# 디지털증거의 법적 효력에 대한 연구

함영옥*, 이재성*, 신용태*
*숭실대학교 컴퓨터학과
e-mail: yoham@cherry.ssu.ac.kr

# A Study on Legal Validity with Digital Evidence

Young-Ock Ham*, Jae-Sung Lee*, Yong-Tae Shin*
*School of Computing Soongsil University

요 약

컴퓨터 및 인터넷의 사용이 증가하여 일반인들 생활에 많은 부분을 차지함에 따라 범죄의 단서가 컴퓨터에 저장되어 있는 경우가 늘고 있으며, 컴퓨터 및 인터넷 자체가 새로운 범죄의 대상이 되기도 한다. 이러한 컴퓨터 및 저장매체에 저장되어 있는 증거는 기존의 증거와 구분하여 디지털 증거라 한다. 디지털 증거는 기존의 증거와는 달리 일반적으로 내용의 변경 및 훼손이 쉬우며, 관리자의 별다른 인식 없이도 수시로 또는 자동적으로 변경될 수도 있고, 또 그 흔적이 전혀 남지 않을 수도 있다. 기래서 디지털 증거의 증거능력을 인정하는 문제에 있어서 아날로그 증거와는 달리 무결성의 법적, 기술적 보장이 필요하다. 이에 본 논문에서는 디지털 증거가 법적인 증거능력을 갖기 위한 조건을 '일심회' 사건의 예로 알아본다.

## 1. 서론

최근 현대사회는 정보화 시회로 수많은 디지털 기기가 사용되고 있다. 컴퓨터, 휴대폰, PDA 등 많은 디지털 기기가 있고, 이들은 인터넷을 통해 서로 연결되어 있다. 뿐만 아니라, 인터넷 뱅킹이나 인터넷 쇼핑과 같이 재화의 이전도 디지털 기기와 인터넷으로 이루어지고 있는 실정이다. 따라서 범죄의 경우에도 디지털 기기와 인터넷을 사용하여 이루어지고, 그 수치도 증가하고 있다. 이러한 디지털 기기에 저장되거나 사용하여 범죄가 이루어졌을 때, 범죄의 증거로서 확보되었을 때 디지털 증거라 한다. 그러므로 디지털 증거(Digital Evidence)란 범죄가 행해졌다는 것을 입증할 수 있거나 범죄와 피해자 또는 범죄와 가해자 사이의 연결고리를 제공할 수 있는 모든 디지털 데이터를 말하는 것으로 이해할 수 있다. 여기에서 디지털 데이터란 컴퓨터상애 있는 데이터뿐만 아니라 이진 형태로 저장되거나 전송될 수 있는 모든 텍스트, 이미지, 오디오 및 비디오 데이터 등을 포함한다.

이러한 디지털 증거는 이진화되어 저장되거나 전송 중인 데이터로 그 특성상 복제가 쉬울 뿐만 아니라 원본과 사본의 구별이 어렵고, 조작, 변경, 삭데 등이 용이하다. 또한 매체 독립적으로 비가시적이라는 특성을 지니고 있으므로 디지털 증거를 법정에 제출하기 위해서는 가시적인 형태로 변환하여 제출하여야 한다. 그러므로 컴퓨터나 다른 디지털 저장장치로부터 수집된 디지털 증거가 법적 효력을 가지기 위해서는 진정성, 무결성, 원본성이 보장되어야 한다. [1]

## 2. 법적효력을 갖기 위한 디지털 포렌식 적용

### 2.1 디지털 증거의 특성

디지털 증거는 물증과 같은 전통적인 아날로그 증거와는 다른 특성을 갖는다. 전통적인 아날로그 증거는 그 증거의 수집·이송·분석·보관·제출·검증 등 절차를 진행함에 있어 증거의 진정성 문제를 육안으로 식별 가능하기 때문에 증거의 진정성 확보방안이 증거로서의 가치문제보다 덜 중요하게 다루어졌다고 할 수 있다. 그런데 디지털 증거는 실질적으로 어떤 '유체물'이 아니고 각종 디지털 매체에 저장된 혹은 전송중인 '정보' 자체다. 그러므로 우리 육안으로 관찰할 수 없을 뿐 아니라(불가시성), 0, 1의 조합으로 이루어진 이진성, 매체의 용량이 커지므로 증거확보에 절대적 시간과 노력을 요하는 방대성, 전원이 끊어지면 데이터가 날아가는 휘발성의 특징이 있다. 디지털 증거는 매체와 독립된 혹은 중립된 정보 내용이 증거로 되는 경우가 대부분이며, 이 경우 정보의 값이 같다면 어느 매체에 저장되어 있든지 동일한 가치를 지니는 특성으로 원본과 사본을 구별할 수 없고 위·변조가 용이한 점(취약성) 등의 디지털 증거의 특성으로 인해 증거의 진정성 확보가 중요한 문제로 대두하게 되었다.

