교 육 학 석 사 학 위 논 문

증거 무결성 보장을 위한 전자공증기반 디지털증거관리 모델

2008년 8월 27일

부경대학교 교육대학원

전산교육전공

김 재 성

교 육 학 석 사 학 위 논 문

증거 무결성 보장을 위한 전자공증기반 디지털증거관리 모델

지도교수 신 상 욱

이 논문을 교육학석사 학위논문으로 제출함.

2008년 8월 27일

부경대학교 교육대학원

전산교육전공

김 재 성

김재성의 교육학석사 학위논문을 인준함.

2008년 8월 27일

주 심　　이학박사　이 경 현　(인)

위 원　　공학박사　송 하 주　(인)

위 원　　이학박사　신 상 욱　(인)

< 차 례 >

< 표 차 례 >

< 그 림 차 례 >

Digital notary based digital evidence management model for the guarantee of an evidence integrity

Jae Sung Kim

Graduate School of Education

Pukyong National University

Abstract

The digital evidence must have a reliability in the process of the acquisition, transportation and custody for the evidence ability. But the current process breaks the principle of integrity in the acquisition, transportation and custody of the evidence. In the chain of custody process of the digital evidence, the evidence in the digital media such as hard disk has the characteristic of invisibility. Thus, it has a problem that the chain of custody is dependent only on the document in the current digital forensic process. In order to solve this problem, we apply digital notary to digital evidence management system, which provides the verification of a timestamp, the authentication of a content, the proof of the delivery and custody of digital data. We design the interaction between the machinery of law and the investigation office for each service of digital notary, and propose the profile of the digital evidence for the chain of custody. The proposed model can guarantee the integrity of the evidence and give a legal effect.

Ⅰ. 서론

컴퓨터 포렌식은 1980년대 중반부터 디지털 증거의 보존, 신원확인, 문서를 다루는 것에서 시작, 법집행기관과 군사기관에서 수사와 정보수집의 주요기술로 인정받아 왔다. 컴퓨터 포렌식이란 컴퓨터 범죄에 대한 수사와 재판을 위해 디지털 증거를 수집・보관・제출하는 일련의 과정을 말한다.

현재는 연구의 중점이 매체나 출력물에서 소스인 디지털 증거로 변화하면서 디지털 증거(Digital Evidence) 자체에 주목하기 시작했고, 디지털 포렌식이란 용어가 보편화되고 있다.

이러한 변화 속에 2007년 6월 1일, 우리나라 형사소송법의 개정으로 국내 사법제도가 미국식 공판 중심주의로 변화하고, 증거 중심의 재판으로 바뀌었다[1]. 하지만 기존의 디지털 포렌식 연구의 초점은 디지털 증거의 수집, 추출, 분석, 복원 등 수사기관의 입장에서 보다 활발히 연구되어지고 있는 실정으로, 법원의 관점이 결여된 이러한 연구는 디지털 증거의 전문법칙 문제, 증거능력 보장 문제가 대두 될 수밖에 없을 것이다. 기본적으로 디지털 증거는 유체물과는 달리 증거능력이 공격받을 수 있는 여지가 많기 때문이다. 현행법은 전자정보를 당해 컴퓨터에 의해 가시성·가독성이 있는 상태로 출력한 문서가 증거로 사용될 경우 이것은 다른 사람의 기록을 전자적 수단을 사용하여 작출한 진술증거로 공판정에서 반대신문을 거치지 않은 전문증거이다.

증거가 아무리 가치 있는 것이라 해도 전문증거로 「증거능력」이 없다면 사실인정의 자료가 될 수 없다. 하지만 전문법칙의 예외규정으로 컴퓨터로 작성한 서면이나 그에 준하는 기록들은 처리과정에서 인위적 수정을 가하지 않은 것이 담보되어 있는 가운데 증거능력을 인정하고 있다.

다만, 그 증거는 특히 신빙할 수 있는 상태였음이 증명되어야한다[1]. 즉, 디지털 증거의 수집・이송・보관・제출단계에서 신뢰성의 정황적 보장과 필요성이 인정되어야 한다. 본 논문은 현행 형사소송법에 근거하여 디지털 증거의 증거능력 보장을 위한 디지털 증거관리 모델을 제시하고자 한다.

본 모델은 공증제도를 증거관리에 도입함으로서 해결할 수 있다. 공증제도란 국가나 법무법인 등의 공공단체가 작성한 공증문서에 의해 소송법적 효력을 부여하여 사회생활에서 당사자간의 분쟁을 예방하기 위한 제도이다. 전자공증제도를 통하여 증거를 보관하고 소송의 증거로 법적 효력을 부여하고자 하는 것이다. 본 논문에서 제안하는 전자공증기반 디지털 증거관리 모델의 전자공증기관은 수사기관, 사법기관과 상호작용하여 증거의 무결성 입증의 어려움을 해소하고 디지털 포렌식 기본원칙을 준수할 수 있도록 한다.

논문의 구성은 2장에서 디지털 증거의 증거능력을 이해하기 위해 먼저 디지털 증거의 증거법적 의의를 살펴보고 증거능력 확보를 위한 방법을 제시한다. 3장에서는 디지털 증거의 무결성 유지를 통한 증거능력 확보 방안으로 전자공증 개념을 도입, 전자공증서비스를 4가지로 제안하면서 증거능력 보장을 위한 전자공증기반 디지털 증거관리 모델을 설계한다. 4장에서는 전자공증기반 디지털 증거관리 모델의 발전방향을 제시하고, 5장에서는 결론을 기술한다.

---

1) 대법원 2001. 3. 23. 선고, 2000도486 판결

Ⅱ. 관련 연구

1. 디지털 증거의 증거법적 의의

가. 증거능력과 증명력

현행 우리 형사소송법은 영미법계의 자유심증주의[2]를 원칙으로 하면서도 대륙법계 전통의 증거법규정들을 절충적으로 규정하고 있다. 증거는 『증거방법』과 『증거자료』의 두 가지 의미를 포함한다.

증거방법은 사실인정의 자료가 되는 유형물 자체(증인, 증거서류, 증거물「하드디스크 같은 유형물 자체」)를 말하며, 증거자료는 증거방법을 조사하면서 알게 된 내용(증언, 증거물의 성질, 전송중인 전자정보를 출력한 문서)을 말한다.

현행법은 법원의 주체적 역할로 얻어지지 않은 증거, 즉 타인의 기록과 같은 2차적 자료에 의해 획득한 지식은 증거자료이자 진술증거로서 전문증거로 간주되기 때문에 원칙적으로 증거능력을 인정하고 있지 않고 있다. 전자정보를 컴퓨터에 의해 가시성·가독성이 있는 상태로 출력한 문서가 증거로 사용될 경우 이것은 다른 사람의 기록을 전자적 수단을 사용하여 추출한 진술증거로서 공판정에서 반대신문을 거치지 않은 전문증거라 할 수 있다.

전문증거는 증거능력이 배제되어 법원의 증명력 판단에 기준이 될 수 없으며 증거로서 가치가 상실된다. 우리 형사소송법에서는 증거능력과 증명

2) 자유심증주의 : 증거의 증명력에 관한 일체의 법률적 제한을 무시하고, 전적으로 법관의 판단에 일임함을 말하며, 모든 증거의 증명력을 미리 법률로써 정하여 두는 법정증거주의와는 반대이다.

력을 명확히 분류하고 있으며 증거능력이란 증거가 주요 사실을 인정하는 자료로 이용될 수 있는 법률상의 객관적인 자격을 말하고 증명력이란 증거가 주요 사실을 인정하는 자료로 사용될 수 있는 법률적인 능력인 증거능력을 전제로 하여 그 증거가 가지는 신빙성의 정도를 가늠하는 것이다.

하지만 현행 형사소송법에는 전문법칙의 예외규정으로 컴퓨터로 작성한 서면이나 그에 준하는 기록들은 처리과정에서 인위적 수정을 가하지 않은 것이 담보되어 있는 가운데 증거능력을 인정하고 있다.

다만, 그 증거는 특히 신빙할 수 있는 상태였음이 증명되어야한다. 아래의 표 1이 그 예이다.

<표 1> 컴퓨터 디스켓에 들어 있는 문건의 증거능력

판결요지】 컴퓨터 디스켓에 들어 있는 문건의 증거능력

(대법원2000도486판결)

"컴퓨터 디스켓에 담긴 문건이 증거로 사용되는 경우 그 기재내용의 진실성에 관하여는 전문법칙이 적용된다 할 것이고, 따라서 피고인 또는 피고인 아닌자가 작성하거나 또는 그 진술을 기재한 문건의 경우 원칙적으로 형사소송법 제313조 제1항 본문에 의하여 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 인정된 때에 이를 증거로 사용할 수 있다."

대법원 2001. 3.23. 선고 2000도 486 판결

증거가 아무리 가치 있는 것이라 해도 『증거능력』이 없으면 사실인정의 자료가 될 수 없을 뿐 아니라, 공판정에 증거로 제출하여 증거조사를 하는 것도 허용되지 않는다. 증거능력을 제한하는 것으로 자백배제법칙, 위법수집증거 배제법칙, 전문법칙 등이 있다.

2007년 6월 1일 개정 형사소송법에는 학설과 대법원 판례로만 적용하였던 위법수집증거 배제법칙 "적법한 절차에 따르지 아니하고 수집한 증거는

증거로 할 수 없다"를 명문화하였다.

또한 "사실의 인정은 증거에 의하여 하며, 범죄사실의 인정은 합리적인 의심이 없는 정도의 증명에 이르러야 한다." 라고 증거 재판 주의를 한층 강화하였다[1].

이러한 형사소송법의 개정은 법정에 제출되는 증거물에 있어서 수집, 운송, 보관에 있어 의심이 없을 정도의 신뢰성을 더욱 요구하고 있다.

나. 일반 범죄증거와 디지털증거의 차이

일반 범죄증거와 디지털 증거의 주요한 차이는 다음과 같다.

- ○ **불가시성** : 유체물이 아닌 정보의 형태로서 가시성과 가독성이 없음
- ○ **취약성** : 원본과 복제본의 구별이 쉽지 않고, 변조나 손상은 용이
- ○ **대량성** : 기업 전산회계 등 데이터베이스 자료는 증거의 양 방대
- ○ **국경초월성** : 장소의 제한을 받지 않고 증거가 존재

일반 범죄증거인 문서, 도구 등은 직접증거로 현출되는 경우가 대부분이다. 물론 디지털 증거의 존재 자체가 증거로 되는 경우는 일반적인 증거법상의 증거물과 직접증거로서 다르지 않다. 하드디스크와 같은 유형물 자체뿐만 아니라, 수집된 디지털 증거(Computer-Generated Record, ATM출력물)가 그 예다[2].

하지만 전자기록의 내용이 증거가 되는 경우, 출력된 서면은 사람이 생성과정에 개입한 데이터로 전문증거(Hearsay Rule)일 것이다.

이러한 전문증거는 앞서 언급한 바와 같이 증거능력을 인정받기 위해서는 특히 신빙 할 수 있는 상태임을 증명해야한다. 즉 증거물의 수집, 운송, 보관에 있어 의심이 없어야한다.

일반 범죄증거와 다른 디지털 증거의 특징 중에서 본 연구에서 중점을 두는 것은 바로 취약성 부분이다. 이는 사후 법정에서 조작여부, 증거 획득 절차의 적정성 등이 문제가 될 수 있기 때문이다.

