이학석사 학위논문

디지털 포렌식 전문가의 필요성과 육성 방안에 관한 연구

2016년 7월

서울대학교 융합과학기술대학원

수리정보과학과(디지털포렌식전공)

박 재 범

디지털 포렌식 전문가의 필요성과 육성 방안에 관한 연구

지도교수 김 명 환

이 논문을 이학석사 학위논문으로 제출함
2016년 7월

서울대학교 융합과학기술대학원
수리정보과학과 디지털포렌식전공
박 재 범

박재범의 이학석사 학위논문을 인준함
2016년 7월

위 원 장 _____ (인)

부위원장 _____ (인)

위 원 _____ (인)

국문초록

주요어 : 디지털 증거, 디지털 포렌식, e-Discovery,
디지털 포렌식 전문가
학 번 : 2014-24858

정보통신기술의 발달에 따라 디지털 사회가 급속하게 진행되면서, 생활의 편의성이 증대된 사회 이면에는 기존 범죄의 디지털화를 통한 수사의 어려움과 새로운 디지털 기술을 활용한 범죄 역시 증가하였다. 이처럼 사회가 디지털화 되어감에 따라 디지털 포렌식 기술의 발전과 디지털 포렌식 전문가의 필요성은 점차 증대되고 있다.

하지만 학계에서 디지털 포렌식과 관련한 제도 및 인력양성에 대한 단편적인 논의는 다수 존재하지만 디지털 포렌식과 디지털 포렌식 전문가 양성과 육성방안에 관한 종합적인 연구는 거의 없다.

이에 본 연구는 디지털 포렌식과 관련한 이론적 연구를 통해 디지털 증거와 디지털 포렌식의 필요성에 대해 고찰하였고, 미국의 e-Discovery 제도와 관련사례연구를 통해 실천적인 방향을 제시하고자 하였다. 또한 국내외 디지털 포렌식 관련기관의 디지털 포렌식 교육현황과 커리큘럼을 조사하여 앞으로의 교육훈련프로그램의 정형적인 형태를 제시하는 것을 목적으로 연구되었다.

이와 같은 연구의 목적을 달성하기 위해 디지털 증거와 디지털 포렌식, 미국의 e-Discovery 제도에 대한 이론연구를 실시하였다. 구체적으로 많은 선행연구를 통해 디지털 증거의 개념과 속성, 유형에 대해 연구하였고, 디지털 포렌식의 개념, 기본원칙, 유형과 절차에 대해 연구하였으며, 현대 사회에서 디지털 포렌식의 필요성과 중요성에 대해서도 연구하였다. 또한 미국의 e-Discovery 제도에 대한 이론연구와 사례연구를 통해 국내 도입가능성에 대해서도 검증하였다.

디지털 포렌식 전문가 양성과 개발을 위해서는 국내외 디지털 포렌식 관련기관의 전문가 현황 및 교육 프로그램에 대한 현황을 조사하였고,

결론에서 디지털 포렌식 전문가 양성 및 교육과정 개발 방안을 제시하였다.

디지털 포렌식 전문가 양성 및 효율적인 교육과정 개발을 위해서는 첫째, 국가 포렌식 체계에 기반을 둔 관련법규의 수립과 각 법 요소 간 균형 있는 발전이 요구되고, 둘째, 관련기관의 상호연계를 위해 국가차원에서 디지털 포렌식 전문인력 개발 협의회를 구성하고, 포괄적인 조정과 지원이 필요하다. 셋째, 전문교육기관을 실무 적합형 전문가 양성과정과 핵심 전문인력 양성과정으로 구분하여 훈련과 개발이 필요하다. 다섯째, 국가차원의 디지털 포렌식 자격제도의 정비와 여섯째, 디지털 포랜식 전문가 양성을 위한 교육 전문인력 개발이 필요하다는 결론을 도출하였다.

