

디지털자료 파기¹⁾명령 집행절차에 대한 연구

김 태 성,[†] 이 상 진[‡]
고려대학교 정보보호대학원

A Study on the Digital Material Disposal Order System

Tae-Sung Kim,[†] Sang-Jin Lee[‡]
Center for information Security Technology(CIST), Korea University

요 약

소송을 위해 사법기관으로 이관된 디지털자료는 법원의 기록물관리규정에 명시된 절차에 따라 파기하며, 피의자의 혐의를 입증하기 위해 수사기관이 수집한 디지털자료는 대검예규 제 876호(디지털 증거의 수집·분석 및 관리규정) 또는 경찰청 훈령 제 766호(디지털 증거 수집 및 처리 등에 관한 규칙)에 의거 명시된 절차에 따라 파기한다. 사법기관은 형사소송과 민사소송 확정판결 시 관계법령을 근거로 하여 소송의 쟁점이 되는 디지털자료에 대해 파기명령한다. 하지만 사법기관의 파기명령 시 이를 집행할 수 있는 구체적인 절차가 존재하지 않으며 유일하게 제시된 저작권법 시행령에는 집행주체를 전문성이 검증된 전문집행관이 아닌 관계공무원으로 명시하였고 파기절차나 방법을 디지털자료의 특성을 고려하여 제시하지 않아 사법기관이 파기명령 한 디지털자료 파기 시 문제가 발생하고 있다. 따라서 본 논문에서는 사법기관의 디지털자료 파기명령을 실효적으로 집행할 수 있는 디지털자료 파기명령집행절차를 제시한다.

ABSTRACT

Digital material transferred to the court for litigation shall be disposed by the procedure in the court records management regulations and the digital material collected by the investigator in order to prove the suspect's allegation shall be disposed by the Supreme Public Prosecutor's Regulation No.876(digital material's regulation of collection, examine and management). the court ordered the disposal of digital material that is the subject of litigation based on the related laws when criminal lawsuits and civil lawsuits are finalized. however, there is no specific procedure to enforce the disposal order of the court, and the enforcement order stipulates that the enforcement agent is not a professional officer who has proven expertise but a related public official. there is a problem in the enforcement of digital material that the court ordered to disposal because it is not specified. therefore, this is paper proposes a procedure for effectively enforcing the court's order to revoke digital material.

Keywords: Disposal Order of Court, Procedure to Enforce the Disposal, Disposal of Digital Material

1. 서 론

우리사회에서 디지털기가 없는 생활은 상상하기 어려우며 복잡한 업무에서부터 간단한 오락에 이르기 까지 다양하게 사용되고 있다. 버클리 대학의 한 보고서에 의하면 전 세계적으로 생성되는 정보의 약

92% 이상이 디지털 형태인 것으로 나타나고 있다 [1]. 우리생활의 일거수일투족이 디지털형태로 기록되고 있으며 이런 디지털형태의 자료는 범죄 혐의를 입증하는 결정적인 역할을 하고 있다. 이에 우리나라에서는 2016.5.29.부로 형사소송법을 개정하여 피

Received(05. 12. 2017), Modified(06. 26. 2017),
Accepted(06. 26. 2017)

[†] 주저자, tsung84@hanmail.net

[‡] 교신저자, sangjin@korea.ac.kr(Corresponding author)

1) 경찰청 훈령 제 776호(2015.5.22.), 대검찰청 예규 876호(2016.12.26.), 형사소송 및 민사소송 판례에서 디지털자료 삭제, 폐기라는 단어를 혼용하여 사용하나 본 논문에서는 디지털자료의 재사용을 방지한다는 의미인 "파기"로 표현한다.

의자가 법정에서 e-mail이나 컴퓨터 파일 등 디지털자료의 작성을 부인하더라도 디지털포렌식 조사관 등의 증언을 통해 진성성립이 인정되면 증거능력을 부여하였다[2]. 하지만 위·변조가 용이한 디지털자료의 특징으로 인해 소송에서 결정적인 역할을 하는 디지털자료가 법정에서 증거로 채택되지 않는 상황²⁾이 발생하기도 한다. 따라서 디지털자료를 법정에서 증거로 인정받기 위한 디지털자료의 수집·분석·관리 연구는 지속적으로 이루어져 왔다. 하지만 이와 반대로 사법기관의 디지털자료 파기명령을 집행하는 파기절차에 대한 연구는 없다.

사법기관은 확정판결 시 다양한 종류의 디지털자료에 대해 파기명령을 하고 있다. 형사소송에서는 형사소송법 제 48조(물수의 대상과 추정) 3항³⁾에 의거 범죄행위로 인하여 생성된 디지털자료에 대해 몰수(파기)를 명령하고 있으며, 민사소송에서는 부정경쟁방지 및 영업비밀보호에 관한 법률 4조(부정경쟁행위 등의 금지청구권 등) 2항⁴⁾에 의거 부정경쟁행위를 조성하는 디지털자료에 대해 파기명령 하고 있다. 또한 저작권위반 디지털자료에 대해서는 저작권법 제 123조(침해의 정지 등 청구) 2항⁵⁾, 133조(불법복제물의 수거·파기 및 삭제) 1항⁶⁾을 근거로 파기명령 하며, 불법적으로 수집된 개인정보는 개인정보보호법 제 36조(개인정보의 정정·삭제) 1항⁷⁾에 의거 삭제명령한다. 그리고 명예훼손이나 사생활침해는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 44조 2의(정보의 삭제요청 등) 1항⁸⁾을 근거로