다. 디지털 증거의 증거능력 확보 방법

디지털 증거가 증거능력을 가지기 위해서는 전문증거임을 감안, 특히 신빙할 수 있는 상태임을 증명해야한다. 이를 위해 첫째는 원본의 변경이나 손상 없이 디지털 증거를 수집해야하는 **원본성**(原本性), 둘째는 복구한 증거가 원래의 압류된 증거와 같은 것임을 증명해야하는 **동일성**(同一性) 이며, 셋째는 전자기록이 서면형태로 출력된 경우는 작성자의 서명과 날인이 없음으로 그 진정의 성립을 인정하여하는 **진정성**(眞正性)을 가져야한다. 따라서 다음과 같은 디지털 포렌식 절차가 반드시 따라야 한다[3].

Step 1. 원본의 훼손이나 변경 없이 얻어져야 한다.

Step 2. 복구된 증거는 원본 증거와 동일함을 증명해야 한다.

Step 3. 변경 없이 데이터는 분석해야 한다.

2. 디지털 증거 수집 절차

가. 디지털 포렌식 유형

포렌식은 크게 데이터 포렌식과 비 데이터 포렌식으로 나누어진다. 비 데이터 포렌식은 물리적 증거, 의학적 증거, DNA 포렌식 등을 예로 들 수 있다. 데이터 포렌식 또는 디지털 포렌식은 분석 대상에 따라 다음과 같이 몇 가지 포렌식 유형으로 분류된다[4].

- **디스크 포렌식** : 물리적인 저장장치인 하드디스크 등 각종 보조기억장치에서 증거를 수집하고 분석하는 포렌식 분야
- **시스템 포렌식** : 운영체제, 응용 프로그램 및 프로세스를 분석하여 증거를 확보하는 포렌식 분야
- **네트워크 포렌식** : 네트워크를 통하여 전송되는 데이터나 암호 등을 특정도구를 이용하여 분석하거나 네트워크 형태 등을 조사하여 단서를 찾는 포렌식 분야
- **인터넷 포렌식** : WWW, FTP, USENET 등 인터넷 응용 프로토콜을 사용하는 분야에서 증거를 수집하는 포렌식 분야
- **모바일 포렌식** : 휴대폰, PDA, 전자수첩, 디지털카메라, MP3 등 휴대용 기기에서 필요한 정보를 입수하여 분석하는 포렌식 분야
- **데이터베이스 포렌식** : 주로 대형시스템의 데이터베이스로부터 데이터를 추출, 분석하여 증거를 획득하는 포렌식 분야
- **암호 포렌식** : 문서나 시스템에서 암호를 찾아내는 포렌식 분야
- **회계 포렌식** : 회계 데이터를 회계 전문가가 분석할 수 있도록 데이터를 정제하는 포렌식 분야

나. 디지털 포렌식 기본원칙

디지털 증거가 법정에서 법적효력을 갖도록 하기 위해서는 반드시 지켜야할 기본원칙으로는 다음과 같은 4가지 원칙을 만족시켜야한다.

- **정당성의 원칙** : 압수증거가 적법절차를 거쳐 얻어져야 한다. 위법하게 수집된 증거에서 얻어진 2차 증거도 증거능력이 없다는 독수의 과실이론[3]에서 비롯된다. 즉, 불법 해킹에 의해 얻어진 증거 및 불법하게 얻어진 패스워드로 파일을 해독했을 경우 복호화된 파일은 증거능력이 없음을 의미한다. 미국의 Scafo vs US[4] 사례가 그 예이다.
- **재현의 원칙** : 같은 조건에서 항상 같은 결과가 나와야 한다.
- **연계 보관성(Chain of Custody)의 원칙** : 증거물 획득-이송-분석-보관-법정제출의 각 단계에서 증거물의 동일성을 증명하여야한다.
- **무결성의 원칙** : 수집 증거가 위·변조되지 않았음을 증명할 수 있어야 한다.

다. 실무현장에서의 디지털 증거 수집 절차

■ 한국정보통신기술협회(TTA) 기준

한국정보통신기술협회에서는 컴퓨터나 디지털 기기가 범죄에 직・간접적으로 연관되어 있는 경우에 이들로부터 단서 및 증거를 확보하는 체계화된 절차를 표 2와 같이 제시하고 있다. 디지털 증거물 수집 단계에서 디스크

3) 1926년 실버스톤일가의 불법 압수된 증거물에서 파생된 증거물의 증거능력 부정

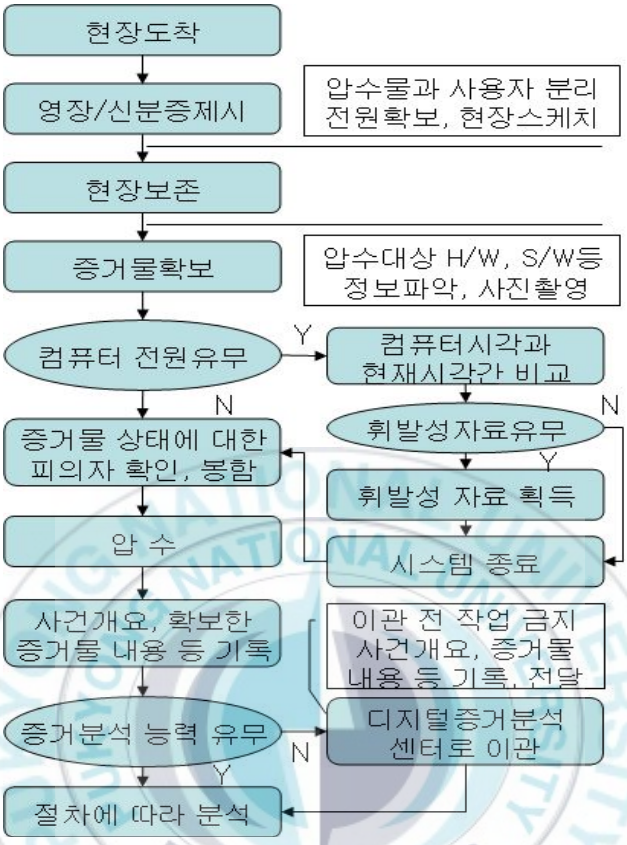
4) 1999년 FBI의 Key Logger System에 의한 증거위법수집 사건

이미징을 제시하고 있으나, 해싱은 분석 단계에서 이뤄지고 있는 점에 주목해야한다. 또한 디지털 증거물의 연계보관관리를 위한 시점확인(Time Stamping)에 대해서도 언급되어지고 있으나 구체적인 방법은 제시되고 있지 않다[5].

<표 2> TTA가 제시한 디지털 포렌식 절차

■ 실무현장에서 디지털 증거 수집 절차

현재 수사기관 과학수사팀에서 이용하는 디지털 증거의 수집 절차는 그림 1과 같다. 연계보관관리를 위한 시점확인을 실무현장에서는 현장스케치나 사진촬영, 시스템시간을 핸드폰, 시계와 같이 촬영하는 등으로 증거물에 대한 연계관리를 실시하고 있다[6].



<그림 1> 실무현장에서의 디지털 증거 수집 절차

그림 1에서 보듯 수집 단계에서 디지털 증거물의 동일성을 증명하기 위하여 증거물의 형상을 기재하고 사진 촬영하는 등 현장스케치 후 문서화하는 과정과 증거목록작성 후 피의자 또는 입회인 서명 과정이 있다. 여기서 디지털 증거물에 대한 연계관리를 문서로 신뢰를 증명하려는 것에는 여러 가지 측면에서 재고될 필요가 있다.

이러한 과정의 근본적인 문제는 눈에 보이는 **매체 중심적 사고로의 접근으로 불가시성의 디지털 증거에 대한 고려가 반영되지 못하고 있다는 것이다.**

또한 아래 표 3, 표 4에서 알 수 있듯 디지털 증거자료의 수집, 보관 및 이송, 분석간 디지털 증거의 증거능력을 유지하기 위한 방안들을 마련하고자 하였다. 하지만 문서만으로 연계보관관리(Chain of Custody), 무결성(Integrity)을 준수하고자 한다면 많은 허점을 내포할 것이다.

우선적으로 디지털 증거현장 조사 체크리스트는 수집을 위한 참고자료에 지나지 않으며, 디지털 증거 보관/이송 체크리스트 또한 많은 허점을 내포하고 있다. 인수자와 인계자는 **매체를 주고받을 뿐이지 매체안의 디지털 증거 내용을 주고받는 것은 아니다.** 인계자가 절대 신뢰할 수 없다면 많은 문제점이 대두 될 것이다.

<표 3> 디지털 증거 보관/이송 체크리스트

<table>
<tr><td colspan="5">디지털증거 보관/이송 체크리스트
(Digital Evidence Preservation CheckList)</td></tr>
<tr><td>1.사건번호</td><td colspan="4"></td></tr>
<tr><td>2.증거물 목록</td><td colspan="4">2-1.
2-2.</td></tr>
<tr><td rowspan="2">3.증거물 담당자 목록 유지</td><td colspan="4">기록하였는가? □ 그렇다 □ 아니다</td></tr>
<tr><td colspan="4">□ 경로 □ 담당자 □ 장소 □ 시간</td></tr>
<tr><td>4.증거물 쓰기방지 조치 및 봉인</td><td colspan="4">□ 그렇다 □ 아니다</td></tr>
<tr><td rowspan="2">5.증거물 포장 용기</td><td colspan="4">이송전 포장하였는가? □ 그렇다 □ 아니다</td></tr>
<tr><td colspan="4">□ Bubble wrap □정전기 방지용 팩 □ 하드케이스 □ 기타</td></tr>
<tr><td>6.증거물의 보관</td><td colspan="4">접근통제가 가능한 공간에 보관하였는가?
□ 그렇다 □ 아니다</td></tr>
<tr><td>7.장소,시간</td><td>장소</td><td></td><td>시간</td><td></td></tr>
<tr><td rowspan="2">8.인수인계자</td><td rowspan="2">인계</td><td>성 명 : (인)</td><td rowspan="2">인수</td><td>성 명 : (인)</td></tr>
<tr><td>연락처 :</td><td>연락처 :</td></tr>
</table>

<표 4> 디지털 증거현장 조사 체크리스트

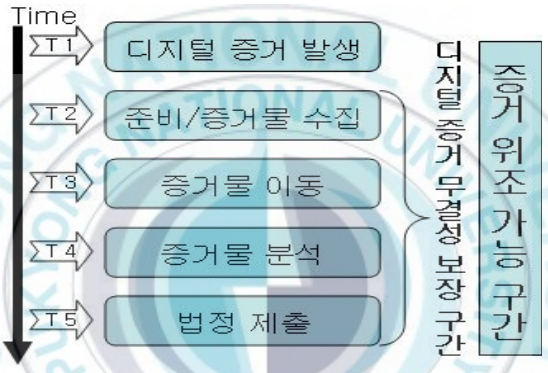
디지털증거현장 체크리스트 (Cyber Crime Scene CheckList)			
1.사건번호			
2.사건개요			
3.사건담당자			
4.증거물 수집 일시·장소	일시 :		
	장소 :		
5.출동당시 증거물의 위치(스케치 또는 사진)	※ 별첨		
6.증거물의 제원	6-1. 제조일자 : 6-2. 고유번호 : 6-3. 모델명 :		
7.증거물의 상태	7-1. 전원이 켜있다	□ 그렇다	□ 아니다
	7-2. 전원이 켜있으면 시스템 시간 기록		
	7-3. 현재시간과 동일한가?	□ 그렇다	□ 아니다
	7-4.틀릴 경우 시스템 시간과 표준시간 오차 확인		
	표준시간 :	시스템 시간 :	
	7-5.휘발성 자료 있는가?	□ 그렇다	□ 아니다
	※있는 경우 압수 여부		
8.컴퓨터 주변기기 유무	이동식 드라이브가 있는가?	☑ 그렇다	□ 아니다
	※있는 경우 압수 여부		
9.현장증인의 언급 내용			
10.압수물이 원본인가	□ 그렇다 □ 아니다(아닌 경우 이유 :		
11.현장조사 때 입회인이 있었는가	□ 그렇다 □ 아니다	입회인	성 명 : (인)
			연락처 :
12.증거물은 잘 보존하였는가	□ 그렇다	□ 아니다	
13.안전한 용기에 넣어서 압수하였는가	□ 그렇다	□ 아니다	

특히, 휘발성 데이터 또는 데이터베이스 일부와 같은 매체 독립적 디지털 증거물의 인수·인계시는 더욱 심각한 무결성의 의심을 초래할 수 있다.