본 연구는 디지털 증거와 디지털 포렌식, 전문가 필요성과 육성과 관련한 이론연구와 사례연구를 진행하여 디지털 포렌식의 중요성 및 인력양성의 필요성과 교육훈련에 대한 정책적 방향성을 제시하였고, 디지털 포렌식에 대한 학문적 기틀을 제공하여, 향후 계속연구를 통해 디지털 포렌식 전문가를 양성하고 개발하는 다양한 제도와 방법을 개발하는데 기여할 것이라는 시사점을 가지지만 연구과정에서 연구대상, 연구내용, 연구방법에서 제한된 한계점 또한 존재한다.

목 차

표 목 차

그 림 목 차

제 1 장 서론

제 1 절 연구의 배경

지식, 정보화 사회는 21세기에 시작되어 급속히 발전되어가고 있다. 새로운 기술과 또 다른 기술의 융합, 지식과 정보의 결합, 기술과 컨텐츠의 결합은 새로운 산업과 업종을 창출한다(오종석·김종관, 2014). 이런 정보통신기술을 활용한 스마트 기기, 클라우딩 기술, 소셜 네트워크서비스 등은 정보에 쉽게 접근할 수 있도록 하고, 편의성을 증대시키는 긍정적인 측면에서 활용되고 있으나, 각종 범죄에도 활용될 가능성도 상존하고 있다. 범죄의 증가는 사회적 비용의 증가를 의미하며, 국가의 안정적이고 지속가능한 성장을 저해하는 요인이 된다. 따라서 정보통신기술의 발전에 따라 증가하는 범죄를 예방하고, 범죄를 증명하기 위한 기술적 발전의 필요성이 제기된다.

정보통신기술의 발전에 따른 범죄의 수사와 법정에서 증거 또는 사실관계를 확인하기 위하여 각종 증거를 과학적으로 분석하여 사용하는 분야를 법과학(Forensic Science)이라고 하며, 이는 지문, 모발, DNA에 대한 감식, 변사체 검시 등의 전통적 분야를 말한다. 컴퓨터의 등장과 네트워크로 연결된 다양한 디지털 기기의 사용으로 인하여 시·공간의 제약이 극복되고 다양한 업무에 적용이 되어 많은 효용을 주고 있으나 해킹, 악성코드 등으로 연결된 범죄 같은 부정적 상황도 많이 발생되고 있어 관련 수사도 필연적으로 늘고 있다.

디지털 포렌식은 법과학 유형의 한 영역이고 비교적 최근에 정립된 개념으로 현대 정보화시대의 범죄 형태는 컴퓨터를 비롯한 임베디드(embedded) 기기[1]인 스마트폰, 태블릿 PC, 스마트 TV, 네비게이션, 블

랙박스, CCTV 등 다양한 디지털 기기가 도입되고 인터넷이 전 세계를 연결하여 다양하고 광범위한 정보가 생성되는 디지털 데이터가 주를 이루는 환경 하에서 디지털 정보를 생성시키지 않고 범죄의 발생이 이루어질 가능성이 거의 없는 현실에 와 있다고 할 수 있다. 데이터 스토리지 업체인 EMC는 IT 시장조사기관인 IDC(International Data Corporation)에 의뢰하여 작성된 '디지털 유니버스 보고서(IDC Digital Universe Study 2011)'에서 "빅데이터, 더욱 길어진 디지털 그림자, 이머징 마켓의 놀라운 성장(Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East)"의 연구 결과를 보면, 전 세계적으로 2012년 한해 생성, 복제 및 유통되는 디지털 데이터의 양은 2.8 제타바이트(Zetta Byte)에 이르고 2020년에는 40ZB까지 성장할 것으로 예측했다. 특히, 디지털 유니버스의 크기를 이처럼 거대한 규모로 팽창시키는 요인에는 개인용 IT 디바이스의 활성화, 인터넷 사용 확대, 소셜 네트워크와 더불어 디지털 TV, 감시 카메라와 같은 디지털 기기가 생성하는 데이터가 크게 작용한 것으로 IDC는 추정했다. 디지털 데이터의 양은 2년마다 2배씩 지속적으로 증가하여 2020년 약 40ZB에 이를 것으로 전망되고 있다. 1제타바이트는 1조 기가바이트(GB)다. 40ZB는 전 세계 해변 모래알의 수(7억50만조)의 약 57배에 해당하는 숫자이며, 2020년에는 전 세계 인구 1인당 약 5,247GB 디지털 데이터를 소유하게 되는 것으로 계산된다(고수연, IT DAILY, 2012). 사이버 상 범죄뿐만 아니라 일반 범죄에서도 디지털 증거가 범죄 사실 확인에 있어 중요한 역할을 하는 이유이기도 하다.