삭제명령한다. 하지만 사법기관의 파기(삭제)명령을 집행하기 위한 구체적인 집행절차는 없으며 디지털자료 파기와 관련된 유일한 법령인 저작권법 시행령에도 집행을 전문집행관이 아닌 단순관계공무원으로 명시해 놓았으며 파기절차와 방법을 디지털자료의 특성을 고려하여 제시하지 않아 파기에 여러 문제가 발생하고 있다. 사법기관에서 파기명령 한 디지털자료의 파기 시 디지털자료가 완전삭제⁹⁾되지 않는다면 복제·복사가 용이한 디지털자료의 특징으로 인해 제 2·3의 범죄 및 피해가 발생가능하다.

사법기관의 명령에 의한 파기가 실효적으로 이루어지기 위해서는 소송기간 중 쟁점디지털자료에 대한 보존절차가 필요하며 파기 시에는 디지털자료의 재사용을 방지할 수 있는 완전삭제가 이루어져야 한다. 특히 부정경쟁방지 및 영업기밀 유출 소송의 경우 기업에 막대한 영향을 미치는 영업기밀이 디지털자료 형태로 유지되며 소송기간이 긴 특징¹⁰⁾을 고려할 때 소송기간 중 소송당사자가 보유하고 있는 쟁점디지털자료의 원본유지는 디지털자료의 완전삭제를 통해 추가피해를 방지할 수 있는 관건이 될 것이다.

본 논문에서는 현재 이루어지고 있는 디지털자료 관리를 알아보고 법원의 파기명령을 실효적으로 집행할 수 있는 디지털자료 관리절차를 증거보존제¹¹⁾를 개선·적용시켜 제안한다. 또한 제안에 따른 소송대상자의 역할 그리고 디지털자료의 재사용을 방지할 수 있는 디지털자료 절차를 제안한다.

II. 관련연구 및 현행 디지털자료 관리절차/명령 판례

2.1 디지털자료 관련연구

일반전자기록물 연구 또는 형사소송을 위해 수집

- 2) 대표적인 사례로 증권당 압수수색 사건이 있으며, 압수된 저장매체의 재복제시 피 압수자의 미 참여로 혐의입증에 결정적인 역할을 하게 될 재 복제 디지털자료의 분석내용을 사법기관에서 증거로 채택하지 않음.
- 3) 문서, 도화, 전자기록 등 특수매체기록 또는 유가증권의 일부가 몰수에 해당하는 때에는 그 부분을 파기할 수 있음.
- 4) 부정경쟁행위나 정당하지 않은 수입을 올리게 하는 물건에 대해 파기청구 할 수 있음.
- 5) 저작권 그밖에 이 법에 따라 보호되는 권리를 가진 자는 침해행위에 의하여 만들어진 물건의 파기나 그 밖의 필요한 조치를 청구할 수 있음.
- 6) 불법복제물 또는 저작물 등의 기술적 보호조치를 무력하게 하기 위하여 제작된 기기·장치·정보 및 프로그램을 발견한 때에는 관계공무원으로 하여금 수거·파기 또는 삭제하게 할 수 있음.
- 7) 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있음.
- 8) 정보통신망을 통하여 일반인에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가

침해된 경우 그 침해를 받는 자는 해당정보를 처리한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재를 요청할 수 있음.

- 9) 논리적으로 삭제하는 방법으로 데이터가 저장된 저장매체의 영역을 반복적으로 덮어쓰음으로서 데이터를 재사용할 수 없도록 만드는 방법[3].
- 10) 영업기밀유출사건의 경우 영업비밀에 대한 개념이 추상적이고 포괄적이기 때문에 영업비밀인지 여부를 판단하는데 6개월 이상 걸릴 때가 많다[4].
- 11) 수사단계에서 디지털자료의 취약성에 기초한 긴급처분 성격을 갖으며 소송대상자로 하여금 쟁점 디지털자료에 대해 삭제하는 것을 금지하는 제도[5].

된 디지털자료 중 소송과 관련 없는 자료의 연구는 쉽게 찾아볼 수 있다. 하지만 사법기관의 명령에 의한 디지털자료 연구는 전무하다.

일반전자기록물 에 대한 연구로는 임태훈의 연구가 있으며 정보시스템 운영 효율성과 관리비용 절감을 위한 불필요 데이터 연구가 있다[6]. 이 연구는 대상이 일반전자기록물이라는 한계를 가지고 있다. 탁희성은 형사소송을 위해 수집한 디지털자료의 보존 및 관리연구를 진행하였으며, 관리의 일부분으로 디지털자료를 하는 절차를 제시하였다[7]. 형사소송 시 디지털자료 관리를 위해 디지털자료보관소를 제안한 연구로는 김준한의 연구가 있으며 디지털자료의 무결성 보장을 위해 디지털자료를 보관하는 인증기관 도입을 제시하였다[8]. 외국의 연구로는 Christian Zoubek의 연구가 있으며 형사소송을 위해 수집된 디지털자료 중 개인정보와 관련된 자료의 선별 방법을 제시하였고 선별 후 디지털자료의 무결성 유지를 위하여 블록단위의 해쉬값 사용을 제안하였다[9].