3. 디지털 증거의 무결성

가. 디지털 증거의 무결성 보장 구간

디지털 증거의 연계보관관리와 무결성은 수사준비 및 증거물의 수집단계에서부터 확보해야한다는 하는 것이다. 그림 2에서 디지털 증거 발생시점과 증거위조 가능구간을 표시하였다[7].



<그림 2> 디지털 증거의 무결성 보장 구간

그러나 위에서 언급한 TTA가 제시한 절차나 수사기관이 이용하는 두 방법 모두 디지털 증거 수집 절차에는 완전한 무결성 확보가 되지 않고 있다. TTA가 제시한 절차는 디지털 증거를 분석단계에서 디스크 이미징 되어온 원본을 해싱함으로써 분석된 복사본과 원본의 동일함을 증명하고 있지만 디지털 증거의 수집과 이송 단계에서 연계보관의 원칙을 간과하고 있으며, 수사기관에서 이용하는 방법 또한 자체 수사기관의 공정한 신뢰를 바탕으로 수집하고 이송하고 분석단계에까지 문서에만 의존하여 접근하고 있다. 다음은 디지털 증거의 수집・이송・분석 단계에서 무결성이 상실 되는 경우를 제시하고자 한다.

나. 무결성 상실의 예

■ 증거 수집・이송 단계

디지털 증거가 발생하고 수사준비 및 증거물 수집단계에서 사건 현장의 수사관이 특정 목적(금전적 매수 등)을 가지고 원본의 훼손을 가한 경우를 가정한다면 그 이후의 증거능력 유지를 위한 모든 조치는 의미가 없을 것이다. 결정적 디지털 증거물인 문서파일을 지워버린다거나 변경을 가 할 수 있다는 것이다. 특정 수사관이 결정적 디지털 증거물인 문서파일을 지워버린다거나 변경을 할 수 없도록 증거 프로파일 생성시 입회인의 확인절차가 반드시 필요하다.

또한 증거 이송단계에서는 디지털 증거의 무결성 훼손 가능성이 더욱 커질 것이다. 결정적 증거가 될 디지털 증거 매체가 동일한 규격의 매체로 바꿔치기 되었을 경우 인수자를 신뢰한 인계자는 디지털 증거물의 특성상 변경되었음을 알 수 없을 것이다. 수사기관 실무에서 사용하는 디지털 증거 보관/이송 체크리스트를 통해 앞서 언급하였다. 이뿐 아니라, 이송 도중에 디지털 증거물에 내용을 변경하는 것 또한 시간적 여유만 있다면 충분히 가능할 것이다.

■ 증거 분석 단계

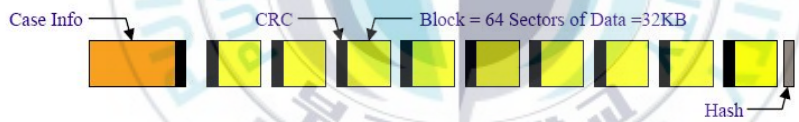
증거 분석단계 또한 최초의 원본 디지털 증거물이 무결성을 유지할 것이라는 장담을 하지 못한다. 2004년 12월부터 경찰청 사이버테러 대응센터 산하 디지털 증거 분석센터가 설치되어 운영 중에 있으며, 현재는 검찰청에서도 디지털 증거 분석센터를 설치하여 운용중이다. 현 실정은 디지털 증거수집과 분석이 이원화 되어 있어 디지털 증거 수집, 이동을 담당하는 수사관과 분석을 담당하는 곳이 상이한 경우가 많다.

아래 표 5는 실무에서 분석센터에 의뢰하는 디지털 증거 수집 및 분석 규정에 있는 서식이다.

<표 5> 대검예규 제410호 별지서식 제8-2호

디지털기기 등 분석지원 요청서				
지원요청	요청일시		요청기관	
	요청부서		주임검사	
	사건번호(사건명)		담당자(연락처, HP)	
	요청내용			
	분석대상물	○ 압수 일시·장소 : ○ 압수물종료 : ○ 사용자(피압수자) : ○ 압수자 :		

진정한 원본의 디지털 증거를 분석센터에서 특정한 목적을 가지고 훼손하는 경우가 발생할 가능성도 배제할 수 없다.



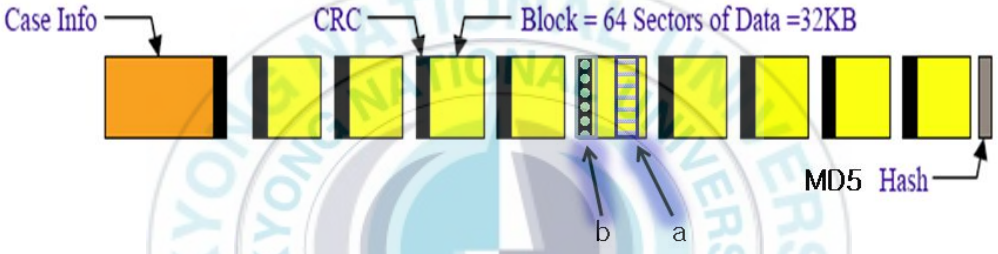
- *Case Info* : the date and time of acquisition + examiner's name + note on acquisition + an optional password.
- *CRC* : for each block of 64 sectors.
- *Hash* : MD5 for the entire bit-stream.

<그림 3> EnCase™의 이미지 구조

그림 3은 EnCase™의 개략적인 이미지 구조를 나타내고 있다. 이미지의 머리 부분은 원본 저장 매체의 전체 개요 및 사건 정보를 포함하고 있다. 이미지의 몸통 부분은 저장매체의 정보를 저장한다. 그리고 64섹터마다 CRC 값을 계산하여 이를 저장하여, 데이터의 오류 발생 여부를 확인한다.

이미지의 꼬리 부분은 이미지의 MD5 해쉬값을 기록한다. 이러한 구조를 가진 저장매체 이미지를 조사/분석을 위해 EnCase™를 실행하면, S/W 자체에 이미지를 마운트 하고, 이미지의 몸통부분에 저장된 CRC 값과 꼬리 부분에 저장된 MD5 값을 검증한다. 대부분의 컴퓨터 포렌식 관련 서적과 문서들은 이러한 해쉬와 체크섬 검사 체계가 디지털 증거의 무결성을 제공한다고 인정하고 있다.

그러나 이 체계는 디지털 증거를 다음과 같이 위조할 수 있는 보안상의 문제점이 있다.[7]



<그림 4> 이미지 MDC 동시위조 공격

① 이미지의 특정 부분을 원하는 값으로 위조한다.(그림 a 부분)

② 위조한 섹터의 CRC 값을 재계산하여, 기존의 CRC 값과 바꿔치기 한다.(그림 b 부분)

③ 조작된 이미지 파일의 해쉬값을 재계산하여, 기존의 해쉬값과 바꿔치기 한다.

④ 원본 저장매체의 내용을 위조하고 해쉬값을 재계산하여 ③의 해쉬값과 동일함을 확인한다.

이러한 문제점은 디지털 증거 무결성을 주장하기 위해 키가 없는 해쉬 알고리즘이나 오류검증 알고리즘을 변조탐지코드로 사용하기 때문에 발생한다. 즉, 메시지 및 변조탐지코드 동시위조 공격이 가능하기 때문에 발생한다.

하드디스크의 정보를 H, 이미지의 정보를 I, MDC(Manipulation Detection Code) 값을 V라 했을 때, H=I이며, V=hash(H)=hash(I)이다.

그러나 위조자가 H, I, V를 모두 변경할 수 있는 현재의 구조에서는, V´=hash(H´)= hash(I´)를 쉽게 재구성하는 보안상의 취약성이 발생한다.

이러한 보안상의 취약성은 법정 소송에서 다음과 같은 두 가지 문제점이 발생한다. 첫째는 디지털 증거가 위조되어 법정에 제출되는 경우이다. 형사소송의 경우 경찰, 검찰과 같은 공신할 수 있는 수사기관이라는 이유 때문에 신뢰할 수 있다고 가정한 것 자체가 무결성의 훼손이며, 민사소송의 경우는 승소를 위해 디지털 증거를 조작하는 경우가 더욱 더 할 것이다. 두 번째, 디지털 증거가 위조되지 않았음에도 불구하고, 용의자 또는 피고소인이 디지털 증거가 위조되었을 가능성을 이유로, 증거 효력을 무력화 시키려 하는 경우이다.

두 번째는 디지털 증거가 위조되지 않았음에도 불구하고, 용의자 또는 피고소인이 디지털 증거가 위조되었을 가능성을 이유로, 증거 효력을 무력화 시키려 하는 경우이다. 다음에 열거한 1999년 9월 발생한 「영남위원회」 사건[5]이 그 예다.

실제 위에서 열거한 사유들로 국립과학수사연구소에서는 일반 범죄증거물의 경우에도 수집 · 운송 · 보관 과정을 전자태그(RFID : Radio Frequency Identification) 방식으로 관리해 위·변조나 오류 가능성을 없애는 증거물 인수인계절차(Chain of Custody)를 제안하였다.

이는 개정 형사소송법상 수사기관의 절차적 엄격성과 공판중심주의를 대비한 변화의 방향인 것이다.

