*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.24, NO.3, Jun. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.3.571

# 디지털 포렌식 기반의 전자기록물 이관 절차 및 도구 개발에 관한 연구*

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

# Research on Development of Digital Forensics based Digital Records Migration Procedure and Tool*

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

## 요 약

디지털 형태로 생성되고 저장 및 관리되어지는 전자기록물은 디지털 데이터의 특성에 의해 데이터의 변조와 같은 보안 위협을 수반하고 있다. 따라서 전자기록물을 취급함에 있어 무결성과 진본성의 검증을 통한 신뢰성 보장은 필수적이다. 본 논문에서는 기존 디지털 포렌식 절차의 분석을 바탕으로 디지털 포렌식 기반의 전자기록물 이관 절차를 제안하고, 기존 전자기록물 관리 도구의 분석을 통해 디지털 포렌식 기반의 전자기록물 이관 도구를 개발하기위한 요구사항을 도출했다. 이를 기반으로 전자기록물의 이관 과정에서 전자기록물의 무결성과 진본성을 보장하기 위한 디지털 포렌식 기반의 전자기록물 이관 도구를 개발했다.

## ABSTRACT

Digital Records, which are created, stored, and managed in digital form, contains security vulnerability such as data modification, due to the characteristic of digital data. Therefore it is necessary to guarantee the reliability by verification of integrity and authenticity when managing digital records. This paper propose digital forensics based migration process for electronic records by analyzing legacy digital forensics process, and derives the requirements to develop digital forensics based electronic records migration tool through analyzing trends of abroad digital records migration technique and tool. Based on these develop digital forensic based digital records migration tool to guarantee integrity and authenticity of digital records.

**Keywords:** Digital Forensics, Digital Records, Electronic Records, Migration, Transfer

## I. 서 론

정보처리 및 컴퓨팅 분야의 기술적인 발전과 더불어 현대사회의 많은 기관들에서 산출되는 기록물은 디지털 형태로 생성, 저장 및 관리되고 있다. 이렇게 디지털 형태로 관리되는 기록물을 전자기록물이라고 하며, 전자기록물은 디지털 데이터의 특성상 저장장비의

접수일(2014년 3월 31일), 수정일(2014년 5월 14일), 게재확정일(2014년 6월 2일)
* 본 연구는 안전행전부 국가기로구언 재원으로 2013년 기록보존기술 연구개발사업의 지원을 받아 수행된 연구임
† 주저자, go467913@ajou.ac.kr
‡ 교신저자, tsshon@ajou.ac.kr(Corresponding author)

물리적 변질, 전자기록 체계의 논리적 변질 등에 의해 그 내용의 무결성 및 진본성이 파괴될 수 있는 취약성을 내재하고 있다. 더욱이 기관 차원의 전자기록물 이관 과정에서 전자기록물이 변질될 수 있는 가능성이 보다 높기 때문에, 해당 이관 과정에 있어 이관된 전자기록물의 무결성(Integrity)과 진본성(Authenticity)을 보장할 수 있는 기술에 대한 연구가 필요하다. 현재 국내외의 많은 기관에서 내부에 보관하고 있는 전자기록물의 파일 포맷 확인 및 메타데이터 정보를 포함한 내용을 장기간 보존하기 위한 연구를 활발히 수행하고 있지만, 전자기록물의 이관 기술에 대한 연구는 비교적 진행이 미비한 실정이다.

따라서 본 논문에서는 전자 증거물의 무결성과 신뢰성을 보장하기 위해 사용되는 디지털 포렌식(Digital Forensics)에 입각한 절차 및 기법을 전자기록물을 이관하는 과정에 접목, 이관된 전자기록물의 무결성 및 진본성을 검증할 수 있는 도구의 개발에 관한 연구를 수행했다. 본 논문의 2장에서는 국외에서 연구되고 있는 전자기록물 이관에 관한 연구사례를 살펴본다. 3장에서는 국내외에서의 디지털 포렌식을 수행하는 절차에 대해 분석하고, 이를 바탕으로 디지털 포렌식 기반의 전자기록물 수집 절차의 요구사항을 분석한다. 4장에서는 3장에서 도출된 요구사항을 만족하는 디지털 포렌식 기반의 전자기록물 이관 절차를 제안한다. 5장에서는 국외 전자기록물 수집 도구의 분석을 바탕으로 디지털 포렌식 기반의 전자기록물 이관 도구의 요구사항에 대해 분석한다. 6장에서는 제안된 절차와 요구사항을 만족하는 디지털 포렌식 기반의 전자기록물 이관 도구 개발을 위한 고려사항을 분석하고, 7장에서는 디지털 포렌식 기반의 전자기록물 이관 도구 개발 결과를 분석한다. 마지막 8장에서는 본 논문에 대한 결론과 향후 연구 방향에 대해 논의하고 논문을 마무리한다.

