

* 요약
* 디지털 데이터를 증거로 삼아 사실관계를 규명하고 증명하는 ‘디지털 포렌식’이 각광받고 있다. 디지털 포렌식은 디지털 데이터가 존재했는지, 데이터를 만들거나 접근한 사람은 누구인지, 데이터가 사건과 관련이 있는지, 데이터의 변경 여부 등을 입증함으로써 증거로 사용될 수 있기 때문에 경찰, 검찰, 국세청, 국방부, 그리고 인터폴과 같은 국제기구에서도 활용되고 있다.

디지털 포렌식을 처리하기 위해서는 크게 여섯 단계를 거친다. 첫번째, **식별** 단계는 증거로 사용될 수 있는 정보를 식별한다. 웹 서버 또는 웹 애플리케이션 방화벽이 개인의 IP 주소를 수집해서 로그로 기록한 것이나 웹 사이트를 방문하면 남게 되는 쿠키가 이에 해당한다. 증거가 식별되면 이 정보가 변경이나 삭제되지 않도록 **보존**한다. 압수수색 영장을 통해 컴퓨터나 스마트폰을 확보하여 로그파일을 제거하거나 수정하지 못하도록 하고 네트워크를 비롯해서 의심되는 시스템에 접근할 수 없게 한다. 세 번째 단계는 **수집**이다. 데이터는 휘발성이 강하므로 레지스트리와 캐시는 라이브 메모리 캡처를 통해 가장 빨리 수집해야 할 대상이고, 수집된 정보는 외장형 하드에 옮긴다. 다음은 **조사**이다. 확보된 증거로부터 데이터를 검색하고 추출한다.

확보된 증거가 파손되었다면 **복원**을 위한 준비를 한다. 파일을 삭제하더라도 겹쳐 쓰지 않는다면 복구 가능성이 존재한다. 그러나 자기장을 이용해 파일을 없애는 디가우징을 했거나, 하드에서 파일이 완전히 깨졌다면 복구하기 힘들다.

이어 **분석**에서는 다양한 기술이 활용된다. 파일 시스템의 구조와 각 파일이 언제 생성되고 수정됐는지 등을 빠르게 분석할 수 있는 디스크 브라우징, 파일 포맷이 있는 데이터를 가시적으로 분석할 수 있는 데이터 뷰잉 등 다양한 기술을 활용해서 저장된 데이터를 분석한다. 이렇게 찾은 정보를 제출하게 되면 디지털 포렌식이 마무리된다.

디지털 포렌식은 우리가 만든 모든 디지털 정보를 알고 있다. 모든 사물이 인터넷으로 연결되는 4차 산업혁명 시대에 사이버보안의 중요성은 아무리 강조해도 지나치지 않는다. 숨은 보물을 찾듯 지난한 과정이 요구되는 디지털 포렌식이 4차 산업혁명 시대에 더욱 기대되는 이유다.

* 코멘트
* 디지털 포렌식은 디지털 기기 속의 정보를 이용하여 증거를 찾아내고 범죄 수사에 사용됩니다. 기사에서는 긍정적인 내용만을 언급하였지만, 악용되어 범죄를 밝혀내는 일이 아니라 개인 정보 유출과 관련된 문제로 연결될 수 있다는 생각이 들었다. 최근 컴퓨터 수리 업체에서 노트북에 있던 영상을 복구시켜 인터넷에 유포하였다는 뉴스가 있었다. 또한 용의자로 추정되던 사람이 무고하다는 것이 밝혀진다면 지나친 사생활 정보 유출이 될 우려가 있다고 본다.