디지털 증거의 증거능력”, 해외연수검사 연구 논문, 2009.07
[43] 강동욱, “디지털증거의 수집에 관한 형사소송법 개정안에 대한 검토”, 법학연구 제18권 제3호, 2010.12
[44] 이소연, “국내 전자기록 연구의 동향 분석”, 한국기록관리학회지 제11권 제2호, 2011
[45] 이소연, “전자기록의 관리와 보존을 위한 국제협력 아젠다 개발”, 국가기록원, 2007
[46] 김명옥, 리상용, “전자기록물의 장기보존을 위한 기능요소 연구”, 한국기록학회지 제10권 제2호, 2010

제 7 장 첨부서류

****

****

****

****

****

****

****

****

****

****

****

****

****

****

****

총괄 연구과제 요약

과제 고유번호	자동부여		공개가능여부	
사업명	2012년 기록보존기술 연구개발 사업			
과제명	디지털포렌식 기법을 적용한 전자기록물 관리기술 고도화 연구			
연구책임자	성 명	손 태 식		
	소속 기관명	아주대학교		
	전자우편	*********	전화번호	XXXXXXXXXXXX

○ 연구목표 (400 ~600자)

본 연구는 국가기록원에서 수집·보존·관리하고 있는 전자기록물에 대해 법적 증거능력을 가질 수 있는지 여부를 고찰하고, 디지털 포렌식 기법의 적용 가능성과 접목 지점 도출을 주요 목표로 수행되었다. 이를 위해 아래와 같이 크게 5가지 목표와 각각에 대한 세부 목표를 수립하고 연구를 수행하였다.

1. 국외 전자기록물 보존 처리에 관한 연구 동향 파악

1-1. 전반적인 국외 전자기록물 관리 동향 조사

1-2. 국외 전자기록물 관리에 디지털 포렌식 적용 사례 조사

2. 국내 전자기록물의 라이프사이클 분석 및 기록물 처리 관련 제도 분석

2-1. 국가기록원의 전반적인 전자기록관리 단계별 프로세스 분석

2-2. 전자기록관리 표준 및 기술 문서 분석

2-3. 전자기록관리 프로세스에서의 증거능력 관련 이슈 파악

3. 국내외 디지털 포렌식 표준 및 특허, 기술 분석

3-1. 국내 디지털 포렌식 표준 및 특허 분석

3-2. 국외 디지털 포렌식 표준 및 특허 분석

3-3. 국내외 디지털 포렌식 도구 및 기술 비교

4. 전자기록의 사법적 증거력 및 공·사 영역에서의 효력 조사

4-1. 국내외 전자기록의 증거능력에 관한 법령 및 판례 분석

4-2. 국내 포렌식 및 기록물관리의 법적 효력에 대한 종합 분석

5. 디지털 포렌식 기반의 전자기록 수집 및 보존 방안 제시

○ 연구내용 (1000~1200자)

본 연구의 5가지 큰 목표와 각각의 세부목표를 달성하기 위해 수행한 연구내용은 다음과 같다.

1. 국외 전자기록물 보존 처리에 관한 연구 동향 파악

1-1. 전반적인 국외 전자기록물 관리 동향 조사

⇒ 미국 NARA(National Archives and Records Administration), 영국 NA(National Archives) 등 해외 주요 국가기록원에서의 디지털 포렌식 관점의 전자기록관리 동향 파악

⇒ DoD 5015.02-STD(미국), ERA Requirement Document(미국), VERS@DOI(호주), Moreq(유럽) 등의 국외 전자기록관리 표준 및 기술 문서에서 기록의 무결성 및 신뢰성 관련 내용 조사

1-2. 국외 전자기록물 관리에 디지털 포렌식 적용 사례 조사

⇒ Stanford University, Oxford University, King's College London 등 해외 주요 대학 도서관을 중심으로 디지털 포렌식 적용 사례 조사

⇒ Digital Lives(영국), Digital Records Forensic Project(캐나다), AIMS(미국/영국), BitCurator (미국), Digital Forensics and Born-Digital Content in Cultural Heritage Collections(미국) 등 전자기록관리에 디지털 포렌식을 접목한 주요 프로젝트 분석 및 시사점 도출