## II. 국외 전자기록물 이관 기술 연구 동향

전자기록물 이관 기술에 대한 연구는 미국과 호주에서 주도하고 있다. 미국의 경우 국립문서기록 관리청(NARA; National Archives and Records Administration) 및 각 연방정부에서 전자기록물을 이관하기 위한 방법에 대한 연구를 진행중이며, 호주 역시 퀸스랜드 기록원, 뉴사우스웨일즈 주정부 등에서 전자기록물 이관에 대한 가이드라인을 제시하고 있다. 하지만 전자기록물의 신뢰성을 보장할 수 있는 기능이 결여되어 있거나 절차의 제시 단계에 머물러 있다.

### 2.1 미국 국립문서기록 관리청

미국의 국립문서기록 관리청은 전자기록물을 보다 효율적으로 관리하기 위해 전자기록물 아카이브(ERA; Electronic Record Achives)를 운용하고 있다. ERA는 인증된 기록저장 기관 간의 네트워크 연결을 통해 온라인 환경에서 전자기록물과 그 메타데이터를 전송하는 기능을 제공하고 있다.[1]

### 2.2 미국 유타 정부

미국 유타 주 정부에서는 2012년 전자기록물 관리 및 이관에 대한 가이드라인을 발표하여 공공기록물의 안전성을 보증하며 관리하기 위한 지침을 세웠다. 이를 위해 전자기록물을 관리하는 과정에서의 접근성(Accessibility), 진본성(Authenticity), 신뢰성(Reliability), 그리고 안전성(Secure) 네 가지 범주에 대한 고려사항을 기술하고 있다.[2]

### 2.3 호주 뉴사우스웨일즈 정부

호주 뉴사우스웨일즈 주정부에서는 정부 기록물 관리 메뉴얼을 수립하여 기록물을 관리하는 지침으로 삼고 있다. 그 중 Guideline 22 "Effectively manage the migration of your digital records"를 통해 문서파일, 전자메일, 데이터베이스 등 전자기록물의 종류 별로 이관함에 있어 포함되어야 하는 요소(Structure, Content, Context 등) 및 주의사항에 대해 기술했다.[3]

## III. 국내외 디지털 포렌식 수행 절차 분석

본 장에서는 전자기록물의 무결성과 진본성을 보장할 수 있는 디지털 포렌식 기반의 전자기록물 이관 절차를 수립하기 위해 국내외의 디지털 포렌식 수행 절차를 분석하고, 이를 통해 디지털 포렌식 기반의 전자기록물 수집 및 이관 절차의 요구사항을 도출했다.

### 3.1 국내 디지털 포렌식 수행 절차 분석

국내에서 사용되고 있는 디지털 포렌식 절차는 크게 대검찰청 디지털 증거 압수 수색 모델과 경찰청 디지털 증거처리 표준 가이드라인 두 가지가 있다.

대검찰청 디지털 증거 압수 수색 모델은 컴퓨터 등의 디지털 장비로부터 디지털 증거물을 수집하거나 분석하는 과정에서 수사업무 종사자가 지켜야 할 사항을 정한 디지털 증거 수집 및 분석규정(대검예규 제 410호)을 제정하여 2006년부터 시행하고 있다. 그 절차는 "증거수집 준비", "영장 집행 및 증거 수집", "운반 및 보관", "분석 및 조사", 그리고 "보고서 작성"으로 구성되어 있으며 세부 절차는 다음 〔Table 1〕과 같다.〔4〕

Table 1. Supreme Prosecutors Office Digital evidence collection and analysis rule

| | Procedure detail |
|---|---|
| Preparing evidence collection | Check warrant |
| | Target system information collection |
| | Team makeup |
| | Preparing Tools |
| Execution of warrant and collection of evidence | Presentation of warrant |
| | Control spot and analysis |
| | System shutdown |
| | Evidence collection |
| | Authentication/Sealing |
| Transportation and storing | Transporting evidence |
| | Registrating evidence |
| | Make duplicate copy |
| | Preserving Original |
| Analysis and investigation | Data restoration |
| | Hash analysis |
| | Signature analysis |
| | E-mail analysis |
| Reporting | Create analysis report |
| | Preserving investigation report |

경찰청에서 발표한 디지털 증거처리 표준 가이드라인은 "사전준비", "증거수집", "증거분석 의뢰", "증거분석", 그리고 "보고서작성"의 절차로 구성되어 있으며, 세부 절차는 다음 〔Table 2〕와 같다. 대검찰청 디지털 증거 압수 수색 모델에 비해 세부 절차가 보다 세분화되어 규정되어 있으며, 국내 다수의 디지털 부사기관에서는 이를 기초로 디지털 포렌식을 수행하고 있다.〔5〕