현재까지 연구는 일반전자기록물 또는 형사소송을 위해 수집된 디지털자료의 무결성 유지 연구가 주로 진행되었다. 하지만 소송종료 후 민사소송을 포함하여 사법기관의 명령을 집행할 수 있는 구체적인 절차와 방법을 제시한 절차 연구는 없다. 따라서 본 논문에서는 디지털자료의 특성을 고려한 구체적인 절차 및 방법에 대해서 제안한다.

2.2 현행 디지털자료관리 방법

디지털자료가 수집되는 형태는 형사소송의 경우 사건특성 및 유형에 따라 수사기관이 저장매체를 압수, 이미징, 파일복사 한다. 수집한 디지털자료는 원본훼손 방지를 위해 사본생성 후 분석하고 혐의사실에 유효한 증거발견 시 사건을 계속 진행하기 위해 검찰에 송치한다. 하지만 사건을 계속 진행할 수 없는 경우 미제편철하며, 내사중지 사건의 경우 디지털자료는 환부 또는 디지털증거분석관이 삭제한다[10]. 검찰은 분석된 디지털자료가 혐의사실 증명가능 판단 시 디지털자료 원본과 분석결과물을 사법기관에 제출하여 기소하며 추후 소송의 디지털자료 재분석소요 또는 추가소송을 위해 디지털자료 사본을 수사통합업무관리시스템에 등록·관리한다.

수사통합업무관리시스템에 등록·관리하는 디지털자료는 해당사건 주임검사의 요청 또는 압수전담검사 촉탁 시 한다. 집행관은 대검찰청 디지털포렌식 전문

가 양성과정 교육이수, 디지털포렌식 수사실무 3개월 이상 경력자, 국내·외 컴퓨터 관련 교육과정 이수를 통해 디지털포렌식 지식이 충분한 수사관이 파기한다. 파기 시는 파기방법, 파기날짜 등을 기록하는 디지털자료 파기(촉탁) 회보서와 디지털자료 파기확인서를 작성하여 디지털자료 파기과정을 기록한다[11].

민사소송은 소송당사자가 양측 법률대리인에게 소송쟁점 디지털자료를 제출하며 제출방법은 저장매체 제출, 저장매체의 쟁점 디지털파일 선별제출 형태이다. 법률대리인은 제출받은 디지털자료를 검토 후 사법기관에 제출하여 소송을 진행한다.

형사소송과 민사소송 동일하게 소송을 위해 사법기관으로 제출된 디지털자료는 소송종료 후 법원의 기록물관리규칙에 의거 파기하며, 사법기관은 확정판결 시 관계법령에 의거 쟁점 디지털자료에 대해 파기명령한다. 하지만 관련법령에 따른 디지털자료 파기명령 시 이를 집행할 수 있는 절차는 저작권 위반 디지털자료를 파기할 수 있는 절차 이외는 존재하지 않는다.

2.3 디지털자료 파기명령 판례

사법기관은 확정판결 시 관련법에 따라 다양한 디지털자료에 대해 파기명령한다. 형사소송의 경우 형사소송법 제 48조 3항에 의거 범죄행위 과정 중 생성된 디지털자료에 대해 파기명령하며 관련 판례로는 특수강도·강간 및 상해의 범죄과정 중 생성된 피해자의 사진파일에 대한 파기명령[12], 강간·치상의 범죄과정 중 생성되어 범죄자의 디지털 카메라에 저장되어 있는 피해자의 나체사진 파일 파기명령[13] 등이 있다.

민사소송에서는 부정경쟁방지 및 영업비밀보호에 관한 법률에 의거 크롤링 행위의 부정경쟁행위로 크롤링 행위를 하는 무단복제 콘텐츠 파기명령[14], 저작권침해로 도서관 책 대여를 위한 서비스 프로그램인 책벌레 프로그램 파기명령[15], 인터넷 키워드 서비스 방법에 사용된 접속시스템 및 그 방법이 특허권을 침해하여 그 시스템의 사용금지 청구와 침해조성물(시스템)의 파기명령[16], 신문사의 뉴스 기사를 무단 복제·복사를 하여 피고가 운영하는 사이트에 게재하여 저작권을 침해하였으며 피고의 저장매체에 보관하고 있는 뉴스기사 파기명령[17], 인터넷 커뮤니케이션 프로그램 무단복제·배포에 따른 저작권 침해

로 소스프로그램에 대한 파기명령[18] 등 다양한 유형의 디지털자료에 대해 파기명령을 하고 있다.