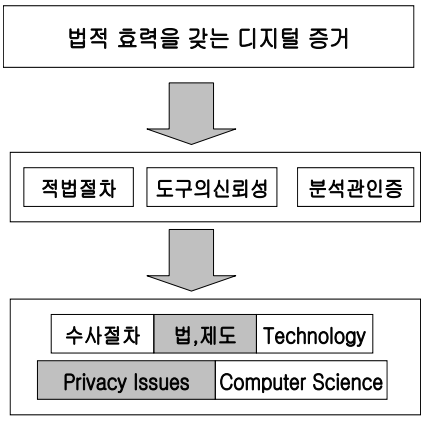
디지털 증거 데이터의 진정성이란 저장, 수집 과정에서 오류가 없으며, 의도된 결과가 정확히 획득되었고, 그로 인해 생성된 자료임을 뜻한다. 무결성이란 범죄 현장에서 관련된 저장매체를 수집한 이후로 내부에 저장된 디지털 데이터가 법정에 제출되기까지 변경이나 훼손 없이 보호됨을 말하며, 신뢰성이란 증거데이터의 분석 등 처리과정에서 디지털 증거가 위조되지 않았고, 의도되거나 의도되지

않은 오류를 포함하지 않음을 뜻한다. 디지털 증거의 원본성이란 자체적으로 가시성과 가독성이 없는 디지털 증거를 변환하여 제출하는 과정에서 제출되는 증거 데이터가 원 매체에 있는 데이터와 동일함을 뜻한다. [2]

현재까지 국내 법정에서 디지털 증거의 증거능력에 대해 다룬 경우는 최근 항소심 판결이 완료된 일심회(一心會) 사건에서 디지털 증거의 법적 증거 허용성과 디지털 포렌식 툴과 절차의 유효성을 적극적으로 해석하는 판결을 하여 무결성과 진정성에 관련하여 디지털 증거의 증거능력 여부 인정하고 있다.

### 2.2 법적 효력을 갖기 위한 디지털 증거

법적 효력을 갖기 위한 디지털 증거란 디지털 증거가 민·형사소송의 법적 증거로서 인정되고 법정에서 활용되기 위한 조건을 말한다. 디지털 증거는 아날로그 자료와는 달리 값만 동일하면 반복된 복사과정에서도 질적 저하가 없다. 그러므로 수집된 증거가 범행의 결과로 나타난 원본 증거인지 복사본인지 명확하게 하는 절차가 필요하다. 특히, 내용이 동일한 디지털 데이터라 할지라도 복사되거나 다른 이전(移轉)방법에 의해 새로 저장되었을 경우 데이터가 생성되거나 접근한 시간이 서로 달라진다. 따라서 증거 수집절차상 각별한 기술적 대책과 절차가 필요하며, 증거능력을 인정함에 있어서 이 부분이 명확치 않을 경우 증거로서의 가치가 상실될 수도 있다. 또한 일반 범죄에서도 중요 증거 또는 단서가 컴퓨터를 포함한 디지털 정보기기 내에 보관하는 경우가 증가함에 따라, 디지털 자료를 법적 증거능력을 갖도록 하는 절차와 방법들을 통칭해 '디지털 포렌식(Digital Forensics)'이라고 한다. (그림 1)은 법적 효력을 갖는 디지털 증거의 추출과정을 보여주고 있다.