Table 2. The national police agency digital evidence processing standard guidelines

| | Procedure detail |
|---|---|
| Preparation | Check warrant |
| | Target system information collection |
| | Team makeup |
| | Preparing Forensics Tools |
| | Setup the procedure and plan for evidence collection |
| Evidence collection | Presentation of warrant |
| | Control spot |
| | Shooting site evidence |
| | Volatility evidence collection |
| | Evidence collection after system shutdown |
| | Packaging evidence, writing detail information |
| | Listing evidence, including witness signature |
| Request for evidence analysis | Sealing evidence |
| | Write a letter of request for evidence analyzing |
| | Evidence transportation |
| | Evidence take over |
| Evidence analysis | Check the evidence storage media |
| | Deciding whether to duplicate |
| | Connect to write protection device |
| | Imaging process |
| | Analyzing requirement |
| 보고서 작성 | Create analysis report |
| | Preserving and managing evidence |

### 3.2 국외 디지털 포렌식 수행 절차 분석

국외의 경우, 디지털 포렌식 분야의 국제 학술대회인 DFRWS(Digital Forensic Research Workshop)에서 발표된 DFRWS Model을 기본 프레임으로, 미국 DOJ(Department of Justice) 등 많은 국외 기관에서 각자 독자적인 디지털 포렌식 절차에 따라 디지털 포렌식을 수행하고 있다. 하지만 〔Table 3〕에서 볼 수 있듯이, 포괄적인 범위에서는 Reference phase에 크게 벗어나지 않고 대동소이한 순서를 보이고 있다.〔6〕〔7〕

Table 3. Comparison of digital forensics procedures [8]

| | Reference phases | DFWRS | Reith et al. | DOJ | Beebe et al. |
|---|---|---|---|---|---|
| 1 | Incident detection | Identification | Identification | | |
| 2 | First response | | | | Incident response |
| 3 | Planning | | Approach strategy | | Preparation |
| 4 | Preparation | | Preparation | Preparation | |
| 5 | Incident scene documentation | | | Documentation of the crime scene | |
| 6 | Evidence Identification | | Examination | Recognition and identification | |
| 7 | Evidence collection | Preservation, Collection | Preservation, Collection | Collection and preservation | Data collection |
| 8 | Evidence transportation | | | Packaging and transportation | |
| 9 | Evidence storage | | | | |
| 10 | Evidence analysis | Examination, Analysis | Analysis | Examination, Analysis | Data analysis |
| 11 | Presentation | Presentation | Presentation | Report | Finding presentation |
| 12 | Conclusion | Decision | Returning evidence | | Closure |

### 3.3 디지털 포렌식 기반의 전자기록물 수집 절차 요구사항 분석

국내외의 디지털 포렌식 절차의 분석결과 공통적으로 1)디지털증거물 수집 준비, 2)디지털증거물 수집, 3)디지털증거물 이송, 4)디지털증거물 분석, 그리고 5)디지털증거물 분석결과의 보고서화의 절차를 따른다. 이는 디지털 포렌식 연구가 시작된 2000년대 초반 DFRWS Model을 기반으로 디지털 증거의 취약성에 주의하여 디지털 증거의 보존을 중심으로 발전된 모델들을 법적인 이슈에 적용하기 위해 디지털 증거의 처리만이 아닌, 사건 발생부터 법정 증언까지 고려한 전체 조사 과정을 다루는 모델로 수립  것이다. 하지만 수집 작업자에 대한 인증과 이관 작업 내역에 대한 검증이 결여되는 등 이관작업에 대한 신뢰성 보장 방법이 부족한 실정이다.

따라서 신뢰성 있는 전자기록물 이관 작업을 위해서 디지털 포렌식 절차에 이관 작업자의 인증, 이관 대상 전자기록물의 해쉬 정보 분석을 통한 전자기록물의 무결성 검증, 이관 작업 전 과정의 로그화를 통한 작업 내용 추적, 그리고 이관 작업 관계자 정보 저장을 통한 부인방지 등의 절차가 필요하다.

## IV. 디지털 포렌식 기반의 전자기록물 이관 절차 제안

국내외 포렌식 절차를 분석해본 결과 전자기록물을 수집하는 수행자에 대한 인증 절차의 부재와 수집 및 이관 작업 내역에 대한 로그 기록 및 보고서의 진본성 보장을 위한 기술의 필요성을 확인하였다.

본 장에서는 국내외의 디지털 포렌식 절차를 분석한 것을 바탕으로 전자기록물의 안전한 이관을 위해 필요한 프로세스에 디지털 포렌식 기술을 적용한 디지털 포렌식 기반 전자기록물 수집 및 이관 절차를 제안한다.

디지털 포렌식 기반 전자기록물 수집 및 이관 절차는 [Fig. 1]과 같이 “이관 준비”, “이관 정보 수집”, “이관 정보 보관”, “이관 정보 이송”, “이관 정보 검증”, 그리고 “이관 완료”로 구성된다.

### 4.1 이관 준비

이관준비 단계에서는 이관 대상 기관에 방문하기 전 이관 대상 시스템에서 사용 중인 파일 시스템 및 대상 파일 사이즈 점검 등 이관 대상 전자기록물과 관련된 정보를 수집한다.