그러므로 포렌식의 특수한 분야로 발전된 디지털 포렌식은 수사와 공판과정에서의 조사를 통한 사건을 규명하는 형사법 절차에서 필수적이고 중요한 분야로 인식되고 있다. 나아가 일반기업체, 금융기관 등의 민간분야에서도 세금 탈루, 비자금 조성 등 기업 관련 범죄의 정보수집, 기업

1) 개인용 컴퓨터와 같은 시스템은 사용자의 취향에 따라 다양한 운영체제와 응용프로그램을 사용할 수 있는 반면 임베디드 시스템은 일반적으로 소프트웨어가 내장되어 있어 원래 목적을 벗어난 형태로 사용되기 어렵다. 이상진, 디지털 포렌식 개론, p.57

이 비밀로 취급하는 내부 정보 유출 문제, 회계 감사 등의 보안 문제 등에 대처하기 위한 디지털 포렌식의 기술이 더욱 더 필요한 실정이다. 이러한 환경 하에서 디지털 포렌식 활용에 대한 중요성과 수요는 점차적으로 증가될 것으로 보이며 관련 인력에 대한 수요는 계속 커지고 있다.

그리고 디지털 기술의 발전 속도와 변화로 인하여 현재 사용되어지는 디지털 디바이스의 종류가 다양화됨에 따라 운영체제와 파일의 형태 또한 다양화되고 있고, 저장장치 용량의 대형화, 웹기술의 고도화로 인한 클라우드 컴퓨팅, 안티포렌식 기술[2]의 대중화 등의 기술발전으로 인하여 디지털 포렌식 수사에 어려움이 증대되는 상황으로 이에 대한 신속한 대처도 필수적이다.

2) 데이터를 완전 삭제(wiping), 데이터 암호화(encryption), 데이터 은닉(steganography) 등의 기법을 활용한다.

제 2 절 연구의 목적

본 연구에서는 수사와 공판 절차에서 디지털 범죄수사의 성패는 디지털 증거에 대한 압수·수색과 효율적 증거분석이라고 할 수 있다. 이에 사건의 실체적 진실을 규명하는 열쇠의 역할을 하는 디지털 증거와 이에 대한 수집, 분석, 보고하는 디지털 포렌식에 대한 이론적 배경을 알아보려 한다.

일반적인 디지털 포렌식 전문가의 경우 컴퓨터공학, 전산학 등 IT분야의 전문적인 기술을 갖추고 고도화되는 정보화시대의 흐름에 발맞추어 많은 연구와 노력에 전력하고 있지만, 형사법에 있어 법의 이념인 실체적 진실 발견과 적법 절차 원칙을 실현하기 위하여 수사와 법정에서의 결정적인 결론을 형성하는 역할을 하는 압수·수색 절차, 디지털 증거능력 문제 등 법적 지식과 다양한 사건해결에 필요한 수사적 지식에 대하여도 충분한 습득이 요구된다. 이런 디지털 포렌식의 특징 때문에 분야별 전문가들의 전문성에 대한 융합이 필수적이다.

그런 요구조건을 갖추기 위하여 국내 외 대학, 대학원 등에서 IT와 법학을 융합한 디지털 포렌식 전문가 육성에 힘쓰고 있으며, 특히 검찰에서 일선 수사관을 대상으로 디지털 포렌식 전문 수사관의 체계적 양성을 위하여 장기간의 교육을 하고 있으며 또한 상시적인 교육을 실시하여 디지털 포렌식 전문 수사관 역량을 강화하고 있는바 이에 대한 현황과 전망 등을 살펴보고자 하며, 또한 경찰, 군 등 국가기관과 유관기관 별 디지털 포렌식 관련 사항 등을 알아보면서 앞으로의 정보화시대 흐름에 따른 국내 디지털 포렌식 인재 양성과 그 역량 강화에 대하여 고찰하고 향후 개선점에 대하여 알아보고자 한다.