(그림 1) 법적효력을 갖는 디지털 증거의 추출과정

디지털 정보는 쉽게 복사, 이전이 가능하며 대용량·소형화된 디지털 저장기기의 발달로 관리주체가 손쉽게 관리할 수 있는 정보의 양이 급격이 증가한(정보의 대량성)반면, 수사기관은 이런 방대한 디지털 정보로부터 범죄수사에 연관된 증거를 검출해 내기가 더욱 어려운 일이 되었다. 따라서 범죄수사의 단서가 될 중요한 데이터를 검색해 내는 특화된 전문 검색도구가 절실히 필요하게 되었다. 그래서 이러한 문제를 다루는 분야를 '디지털 포렌식' 이라고 부른다. [1],[7]

디지털 포렌식(Digital Forensics)은 "컴퓨터를 매개로 이루어지는 행위에 대한 법적 증거 자료 확보를 위하여 컴퓨터 저장매체 등의 컴퓨터 시스템과 네트워크로 부터 자료나 정보를 수집, 분석, 보존절차를 통하여 법적 증거물로서 제출할 수 있도록 하는 일련의 행위"를 의미한다.

디지털 포렌식은 넓은 의미로는 법적인 문제에서 보는 관점 및 범죄수사적인 입장에서 보는 관점을 포함하는 개념이며, 좁은 의미로는 범죄수사적인 입장에서 수사를 위해 필요로 하는 증거를 컴퓨터에서 찾아내서 정확히 분석하고 범인을 검거하는데 단서를 찾고 손상된 부분을 복구하는 피드백 과정까지를 포함하는 기술적이고 입체적인 부분을 말한다. 이러한 디지털 포렌식을 제대로 수행하려면 전문화된 도구(장비)와 전문적인 인력(사람)과 표준화된 지침(제도)가 필요하다고 할 수 있다. [5],[6]

### 2.2 디지털 포렌식의 적용

컴퓨터에서 찾아낸 증거가 법적인 효력을 갖기 위해서는 법적인 측면과 기술적인 측면이 조화되어야 한다. 디지털 포렌식은 '정보처리 기기를 통하여 이루어지는 각종 행위에 대한 사실관계를 확정하거나 증명하기 위해 행하는 절차와 방법'이라고 할 수 있다.

디지털 증거물에 대한 포렌식의 적용단계는 네단계로 구성된다. 첫 번째 '확인' 단계에서는 저장장치에 저장된 정보의 유형과 형태를 확인하는 단계로 증거자료 확보가 이 확인 단계의 핵심이다. 특히, 법적 증거능력이 있는 정보를 잘못 취급하여 증거물로서의 가치를 상실할 수도 있으므로 주의를 요한다. 두 번째 '보존' 단계는 전자적으로 저장된 자료를 확인한 후 변경되지 않도록 보존하는 단계이다. 만약, 자료를 읽을 수 있는 기기의 변경이 있다면 법적인 절차에 따라 변경된 원인을 규명해야 한다. 세 번째 '분석' 단계는 전자적으로 저장된 자료를 추출·처리·판단하는 단계로 분석용 도구를 이용하여 전자자료를 분석하는 단계이다. 전자자료 분석용도구는 Encase, UTK(Ultimate Toolkit), X-Way, Forensics등이 있다. 네 번째 '제출' 단계는 확인·보존·분석 단계에서 추출된 전자 증거물에 대한 법적 증거능력과 증명력을 확보하여 법적 증거자료로서 인정될 때 그 목적을 달성하는 것이다. 그러므로 컴퓨터와 연관된 기술적 문제를 포함하고 있는 범죄는 합법적인 절차를 통해 법적 요구사항을 반드시 만족해야 하며 이것을 수용할 수 없으면 디지털 증거로서 부적합하게 된다.