---

5) 대법원 2001. 3. 23. 선고, 2000도486 판결

다. 디지털 증거의 무결성 상실로 법적 증거제출 실패사례

○국내 사례(경남 진주 농협 사건)

2001년 10월 경남 진주에서는 농협 등에 명예훼손의 내용이 담긴 편지가 전달된 적 있다. 수사기관은 피고인의 컴퓨터를 압수, 수색해 결정적 단서가 될 수 있는 문서파일을 발견하고 디지털 증거물로 채택했다. 그러나 용의자는 증거로 사용된 한글파일 '#529487.hwp'의 **최초 생성일자가 범행일자 이후라며 재심을 청구**했고, 재판부는 재심 후 기각했다. 이 사례는 디지털 증거의 획득, 분석, 이동, 보관 등 절차 연속성을 보장하는 연계표준의 중요한 사례

○ 국내 사례(영남위원회 사건)

1999년 9월 발생한'영남위원회'사건에서 수사기관은 피고인들이 소지한 컴퓨터 기록을 압수하고 그 증거에 의해 영남위원회의 목표, 노선, 체계, 강령, 조직 등을 인정한 후 '영남위원회'가 국가보안법상 이적단체에 해당한다고 했다. 그러나 피고인들은 불법녹취, 불법촬영 등 적절한 절차에 의해 수집되지 않았기 때문에 압수방법이 위법이며, **증거는 압수된 이후 조작됐다고 주장(무결성 상실을 주장한 대표적 사례)**했다. 법원 역시 압수 후의 보관 및 출력과정에 조작 가능성이 있으므로 전문법칙을 적용, 형소법 313조 1항에 의거 그 작성자에 의해 성립의 진정함이 있어야 증거로 사용할 수 있음으로, 피고인이 성립의 진정을 인정하지 않고 수사기관이 증명하지 못함으로서 증거물의 증거능력을 부정하는 결론을 내렸으며, 이후 디지털 증거물의 표준에서 중요한 선례

○ 국외 사례(Scarfo vs. US)

1995년 1월 15일 수색영장을 발부 받은 FBI 수사관이 범죄의 증거를 확보하기 위해 용의자의 하드디스크 등을 검사한 결과 범죄의 단서가 될 만한 자료를 수집하였으나, 그것이 암호화되어 있어 그 자리에서 해독할 수 없자, **용의자 몰래 일종의 모니터 프로그램을 설치(Key Logger System)**해 놓고 패스워드를 획득 한 후 나중에 압수, 수색영장을 발부 받아 다시 용의자 컴퓨터에 접근 유죄를 입증할 증거를 수집하였으나 **"위법 수집된 증거"**로 보아 불법적 수사로 판결

Ⅲ. 전자공증기반 디지털 증거관리

1. 전자공증의 개요

공증이란 사회생활에서 발생하는 여러 사항을 문서화할 때 그 문서를 공적으로 증명하는 것을 말한다. 당사자간의 분쟁을 예방하거나 분쟁 발생시 유력한 증거로 활용하고, 나아가 재판절차를 거치지 않고 간편하게 권리를 실행 수 있어 생활 속에 보편화 되어 있다.

전자문서에 대한 증명으로써 전자인증이 주로 사용되어 왔으며, 당사자간 전자문서의 위·변조 여부에 대한 확인과 디지털 서명자가 문서작성과 서명한 사실을 부인하지 못하게 하는 기능을 수행하였다. 그러나 전자문서 내용에 대한 확실성을 제3자에게 보장할 수 있을 것인가라는 의문이 제기된다.

전자인증제도로는 현행 형사소송구조에서 경찰과 검찰의 송치과정이나, 각 수사단계에서의 인수·인계나 법정의 제출에서 공판정의 현출과정을 처리하기에는 역부족이다.

즉, 전자인증제도는 전자서명(PKI 기반)을 수단으로 당사자간의 내용의 존재나 진정성을 확인할 수 있는 제도인데 반해, 언급하고자하는 전자공증제도는 전자공증기관을 통해 제3자가 내용을 확인할 수 있는 제도라고 할 수 있다.

전자공증의 내용은 공증사무의 내용과 유사하다. 전자공증을 통하여 증거 보관 및 소송의 증거, 내용의 진정성 보장, 시점확인서비스 등의 효과에 법적인 효력을 부여하고자 하는 것이다.

이런 사유로 전자공증의 개념은 『전자문서의 작성자에 대한 확인이나 전자문서의 전송 및 보존 중의 소실을 방지하기 위하여 공증인이 기 작성된 전자문서의 작성자나 동일성에 관한 내용을 작성·보관하여 전자문서의 작성자 및 전자문서의 존재와 내용을 증명하는 제도』라 할 수 있다. 본 논문에서 굳이 전자인증과 전자공증의 개념에 차이를 두는 것은 아래 표 6의 비교 때문이다.

<표 6> 전자인증과 전자공증의 비교

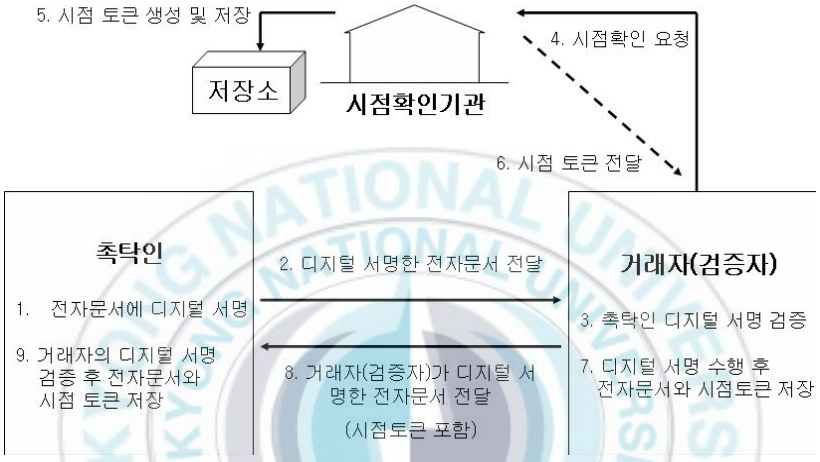
구 분	전자인증	전자공증
제도의 목적	신원확인	사실증명
서비스 성격	문서증명	사실행위/법률행위 증명
서비스 주체	공인인증기관	전자공증기관
효 력	진정성 증명	소송법 상의 추정적 효력
우편제도와 비교	일반우편	내용증명 우편

전자공증 모델로는 양자 증명 모델과 제3자 증명 모델로 나눌 수 있다[8]. 먼저 양자 증명 모델은 촉탁인과 거래자(검증자)간의 분쟁 발생시 전자문서의 내용증명을 위한 방식으로 전자공증기관 설립 없이 기존의 공인인증기관을 TTP로 활용할 있는 장점을 가진다.

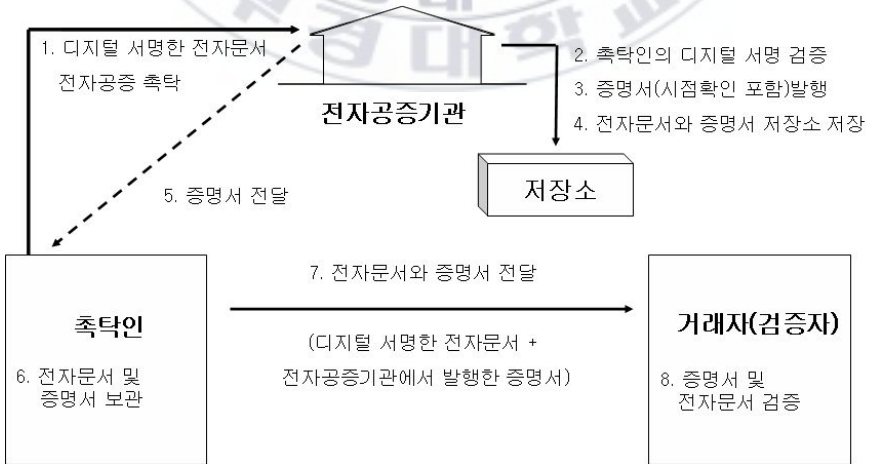
이 방식은 개인간 전자상거래상에 적합하며, TTP는 단지 전자문서의 해쉬값만을 보관함으로서 공증 요청이 처리된다. 그림 5는 양자 증명 모델을 도식으로 표현하고 있다.

본 논문에서 제시하고자 하는 모델은 그림 6의 제3자 증명 모델이다. 즉, 전자공증기관을 활용하는 것으로 촉탁인이 증명이 필요한 전자문서에 디지털 서명을 하여 전자 공증기관에 공증을 요청하면, 전자공증기관에서는 디

지털 서명을 검증하여 시점확인을 포함하는 증명서를 발행하고, 공증된 전자문서와 증명서를 저장소에 저장하고 증명서를 요청자에게 발급하는 방식이다. 공증기관의 공증서비스로 보다 높은 신뢰성을 확보하고, 다음에 제시하는 전자공증서비스를 실현할 수 있기 때문이다.



<그림 5> 양자 증명 모델



<그림 6> 제3자 증명 모델

2. 공증 모델 적용을 위한 실무 절차

제3자 공증모델을 통한 전자공증 서비스를 디지털 증거 관리에 어떻게 적용할 것인가에 대해서는 대검찰청 예규 제410호(2006. 11. 21) 『디지털 증거 수집 및 분석 규정』을 기준으로 현장실무에서 사용되는 디지털 포렌식 절차를 적용한다.

단계별로 실무 절차를 살펴보면, 우선 수사기관은 디지털 포렌식 장비확보 등 수사준비를 완료한 다음 사건현장에 도착하여 현장분석, 사진촬영, 정보처리시스템의 시간과 한국표준시간과 비교 기록 후 디지털 증거물 획득을 위한 작업을 한다.

획득하고자 하는 디지털 증거물에는 디지털기기나 저장 매체와 같은 증거도 있으며, 휘발성 데이터와 같은 매체 독립적(Media-independent) 증거도 있다. 특히 24시간 연속서비스를 제공하는 시스템의 경우는 매체 독립적 증거에 대한 접근방식이 필요하며, 디지털 증거의 획득과 보존에 있어 더욱 신뢰성이 보장되어야 할 것이다.

실무에서는 휘발성 데이터(메모리 또는 임시파일에 저장되는 증거, 프로세스 구동 상태, 사용 중인 파일 내역 등)의 수집 후 MD5, SHA-1 등을 활용하여 해쉬 처리하고, 저장 매체의 경우도 Disk Imaging 후 해쉬 처리함으로서 무결성을 입증하고 있다.

이후 압수・수색대상자 또는 전산관리자를 입회시켜 서명하게 함으로써 수색된 결과물이 정보처리시스템에서 검색된 것임을 확인한다. 이 모든 절차는 현재 대검예규 제410호 제9조에서 확인 할 수 있으며, 서식은 표 7과 같다.

<표 7> 대검예규 제410호 별지서식 제4호

압수·수색시 자료 확인서	
1. 압수·수색·검증 착수 및 종료시간	
2. 정보처리시스템의 종류와 구성	
3. 정보처리시스템의 설정시간	
4. 검색도구와 방법	
5. 수집된 자료 내용 요지	
6. 수집된 자료 해쉬값(Hash Value)	
7. 자료의 수집 방법	
8. 디지털 포렌직 수사관	
9. 입회인 소속	

위의 자료 확인서에 기재된 내용이 사실과 같음을 확인한 후 서명합니다.

2008년 월 일 위 입회인 ０００ (서명 또는 인)

압수 이후 보관 및 이송 단계에서 연계관리를 위한 방법으로 압수대상 정보처리시스템 또는 저장매체에 표 8과 같은 서식의 부전지를 작성, 압수・수색대상자의 확인서명을 받고 있으며, 압수한 디지털기기 등은 각 품목별로 표 10과 같이 관리번호를 부여하고, 이를 인수・인계시 표 9와 같은 인수인계표를 작성하고 있다.

<표 8> 대검예규 제410호 별지서식 제3호

바코드 부착 란		
요청부서/주임검사		
제조사/모델명/제조번호		
시스템시간	년 월 일 시 분	
압수일시	년 월 일 시 분	
압수장소		
사용자		
피압수자		참관인
압수자		

<표 9> 대검예규 제410호 별지서식 제6호

압수품인수인계표

지원번호 :
증거번호 :

요청부서 :

바 코 드 부 착 란

인 계 자			인수인계	인 수 자		
소 속	성 명	서 명	시 간	소 속	성 명	서 명

<표 10> 대검예규 제410호 별지서식 제5호

압수품 관리표

지원번호 :
증거번호 :

바코드 부착 란

■ 기본정보

요청기관		압수·수색 담당	
요청부서		Imaging 담당	
주임검사		분석 담당	

■ 상세정보

압수품 정보			
유형	□Computer □HDD □USB Thumb Drive □기타( )		
제조사		모델명	
S/N			
용량			
상태	□ 양 호 □ 손 상 ( )		

① Computer 정보			
유형	□Desktop □Laptop □Server □기타 ( )		
CMOS 암호	□ 있 음 □ 없 음 암호 =		
시스템 시간		압수수색 당시시간	

실무 디지털 포렌식 절차에서 디지털 증거의 증거능력 확보를 위한 상기 문서서식들을 전자 문서화하여 디지털 증거 프로파일을 생성함으로써 서면에 의존하던 무결성 및 연계보관 취약성을 해결할 수 있다.