종합하면, 디지털 포렌식에 대한 관심과 전문인력에 대한 요구가 점점 확대되어 감에도 불구하고 체계적이고 종합적이지 못한 국내 디지털 포렌식 관련 교육 커리큘럼과 전문인력 양성 프로그램 및 자격제도는 관련

산업과 전문인력 개발에 한계를 가지고 있어 시급한 개선이 필요하다. 이에 본 연구에서는 다음과 같은 목적으로 연구되었다.

첫째, 최근 사회적 관심이 높아지고 있는 디지털 증거와 디지털 포렌식에 대해 선행연구를 바탕으로 이론연구를 진행하여 주요 개념들에 대한 재정립을 통해 학문적 발전에 기여하고자 한다.

둘째, 국내에서 체계화 되지 않은 제도인 e-Discovery(전자증거개시)의 개념과 미국의 e-Discovery제도에 대해 살펴보고 국내 도입가능성에 대해 검토하고자 한다.

셋째, 국내외 디지털 포렌식 관련기관의 현황을 조사하고, 국내 검찰조직과 경찰조직을 중심으로 전문가 현황과 양성방안, 교육과정에 대한 검토를 통해 앞으로의 발전 방향을 제시하고자 한다.

제 2 장 디지털 증거와 디지털 포렌식의 필요성

제 1 절 디지털 증거

1. 디지털 증거의 개념

디지털 포렌식의 대상인 디지털 증거는 전자적 증거(electronic evidence)라는 용어와 혼용되어 사용되어 지고 있으나, 전자적 증거라고 하면 소송과정에서 다양한 형태의 컴퓨터 기기에 전자적으로 저장된 정보(Electronically stored information)가 증거로 사용될 수 있는 것을 의미하는데(Vilonino, 2003), 이는 아날로그 형태의 증거를 포함하는 개념으로 0과 1이 조합된 디지털 형태로 컴퓨터나 컴퓨터 기반 디바이스를 통하여 생성되고 검색 가능한 형태로 저장되는 정보인 디지털 증거보다는 넓은 개념이라고 볼 수 있다.

하지만 관련 학계에서 전자적 증거, 디지털 증거, 컴퓨터 관련 증거가 명확한 구분이 없이 사용되어 지고 있으며 과거 초창기 컴퓨터에 한정된 증거에 대한 개념부터 시작한 연유에서 컴퓨터 관련 증거라는 용어가 곧 디지털 증거라는 개념으로 인식되었으나 다양한 디지털 기기의 출현으로 디지털 증거로의 개념의 확대가 필요하게 되었다.

국내 법체계에 있어서 디지털 증거에 대한 정의는 아직 명확하지 않다. 현행 형법에서 제48조 제3항 등에서 전자기록[3]이라는 용어를 찾아볼 수 있고, 형사소송법 제106조(압수) 제3항에서 압수의 목적물로 컴퓨터

3) 형법 제48조(몰수의 대상과 추징) ③ 문서, 도화, 전자기록 등 특수매체기록 또는 유가증권의 일부가 몰수에 해당하는 때에는 그 부분을 폐기한다. 이 외 같은 법 제 140조 제3항, 제141조 제1항 등 여러 조항에서 전자기록에 관한 용어를 찾아볼 수 있고, 전자정부법, 전자서명법, 전자문서및전자거래기본법 등의 법률에서 '전자'라는 개념을 사용하고 있다.

용디스크, 그 밖의 이와 비슷한 정보저장매체로 규정되어 있으나 전자기록 그 자체에 대한 압수대상 규정은 없으며, 형사소송법 제266조3(공소제기 후 검사가 보관하고 있는 서류 등의 열람·등사) 제6항에 정보[4]라는 일부 디지털 증거를 지칭할 수 있는 개념이 있다.

미국에서는 전자적으로 저장된 정보(ESI, Electronically Stored Information)에 대하여 2006년 미국 연방민사소송규칙을 개정하면서 증거개시의 표준 속에 개념으로서 구체화시켰다.