### 4.2 이관 정보 수집

이관정보수집 단계에서는 ID/Password 기반의 사용자 인증과 같은 인증기술을 적용하여 이관 작업을 보유한 정당한 사람이 이관 작업을 진행하는지 여부를 검사한다. 사용자 인증이 정상적으로 수행되면, 이관 대상 시스템의 운영체제 정보 등의 시스템 정보와 이관 시점의 시간 정보를 수집한다. 이관 정보 수집의 마지막에는 이관 주 대상이 되는 전자기록물을 수집하고, 수집된 전자기록물의 수정을 방지하기 위해 이미징(Imaging) 작업을 진행한다.

### 4.3 이관 정보 보관

이관정보보관 단계에서는 이관정보수집 단계에서 이미징한 전자기록물을 암호화하여 기밀성을 보장하고, 이관 과정의 무결성 검사에 사용할 해쉬 정보를 생성한다. 그리고 생성된 해쉬 정보와 더불어 이관작업 수행자 정보, 이관 대상 시스템정보, 이관 작업 시점, 이관 대상 전자기록물 내역 등 이관 절차 별로 수행된 작업의 모든 내역을 로그(log)화 하여 chain of custody를  보장할 수 있도록 한다. 해당 로그는 제안되는 이관 절차 중 이관 완료 작업에서 생성할 보고서에 포함된다.

### 4.4 이관 정보 이송

이관정보이송 단계에서는 수집된 전자기록물을 수록한 저장 매체에 쓰기방지 장치를 장착하고 물리적으로 차폐하여 이관 대상 기관으로부터 기록수집 기관으로 이송한다.

### 4.5 이관 정보 검증

이관정보검증 단계에서는 기록수집 기관으로 전자기록물을 수록한 저장매체가 도착한 뒤 다시 한 번 사용자인증을 수행하여 이관 작업을 진행한 사람인지 여부를 검사한다. 그리고 해쉬 값의 검증을 통한 비트스트림(bit stream)의 변조여부 검사를 통해 이관된 전자기록물의 진본성 및 무결성을 검사하고, 이관 정보 보관 단계에서 생성한 로그의 추적을 통해 이관 과정에서의 작업 내역을 검사한다. 마지막으로 이관정보에 대해 검증이 완료된 전자기록물을 복호화 및 이미징을 해지하여 기록수집 기관의 내부 시스템으로 저장한다.

### 4.6 이관 완료

이관완료 단계는 이관정보검증 단계에 이어서 진행되며, 전체 이관 과정을 기록하여 보고서화 하고 이관 작업자가 이에 수기서명을 첨부하여 보관한다.

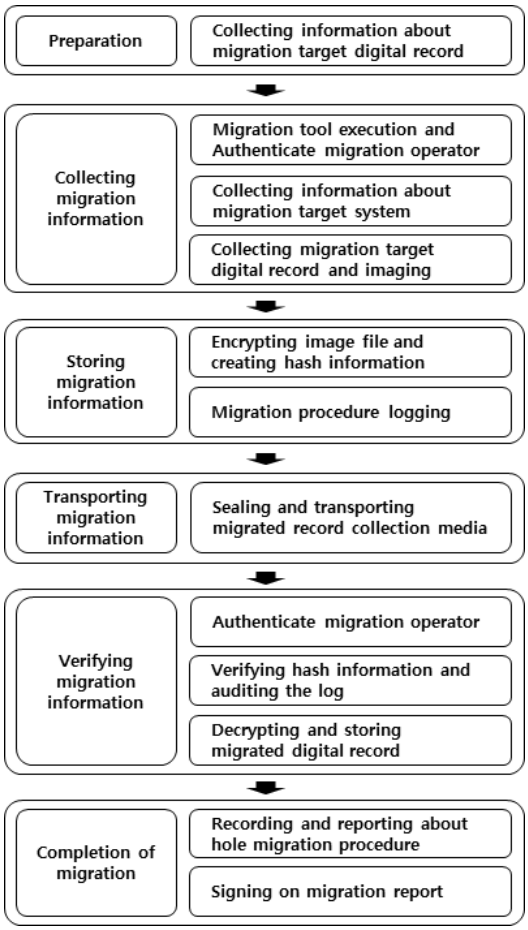


Fig. 1. Digital forensics based collection & migration process for electric record

## V. 디지털 포렌식 기반의 전자기록물 이관 도구 요구사항 분석

본 장에서는 국외에서 전자기록물을 수집하기 위해 사용되는 도구를 파악하고, 각 도구의 기능을 비교 분석한다. 이를 통해 디지털 포렌식 기반의 전자기록물 이관 절차를 수행하기 위한 도구에 추가적으로 필요한 기능적 요구사항을 도출한다.