전자공증서비스를 제공하는 가상의 전자공증기관과 증거 무결성 확보를 위한 수사기관의 절차들은 전자공증기반 디지털 증거관리 모델에 유기적으로 결합될 수 있다.

4. 전자공증기반 디지털 증거관리 모델

가. 전자공증서비스의 4가지 제안

본 논문에서 제안한 전자공증기관은 아래의 4가지 전자공증서비스를 제공함으로 전자공증 디지털 증거관리 모델을 완성할 수 있다.

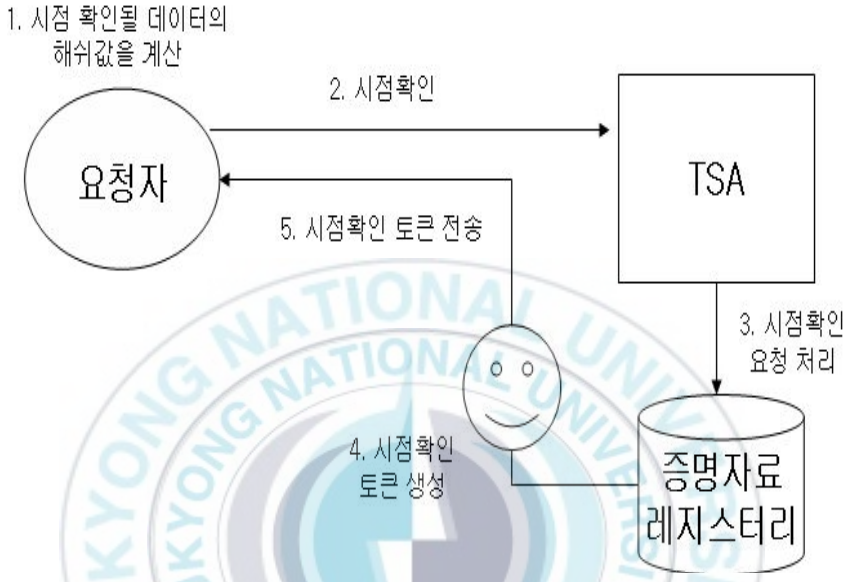
■ **시점확인서비스**

디지털 증거의 신빙성 확보를 연계보관관리(Chain of custody) 방안으로 시점확인서비스가 반드시 필요하다는 것은 익히 잘 알려져 있다. 시점확인서비스는 데이터가 특정 시점에 존재하였다는 것을 신뢰할 수 있는 제3의 기관 TTP(Trusted Third Party)[6]이 제공해주는 서비스로서 e-Business가 활성화되면서 그 필요성 부각되었다.

디지털 데이터와 특정 시점을 암호학적으로 연결시켜서 데이터의 존재시각과 데이터에 대한 변조 여부를 확인할 수 있는 시점토큰(Time stamp

6) TTP : 제3의 신뢰 기관, 사용자 인증, 부인 방지, 키 관리 등에서 당사자들로부터 신뢰를 얻고 중재, 인증, 증명, 관리 등을 하는 기관

token)[7]을 생성하는 서비스로서 디지털 데이터의 생성, 유통, 저장, 관리 과정에서 데이터의 존재 시점이나 그 내용이 변조되지 않았음을 입증한다. 시점확인서비스 절차는 그림 7과 같다.



<그림 7> 시점확인서비스 절차

전자인증에서 요청자가 전자문서의 해쉬값을 계산하여 공인인증기관으로 보내면 TSA에서 수신한 시간을 부여하여 시점 토큰을 발행하는 방식으로 시점확인서비스를 활용하고 있으나, 전자공증에서는 전자인증과는 달리 전자문서(데이터) 전체를 전자공증기관에 보내 시점확인을 요청하면, 증명서 내 시간 필드에 수신시간을 추가한 다음 전자공증기관이 디지털 서명하여 요청자에게 전송하는 방식을 사용한다.

전자공증기관이 실세계 공증에서의 확정일자 부여를 전자화한 것이라 할 수 있다.

---

7) 시점 토큰(time-stamp token) : 특정 시점에 데이터가 존재하였다는 증거를 제공해 주는 토큰으로 시점확인 요청자가 제출한 데이터의 해쉬값과 데이터의 인증기법이 결합되어 생성

■ **내용증명서비스**

보관된 전자문서의 진정성을 제3자의 입장에서 증명하는 서비스이다. 즉, 전자문서가 작성된 시점 이후 그 내용에 대한 변경이 없음과 전자문서의 소유자를 확인해 주는 서비스이다.

내용증명 서비스는 증명 의뢰단계와 증명 검증단계로 나누어진다. 먼저 증명 의뢰단계에서는 촉탁인이 전자문서에 디지털 서명을 한 후 전자공증기관으로 증명을 의뢰하면, 전자공증기관은 그 전자문서에 대한 디지털 서명을 검증하고, 이상이 없을 경우 증명서를 발행하게 된다.

전자공증기관은 증명서에 자신이 디지털 서명을 함으로써 증명서의 진정성을 보장한다. 촉탁인은 전자문서와 증명서를 함께 사용하여 거래자(검증자)에게 전송하게 되고, 거래자(검증자)는 증명서의 전자공증기관 디지털 서명을 검증하여 증명서의 진위를 확인한 다음, 전자문서의 메시지 요약값을 계산하여 증명서 내에 포함되어 있는 메시지 요약값과 비교함으로써 전자문서와 증명서의 동일함을 검증하게 된다.

전자공증기관에서 내용증명을 받은 전자문서는 원본성을 증명 받은 것으로 재사용 및 제3자 유통이 가능하게 되는 것이다.

■ **배달증명서비스**

실세계의 사실증명서비스 중 하나인 우체국의 내용증명서비스와 유사한 기능이다. 촉탁자가 내용문서 3부를 작성하여 우체국에 제출하면 1부는 우체국이 보관, 1부는 거래인(검증자)에게 발송, 1부는 촉탁자(발송자)에게 반환하는 것으로 배달을 증명하는 현실의 우편 내용증명서비스처럼 전자공증기관이 전자문서의 배달증명 요청을 접수하고 내용증명을 수행한 후 거래인(검증자)에게 전송을 하는 서비스이다.

■ 전자문서(데이터) 보관서비스

공증된 전자문서를 전자공증기관에서 안전하게 보관해 주는 서비스로, 사후에 이용자의 요청에 따라 보관한 전자문서에 대한 원본 등을 발급받을 수 있도록 하는 서비스이다. 분쟁 발생시를 대비한 증거력 확보 차원뿐만 아니라, 전자문서의 보관 인프라 구축이 미비한 기관을 위하여 전자문서 보관을 대행해 주는 서비스이다.

전자문서 보관 방법에는 원본 자체를 보관하는 방식과 전자문서의 해쉬값만 보관하는 방식이 있다. 각 방식은 장단점이 있으며, 디지털 포렌식 관점에서 본다면 수집되는 증거물의 데이터 크기에 따라 각각 적용하는 것도 고려될 수 있다.

나. 디지털 증거 프로파일 구조

디지털 증거의 무결성 확보는 어떤 디지털 데이터가 증거로서의 가치가 있다고 인정하여 대상이 되는 디지털 증거에 프로파일링(Profiling[8])을 할 때부터 시작된다. 증거로서의 허용성과 증명력의 판단은 최종적으로 법관에 있기에 디지털 증거 프로파일 생성시 디지털 증거를 구별하고 분류하는 작업은 매우 중요한 일이다.

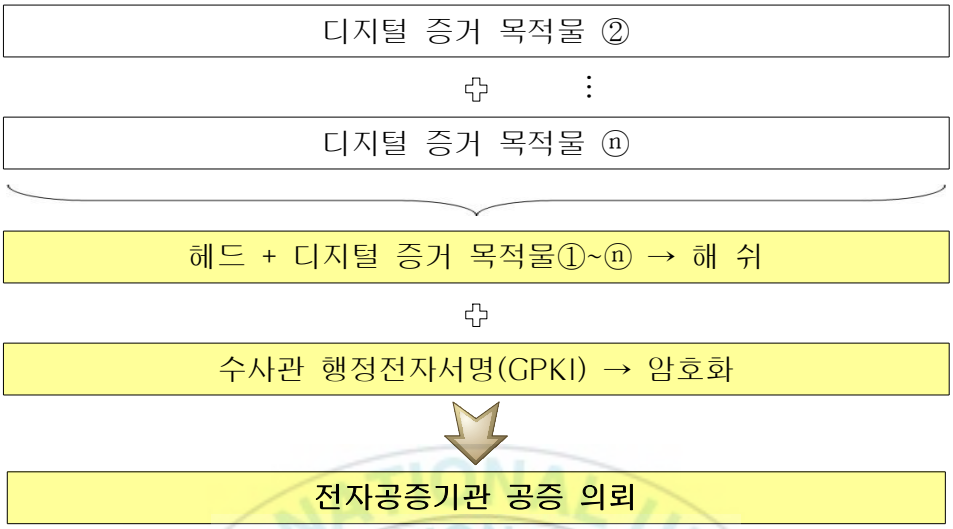
디지털 증거 목적물(Digital Evidence Object)은 압수품관리표(표 10)에 열거된 내용들이 모두 포함된 체 각각 디지털 증거 식별값(Label Value)을 부여하여 구분한다. 특히 매체 독립적인 디지털 증거들의 경우는 디지털 증거의 개체 식별을 위한 디지털 증거의 존재값(Real Value)과 식별값을 조합하는 방식으로 프로파일링을 실행한다[9].

8) Profiling : 경찰이 범죄자 검거를 위해 불심 검문·수색 등으로 증거를 수집, 압축해가는 과정

예로 휘발성 데이터가 존재하였음을 증명하기 위한 사진촬영이나, 매체 독립적 디지털 증거물 획득 과정의 영상촬영 등이 존재값으로 프로파일링 되어야 한다. 디지털 증거 프로파일 생성 구조에 포함될 내용은 그림 8과 같다.

번 호	내 용		구 분
1	사건번호, 사건개요		디지털 증거 요약 (헤드)
2	압수·수색 영장 정보		
3	압수·수색 착수 / 종료 날짜 시간		
4	디지털 증거물 수집 장소 / 방법		
5	디지털 증거 목적물 List 수		
6	수집된 자료 내용 요약		
7	입회인 또는 피의자 정보		
8	MoC(Match-on-Card) 고유번호		
9	확인서명(지문, 주민카드 정보 등)		
10	공증 의뢰자 정보(인계자)	배달 증명	
11	수신기관 정보(인수자)		

번 호	내 용		구 분
1	증거번호 식별값(Label Value)		디지털 증거 목적물 ① (내용)
2	압수품 유형(매체 OR 매체 독립적)		
3	제조사, S/N, 시간, 디스크 용량, 운영체제 및 버전, 기타 정보	매체 독립적 증거물 생략	
4	이미징 담당자		
5	이미징, 해쉬 도구 정보		
6	**이미징 해쉬값**		
7	이미징 파일 Bad Sector 정보		
8	매체 독립적인 경우 존재값		
9	데이터 소스(크기 제한 선택적 첨부)		



<그림 8> 디지털 증거 프로파일 구조

프로파일 중 헤드 부분의 입회인 또는 피의자로부터의 확인을 위한 방법으로 기존의 서명 등의 방식에서 벗어나 지문인식기와 같은 장비를 활용하여 확인서명을 전자화 한다. 디지털 증거물에 대한 압수, 수색에 대한 확인 절차임으로 지문 데이터베이스를 따로 구축할 필요는 없다.