2. 국내 전자기록물의 라이프사이클 분석 및 기록물 처리 관련 제도 분석

2-1. 국가기록원의 전반적인 전자기록관리 단계별 프로세스 분석

⇒ EDMS-RMS-CAMS를 거치는 전자기록의 life-cycle에 대한 전반적인 분석

2-2. 전자기록관리 표준 및 기술 문서 분석을 통한 전자기록의 증거능력 관련 이슈 파악

⇒ 국가기록원의 전자기록관리 주요 표준 문서 분석을 통해 전자기록의 신뢰성·무결성 측면에서의 기술적 미비점 도출

3. 국내외 디지털 포렌식 표준 및 특허, 기술 분석

3-1. 국내 디지털 포렌식 표준 및 특허 분석

⇒ 경찰청 디지털증거 처리 표준 가이드라인과 TTA 표준(TTAS.KO-12.0057, TTAS.KO-12.0058) 분석 및 관련 국내 특허 조사

3-2. 국외 디지털 포렌식 표준 및 특허 분석

⇒ NIST Special Publication 800-86, RFC 3227, NIST CFTT 분석 및 관련 국외 특허 조사

4. 전자기록의 사법적 증거력 및 공·사 영역에서의 효력 조사

4-1. 국내외 전자기록의 증거능력에 관한 법령 및 판례 분석

⇒ 국내외 전자문서 효력·관리 및 사법적 증거력에 관한 법령 분석

⇒ 전자기록의 증거능력과 관련한 주요 판례 분석(대법 2007도7257, 대법 99도2317)

4-2. 국내 포렌식 및 기록물관리의 법적 효력에 대한 종합 분석

⇒ 법령 분석 내용 및 법률 자문을 통해 기록원에서 관리하는 전자기록의 증거능력에 관한 종합 고찰

5. 디지털 포렌식 기반의 전자기록 수집 및 보존 방안 제시

⇒ 전자기록 수집 및 관리 케이스 별 신뢰성 이슈에 관한 디지털 포렌식 관점의 해결방안 제시

⇒ 디지털 포렌식 기반 전자기록물 관리 전체 프레임워크 제시

⇒ 디지털 포렌식 기반 도구 및 시스템 설계 예제 제시

○ 연구성과(응용분야 및 활용범위포함) (400 ~600자)

● 주요 연구 성과

1. 국외 전자기록물 보존 처리에 관한 연구 동향 파악 및 국가기록원에서 접목 가능한 부분과 시사점 도출
2. 국내외 전자기록 관련 디지털 포렌식 기반 표준 및 특허 조사를 통해 최근 디지털 포렌식 기술 동향 파악 및 시사점 도출
3. 전자기록의 증거능력에 관한 국내외 증거법과 기록관리 법령을 분석하여 국가기록원에서 관리하는
4. 전자기록의 사법적 허용성에 관한 결론 도출
5. 국내 전자기록의 life-cycle 분석 및 기록물 처리 관련 제도 및 표준 분석을 통해 기록의 무결성 및 신뢰성 관련 이슈사항 도출
6. 디지털 포렌식 기반의 전자기록 수집 및 보존 방안 제안

● 연구결과의 활용방안

본 연구는 국가 전자기록물 관리에 디지털 포렌식 기술의 적용 방안을 제시함으로서 전자기록물 관리 기술의 고도화 추구 및 기록관리 연구를 선도한다. 또한, 국가 전자기록물의 생산이전, 생산, 준현용, 비현용의 4단계 라이프 싸이클의 각 주요 관리단계에서 디지털 포렌식 기법을 적용하여 신뢰성을 보장하는 첨단 전자기록관리시스템 구축에 활용한다. 특히, 전자기록물 이전(migration)단계에서 디지털 포렌식 도구 및 절차의 적용은 전자기록물의 무결성 및 진본성을 보장하는데 크게 이바지 할 것이다.

○ 총괄 참여연구원

성 명		소속/직위		성 명		소속/직위	
손태식		*********		한규석		*********	
고종빈		*********		유형욱		*********	
이석준		*********		이석철		*********	
조재익		*********		정만현		*********	
양대엽		*********					

Keywords (5개 내외)	***한글***	전자기록관리, 전자기록, 디지털 포렌식, 증거능력, 국가기록원
	영문	Electronic Record Management, Electronic Records, Digital Forensics, Digital Evidence, National Archive

주1) 연구목표, 연구내용, 연구성과를 서술형으로 기재

2) 국가연구개발사업 DB를 통한 공개를 희망하지 않는 경우 공개가능여부란에 “공개불가"로 표시

3) 연구성과는 그간의 연구결과 및 기대성과를 서술