### 5.1 국외 전자기록물 수집 도구 사용 현황

영국국립도서관 주관으로 2009년 수행된 Digital Lives 프로젝트는 전자기록 보존 및 관리를 위해 실제 디지털 포렌식 기술의 적용하는 방안에 대해 처음으로 연구를 수행했다. 전자기록의 진본성 보장을 위해 매체이전 단계에서 FTK Imager 등의 디지털 포렌식 도구를 적용하는 방법과 함께 전자기록 관리 workflow에서 디지털 포렌식 기술 및 절차를 접목시키는 방안에 대해 제시했다.〔9〕

Andrew W. Mellon 재단의 지원을 받아 University of Virginia Libraries, University of Hull Library, Yale University Library 등이 공동으로 연구해, 디지털 방식으로 생성된 기록물을 관리하기 위한 방법론 및 지속가능한 프레임워크를 제시한 AIMS 프로젝트에서는 기록의 수집을 위해 FTK Imager 3.0을 통해 다양한 매체에 저장된 디지털 기록물에 대해서 이미징(Imaging)을 수행하고, 수집된 디지털 기록물의 정보를 식별하기 위해 AccessData FTK 3.3을 사용해 이미지(Image) 데이터에서 가치 있는 정보를 수집했다.〔10〕

Bitcurator는 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 공동연구로 진행된 Bitcurator 프로젝트에서는 오픈소스 기반의 전자기록 수집도구와 이미지 파일에서 특징적인 정보를 추출하는 분석 도구 등을 통합한 리눅스 기반의 전자기록 프로세스 환경을 개발했다. 해당 프로젝트에서는 Guymager 등의 이미징 도구를 사용해 데이터를 처리했다.〔11〕

### 5.2 국외 전자기록물 수집 도구 시사점 분석

앞서 언급한 프로젝트에서는 대부분 EnCase나 FTK 등 디지털 증거를 수집하기 위해 기존부터 사용중인 도구를 사용했다. 하지만 이 중 일부 도구는 CFTT(Computer Forensics Tool Testing Program)와 같은 특정 적합 기준을 통과하지 못했으며 사용자 인증, 서명, 그리고 시스템 정보 조사 등과 같은 기능을 제공하지 않고 있다. 사용자 인증 및 서명과 같은 기능은 전자기록물의 신뢰성 보증 측면에서 매우 중요한 문제로 작용될 수 있으며, 시스템 정보의 수집은 전자기록물의 기원에 대한 정보로서 활용될 수 있다.

따라서 디지털 포렌식 기술을 기반으로한 전자기록물 이관 도구에는 전자기록물을 입수하기 위한 이미징 기능 외에도 사용자의 인증 및 서명 첨부, 그리고 시스템 정보 수집 기능과 같이 도구를 통한 이관 작업의 신뢰성 향상을 위한 기능이 필요하다.

| Tool (version) | Platform | Imaging | Hash | Browsing | Digital Signature | Time Stamp | User Login | System Inspection | Encrypt | Forensic Project | Open Source |
|---|---|---|---|---|---|---|---|---|---|---|---|
| dd | Unix | O | X | X | X | X | X | X | X | - | O |
| Karen's directory Printer (5.3.2) | Window | X | O | O | X | O | X | X | X | AIMS | O |
| DROID (6.01) | Window | X | X | O | X | X | X | X | X | AIMS | O |
| JHOVE (1.9) | Window | X | X | O | X | X | X | X | X | - | O |
| BEAM Ingester (0.2) | Window | O | X | X | X | X | X | X | X | BEAM | O |
| FTK Imager (3.1.2) | Windows | O | O | O | X | O | X | X | O | AIMS Digital Lives | X |
| FTK (4.2.1) | Windows | X | X | O | X | X | X | X | O | AIMS Digital Lives | X |
| EnCase Imager(7.06) | Windows | O | O | O | X | O | X | X | O | - | X |
| Guymager (0.7.1) | Unix | O | O | O | X | O | X | X | X | BitCurator | O |
| Tableau Imager (1.2) | Windows | O | O | O | X | O | X | X | X | - | X |

Fig. 2. Comparison of Digital Forensics Tool〔12〕

## VI. 디지털 포렌식 기반의 전자기록물 이관 도구 개발을 위한 고려사항 분석

디지털 포렌식 기술을 전자기록물 이관 도구에 성공적으로 적용하기 위하여 국내외 적용 사례 분석과 절차의 확립도 중요하지만, 실제 해당 도구의 도입을 위해서 추가적으로 고려되어야 할 요소들이 존재한다. 앞서 4장과 5장에서 언급된 이관 절차 및 기능 요구사항을 포괄하는 전자기록물 이관 도구를 현 시정에 맞게 개발·적용하기 위하여, 현 디지털 기록물 이관 과정에서 발생 가능한 문제점을 분석하고 이를 바탕으로 고려사항을 도출하였다. 고려사항은 크게 기능적인 부분과, 기능 외적인 충족 요건으로 분류 할 수 있으며 각각에 대한 설명은 아래와 같다.