III. 디지털자료 파기절차 도입의 필요성

사법기관에 제출되어 소송의 결과를 좌우하는 디지털자료는 은폐나 조작이 이루어져서는 안 된다. 하지만 디지털자료는 언제든지 쉽게 변경 및 수정이 가능한 상태로 존재한다[19]. 이에 디지털자료의 은폐나 조작을 방지하기 위하여 미국과 우리나라에서는 관련제도를 입법화 하였다.

e-discovery가 적용되는 미국에서는 litigation hold 제도를 통해 소송에 쟁점이 되는 디지털자료의 원본보존 의무를 입법화 하여 법정에 제출되는 디지털자료의 은폐나 조작을 방지한다. 또한 쟁점 디지털자료의 은폐나 조작정황 발견 시 소송당사자에게 불리한 추정을 하여 패소판결하기도 한다¹²⁾. 우리나라도 민사소송법 제 8조 증거보전제도에 의거 소송계속 전 또는 소송계속 중 특정 증거를 미리 조사하여 쟁점 디지털자료의 변조나 위조를 방지 한다¹³⁾. 하지만 미국의 litigation hold 제도와 우리나라의 증거보전제도의 목적은 사법기관에 제출되며 소송의 결과에 영향을 미치는 디지털자료의 은폐·조작 방지를 목적으로 하며 쟁점디지털자료가 사법기관에 제출된 이후 소송당사자가 보유하고 있는 쟁점디지털자료의 원본에 대해서는 어떠한 강제력도 행사하지 않는다.

디지털자료는 은폐·조작 및 복제·복사가 용이하다. 소송당사자는 소송기간 중 디지털자료의 특성을 활용하여 확정판결 후에도 쟁점디지털자료의 재사용을 가능하게 할 수 있으며, 이것은 제 2·3의 범죄 및 피해를 발생하게 한다. 특히 부정경쟁방지 및 영업비밀 보호 소송의 경우 영업비밀에 대한 개념이 추상적이고 포괄적이기 때문에 소송기간이 6개월 이상 지속될 때가 많으며 5년 이상[4][20] 지속되기도 한다. 이런 경우 소송당사자가 가지고 있는 쟁점디지털자료에 대한 명확한 선정 및 관리가 이루어지지 않는다면

확정판결 후 쟁점디지털자료가 재사용될 우려가 있다¹⁴⁾.

사법기관에서는 형사소송법 제48조 3항, 부정경쟁방지 및 영업비밀보호에 관한 법률 4조, 저작권법 123조 2항, 133조 1항, 개인정보보호법 제36조 1항 등을 근거로 하여 다양한 디지털자료에 대해 파기명령을 하고 있다. 하지만 저작권과 관련된 디지털자료 파기명령을 제외하면 사법기관의 파기명령을 집행할 수 있는 제도는 없으며 저작권위반 디지털자료의 파기제도 또한 파기절차 및 방법에 있어서 개선해야 될 부분이 많이 있다. 따라서 이번 장에서는 재사용이 용이한 디지털자료의 대표적인 특징을 간단히 알아보고 법원의 파기명령을 집행할 수 있는 유일한 관련법인 저작권법 시행령의 개선요소 확인을 통해 사법기관의 다양한 파기명령에 적용시킬 수 있는 일관된 파기절차 도입의 필요성에 대해 알아본다.

3.1 디지털자료의 특징

3.1.1 원본과 사본의 동일성

디지털자료는 유체물이 아니고 각종 디지털매체에 저장된 혹은 전송 중인 정보 자체이다[21]. 아날로그 방식으로 정보를 복사하는 경우 복사본의 S/N(신호/잡음)비가 감소하여 복사본 구분이 가능하지만 [22] 디지털자료는 신호의 유무만 검출하여 디지털 신호를 다시 만들어 기록하므로 원본과 데이터자체가 동일하다. 원본과 사본의 동일성 검증은 비트열로 비교해보면 알 수 있지만 실무적으로는 해쉬값 비교를 통해서도 충분히 확인할 수 있다. 따라서 원본의 동일성을 입증하기 위해서 원본의 해쉬값을 계산하여 안전하게 보관한 후 사본의 해쉬값을 계산하여 비교하는 절차를 거치면 된다. 이러한 방식으로 주어진 디지털자료의 위조, 변조, 조작을 확인하는 것이 사용되고 있다[23].

3.1.2 재생산의 용이성

복사된 디지털자료는 원본과 동일한 가치를 지니며 이진정보를 처리할 수 있는 저장매체라면 어느 것

12) 듀퐁 vs 코오롱의 영업기밀 침해 손해배상청구소송이 대표적 사례이다. 법원은 코오롱 측에서 쟁점이 되는 디지털자료를 삭제하여 litigation hold를 위반한 것으로 간주하여 불리한 추정을 하였고 코오롱 측에 제재를 가함.

13) 민사소송법 제 375조(증거보전의 요건) 법원은 미리 증거조사를 하지 아니하면 그 증거를 사용하기 곤란할 사정이 있다고 인정한 때에는 당사자의 신청에 따라 증거조사를 할 수 있다.

14) 실례로 디지털자료의 재사용을 소송의 중요요소로 판단하고 불법계입물이 대량으로 복제되어 유통될 것을 고려하여 관계공무원의 강제집행 및 관련법령의 입법이 헌법에 위법되지 않음을 판결한 사례가 있다[16].

이라도 복사된 디지털자료를 저장할 수 있다[22]. 이것은 전송과정에서 정보의 변질이 거의 발생하지 않는 특징과 결합되어 디지털자료 재생산이 용이한 특징을 알 수 있다. 다양한 저장매체에 저장 가능한 특징은 디지털자료의 파괴 시 복사를 통해 다양한 저장매체에 은닉되어 있을 수 있는 디지털자료 파괴 필요성을 의미하며 삭제는 하더라도 운영체제의 특징에 따라 파일을 복구할 수 있기 때문에 디지털자료 파괴 시 재사용이 불가능하도록 완전삭제를 해야 한다.

