# [정보보호] 디지털 포렌식 소개 및 향후 고려사항

전통적으로 법정에서 인정되어온 증거들은 범행에 사용된 물리적인 도구나 범인의 행적을 증명할만한 흔적(유류지문, 족적 등), 또는 범행 사실과 관련된 기록을 담고 있는 음성 및 손으로 작성된 문서들이었다. 그러나 컴퓨터 및 인터넷의 사용이 증가되고 일반인들 생활에 많은 부분을 차지함에 따라 범죄의 단서가 컴퓨터에 저장되어 있는 경우가 늘고 있으며, 컴퓨터 및 인터넷 자체가 새로운 범죄의 대상이 되기도 한다. 이러한 증거들을 기존의 증거와 구분하여 디지털 증거라 부른다. 하지만 디지털 증거는 그 특성상 전문증거에 해당되어 법정에서 증거로 인정받지 못하는 경우가 발생할 수도 있다. 이에 본 보고서에서는 디지털 증거가 증거능력을 갖기 위한 조건에 대해 살펴보고 관련 표준화 및 연구 동향을 알아본다.

## 디지털 증거의 특성 및 국내 법정의 현실

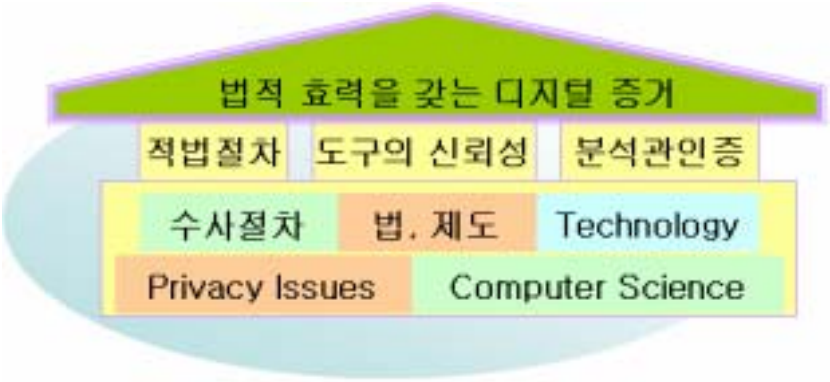
디지털 증거란 이진화되어 저장되거나 전송 중인 데이터로 그 특성상 복제가 쉬울 뿐만 아니라 원본과 사본의 구분이 어렵고, 조작, 변경, 삭제 등이 용이하다. 또한 매체 독립적으로 비가시적이라는 특성을 지니고 있으므로 디지털 증거를 법정에 제출하기 위해서는 가시적인 형태로 변환하여 제출하여야 한다. 이에 따라 컴퓨터나 기타 디지털 저장장치로부터 수집된 디지털 증거가 법적 효력을 가지기 위해서는 진정성, 무결성, 신뢰성, 원본성이 보장되어야 한다[1].

증거 데이터의 진정성이란 저장, 수집 과정에서 오류가 없으며, 의도된 결과가 정확히 획득되었고, 그로 인해 생성된 자료임이 인정됨을 뜻한다. 무결성이란 범죄 현장에서 관련된 디지털 저장매체를 수집한 이후로 내부에 저장된 디지털 데이터가 법정에 제출되기까지 변경이나 훼손 없이 보호됨을 말하며, 신뢰성이란 증거 데이터의 분석 등 처리 과정에서 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 의미한다.

하지만 현재까지 국내 법정에서 이러한 디지털 증거의 증거능력에 대해 다룬 경우는 찾기 어려우며 최근 항소심 판결이 완료된 국가보안법 위반 사건에서 유일하게 디지털 증거의 무결성과 진정성에 관련하여 증거능력 여부를 논하고 있다[2]. 이는 피고 및 변호인 측에서 디지털 증거의 취약성에 대해 인지하지 못하고 있었기 때문이라 판단되나, 관련 판례가 존재하고 개인의 프라이버시를 중시하는 사회적 분위기가 확산됨에 따라 디지털 증거에 대한 증거능력을 문제시하는 판결이 증가될 것이라는 전망이다.

## 법적 효력을 갖는 디지털 증거의 수집 조건

위에서 언급한 조건을 만족하는 디지털 증거를 확보하기 위해서는 적법한 절차와 수단 확립, 신뢰할 수 있는 포렌식 도구 확보, 디지털 증거 분석관 인증제도 구축이 선행되어야 한다.