### 6.1 기능적 고려사항

기능적 고려사항은 앞서 제안된 디지털 포렌식 기반의 이관 절차를 수행하기 위해 추가되어야 하는 기능으로써, 현재 국내의 전자기록물 이관 과정에서 발생할 수 있는 문제점들을 기반으로 도출되었다.

#### 6.1.1 사용자 인증 기능

앞서 5장에서 분석한 것과 같이 현재 사용되고 있는 전자기록물 이관 도구에는 도구 사용자를 인증하는 기능이 포함되어 있지 않다. 이런 경우 인가받지 않은 사용자가 이관 도구를 이용하여 악성자료를 이관하거나, 이관 도구 내부에 저장된 전자기록물을 무단으로 열람하거나 유출할 수 있다. 따라서 수집된 전자기록물이 법적인 증거능력을 갖추기 위해서는 chain of custody 관점에서 도구의 사용자 또는 이관자를 인증하는 것을 기점으로 어떤 전자기록물이 언제, 누구에 의해 이관되었는지 등의 정보를 로그에 기록하여 이관 과정의 신뢰성을 보장할 필요가 있다.

#### 6.1.2 사용자 시간 입력 기능

전자기록물 이관을 수행 시, 수행 시점의 시간 정보는 전체적인 이관 절차의 기록과, 향후 이관된 전자기록물의 검증 차원에서 사용될 수 있는 중요한 정보로써 정확성이 요구된다. 실제 전자기록물 이관을 수행할 대상은 인터넷의 접속 여부, 지속적인 관리 여부가 불투명한 여러 기관들의 불특정 다수의 컴퓨터이다. 윈도우 운영체제를 사용하는 컴퓨터의 경우 사용자에 의해 임의로 시간 변경이 가능하며, 해당 컴퓨터에서 사용된 이관 도구에 대하여 변경된 시간이 적용 될 수 있다. 따라서 시간 정보의 오류가 발견되었을 경우 시간 정보를 정정하기 위해서 도구 시작 단계에서 사용자로부터 시간정보를 확인받고 수정된 시간 입력 기능이 필요하다. 본 기능을 통해 이관 시점의 정확성을 보장함으로써, 보다 신뢰성 높은 이관 작업을 수행할 수 있다.

#### 6.1.3 전자기록물 유효성 검사 기능

이관 도구를 통해 이관되는 전자기록물은 수십 개에서 수천 개의 다양한 종류의 포맷을 갖는 파일들이다. 전자기록물의 관리 차원에서의 이관 대상은 가용성이 보장되어 실행 가능한 전자기록물로서, 이를 검증하기 위하여 이관 과정에서 전자기록물의 유효성 검증을 통한 파일의 자동 선별 기능이 필요하다. 이는 도구의 파일 선택 과정에서 파일 시그니쳐라는 디지털 파일의 앞부분에 위치한 일련의 바이트들의 분석을 통한 유효성 검사를 수행함으로써 이러한 문제점을 해결할 수 있다. 해당 기능을 구현하기 위해서 전자기록물로 인증된 파일 시그니쳐들로 이루어진 데이터베이스를 구축하고 선택받은 파일의 파일 시그니쳐와 비교해 봄으로써 해당 파일의 유효성을 검사한다. 전자기록물의 유효성을 검증하는 과정을 통해 전자기록물에 대한 유효성 검사를 이관 과정에 포함시킴으로써, 효율적인 이관 결과를 기대할 수 있다.

#### 6.1.4 해쉬 정보 확인 기능

이관 도구를 통해 전자기록물을 이관 과정에서 비트스트림(bitstream)의 훼손 또는 외부로부터의 데이터 변조 시도 등에 의해 데이터의 무결성 및 진본성이 훼손될 가능성이 있다. 따라서 디지털 포렌식 관점에서 원본 기록의 무결성 및 진본성을 증명하기 위해, 전자기록물의 수집과 동시에 원본 기록 전체에 대한 해쉬 정보와 이관 도구를 통해 수집한 이관본의 해쉬 정보를 비교 검증하고 해당 정보를 보존할 필요성이 있다. 이관 대상 전자기록물의 해쉬 정보를 검증함으로써 이관 과정에서의 무결성을 보장할 수 있고, 해쉬 정보를 보존함으로써 전자기록물의 진본성을 보장하는데 사용할 수 있다.

### 6.2 기능 외적 충족요건

기능 외적 충족요건은 해당 전자기록물 이관 도구를 개발함에 있어서 기능 외적으로 충족되어야 할 요건들로써, 해당 도구가 실제로 현 이관 과정에서 사용되기 위하여 고려하여야 할 사항에 대한 분석을 통하여 도출되었다.