3.1.3 대량성

저장기술의 발달로 대량의 정보가 저장매체에 저장되고 고도화된 정보통신망을 통해 대량으로 유통되고 있는 디지털자료의 특징을 “대량성”이라고 한다 [24]. 디지털자료를 복사, 저장, 전송하는 재생산의 용이성은 많은 사본의 생성을 가능하게 하였고 저장기술의 발전은 아주 작은 저장매체에도 방대한 분량의 정보를 저장할 수 있게 되었다[25]. 이런 특징을 고려한 파괴를 위해선 쟁점디지털자료가 재생산 및 정보통신망을 통해 유통되기 전 디지털자료에 대한 보전절차가 필요하다.

3.2 저작권법 시행령의 개선 필요성

현재 사법기관의 디지털자료 파괴명령을 적용시킬 수 있는 제도는 저작권법 시행령을 제외하면 전무하며, 저작권법 시행령 또한 개선소요를 가지고 있다. 저작권법 시행령 제 69조를 관련내용은 표 1과 같다.

저작권법 시행령은 집행주체를 단순히 관계공무원으로 명시해 놓아 검찰에서의 디지털자료 파괴 집행주체인 디지털포렌식 전문가 양성과정 교육이수, 포렌식 수사실무를 수행한 경력자, 포렌식 관련 지식이 충분하다고 인정되는 수사관과 대비되며 집행절차에 있어서도 단순히 관계공무원이 집행권한을 표시하는 증표를 디지털자료 소유주에게 보여주고 중발생한 특이사항을 수거·파괴·삭제 대장에 기록하는 절차만을 제시하고 있다. 이것은 디지털자료의 복제·복사 및 은폐·조작의 특성을 고려하지 않은 절차이며 쟁점디지털자료의 식별, 보존, 파괴방법을 제시하지 않아 쟁점디지털자료의 재사용을 가능하게 한다.

사법기관에서 파괴명령 한 디지털자료는 어떠한

Table 1. Article 69 of the Enforcement Decree of Copyright Act

Enforcement Decree of Copyright Act	
Article 69 Procedures and methods of collection, disposal and deletion	① The officials involved in collecting, disposing, and deleting must have a certificate indication their authority and show it to the person concerned ② When a public official collects, destroy or deletes illegal copy, it shall give the owner or occupier a certificate of collection in accordance with the provisions of the Ordinance of the Ministry of Culture and Sports, and record the contents in the collection and deletion records. ③ Illegal copies may be discarded after 3 months from the data of collection unless the parties have objected. However equipment and programs designed to defeat technical protection measures are disposed within 6 months from the date of collection.

방법으로도 재사용 되어서는 안 된다. 하지만 디지털자료의 특성을 고려하지 않은 파괴절차 및 적절하지 않은 파괴방법은 파괴 후 쟁점디지털자료의 카빙 등의 방법을 통해 쟁점 디지털자료의 복구 및 재사용을 가능하게 한다[15].

형사소송을 위해 수집된 디지털자료는 대검예규 제 876호(2016.12.26.)에 의거 파괴되며, 형사소송·민사소송을 위해 사법기관에 제출된 디지털자료는 법원의 기록물관리규칙 제2625호(2015.10.29.)에 의거 파괴된다. 사법기관은 확정판결 시 다양한 디지털자료에 대해 파괴명령 하지만 이를 집행할 수 있는 절차는 저작권법 시행령을 제외하면 존재하지 않으며 저작권법 시행령도 파괴절차 및 파괴방법에 있어서 보완해야 될 부분이 있다.

15) 한국과학기술원 데이터베이스연구실 문송천 교수 및 권영철 연구원 팀이 중고 하드디스크 구입 후 전문 데이터복구 프로그램을 통해 포맷/삭제된 하드디스크의 파일 중 일부를 복구·재사용할 수 있음을 증명하였다[26].

IV. 제안하는 파기명령집행 절차

파기가 실효적으로 이루어지기 위해서는 쟁점디지털자료의 명확한 식별이 이루어져야하며, 명확한 식별 후에는 확정판결 전까지 소송당사자가 보유하고 있는 쟁점디지털자료 원본에 대한 보전이 이루어져야 한다. 특히 디지털자료를 담고 있는 저장매체의 일관된 압수절차가 없는 민사소송에서 원본보전은 파기를 위해 중요한 역할을 할 것이다. 또한 확정판결 후 파기 시에는 파기명령 된 디지털자료의 재사용을 방지할 수 있는 완전삭제의 방법으로 파기가 이루어져야 한다.

본 논문에서는 민사소송에 적용시킬 수 있는 파기명령집행절차를 제안하며, 파기명령집행절차는 사법기관의 판단을 통해 소송 전 또는 계속 중 쟁점 디지털자료를 조사하는 증거보전제도를 개선·적용시켜 쟁점디지털자료를 보전명령 하는 디지털자료 관리절차를 제안하고, 제안하는 디지털자료 관리절차에 따라 쟁점 디지털자료를 식별·보전하는 소송당사자의 역할 그리고 파기명령 된 디지털자료의 재사용을 방지할 수 있는 파기절차를 제안한다.