디지털 포렌식의 기본원칙은 정당성의 원칙, 재현의 원칙, 신속성의 원칙, 연계보관성의 원칙(Chain of Custudy)의 원칙, 무결성의 원칙을 말한다. 첫째, 정당성의 원칙으로 컴퓨터에 있는 증거가 법에서 정한 적법절차에 의해 수집되어져야 한다. 둘째, 재현의 원칙으로 컴퓨터나 시스템을 사고 피해 직전과 같은 조건에서 현장 검증을 실시하였다면, 피해 당시와 동일한 결과가 나와야 한다. 셋째, 신속성의 원칙으로 시스템의 휘발성 정보수집 여부는 신속한 조치에 의해 결정되므로 모든 과정은 지체 없이 신속하게

진행되어야 한다. 넷째, 연계 보관성의 원칙으로 증거 수집에서부터 증거제출에 이르기까지 증거 취급의 전 과정을 투명하게 관리하는 절차의 연속성으로서, 컴퓨터나 시스템에서 증거물을 획득한 다음 이를 이송하고 분석, 보관, 법정에 제출하는 각 단계에서 그 과정의 담당자나 책임자를 명확히 하는 과정을 말한다. 증거를 분석하고 수집하는 과정 중에 증거가 변경되지 않았음을 입증할 수 있어야 하며 사법기관(경찰, 검찰, 법원 등)에 증거제출 단계에서 디지털 증거가 훼손되거나 변경되지 않았음을 입증할 수 있어야 한다. 다섯째는 무결성의 원칙으로 수사를 통하여 수집된 증거가 위조나 변조가 되지 않았음을 증명할 수 있어야 한다. 디지털 포렌식에 있어서 이러한 다섯 가지 기본원칙이 지켜져야 포렌식을 통하여 얻어진 증거가 증거능력을 인정 받을 수 있을 것이다. 또한 디지털 포렌식 기술은 크게 백업, 복구, 분석 기술로 나뉜다. 디지털 증거를 확보하기 위해서는 <표 1>에서 보는 것과 같은 기술들을 포함한 통합 기술이 필요하다. [2],[7]

<표 1> 디지털 포렌식 기술 필요조건

| 기술 분류 | 정 보 |
|---|---|
| 백업 | 휘발성 정보 |
| | 시스템 상태 정보 |
| | 전체 백업 |
| | 네트워크를 통한 백업 |
| 복구 | 은닉 데이터 검색 |
| | 은닉 데이터 탐지 및 복구 |
| 분석 | 역추적 |
| | 증거물 복원 |
| | 피해시스템 분석 |

디지털 데이터의 백업은 휘발성을 갖는 디지털 데이터의 특성과 운영되는 시스템의 성격에 따라 수행되어야 한다. 특히 최근의 시스템은 그 규모와 처리하는 데이터의 양이 매우 방대하다는 것을 고려해야 하며, 백업 작업을 수행하는 동안에도 데이터의 훼손이나 손실이 발생하지 않도록 해야 한다. 불법적인 데이터는 수집되기 전에 삭제될 가능성이 높기 때문에, 이를 복구할 수 있는 기술이 반드시 필요하다. 또한 복구된 데이터가 수사에 유리하도록 생성된 것이 아니라 혐의자에 의해 삭제되었다는 것을 증명할 수 있는 기술도 요구된다.

## 3. 디지털 포렌식의 압수·수색의 문제점

### 3.1 압수·수색 대상의 문제

형사소송법은 입수에 대하여 “증거물 또는 몰수할 것으로 사료되는 물건을 압수할 수 있다” 라고 그 대상을 유체물인 증거물 또는 몰수물로 제한하고 있다.(형사소송법 제 106조) 그러나 오늘날 컴퓨터가 일반화되고 각종 정보가 컴퓨터, USB 메모리, 디스크 등 전재매체에 저장됨에 따라 무형물인 ‘전자기록 내지 데이터’ 도 그 대상으로 볼 수 있는지, 그 개념은 무엇이지, 압수의 방법은 어떻게 해야 하는지 등이 문제 이다.

무형물인 전자기록의 내용이 압수의 대상이 되는가에 대해서는 긍정설과 부정설로 나뉘어져 있다. 부정설은 형사소송법이 유체물에 한하여 압수를 허용하고 있는 점, 형사소송법상 강제조치는 법률에 열거한 것에 한정하여야 한다는 점을 그 논리적 근거로 한다. 그러나 종이에 잉크로 인쇄된 정보와 전자 기록매체에 저장된 배타적 지배가 가능한 법률상의 물건에 해당된다는 점을 고려할 때, 정보를 저장하고 있는 용기에 불과한 전자적 매체만을 압수수색의 대상으로 한다는 것은 옳지 않다고 생각됨으로 긍정설이 타당하다고 사료된다.