그림 9와 같은 현재 개발 보급되고 있는 지문인식기술과 스마트카드를 접목한 MoC(Match-on-Card) 장비를 사용함으로써 전자여권, 전자운전면허증, 전자주민등록증 및 전자ID카드, 전자의료카드 등으로도 다양하게 개인의 서명을 대체 할 수 있다.

<그림 9> Match-on-Card 장비

Moc 장비별 고유값을 부여하고 지문 또는 주민등록, 운전면허카드 등의 데이터를 저장한다.

또한 헤드 부분에는 전자공증기관에 내용 증명과 동시에 배달증명서비스를 요청하기 위한 공증 의뢰처와 수신처의 정보도 포함된다.

각 매체별 첨부되어질 디지털 증거 목적물 내용 중 디지털 증거물 소스 보관 방법에는 원본 자체를 보관하는 방식과 전자문서의 해쉬값만 보관하는 방식이 있다. 각 방식은 장단점이 있지만, 매체 독립적 디지털 증거물의 경우는 원본 자체를 보관하여야 한다. 휘발성 데이터나 24시간 서비스하는 서버의 일부 데이터 등이 그것이다. 물론 증거물의 데이터 크기에 제한을 두어 일정한 데이터 크기를 넘어서는 경우는 해쉬값만 보관하여야 할 것이다. 또한 대용량 보조기억매체(하드디스크) 전체의 경우도 해쉬값만 보관하는 것이 효율적일 것이다.

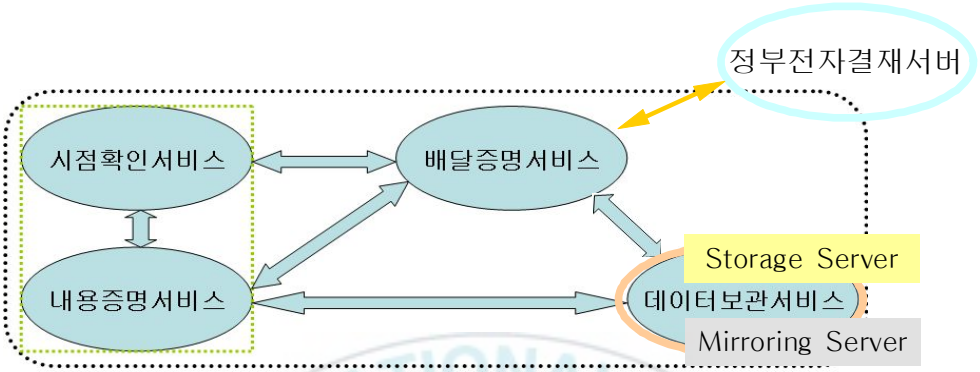
프로파일 구조를 요약하면 디지털 증거 요약 헤드부분은 다음에 기술한 증거 프로파일 관리에서 증명서 발행에 재 활용되어야할 디지털 증거물에 대한 전체 개요를 포함하는 부분이며, 디지털 증거 목적물들은 전자공증기관의 데이터 저장소에 보관되어 무결성 입증에 사용되어질 것이다.

헤드부분과 디지털 증거 목적물들을 해쉬 처리한 후 수사관의 전자서명으로 암호화한 후 전자공증기관에 공증 의뢰하게 된다.

다. 디지털 증거 프로파일 관리

디지털 증거 프로파일을 보관・관리하는 전자공증기관은 증거관리체계를 운영하는 기관에서 임의적 무단접근이 불가한 기관에 설치되어야 할 것이며, 직무분리원칙(Separation Duty Rule)이 적용되어야한다.

전자공증기관에서 디지털 증거 프로파일을 관리하는 구조는 그림 10처럼 4가지 서비스를 통하여 디지털 증거 프로파일을 관리하게 된다.



<그림 10> 디지털 증거 프로파일 관리

수사기관이 디지털 증거물에 대한 시점확인을 요청하면, 증명서(표 11)내 시간 필드에 수신시간을 추가(시점확인)한 다음 전자공증기관이 디지털 서명(진정성)하여 요청자에게 전송하는 방식으로 전자문서가 작성된 시점 이후 그 내용에 대한 변경이 없음과 디지털 증거물의 공증의뢰자를 확인해 주는 구조이다.

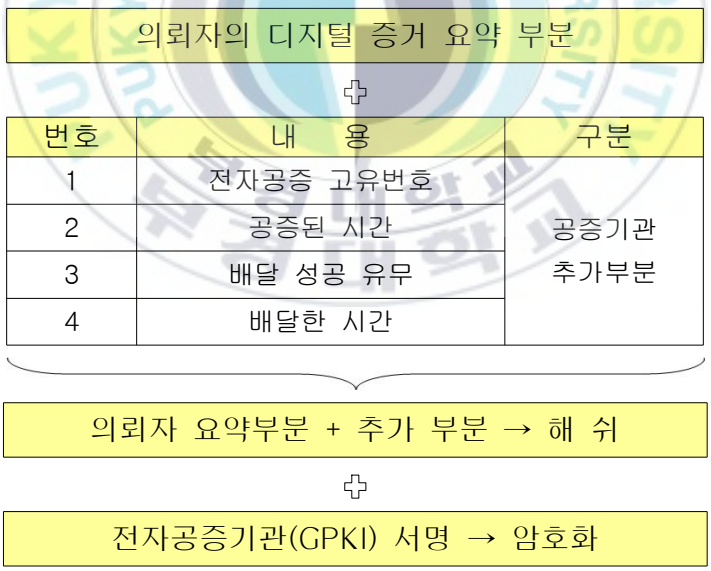
시점확인서비스와 내용증명서비스는 동시 상호 연동된다. 전자공증기관에서 내용증명을 받은 공증된 디지털 증거물에 대한 증명서는 원본성을 증명 받은 것으로 재사용 및 제3자 유통이 가능하게 되는 것으로 수사기관이 증거물 이송단계나 사건 이첩단계에서 직접 사용도 가능하며, 배달증명에 성공유무 확인을 위한 근거로도 활용될 수 있다.

배달증명서비스의 사용은 인수·인계시의 시간적 정확성이나 인계의 명확성을 위해 더욱 효율적이며, 증명서와 공증 의뢰한 디지털 증거물까지 배달될 수 있다. 수사기관은 디지털 증거물에 대한 인수·인계 단계에서

배달증명 요청을 하게 되고, 전자공증기관은 디지털 증거물에 대한 내용증명을 수행한 후 인수자, 인계자에게 배달증명서와 디지털 증거물을 각각 전송 하고, 전자공증기관 또한 배달증명서를 보관하게 된다. 본 연구에서 증명서와 디지털 증거물의 배달은 기존 정부전자결재시스템(온-나라시스템[9]) 연계함을 제안한다.

전자공증기관의 증명서 제안 구조는 그림 11과 같이 디지털 증거의 전체 개요를 포함하고 있는 의뢰자의 디지털 증거 헤드부분과 전자공증기관이 추가한 전자공증 고유번호, 공증된 시간, 배달한 시간, 배달 성공 유무 필드들로 구성된다.

증명서는 의뢰자의 디지털 증거 요약 부분과 공증기관의 추가필드를 해쉬 처리 후 전자공증기관의 행정전자서명으로 암호화한 후 의뢰자 또는 배달 대상에게 전송하게 된다.

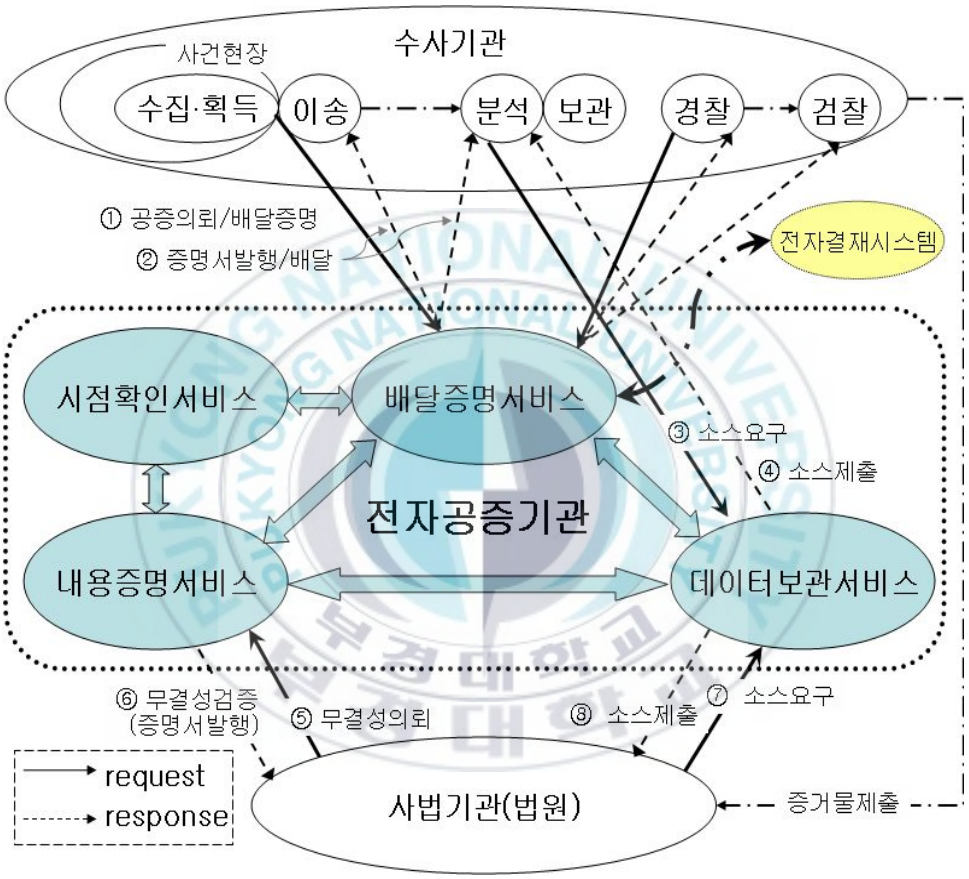


<그림 11> 전자공증기관의 증명서

9) 온-나라 시스템은 2006년부터 시행된 정부 각 부처의 업무를 체계적으로 분류하고 통합, 관리하는 혁신적인 업무관리 시스템

라. 전자공증기반 증거관리 모델 상호작용

그림 12는 수사기관과 사법기관 그리고 전자공증기관과의 상호 작용을 나타내고 있다.



<그림 12> 전자공증기반 증거 관리 모델

① 공증 의뢰/배달 증명

수사기관은 사건현장에 도착, 상기에서 열거한 순서대로 압수·수색 절차를 진행할 것이며, 전자문서로 된 자료확인서 표 7, 압수품관리표 표 10을 작성, 입회인 또는 피의자의 확인을 받음으로서 디지털 증거 수집시의

무결성을 확보할 수 있다.

여기서 입회인 또는 피의자의 확인은 지문과 같은 다양한 방법으로 대체될 수 있으며, 현장스케치를 위한 사진촬영 데이터들과 함께 디지털 증거 프로파일을 생성(그림 8), 행정전자서명으로 공증 의뢰를 요청한다. 이때, 디지털 증거물의 제한된 크기에 따라 데이터보관서비스를 위한 소스를 전송할지 결정한다. 휘발성 데이터나 매체 독립적(데이터베이스 일부) 데이터와 같은 디지털 증거물은 데이터보관서비스를 활용한다. 전자공증이 불가한 대용량 디스크와 같은 매체나 소스는 디스크 이미징한 결과에 대한 해쉬값만 전송하고 대검찰청 『디지털 증거수집 및 분석 규정』을 따른다.