4.1 디지털자료 관리절차

소송당사자는 소송 전 또는 과정 중 사법기관에 쟁점 디지털자료에 대한 증거보전신청을 한다. 사법기관은 판단 후 소송당사자에게 쟁점 디지털자료 관리(Holding) 명령하며, 관리명령은 음란물, 이적표 현물, 개인정보, 영업기밀 등 파기명령이 합리적으로 예상되는 사이버금제품목과 사법기관의 판단 하에 이루어진다. 소송 당사자는 상호협의 하에 관리명령 받은 쟁점디지털자료의 범위와 종류, 제출방법 등을 결정한다. 협의를 통해 결정된 디지털자료 목록정보는 디지털자료 패키지(해쉬값, 파일명, 용량 등)를 기재하여 법원에 제출한다. 쟁점 디지털자료의 관리의 확정판결 전까지 사이버금제품목 사용금지를 의미하는 봉인조치 하며 영업기밀 자료와 같이 소송기간 중 사용이 불가피한 쟁점디지털자료에 대해선 적절한 관리를 한다. 소송당사자에 의한 보전이 적절하지 않다고 판단될 경우 공신력 있는 제 3기관인 디지털자료보관소에 임치¹⁶⁾할 수 있다. 소송기간 중 소송에 필요

한 디지털자료는 소송당사자가 직접 사법기관에 제출하거나 디지털자료보관소에 보관된 디지털자료의 경우 디지털자료 전자서명 및 디지털자료 패키지(해쉬값, 파일명, 용량 등)를 사법기관에 제출한다. 사법기관은 기존에 보관하고 있던 디지털자료 패키지와 소송당사자 또는 디지털자료보관소에서 제출받은 패키지와 비교하여 디지털자료의 무결성을 검증한다. 증거보전제도를 개선·적용시킨 디지털자료 관리절차를 그림 1과 같이 도식화 할 수 있다.

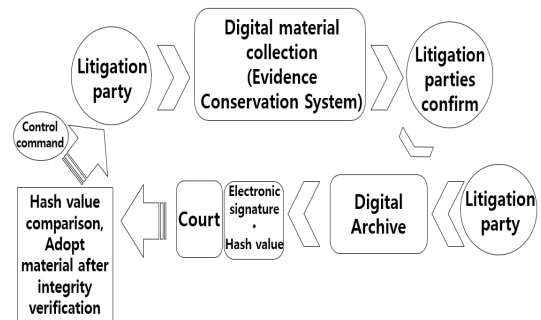


Fig. 1. Improvement of evidence preservation system applied digital material management procedure

4.2 소송당사자의 역할

소송당사자의 역할은 소송당사자간 상호협의 된 쟁점 디지털자료를 식별(Identification), 수집(Preservation), 제작(Producing) 절차와 사법기관의 관리명령을 이행하는 디지털자료 관리(Holding)절차가 있다.

식별절차는 법정에서 보전명령을 한 디지털자료의 예상되는 물리적/논리적 위치를 파악하는 과정이다. 최근에는 스마트기구나 태블릿 PC 등의 사용이 증가하여 잠재적 자료의 범위가 매우 넓기 때문에 디지털자료 식별범위를 소송당사자간에 명확히 해야 한다 [28].

수집절차는 디지털자료의 무결성을 훼손하지 않고 저장매체에서 디지털자료를 수집하는 과정이며 잠재적인 자료까지 수집한다. 무결성을 보장하기 위해 검증된 도구를 사용하며 원본을 복제 또는 이미징하거나 별도의 논리적 디지털자료로 만들어 수집한다 [29].

제작절차는 상호간에 검토가 용이한 PDF 형태의 자료와 메타데이터(파일명, 파일 생성시간, 파일크

16) 임치제도란 시스템 유지보수, 기술이전 등의 목적으로 상호간 합의하에 제 3의 기관에 디지털자료를 보관하고 일정한 조건이 발생시 해당자에게 교부해주는 제도[27].

기)가 손상되지 않은 원본 이미징 형태의 자료로 제작한다. 제작이 완료된 디지털자료는 소송당사자간 열람 후 디지털자료보관소에 임치한다.

관리절차는 인적자원관리와 디지털자료 관리로 구분한다. 인적자원관리는 관리명령 된 디지털자료를 사용하는 인원에 대한 교육이며, 관리명령 된 디지털자료의 삭제·복사·수정의 금지 등에 관한 교육이다. 또한 디지털자료에 대한 관리책임자를 두어 디지털자료를 관리하고 접근이 허용되는 인원을 제한하며 허용되는 인원에 대해서는 보안교육을 실시한다. 디지털자료 관리는 특정디지털자료가 쟁점디지털자료라는 것을 식별할 수 있도록 디지털자료에 표시하여 다른 자료와 구분하며 비밀번호를 설정하여 관리한다. 디지털자료가 저장되어있는 디지털기기를 별도의 공간에 위치시킴과 디지털자료 사용 시는 사용기록을 남긴다.