다만 수색 대상에 관해서는 범죄 행위와 관련된 자료만이 저장된 컴퓨터 장비뿐이 아니라 범죄 행위와 무관한 자료가 함께 저장되어 있는 장비도 실질적으로 컴퓨터에 저장된 자료가 범죄행위와 관련된 자료가 저장되어 잇을 개연성만 있으면 조사할 수 있다는 견해가 지배적이다.

현실적으로 무형물인 디지털 자료의 경우에도 프린트물 등 가시적인 형태로 나타나는 경우에 저장장치 혹은 프린트물과의 일체성을 인정할 수 있으므로 압수·수색의 대상이 되는 것이 타당하다. 그러나 그 한계에 있어서 저장장치 등의 특수성이 고려되어야 할 것이다. 즉, 범인 소유의 시스템으로 단독으로 사용하는 경우의 시스템 혹은 저장장치를 압수하는 것은 허용이 된다고 할지라도, 다수의 이용자가 공동으로 사용하거나 업무상 중요한 역할을 하는 시스템의 경우 범죄와 관련이 있다는 이유로 압수를 허용하게 되면 관리자, 소유자로 하여금 막대한 피해를 입게 하여 비례상의 원칙에도 어긋나게 되므로 압수는 허용되지 않는 것이 타당할 것이다.

### 3.1 압수·수색 방법의 문제

먼저 무형물로서 압수대상이 되는 전자기록은 ‘전자매체에 저장되어 있는 데이터 내지 정보’를 의미한다. 전자기록은 ‘저장방식이 0과 1의 조합인 이진수 방식으로 존재하는 정보’ 와 ‘전압이나 전류처럼 연속적으로 변화하는 물리량을 표현한 정보’이다.

유체물은 점유를 취득하는 방법으로 압수할 수 있지만, 무형물인 전자기록은 어떻게 압수할 것인가 문제된다. 컴퓨터 등 전자매체에 저장되어 잇는 파일, 로그기록 등의 자료는 비실재성의 특징이 있어, 전자기록도 압수가 가능하다는 긍정설에 의하더라도 무형의 자료 그 자체를 압수하기란 대단히 어렵기 때문이다. 이와 관련하여, 판례는 전자증거의 증거능력의 요건으로 원래의 저장매체에서의 전자기록과 법원에 증거로 제출된 전자기록과의 동일성을 요구하고 있다.(대판 2007도7257) 현실적으로는 판례가 요구하는 동일성 요건을 충족하면서 무형의 자료를 확보하기 위하여, 전자기록이 저장된 원래의 저장매체 전체를 ‘하드카피’ 내지 ‘이미지’ 하거나 일부 범죄혐의와 관련된 파일을 특정하여 ‘CD, 기타 외부저장장치에 저장’한 후 피의자 내지 입회자의 서명을 받아 보인한 다음 이를 압수하고 있다.

수색의 경우 건물 또는 조사받을 물건을 소유하고 있는 사람이 수색에 자발적으로 동의한다면 경찰은 수색 영장을 발급받지 않아도 된다. 심지어 경찰은 범죄가 일어났다는 상당한 증거를 보이지 않아도 된다. 동의가 있을 경우 범죄가 일어났다는 확신이 전혀 없을 경우에도 적법하게 수색을 할 수 있다. 여기서 중요한 것은 동의가 자발적이어야 하고, 동의를 하는 사람은 그럴만한 권한이 있어야 한다. [4]