이러한 법체계에서 디지털 증거나 전자적 증거 등에 대한 명확한 정의를 하지 않는 이유는 전자시스템이 계속 발전됨에 따라 그 개념이 유동적으로 바뀔 수 있어 가변적일 수 있기 때문이다. 이런 디지털 증거는 컴퓨터 메모리, 이메일, 메신저, 쿠키파일 등에 다양한 형태로 존재한다.

다만, 디지털 증거의 정의에 대하여 대검찰청 예규 등에서 찾아 볼 수 있는데 「디지털 포렌식 수사관의 증거 수집 및 분석 규정[5]」 제3조(정의)에서 보면, 디지털 증거란 범죄와 관련하여 디지털 형태로 저장되거나 전송되는 증거로서의 가치가 있는 정보를 말한다고 정의되어 있으며, 경찰의 경우 경찰청 훈령「디지털 증거 수집 및 처리 등에 관한 규칙[6]」 제2조 제1호에서 디지털 데이터란 전자적 방법으로 저장되어 있거나 네트워크 및 유·무선 통신 등을 통해 전송 중인 정보를 말한다고 정의하고, 같은 조 제4호에서 디지털 증거란 디지털 압수물 중 범죄사실의 증명에 필요한 디지털 데이터를 말한다고 정의되어 있다.

---

4) 제266조3(공소제기 후 검사가 보관하고 있는 서류 등의 열람· 등사) ⑥ 제1항의 서류 등은 도면, 사진, 녹음테이프, 비디오테이프, 컴퓨터용디스크, 그 밖에 정보를 담기 위하여 만들어진 물건으로서 문서가 아닌 특수매체를 포함한다. 이 경우 특수매체에 대한 등사는 필요 최소한의 범위에 한한다.

5) 대검예규 제815호(2015. 7. 16. 일부개정)

6) 경찰청 훈령 제766호(2015. 5. 22.제정)

2. 디지털 증거의 속성

디지털 수사의 핵심은 디지털 증거에 대한 압수수색에 있다고 할 수 있으며 대상이 되는 디지털 증거는 일반 증거와는 아래와 같이 일반적으로 비가시·비가독성, 매체독립성, 증거와 매체의 이중증거성, 조작가능성(취약성), 대량성, 네트워크 관련성, 전문성의 이질적인 성질을 가지고 있기에 전문가에 의한 특별한 압수수색이 이루어져야 한다.

2.1. 비가시·비가독(invisible and unreadable)성

디지털 증거는 디지털 저장매체에 저장되어 있거나 전송되는 정보이다. 인간의 지각능력으로 보거나 읽어 파악할 수 없어 그 실체를 알 수 없는 무형물이다. 우리가 물리적으로 인지할 수 있는 것은 디지털 저장매체나 디지털 전송매체일 뿐이다. 디지털 증거는 잠재적인 증거로서 변환절차를 거쳐야만 현시적인 증거로서 기능을 할 수 있다(전명길, 2011). 증거조사의 방법에 있어 서면일 경우에는 제시와 낭독의 절차를 거치지만 디지털 증거의 경우 출력이라는 변환절차를 거쳐 그 출력물을 제시하고 낭독하는 절차가 필요하게 된다.

2.2. 매체독립성

디지털 증거는 유체물이 아닌 무체물로서 매체독립적인 '정보' 그 자체이다. 이 정보의 값이 같다면 어느 매체에 저장되어 있든지 동일한 가치를 지니게 된다. 즉 디지털 증거는 저장매체에 의존하지 않고 저장매체를 옮기더라도 원형 그대로 보존된다. 그러나 법정에 증거로 제출되는 경우 외 동일 매체 또는 다른 매체에 복사 또는 기타의 방법으로 이전되는 경우 원본과 사본의 구별이 불가능해지는 문제가 있다(한성훈, 2015). 이런 이유로 디지털 증거의 무결성과 동일성이라는 문제가 발생하게 되

며 이 문제는 디지털 증거가 증거능력을 갖추기 위한 필수적 요건이다(권오걸, 2011).