4.3 파기집행절차

디지털자료의 파기란 이용가치를 상실한 정보시스템의 데이터나 저장매체의 데이터를 사용할 수 없도록 하는 작업이다. 파기 후 어떠한 방법으로도 파기 전 자료의 내용을 확인할 수 없어야 하며 디지털자료의 파기절차를 사전준비단계, 집행단계, 결과보고단계로 나누어 제안한다.

4.3.1 사전준비(Preparation) 단계

사법기관의 디지털자료 파기명령 시 파기를 위한 사전준비를 한다. 저장매체 유형에 따라 파기방법을 결정하고 운영체제가 있는 플래시메모리, 하드디스크는 탑재된 운영체제의 종류 및 버전을 확인하여 파기 준비 한다. 디지털기기 수량을 확인하여 적정집행관을 선정하며 집행관별로 역할과 책임을 나눈다. 파기 시 디지털기기 소유주의 업무지장 범위를 판단하여 파기 장소와 날짜를 정하며 파기대상 디지털자료의 중요도나 민감도에 따라 적절한 보안통제 수준을 결정한다[30].

4.3.2 파기집행(Execution) 단계

저장매체는 과도한 파기를 방지하며 파기 후 저장매체의 재사용을 가능하게하기 위해 포렌식도구를 활용한 선별파기를 하며 선별파기는 파기명령 된 디지

탈자료의 식별 및 덮어쓰기로 이루어진다.

디지털자료 식별은 디지털자료보관소에서 보관하고 있는 파기명령 된 디지털자료의 해쉬값을 활용하여 식별하며 해쉬값 비교 또는 해쉬값 유사도 비교를 통해 식별한다[31]. 식별된 자료는 국가 및 학계에서 제정하거나 발표한 완전삭제 알고리즘을 활용하여 메타데이터영역과 데이터영역을 덮어쓰기 한다.

4.3.3 결과통보(Reporting) 단계

파기완료시 집행관은 파기된 디지털자료의 해쉬값, 디지털기기 종류 및 수량, 저장매체 종류 및 용량, 디지털자료 은닉여부, 사용한 덮어쓰기 알고리즘 및 덮어쓴 횟수 등을 기록한 집행결과보고서를 작성하여 디지털자료 소유주의 서명을 받는다. 또한 향후 집행관의 잘못된 집행으로 문제가 발생할 것을 대비해 파기 전 과정을 영상촬영하며 촬영한 영상은 집행결과보고서와 함께 법원과 소송당사자에게 제출한다. 디지털자료 파기절차의 사전준비, 파기, 결과통보의 단계를 그림 2와 같이 나타낼 수 있다[30].

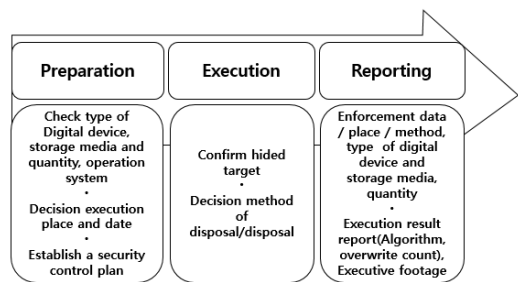


Fig. 2. Digital material Disposal Enforcement Procedures

V. 결 론

디지털자료를 법정에서 증거로 인정받기 위한 디지털증거관리의 연계성(Chain of Custody) 연구는 지속적으로 이루어져 왔다. 하지만 반대로 사법기관의 파기명령을 집행하는 디지털자료 집행관련연구는 전무하다. 기술의 발전으로 디지털기기는 우리 일상생활의 일부분이 되었고 디지털기기가 생산하는 디지털자료는 개인 또는 기업의 재산을 포함할 수 있으며 개인의 사생활을 포함하는 자료가 될 수 있다. 하지만 사법기관의 디지털자료 파기명령에도 적절한 파

기가 이루어지지 않는다면 디지털자료의 특징으로 인해 파괴명령 된 디지털자료의 재사용이 가능하며 이것은 제2·3의 피해 및 범죄를 일으킨다.

디지털자료는 은닉, 변조, 유출이 용이하다. 디지털자료가 스테가노그래피, 비 할당영역에의 저장 등을 통해 은닉된다면 파괴대상 디지털자료의 해쉬값 비교를 통한 식별이 제한될 것이다. 따라서 집행관은 파괴 시 파괴명령 된 디지털자료의 은닉, 변조를 탐지하는 대응책을 가지고 있어야 한다. 추가로 외부저장매체, 클라우드, e-mail, 메신저 등의 방법을 통해 디지털자료의 유출을 방지할 수 있는 입법적인 조치도 필요하다. 본 논문에서 제시하는 디지털자료 관리절차, 소송당사자의 역할, 파괴절차는 파괴명령 된 디지털자료의 재사용을 방지하며 동시에 제2·3의 피해 및 범죄를 예방할 수 있을 것이며 이를 위해서는 디지털자료 파괴절차에 대한 명확한 입법도 진행되어야 할 것이다.