### 3.1 '일심회' 사례에서의 디지털증거의 증거능력 문제

'일심회' 사건의 경우 압수물인 디지털 저장매체로부터 출력된 문건들의 증거능력 여부에 관하여 변호인들은 압수물인 디지털 저장매체로부터 수사기관이 출력하여 제출한 문건들의 증거 능력에 관하여, 검찰이 위 저장매체의 데이터가 본래 존재하였던 상태와 전혀 다름이 없이 수집, 제출되었다는 사실과 위 디지털 증거의 분석처리과정에 대한 신뢰성에 대하여 그 입증책임을 다하지 못하였고, 법원이 검증절차에 참여하여 이를 주도적으로 진행한 증인 정OO의 디지털 증거 분석능력과 그 증언은 신뢰할 수 없으므로, 위 문건들은 독립적인 증거로 사용할 수 없다고 주장했다. 그러나 법원은 압수수색영장에 의해 피고인들의 거주지 또는 사무실 등에서 압수된 각 디지털 저장매체 원본들은 피고인들의 참여 하에 이미징 작업을 하는 경우를 제외하고는 계속 봉인되어 있었으므로, 압수된 이후 법원에서의 검증절차에 이르기까지 보관과정의 신뢰성이 인정되고, 또한 디지털 저장매체 원본과 이미지 파일 사이에 디지털 기기 등의 데이터가 서로 일치함을 증명하는 방법으로 일반적으로 이용되는 해쉬값이 동일하므로 디지털 저장매체 원본과 이미지 파일 사이의 데이터의 동일성이 인정되며, 피고인들 및 검사, 변호인들이 모두 참여한 가운데 인케이스(Encase) 프로그램을 이용하여 적절한 방법으로 검증 절차가 진행되었으므로 증거 문건들은 증거능력이 적법하게 부여되었다고 판결하였다. [4],[8]

## 4. 결론

디지털 증거는 특수한 도구의 전문적인 기술을 사용하여 수집, 분석될 수 있는 자장과 전자파로 이루어져 있기 때문에 유형적이고 물리적인 증거와는 차이가 있다. 하지만 디지털 증거의 경우에는 전문적인 지식과 특수한 도구가 필요하다는 점을 제외하고는 그 발견과 수집, 이용에 있어서 물리적인 증거와 크게 다르지 않다고 할 것이다. 그러므로 디지털 증거가 법정에 제출되는 경우에 증거로서의 가치를 상실하지 않도록 적법한 절차와 수단을 토대로 획득되어야 한다. 명확한 법적 근거가 없는 수집 및 분석 행위는 절차상 위법성으로 인해 증거 능력 자체에 문제가 생길 수 있다. 또한 디지털 증거의 신뢰성 및 무결성을 확보하기 위해 신뢰성 있는 디지털 증거 수집 장비 및 시스템을 확보해야 한다. 법적 효력을 갖는 신뢰성 잇는 디지털 증거를 확보하기 위해서는 적법한 절차와 수단 확립, 신뢰할 수 있는 포렌식 도구 확보, 표준화된 절차, 디지털 증거 분석관 인증제도 등이 우선 필요하다. 그랬을 때 디지털 증거가 법적 효력을 갖고 범죄 수사에 적법하게 사용될 수 있을 것이다.

물론 '일심회' 판결을 보면, 적법한 절차에 의한 압수·수색, 디지털 저장매체에 인증된 도구 및 프로그램등을 이용하여 증거를 획득하였을 때 디지털 증거가 증거능력이 있음을 판결로서 판결을 하였지만 대량화되어지는 정보와 양적으로 증가하는 많은 범죄 사건들을 각각의 판례로서 결정한다는 것은 성문법주의를 표방하는 형법상의 원칙에도 미흡하고 맞지 않으므로 제도적 절차적 인증제도가 필요하다고 하겠다.

## 참고문헌

[1] 김형성, 김학신, "Computer Forensics의 법적 문제 연구", 성균관 법학 제18권 제3호 2006. 12.

[2] 고려대학교 산학협력단, "외국판례에 나타난 디지털증거 수집분석보존 과정에서의 무결성 논란에 비추어 본 디지털 증거의 활용방안". 대검찰청, 2006.

[3] 이형우, 이상진, 임종인, "컴퓨터 포렌식스 기술", 정보보호학회지, 2002. 10.

[4] 노정환, "현행 압수수색 제도의 문제점에 대한 고찰", 인터넷 법률신문, 2008.12.29. 제3709호

[5] 황현욱, 김민수, 노봉남, 임재명, "컴퓨터 포렌식스: 시스템 포렌식스 동향과 기술", 정보화정책 제13권 제4호, 2006.

[6] 전상덕, 홍동숙, 한기준, "디지털 포렌식의 기술 동향과 전망", 정보화정책 제13권 제4호 2006.

[7] 숭실대학교 산학협력단, "디지털증거의 무결성 유지를 위한 절차와 시설에 관한 연구", 대검찰청, 2006.

[8] 사이버 포렌식 협회, http://cfpa.or.kr