2.3. 디지털 증거와 디지털 매체의 이중증거성

디지털 증거는 특정한 정보를 담고 있는 저장매체 또는 특정한 정보를 전송하는 전송매체가 디지털의 형태를 가지고 있는 경우가 디지털 증거라고 할 수 있고 디지털 '매체'라는 형식적 요소와 '정보'라는 내용적 요소로 구성되어 있다고 볼 수 있다. 디지털 증거에 대한 증거조사의 대상이 되는 것은 디지털 정보를 처리, 전송하는 매체가 아니라 디지털 정보 그 자체라는 견해[7]가 있으나, 반드시 정보 그 자체만이 증거로 되는 것은 아니다. 정보를 저장하거나 전송하고 있는 디지털 매체도 증거가 될 수 있다. 예를 들어 타인의 나체를 촬영한 디지털 기기는 디지털 정보인 화상 자료와 기기 모두 증거가 된다. 이를 디지털 증거와 디지털 매체의 이중증거성이라고 한다(권오걸, 2011).

2.4. 조작가능성(취약성)

디지털 형태로 저장되어 원본과 동일하게 쉽게 복제되거나 변조, 손상이 용이하므로 소송절차에서 증거 조작여부, 증거 수집 절차의 적정성 등의 문제점이 발생할 여지가 크다. 그러므로 디지털 증거를 수집할 때는 수집 이후부터는 디지털 증거가 변조되지 않았다는 것을 입증할 수 있도록 무결성을 확보하는 절차와 기술이 필요하다(탁희성·이상진, 2006). 특히 전자적 정보에는 메타데이터가 항상 생성되는데 제목, 주제, 작성자, 저장된 위치, 작성시간, 엑세스 시간, 수정시간 등의 부가적인 정

7) 형사소송법 제106조 제3항에서 압수의 목적물이 정보가 될 수 있는가의 문제와 실무에서 피의자 등의 디지털 기기 등에 대한 압수집행 실무의 경우 디지털 포렌식 절차 후 디지털 기기 등에 대한 가환부 또는 환부할 경우가 많은데 이럴 경우 그 정보 만을 압수하였다고 볼 수 있지 않겠느냐 하는 견해가 있다.

보를 가지고 무결성을 확인하는 자료로 이용되어 위 적정성, 조작 문제점 등의 해결에 중요한 정보를 제공한다.

2.5. 대량성

디지털 저장매체의 급격한 발전으로 적은 비용으로 대용량의 정보를 저장하고 전송할 수 있게 되었다. 일반 기업의 회계자료는 데이터베이스 자료나 서버에 저장된 자료 등의 형태로 존재할 수 있는데 대용량의 서버나 데이터베이스에 있는 데이터가 TB(Tera Bytes) 용량에 이를 만큼 방대하여 특별한 도구(Tool)없이 관련 디지털 증거자료를 수집 분석하기는 불가능한 현실이다. 예를 들어 1 기가 바이트(Tera Bytes) 정도의 데이터라면 1.5톤 트럭 한 대 분량의 자료가 출력되며, 2 테라(Tera) 바이트 분량은 웬만한 대학의 도서관 소장 문헌의 분량에 해당할 정도에 달한다(최신득, 2008).

그리고 개인컴퓨터 뿐만 아니라 여러사람이 공동으로 사용하는 서버의 경우에 있어 디지털 포렌식의 업무를 수행할 경우 범죄와 관련 없는 개인정보 등의 데이터가 수집될 가능성이 크므로 법적 문제가 발생될 수 있다. 영장주의 원칙상 포괄적 영장은 허용되지 않고 영장의 허용범위를 넘어서 수집한 디지털 증거는 적법절차에 따르지 않고 수집된 것으로 인정되어 증거능력이 부여될 수 없다. 그러므로 대용량의 저장매체를 압수하여 관련 디지털 증거를 수집하는 경우에 있어 대용량에 대응하는 강력한 성능을 가진 시스템이 필요하고 전문가에 의한 디지털 증거 분석이 필요하다고 할 수 있다.