공증의뢰와 동시에 이송을 담당하는 수사관은 분석센터에 도착할 때까지 디지털 증거물의 무결성의 입증과 연계관리(Chain of Custody)를 위해 배달증명서비스를 요청한다.

앞서 언급한 이송단계에서 가장 큰 문제점인 디지털 증거물의 내용에 대한 인수・인계의 문제점을 해결하는 중요한 서비스이다. 배달증명서비스를 통해 인수・인계표(표 9)와 같은 서식은 필요 없을 것이다.

전자공증기관은 배달증명서 1부는 인계자에게 전송하고, 1부는 전자공증기관이 보관, 또 1부는 인수자에게 전송하게 된다.

② 증명서 발행/배달

전자공증기관은 행정전자서명 검증 후 유효한 공증의뢰임을 확인하고, 증명서에 시간필드를 추가한 다음(시점확인서비스) 전자공증기관이 디지털 서명하여 공증의뢰자와 배달대상에게 전송한다.

그리고 공증의뢰 한 디지털 증거물들은 저장소로 이동되어 데이터보관서비스를 준비한다.

③, ④ 소스요구 / 제출

디지털 증거물 분석센터에서는 전자공증기관에 분석과정에 필요한 디지털 증거 목적물(Digital Evidence Object)에 대한 소스 요구를 할 수 있으며, 전자공증기관은 데이터보관서비스를 통해 소스를 전송한다. 디지털 증거물에 대한 분석이 이뤄지고 최종 디지털 증거물을 사법기관에 제출하게 되는데, 여기에서 송치 배달증명과정이 필요하다. 이 과정은 현재 우리 형사소송구조에서 볼 수 있는 과정으로 검찰이 직접 현장을 지휘한 사건이거나 디지털 증거 조사·분석자이면 생략되겠지만, 경찰이 주관한 사건이라면 검찰에 송치하는 과정이 있게 된다. 이때 검찰에서는 경찰의 수집·이송·조사·분석의 과정의 무결성을 확인하기 위해 내용증명서비스와 데이터보관서비스를 재사용할 수도 있으며, 또한 이때 경찰이 인수·인계과정의 무결성 확보와 연계관리를 위해 검찰에 대해 배달증명서비스를 전자공증기관에 요청함으로써 검찰의 재확인을 줄일 수 있다.

마지막으로 전자공증기관과 사법기관과의 상호작용이다. 사법기관이 무결성을 의뢰하고 전자공증기관이 검증한다던지 공판정에 현출될 디지털 증거물이 있을 경우 소스를 요구하고 제출하는 등이 그것이다.

⑤, ⑥단계에서 무결성이 증명되면 사법기관은 ⑦, ⑧단계에서 전자공증기관에게 소스 제출을 요구할 수 있다.

이처럼 전자공증기관의 유기적 상호작용을 통해 각 수사기관간의 연계보관관리, 무결성 입증의 어려움을 덜고 신용성의 정황적 보장으로 법적효력을 기할 수 있다.

그러나 매체 독립적이지 않은 디지털 증거나 하드디스크와 같은 직접증거(매체 자체가 증거물)에 대해서는 표 8이나 표 9, 표 10과 같은 기존 실무의 규정에 따른 절차가 동반되어야 할 것이다.

Ⅳ. 디지털 증거관리 모델 발전 방향

1. 전자공증기관의 선정과 민간 디지털 포렌식의 고려

전자공증기관과의 디지털 증거 프로파일 생성 후 전송 구조는 공개키 기반 구조를 제안하였다. PKI 인증기반은 대상 사용자 및 서비스의 성격에 따라 두 가지로 구분할 수 있다. 즉 인터넷상의 불특정 다수 사용자들에게 보안서비스를 제공하는 체계와 인트라넷의 특정 단체에 소속된 사용자들에게 보안서비스를 제공하는 체계이다. 우리나라 인증 기반은 지식경제부의 NPKI(National PKI)와 행정안전부의 GPKI(Government PKI)로 구분할 수 있다.

NPKI는 1999년 2월에 제정되었고 최근에 개정된 『전자서명법』에 근거를 두고 있으며 한국정보보호진흥원(KISA)이 최상위 인증기관(Root CA)의 역할을 맡고 있다. 여기에 6개의 공인인증기관(CA)이 하위 인증기관으로서 개인과 법인에게 인증서를 발급하고 있다. 주로 인터넷상의 전자상거래를 대상으로 보안서비스를 제공하고 있다.

이에 반해 GPKI는 2001년 7월에 제정된 『전자정부구현을 위한 행정업무 등의 전자화촉진에 관한 법률』에 근거를 두고 정부전자관인 인증관리센터가 최상위 인증기관(Root CA) 역할을 맡고 있으며, 5개의 중앙사무관장기관(CA)이 하위 인증기관으로서 가입기관(행정기관 및 공무원)에게 인증서를 발급하고 있다. 주로 인트라넷상의 행정업무를 대상으로 보안서비스를 제공하고 있다. 표 11은 두 PKI기반 인증체계를 비교한 것이다.

<표 11> NPKI와 GPKI의 비교

구 분	NPKI (National Public Key Infrastructure, 국가 공개키 기반구조)	GPKI (Government Public Key Infrastructure, 정부 공개키 기반구조)
운영주체 (ROOT CA)	지식경제부**(한국정보보호진흥원, KISA)** 운영 전자인증 체제	행정안전부**(정부전산정보관리소, GCC)** 운영 전자인증 체제
사 용 처	일반 국민 사용(전자상거래)	공무원 사용(행정업무)
공인인증 기관(CA)	금융결제원, 한국정보인증, 한국증권전산, 한국전자인증, 한국전산원, 한국무역정보통신(6개)	국회, 헌법재판소, 중앙선거관리위원회, 행정자치부, 대법원(5개)

전자공증기관의 주체는 어디가 되어야 할 것인가에 대해서는 본 연구가 수사기관의 형사소송법적 관점에서 제안한 바, 정부전산정보관리소가 공인인증기관과 전자공증기관으로서의 역할을 담당하여야 한다. 기존의 인프라를 그대로 활용할 수 있도록 공인인증기관과 전자공증기관은 일원화 되어야 할 것이다. 또한 전자서명법이나 전자정부법은 개정이 이뤄져야 할 것이다.

그러나 디지털 포렌식 기술의 활용도는 비단 수사기관의 형사소송법적 문제만이 아니다. 일반 기업체 및 금융회사 등의 민간분야에서도 디지털 포렌식 기술의 수요가 급격히 증가하는 추세이며, 그 예로 보험사기 및 인터넷 뱅킹 피해보상에 대한 민사법적 증거 자료 수집이나 기업 내부 정보유출 방지, 회계 감사 등의 내부 보안 강화 및 유지에 활용되고 있다.

미국의 경우는 사베인-옥슬리법(SOX[10])의 결과로 2006. 12. 1 발효된

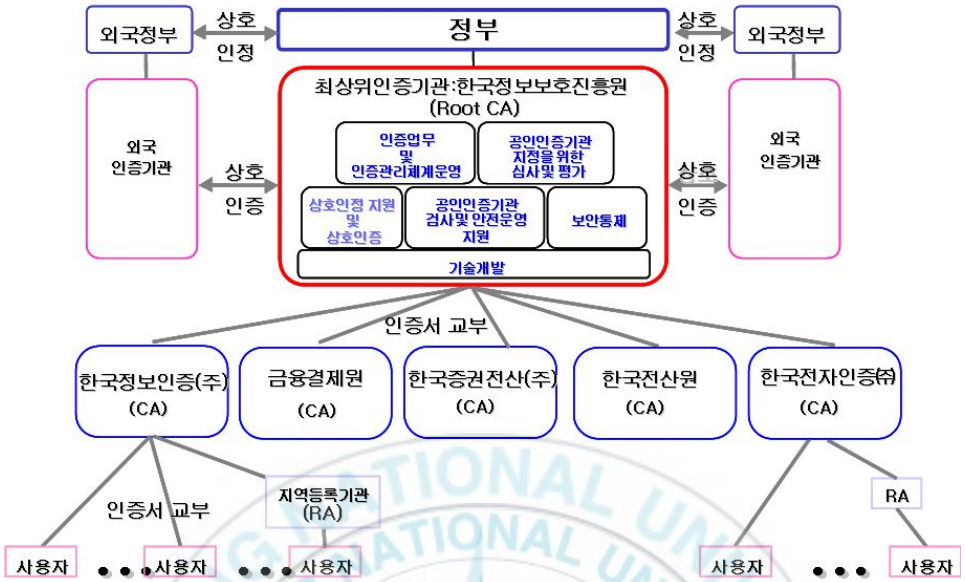
10) 기업회계 및 재무보고의 투명성/정확성 고양을 목적으로 하여, 기업지배구조(Corporate Governance)의 본연의 모습과 감사제도를 근본적으로 개혁함과 동시에 투자가에 대한 기업경영자의 책임과 의무, 벌칙을 규정한 미국연방법

e-Discovery[11]는 기업들에게 외부로 나가는 모든 정보를 기록하게 해 기업들의 정보보호를 강화하도록 했다. 이 법안에 따라 소송에 처한 모든 기업은 이메일을 비롯한 기업 내 모든 전자정보를 저장 및 검색, 소송개시일 120일 이내에 제출해야만 한다. 민·형사 소송에서 디지털 증거 제출이 의무화됨으로서 기업 내부 통제 중요성이 요구되어지고 전자적인 증거의 발견에 더욱 주목하고 있다.

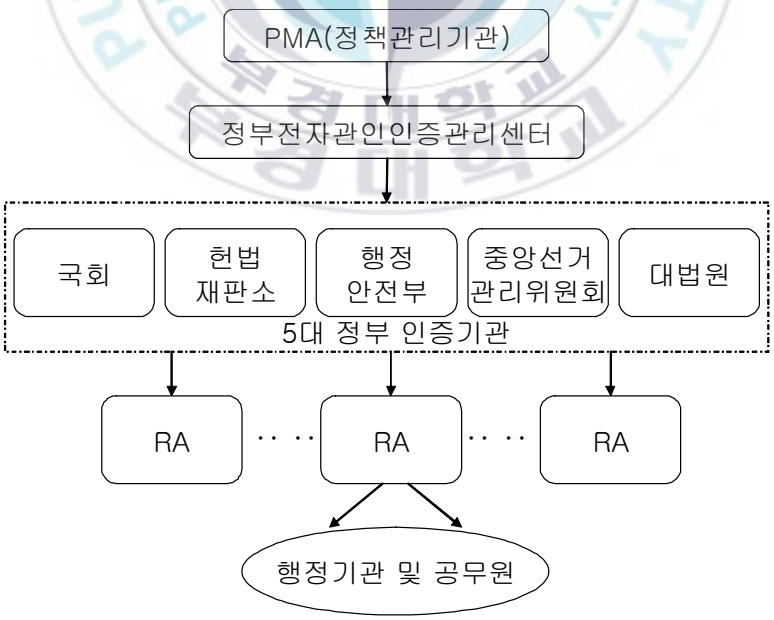
예로, 2006년 마이크로소프트는 Z4 테크놀로지와의 특허침해소송에서 패소, 250억원을 배상했다. 마이크로소프트 역시, Z4 테크놀로지로부터 이메일과 데이터베이스 증거개시요청(Discovery)을 받았으나 자료를 제출하지 못했다. e-Discovery 시행이 본격화 되면서 민간 포렌식 서비스의 수요가 확대된 것이다. 매출 10억불 이상의 미국 기업들은 연평균 140여건의 소송이 발생되고 있다. 미국의 e-Discovery는 미국 기업과 특허법이나 기타 민사소송에 휘말릴 수 있는 국내 기업들에게 아주 중요하고 큰 의미를 갖는다. 이를 위해서 미국과 관계된 국내 기업은 전자정보관리정책을 세우고 전자정보를 인덱싱하여 빠른 시간 내 검색할 수 있는 시스템구축이 필요할 뿐만 아니라, 국내 기업의 글로벌화 및 국제화에 따른 디지털 포렌식 분야 기술 개발이 절대적인 시점이다[10]. 이처럼 민간분야도 전자공증기반의 디지털 포렌식 증거관리를 위한 전자공증기관이 반드시 존재하여야 할 것이다. 따라서 국가적 수사기관의 형사소송법적 관점에서의 전자공증기관은 정부전산정보관리소를 제안하며, 민간분야의 디지털 포렌식 증거관리를 위한 전자공증기관으로는 한국정보보호진흥원을 제안한다. 그림 13, 그림 14에서 보듯 인증업무 및 인증관리체계운영, 공인인증기관 검사 및 보안통제 등 총체적 역할을 담당하는 Root CA가 전자공증기관을 담당해야 한다.