#### 6.2.1 쉬운 유저 인터페이스를 적용한 자동화 도구

개발된 전자기록물 이관 도구를 사용하는 실제 사용자들은 컴퓨터에 익숙하지 않은 경우가 대부분이며, 전자기록물 이관 도구는 해당 사용자들의 지속적인 사용을 유도하기 위하여 간단한 유저 인터페이스로 구현되어야 한다. 앞서 4장에서 제안된 디지털 포렌식 기반의 전자기록물 이관 절차를 수행하기 위해 5장에서 도출된 요구 기술이 해당 도구에 포함되어야 하며, 컴퓨터 분야 비전문가인 사용자들을 고려하여 사용하는 데에 있어 불편함을 최소화시키기 위해 구성 기능들이 자동으로 실행되도록 구현할 필요성이 있다.

#### 6.2.2 기존 절차 대비 효율성 보장

기존의 전자기록물 이관 방법은 이동식 저장 장치를 이용하여 대상 전자기록물을 복사해 오는 것이며, 이 과정에서 소요되는 시간은 복사 시간이 전부이다. 이에 비하여 디지털 포렌식을 접목한 전자 기록 물 이관도구는 앞서 확립된 절차에서 볼 수 있듯이 복사 절차 이외에도 여러 절차를 포함하고 있으며, 각각의 절차들은 수행하는데 있어 이미지 생성, 데이터의 암호화, 해쉬값 생성 등의 추가적인 시간을 필요로 하게 된다. 많은 양의 전자기록물을 이관하는 과정에서 이러한 추가적인 요소에 소요되는 시간은 사용자의 관점에서 매우 크게 작용될 수 있으며 기존 복사 소요 시간 대비 해당 도구를 사용하여 이관을 수행하는 데에 있어 소요되는 시간의 차이를 줄일 필요성이 있다. 각각의 절차에 사용되는 알고리즘은 종류에 따라 소요되는 시간이 각양각색임으로, 해당 절차의 중요성을 판단하여 적절한 사용을 통한 전체적인 이관 시간의 단축이 필요하다.

#### 6.2.3 다양한 저장 장치 지원

이관할 전자기록물은 몇 바이트에서 수 테라바이트까지 다양한 크기를 가질 수 있다. 해당 전자기록물을 성공적으로 이관하기 위하여, 개발된 디지털 포렌식 기반의 전자기록물 이관 도구는 다양한 저장 장치를 지원해야 한다. 고려되어야 할 저장 장치는 수 기가의 저장 공간을 지닌 이동식 저장 장치 USB에서 외장하드, 수 테라의 저장 공간 보유가 가능한 NAS까지 다양한 저장 장치가 될 수 있으며, 전자기록물 이관 도구는 이러한 저장 장치들에서의 원활한 사용이 가능한 유연한 구조를 고려하여 설계 및 개발되어야 한다.

## VII. 디지털 포렌식 기반의 전자기록물 이관 도구 개발 결과

앞서 확립된 디지털 포렌식 접목 절차와 4장에서 도출된 기능적 고려사항을 포괄하는 전자기록물 이관 도구를 개발함으로써, 해당 이관 과정에 디지털 포렌식 접목의 실제 활용 가능성을 확인하였다. 본 도구는 C#으로 개발되었으며, 윈도우즈 운영체제 XP에서 8까지 호환이 가능하다.

### 7.1 사용자 인증 기능 구현

사용자가 이관 도구를 실행하면 사용자 인증 기능이 호출되며, 이를 위한 화면이 출력된다. 인가된 사용자 정보를 입력한 경우에만 이관 도구에서 제공하는 기능을 사용할 수 있도록 한다.


Fig. 3. User authentication

### 7.2 사용자 시간 입력 기능 구현

이관 대상 컴퓨터의 정보를 획득하는 과정에서 해당 시스템의 시간정보가 출력되며, 시간 정보가 유효하지 않을 경우 사용자에 의해 현재 시간을 입력받을 수 있다. 변경된 시간 정보는 이관 과정이 끝날 때 까지 실시간 적용되어 이관 종료 과정에서 유효한 결과물의 출력을 가능하게 한다.

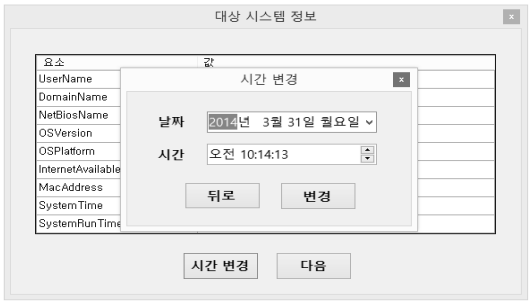


Fig. 4. Task performed time modification

### 7.3 전자기록물 유효성 검사 기능 구현

사용자로부터 선택받은 폴더의 내부 파일들에 대하여 유효성 검사를 수행하여 유효하지 않은 파일들을 출력하며, 출력된 파일들의 목록에 대하여 사용자가 이관에 포함시킬 파일을 추가적으로 선택할 수 있다. 선택한 모든 파일에 대한 유효성 검사를 일괄 적용시킴으로써, 관리차원에서의 유효한 전자기록물 획득을 기대할 수 있다[13].