2.6. 네트워크 관련성

첨단 통신기술과 정보통신망의 발달로 컴퓨터를 비롯한 다양한 디지털 기기 등은 네트워크로 연결되어 있고 특정 매체에 저장된 정보는 네

트워크를 통하여 전 세계적으로 전송되어 저장될 가능성이 있는 현실에서 디지털 정보를 수집하기 위하여 네트워크를 통하여 접근해야 하는 필요가 있다. 이럴 경우 압수수색의 장소가 어느 범위에서 특정되어야 하는 문제가 발생되고 네트워크로 연결된 원격지의 서버에 관련 디지털 증거가 있을 경우 원격지에 대한 압수수색이 가능한가가 문제가 될 수 있다. 이때 재판 관할권 문제가 발생할 수 있으며 디지털 증거조사를 위해 국제공조가 필요하게 된다.

2.7. 전문성

디지털 방식으로 저장된 정보를 파악하고 수집하여 해석하는 방법에 대하여 여러 가지 다양한 기술과 프로그램에 대한 전문적 지식이 필요하고 디지털 증거의 수집과 분석에 전문적 기술이 사용되고 많은 전문가가 개입할 여지가 생기며 증거법적으로 문제가 발생할 소지가 많다(양근원, 2006).

3. 디지털 증거의 유형

3.1. 디지털 증거와 아날로그 증거의 차이

아날로그(analog)란 어떤 수치를 연속적인 방법으로 나타낸 것이라는 사전적 정의가 있다. 시간의 경우 시간의 흐름은 아날로그 적 흐름인데 예를 들어 아날로그시계를 생각해 보면, 초와 초 눈금 사이에 물 흐르듯이 초침이 지나가는 시계를 연상해 볼 수 있는데 각 초(second)가 존재하지만 그 초간 중간 영역에 해당하는 어중간한 값의 시각이 존재한다. 그와는 반대로 디지털(digital)은 0과 1, on과 off 같은 중간에 어떠한 값이 없는 똑 부러지는 형태의 체계를 이룬다. 단순함으로 혼동이 없기에 오류가 발생할 여지가 아날로그에 비하여 무척 낮다. 현대 인류문명이

거의 모든 분야에서 디지털화 되고 있는 현실에서도 인간이 보고 느끼는 모든 감각은 아날로그 적일 수밖에 없고 어떠한 종류의 신호라도 디지털로 표현하면 부드럽게 표현하는데 한계가 있을 수밖에 없다. 모든 전자기기는 0과 1의 디지털 개념으로 움직이는 장치인데 그 신호를 처리하고 저장하는 방법에 있어 아날로그 방식으로 수행하는지 또는 디지털 방식으로 수행하는지의 구분으로 나눌 수 있다. 과거의 전자장비는 아날로그 방식으로 수행되었는데 0과 1이 아닌 신호의 강·약으로 신호를 처리하고 저장하였다. 그러나 강·약의 신호를 바꾸는 과정에서 시간이 소요되고 불필요한 노이즈가 발생되는 단점이 있었고 저장, 전송되는 과정에서 신호의 변질(변화)될 가능성이 컸다. 이런 아날로그 방식의 단점으로 인해 정보처리의 방식이 디지털 방식으로 급속하게 변화되면서 정보통신 발달과 맞물려 정보처리에 혁신이 있어 왔고, 형사적 절차의 수사와 재판 과정에 있어 증거의 형태에도 디지털 증거의 차지하는 비중이 커지고 있다. 전통적 아날로그 증거라고 할 수 있는 증인의 증언, 서증, 전문가의 감정 등과 동시에 많은 정보들이 디지털화되어 수사과정과 공판절차에 제출되고 있다.

그러나 국내 형사법 관련 규정은 아직 아날로그적 증거에만 치우쳐 디지털화 환경에 특화되어 있지 못하다. 그 예로 디지털 증거가 형사소송법 상 압수의 대상인 물건[8]에 포함되는지 여부에 대하여 침묵으로 일관하고 있다(권오걸, 2011).