---

11) e-Discovery : 2007년 1월 미국 연방 민사소송규칙이 개정되어 증거의 발견과 공개원칙인 Discovery에 전자적 데이터를 포함시킴. ※ 미국 소송절차는 우리나라 민사절차와 달리 소송에 처하게 된 당사자가 소송과 관련하여 자신이 무엇을 가지고 있는지 발견하여 상대방에게 공개



<그림 13> NPKI 전자서명 인증관리 체계도



<그림 14> GPKI 전자서명 인증관리 체계도

2. 증거 프로파일 전송 방법의 유·무선 통합 환경 제공

유선 환경이 제공되는 사건현장에서는 기존 보급되어 있는 PKI 기반 환경을 그대로 적용할 수 있다. 하지만 사건현장이 유선 인터넷이 지원되지 않는 곳이라면 디지털 전자공증을 위해서 무선 인터넷 환경을 고려해야할 것이다. 즉, 무선 PKI(Wireless Public Key Infrastructure) 기반을 지원해야하는 것이다. 유선 환경에서는 SSL(Secure Sockets Layer), TLS(Transport Layer Security) 전송 프로토콜을 사용하는데 반해, 무선 환경에서는 Wireless TLS 전송 프로토콜을 사용한다. 또한 무선 단말기의 제한된 성능으로 인해 사용되는 암호화 알고리즘에 차이가 난다. 유선 PKI 기반에서 사용하는 RSA의 키 길이가 1024비트인데 반해 WPKI에서 사용하는 ECDSA[12]는 약 160비트로, RSA의 보안강도를 가지면서도 보다 빠른 연산이 가능하기 때문이다. 현재 한국정보보호진흥원에서는 무선 인터넷 PKI 구축을 위해 무선 PKI 모델, 기술규격 및 표준개발, 운용기술 및 평가기술을 개발하여, 무선 PKI의 최상위기관으로 Root CA의 구축하고 실질심사에 필요한 평가기준 및 지침도 완성하였다. 현재 공인인증기관(CA)들 중 한국증권전산, 한국정보인증, 금융결제원에서 무선 PKI 인증서비스를 실시하고 있으며, 2000년부터 이동통신사별 독자적인 WPKI 모듈을 개발 Mobile Commerce(Finance, Shopping, Payment, Mobile-Ad 등)를 중심으로 모바일 뱅킹 및 증권서비스를 시작하였다. SK Telecom의 MONETA Service, 대우증권의 무선공인인증을 통한 증권거래, LG Telecome BankOn 등이 그 사례이다. 전자공증기관의 전자공증서비스 또한 유·무선 통합 환경이 반드시 제공되어야 할 것이다[11].

---

12) ECDSA는 ANSI의 미 은행 연합(American Bankers Association)에 의해 X9.62로 표준화 되어 현재 널리 쓰이고 있는 전자 서명. ECDSA는 기존의 미 연방 표준인 DSA(Digital Signature Algorithm) 전자서명을 타원곡선을 이용한 전자서명 알고리즘으로 변형한 것

Ⅴ. 결론

국내 사법 제도가 미국식 공판 중심주의로 변화하고, 한미 자유무역협정(FTA)의 결과로 증거 중심의 재판으로 바뀌고 있는 시점에 아직 기존의 디지털 포렌식의 연구방향은 디지털 증거의 수집, 추출, 분석, 복원 등 수사기관의 입장에서 보다 활발히 연구되어지고 있는 실정에서 디지털 포렌식의 궁극적인 목표인 제출된 증거가 법원의 공판과정에서 법적 증거능력을 인정받는 것이라는 점에 초점을 두고 본 연구를 시작하였다.

디지털 증거물을 수집·보존하는데서 그치는 것이 아니라, 수집·보존된 자료를 법적『증거』가 될 수 있도록 하는 『증거화』 작업에 더욱 큰 의미가 있기 때문이다. 디지털 증거 내용물은 원칙적으로 전문법칙(hearsay is no evidence)의 적용을 받아 전문증거이다.

증거능력이 없는 디지털 증거를 현행법의 전문법칙의 예외로 적용시키기 위해서 디지털 증거는 신용성의 정황적 보장과 필요성이 반드시 갖춰져야 한다. 이를 위해 증거물의 수집, 운송, 보관에 있어 의심이 없을 정도의 신뢰성을 확보하는 것이 무엇보다 중요하다. 따라서 디지털 포렌식의 기본원칙인 정당성의 원칙, 재현의 원칙, 연계보관관리의 원칙, 무결성의 원칙을 반드시 준수해야한다. 하지만 증거물의 수집단계에서부터 무결성의 원칙은 깨질 수가 있음을 예를 들어 설명하였다. 법원 관점에서는 수사관 또한 절대 신뢰할 있는 자가 아니라는 사실을 잘 인지하여야한다. 이송·보관단계에서도 마찬가지로 실무현장의 매체 중심적 사고로 접근하여 불가시성의 디지털 증거에 대한 연계보관관리를 문서에 의존하는 것에 대한 문제점을 제시하였다. 또한 분석단계에서도 실무현장의 디지털 증거 수집과 분석이 이원화로 인해 무결성이 훼손될 수 있음을 예로 설명하였다.

이와 같은 이유로 디지털 증거물은 최종 법원에 제출될 때까지 디지털 포렌식의 기본원칙을 준수하기 위한 현행 형사소송법에 근거하여 증거능력 보장을 위한 디지털 증거관리 모델이 필요했다. 특히, 매체 독립적 증거에 대한 증거능력보장이 절대적으로 필요하여, 전자공증기반 디지털 증거관리 모델을 제안하였다. 신뢰할 수 있는 제3의 기관을 통해 공증이라는 현실세계의 제도를 활용함으로써 사실행위, 법률행위의 증명으로 소송법 상의 추정적 효력을 끌어내고자 하였다.

전자공증기관의 전자공증서비스를 4가지로 제안하면서 각 서비스별 수사기관 사법기관간의 상호작용 모델을 설계하였으며, 디지털증거 프로파일에 대한 생성과 관리 구조의 예를 들었다. 또한 디지털증거 프로파일을 보관·관리하는 전자공증기관은 증거관리체계를 운영하는 기관에서 임의적 무단접근이 불가한 기관에 설치되어야 하며, 직무분리원칙(Separation Duty Rule)이 적용되어야 함을 법원의 관점에서 제안하였다. 더불어 미국의 e-Discovery 제도를 대비, 미국 기업과 특허법이나 기타 민사소송에 휘말릴 수 있는 국내 기업들에게 디지털 포렌식 환경이 절대적인 시점에 민간분야의 디지털 포렌식 증거관리를 위한 전자공증기관으로는 한국정보보호진흥원을 제안하는 한편, 국가적 수사기관의 형사소송법적 관점에서의 전자공증기관은 정부전산정보관리소를 제안하였다.

마지막으로 다양한 디지털 포렌식 환경을 고려하여 전자공증기관의 전자공증서비스는 유·무선 통합 환경을 바탕으로 가용성과 기밀성을 함께 지속연구 발전시켜야 할 것이다.

[참 고 문 헌]

[1] “형사소송법”, 일부개정 2007. 12. 21, 법률 제8730호

[2] 이진태, "사이버범죄관련 증거의 증거조사 방법과 증거능력", 중앙대학교 법과대학, 2003

[3] 김형성, 김학신 "Computer Forensics의 법적 문제 연구", 성균관대학교 비교법연구소 성균관법학 제18권 제3호, 2006

[4] 김소정, 임종인, 오일석 "사이버범죄의 암호화된 증거 수집에 관한 연구", 정보보호학회지 제13권 제5호, 2003

[5] 한국정보통신기술협회, "컴퓨터 포렌식 가이드라인"

[6] 박상균, "디지털 증거 분석 절차", 경찰청 사이버테러대응센터

[7] 김현상, 최재민, 이상진, 임종인 "무결성을 보장하는 디지털 증거 수집 절차", 한국정보보호 학회 하계 학술대회, 2005

[8] 구영진 "디지털 서명 기반의 전자공증에 관한 연구", 석사학위 논문, 성균관대학교 정보통신대학원, 2005

[9] 김종섭 "디지털증거의 신뢰성 보증 모델", 박사학위 논문, 경기대학교 대학원, 2003

[10] 노환철 "미국 기업과 관계된 분쟁과 E-Discovery", 정보보호21C 통권 제89호, 2008

[11] 한국정보보호진흥원, "무선 PKI 구축 현황과 전망" (http://www.kisa.or.kr)

감사의 글

교단에 서고 싶은 오래된 나의 꿈을 위해 시작한 2003년도 대학원 생활이 어느 듯 6년이 되어버렸습니다. 발령이 잦은 직장생활로 인해 휴학과 복학을 반복하며 힘겹게 여기까지 올 수 있었던 것은 정말 많은 분의 도움이 있어 가능했습니다. 입학부터 도움을 주신 故 박지환 교수님, 이글을 쓰고 있는 순간까지도 저에게 길을 안내해주신 신상욱 교수님, 그리고 본 논문이 완성될 때까지 노고를 아끼지 않으시고 조언을 해주신 이경현 교수님, 송하주 교수님께 진심으로 감사를 드립니다.

또한 항상 저를 미소 짓게 하며, 힘을 주시는 연구실의 태훈씨, 수완이, 도희, 태식이, 태림이 이 모든 분께 깊은 감사를 드립니다. 비록 많은 시간을 함께하지는 못했지만 쌓은 정은 정말 컸습니다.

그리고 직장생활과 학업을 병행할 수 있도록 도와준 아내의 응원은 무엇보다 큰 힘이 아니었나 싶습니다. 해양경찰이라는 특수한 근무여건으로 교대근무를 하며, 비번 날 학교를 찾는 나를 대신해 혜랑이, 종윤이를 잘 키워주었기에 마음 놓고 학교에서 학업을 할 수 있었습니다.

끝으로 언제나 제가 가는 길이 옳은 길이기를 기도해 주시는 사랑하는 부모님과 이 기쁨을 나누고자 합니다.

2008년 여름

김 재 성