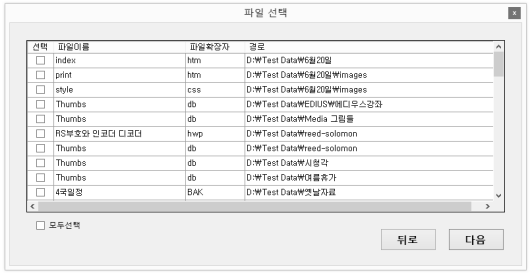


Fig. 5. Digital record validation check

### 7.4 해쉬 정보 확인 기능 구현

원본 전자기록물 전체에 대한 해쉬 정보와 이관 도구를 통해 수집한 이관본의 해쉬 정보를 비교 검증하고, 해당 정보를 이관 전 과정에 대해 기록한 PDF 파일 포맷 형식의 보고서에 포함한다.

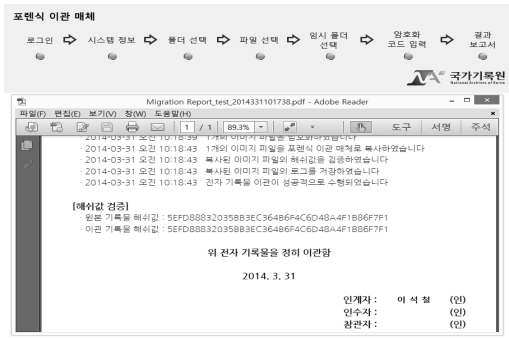


Fig. 6. Hash information validation and result report of migration process

## VIII. 결 론

디지털 형태로 생성·보관되는 기록물의 양이 급증하고, 기관 간에 전자기록물의 이관이 빈번히 발생하는 현 시점에서 이관된 전자기록물의 무결성과 진본성을 보장할 수 있는 이관 절차 수립에 대한 필요성이 높아지고 있다.

본 논문에서는 전자 증거물의 무결성과 신뢰성을 보장하기 위해 사용되는 디지털 포렌식 기법을 전자기록물의 이관 절차를 수립하기 위한 요구사항과 해당 이관 절차를 수행할 수 있는 도구를 개발하기 위한 요구사항을 도출했다. 이를 기반으로 디지털 포렌식 기법을 적용한 전자기록물 이관 도구를 개발했다.

향후 연구에는 전자기록물의 증거능력을 확보하고 법적 유효성을 확립하는데 특화된 기술을 개발하고, 이를 바탕으로 하는 디지털 포렌식 기반 기록물 위변조 검증 기술의 개발이 필요하다.

## References

[1] The national archives and Records Administration, "The Electronic Records Archives Status," Dec. 2010.
[2] State of Utah, "Electronic records management/migration," June. 2012.
[3] State of New South Wales, "Effectively manage the migration of your digital records," 2009.

〔4〕 The national police agency, "Digital evidence processing standard guideline," 2006.
〔5〕 Supreme Prosecutors Office, "Digital evidence collection and analysis rule," 2008.
〔6〕 IETF, RFC 3227, "Guidelines for Evidence Collection and Archiving," 2002.
〔7〕 NIST, "Guide to Integrating Forensics Techniques into Incident Response (Special Publication 800-86)," 2006.
〔8〕 Aleksandar Valjarevic, "Analyses of the State-of-the-art Digital Forensic Investigation Process Models," 2012.
〔9〕 British Library, "Digital Lives," 2009.
〔10〕 University of Virginia Libraries, Stanford University Libraries and Academic Resources, University of Hull Library, Yale University Library, "AIMS(An Inter-Institutional Model for Stewardship)," 2009~2011.
〔11〕 SILS at University of North Carolina, MITH at University of Maryland, "BitCurator," 2011~2013.
〔12〕 Yongmin Park, "Requirements analysis of Digital Records Migration based on Digital Forensics," Conference on Information Security and Cryptology(CISC) - Winter 2013, pp. 193-196, Dec. 2013.
〔13〕 Jae-Young Lee, Joo-Ho Choi, "Validation and the Format of the Electronic Record Digital Component Technology Research," Journal of Korean Society of Archives and Records Management, 12(3), pp. 29-46, Dec. 2012.

## 〈저자소개〉

이 석 철 (Seokcheol Lee) 학생회원
2012년 2월 : 아주대학교 정보 및 컴퓨터공학부 졸업
2012년 3월~현재: 아주대학교 컴퓨터공학과 석박사통합과정
〈관심분야〉 디지털 포렌식, 전기자동차 보안, 스마트그리드 보안

유 형 욱 (Hyunguk Yoo) 학생회원
2011년 8월 : 아주대학교 정보 및 컴퓨터공학부 졸업
2011년 9월~현재 : 아주대학교 컴퓨터공학과 석박사통합과정
〈관심분야〉 전력제어시스템 보안, 디지털 포렌식, 비정상행위탐지

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