디지털 증거는 법정에 제출되는 경우에 증거로서의 가치를 상실하지 않도록 적법한 절차와 수단을 토대로 획득되어야 한다. 명확한 법적 근거가 없는 수집 및 분석 행위는 절차상의 위법성으로 인해 증거 능력 자체에 문제가 생길 수 있다. 이를 위해 공신력 있는 기관에서 논리적이고 체계화된 디지털 포렌식 표준 가이드라인을 제정할 필요가 있다.

또한 디지털 증거의 신뢰성 및 무결성을 확보하기 위해 신뢰성 있는 디지털 증거 수집 장비 및 시스템을 확보하여야 한다. 이를 위해 산재하고 있는 여러 포렌식 도구들에 대한 검증 항목 및 절차 수립, 더 나아가 포렌식 도구 테스트 베드 구축을 통하여 사용자(분석관)로 하여금 신뢰할 수 있는 도구를 선택할 수 있도록 해야 한다.

하지만 디지털 포렌식 표준절차가 존재하고 신뢰성 있는 도구를 사용한다 하더라도 디지털 증거 수집의 주체인 분석관의 자격이 적절하지 않다면 그 분석관이 수집한 결과를 신뢰할 수 없을 것이다. 그러므로 포렌식 도구 사용능력 및 디지털 증거에 대한 이해와 그 수집 절차 숙지 여부를 평가하는 분석관 인증제도를 구축하여 인가된 분석관만이 디지털 증거 수집 작업에 관여할 수 있도록 하도록 한다.

디지털 증거처리 표준화와 디지털 포렌식 도구 검증 절차 수립은 관련 기술과 컴퓨터 과학에 근거하여야 하고, 지역 사회의 법과 제도 테두리 내에 존재해야 하며 일반적인 수사절차에 위배되지 않아야 한다. 또한, 용의자의 프라이버시를 침해하지 않아야 한다는 조건도 만족해야 한다.

**관련 연구 및 국내외 표준화 동향**

CFTT(http://www.cftt.nist.gov/)는 미국 내 법 집행기관의 요구에 따라 NIST(National Institute of Standards and Technology)에서 수행하고 있는 프로젝트로서, 디지털 포렌식에 사용되는 도구들의 요구사항을 정의하고 각 도구들을 검증하는 방법 및 절차를 수립하여 디지털 포렌식 도구의 테스트 베드를 구축하는 것을 주된 목적으로 한다. 이를 통해 신뢰성 있는 디지털 포렌식 도구를 선별하여 사용함으로써 정확한 디지털 증거를 획득하고자 함이다.

또한 Guidance Software(http://www.guidancesoftware.com/) 사와 Access Data(http://www.accessdata.com/) 사에서는 자사의 제품(Encase, FTK, 각각)에 대한 교육과 도구사용능력 인증제를 실시하고 있다.

디지털 증거의 증거능력 확보와 관련된 국내 표준활동으로는 2007년부터 TTA에서 추진 중인 “디지털 포렌식을 위한 데이터 수집” 과제가 존재하며, 이를 중심으로 디지털 증거 수집 가이드라인 표준화와 디지털 포렌식 도구 검증을 위한 표준화 작업이 진행 중에 있다. 국가별 법제도 등이 상이함으로 인해 현재까지 관련 국제 표준은 제정된 바가 없으나 2009년부터 시작되는 ITU-T SG17 차기 회기에 포렌식 관련 Question이 신설될 예정에 있다.

**결론**

각 국가별로 자국의 사법환경을 반영한 디지털 증거 수집절차 등 제도적 표준을 통합하여 하나의 국제표준으로 수렴하는 것은 무의미한 일이 될 것이다. 그러므로 디지털 포렌식과 관련된 국제표준은 제도적인 차원이 아닌 기술적인 측면에서의 표준화가 주를 이룰 것이라 예상된다. 국내 연구기관과 관련 산업체는 우수하고 시기 적절한 국내표준 개발을 통해 국내 기술이 국제 표준으로 제정될 수 있도록 하여야 할 것이다. 또한 디지털 증거의 증거력에 대한 문제제기에 대해 대처할 수 있는 방안으로 국가적 차원에서의 증거분석관 인증제도가 마련되어야 하겠다.

**참고자료**

[1] 고려대학교 산학협력단, 외국판례에 나타난 디지털증거 수집·분석·보존 과정에서의 무결성 논란에 비추어 본 디지털 증거의 활용방안, 대검찰청, 2006

[2] 김정옥, 디지털증거의 증거능력 인정 요건 - 일심회 판결을 중심으로, 디지털 포렌식연구, p. 133-146, 2007

길연희 (한국전자통신연구원 정보보호기반그룹 연구원, yhgil@etri.re.kr)