References

- [1] Peter Lyman and Hal R. Varian, "How Much Storage is Enough?," ACM Queue vol.1, no.4 June 2003.
- [2] Myung-Sun Roh, "Interpretation of Article 313 of the amended Criminal Procedure Act and improvement of Legislation," Legal Association, Law 65(9), pp.5-38, 2016.
- [3] Forte, D. and Power, R., "A tour through the realm of anti-forensics," Computer Fraud & Security, Vol.2007, Issue.6, pp.18-20, 2007.
- [4] Kwang-Min Park and Hae-Sung Yun, "Examination of Trade Secret concept in Unfair Competition Prevention and Trade Secret Protection Act," Sungkyunkwan University Law No. 18 Chapter 1, pp 413-436, 2006.
- [5] Yoon-jae Lee, "Duties of Cooperation in the Execution of a Digital Warrant Seized Warrant," Criminal Law Research 2(2), pp.302-332. 2013.
- [6] Tae-Hoon Lim, Ji-Su Seok and Sun-Young Kim, "A Basic Study for Guidelines for Data Disposal", Information Management Research 41(4) pp.165-186. 2010.
- [7] Hee-Sung Tak, "Improvement of the Legal System on the Preservation and Treatment of Digital Evidence as Confidential Material," Korea Criminal Policy Institute, 2011.12.
- [8] Jun-Han Kim, "A Study On The Procedure for ensuring the integrity of reliable digital evidence," Journal of Security Engineering 10(5), pp.527-538, 2013.
- [9] Christian Zoubek, "Selective deletion of non-relevant data," DFRWS 2017 Europe, pp. S92-S98, March 2017.
- [10] Hyeon-Hee Chung, "Management plan considering life cycle of digital evidence," Graduate School of Information Security, Korea University Digital Forensic Department, Dec, 2014.
- [11] Office Regulation No. 876, "Regulation for collection, analysis and management of digital evidence Revised Supreme Prosecutors," Dec 2016.
- [12] Jeonju Provincial Court GounSan Support Decision 2007 Gyeonggi 72th Edition "violation of the Act on Punishment of sexual Violence Crimes and Protection of Victims," Sep 2007.
- [13] Ulsan District Court Sentence 2012 kyodon 543, 2012 kyodo 31 (merger), "violation of the law on punishment of sexual violence crime and protection of victims, etc.," Jun 2013.
- [14] Seoul District Court, "sentenced to 2015 junior 517982 (unfair competition act)," Feb 2016.
- [15] Seoul Central District Court, "Decision 2014 Decision 557464 Judgment (Compensation for damages)," Dec. 2015.
- [16] Seoul District Court, "Decision 2006 Decision 14061 (Prohibition of infringement of patent rights)," Aug. 2007.
- [17] Seoul High Court, "Decision 2006

- Decision 2355(Prohibition of copyright infringement)," Nov. 2006.
- [18] The Constitutional Court, "2000 The second edition of Article 12, No. 74, 880 [Constitution]," Oct. 2002.
- [19] Alan M. Gahtan, "Electronic Evidence," Carswell, Thompson Professional Publishing p32-35, 1999.
- [20] [Http://www.yonhapnews.co.kr/](http://www.yonhapnews.co.kr/) Kolon, sued DuPont for 6 years.. Aramid freely produced (2 in total).
- [21] Hey-wuk Won, "Evidence of Evidence and Evidence for Computer Related Evidence," Research on Investigation, 2000.6.
- [22] Sang-yeon Lee, "Digital evidence and its evidence ability and evidence investigation," The Law Society 53rd, 2011.
- [23] Supreme Court, "Decision of Supreme Court Decision of the Whang Jae San," July 2013.
- [24] Bum-sik Kim, "Study on the improvement of search and seizure of digital evidence in police investigate," Law Research Institute Center for International Area Studies Hankuk University of Foreign Studies, 38(4) pp. 169-190, 2014.
- [25] Byung-gon Jung, "A Study on the Collection and Evidence of Digital Evidence," Chosun University Graduate School of Law, Fed 2012.
- [26] Song-Chun Moon and Young-cheolk Won, "Personal Information Domestic Outflow Serious," Journal of the Korean Society for Information Science and Technology, 22(5), pp.42-43, May 2004.
- [27] Seung-woo Son, "Technology Escrows," Chung-Ang Law Association, pp.721-745, Aug 2007.
- [28] <http://www.edrm.net/frameworks-and-standards/edrm-model/identification>
- [29] <http://www.edrm.net/frameworks-and-standards/edrm-model/collection/>
- [30] Chang-hoon Lee, "Study on Digital Investigation Model for Privacy Acts in Korea," Journal of the Korean Institute of Navigation Engineers 15(6), Dec 2011.
- [31] Sang-soo Cho and Yong-tae Sin, "In the process of ensuring the integrity of digital evidence," Information Communication 39(2), 2012.

 <저자소개>



김 태 성 (Tae-sung Kim) 학생회원
 2007년 3월: 공군사관학교 산업공학과 졸업
 2016년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
 <관심분야> 디지털포렌식, 정보보호



이 상 진 (Sang-jin Lee) 종신회원
 1987년 3월: 고려대학교 수학과(학사)
 1989년 3월: 고려대학교 수학과(석사)
 1994년 3월: 고려대학교 수학과(박사)
 1989년~1999년: ETRI 선임연구원
 2001년 9월~현재: 고려대학교 정보보호대학원 교수
 2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
 <관심분야> 디지털포렌식, 스테가노그래피, 해시함수