3.2. 디지털 증거의 유형 분류방법

디지털 증거의 유형을 나누는 방법에 있어 생성주체에 의한 방법, 디

8) 형사소송법 제106조(압수)③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이항에서 “정보저장매체 등”이라 한다)인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체 등을 압수할 수 있다.

지털 정보의 존재형식에 따른 방법, 휘발성 여부에 따른 방법 등 여러 가지 분류 방법이 있다.

3.2.1. 생성주체에 의한 분류

사람의 처리과정에 의하여 생성된 디지털 증거와 컴퓨터 자체에 의하여 생성된 정보로 나눌 수 있다. 사람의 처리과정에 의하여 생성된 디지털 증거는 작성자의 동의가 없는 한 법적인 증거능력이 인정되지 않고, 컴퓨터 자체에 의하여 생성된 디지털 증거는 파일명, 해쉬값 등의 디지털 증거를 식별하는데 도움이 되는 메타데이터를 말하며 이는 디지털 기기가 작동하는 과정에서 자동으로 생성된다.

3.2.2. 저장된 증거와 전송 중인 증거

디지털 증거가 디지털 디바이스 내에 존재하거나 네트워크를 통하여 전송 중인 증거로 나눌 수 있다. 이는 증거조사의 방법에 따른 디지털 증거의 수집방법으로 구분될 수 있는데, 디지털 디바이스 내부에 저장되어 있는 증거일 경우 법관이 발부한 압수수색영장에 의거 이를 압수할 수 있으나, 네트워크를 통하여 전송 중인 디지털 증거의 경우 감청에 해당하므로 통신비밀보호법상의 통신제한조치 허가서에 의하여 수집이 가능하다(권오걸, 2011).

3.2.3. 휘발성 증거와 비휘발성 증거

휘발성 증거는 특정 프로그램이 실행될 때 생성되는 데이터이나 전원이 차단되거나 프로그램이 종료될 시 사라지는 성질을 가진 정보를 말한다. 컴퓨터에서 주기억장치인 RAM, 비디오 카드나 네트워크 카드 등에 존재하는데 주로 메모리에 저장되는 정보로 이를 수집하기 위해서는 파일 형태로 별도 저장되거나 사진촬영 등의 방법으로 수집되고 컴퓨터 시

스템 등을 이용하여 범행 중인 상태를 나타내는 중요한 자료가 될 수 있다(김교성, 2014). 비휘발성 증거는 시스템의 전원 공급이 차단되거나 시스템이 종료되더라도 지워지지 않고 유지되는 정보를 말한다. 컴퓨터의 하드디스크, ROM, CD, USB 등에 저장된 정보는 비휘발성 증거가 된다.

제 2 절 디지털 포렌식

1. 디지털 포렌식의 개념

디지털 포렌식(Digital Forensic)이란 컴퓨터, 네트워크, 그리고 디지털 기기 등에 존재하는 다양한 전자적 증거를 인식하여 수집, 보존, 문서화, 분석, 검증, 제시하는 일련의 과학적 방법을 말한다(Lang et al., 2014). 쉽게 디지털 증거물 등을 사법기관에 제출하기 위하여 디지털 데이터를 수집, 분석, 보고서를 작성하는 일련의 작업을 의미한다.[9)]

디지털 포렌식의 개념이 형성되기 이전에는 컴퓨터 포렌식(Computing Forensics)이라는 개념이 사용되고 있었다. 1984년 초 미국 FBI는 컴퓨터 증거의 중대성이 높아지고, 검찰이나 수사관들의 컴퓨터 증거에 대한 수요가 증가함에 따라 컴퓨터 분석 및 대응팀(Computer Analysis and Response Team)을 설치하였다(Whitcomb, 2002). 그러다가 1991년 국제 컴퓨터 수사전문가 협회(International Association of Computer Investigative Specialist)에서 교육과정을 개설하여, 디지털 포렌식이라는 용어를 처음 사용하게 되었다(송봉규·장석헌, 2013). 이후 컴퓨터 자체에 대한 압수·수색 문제, 관련 증거, 보안 등에 대한 연구가 진행되어 이 분야를 컴퓨터 포렌식이라고 불리어지다 이후 아날로그에서 디지털로의 데이터 저장방식의 변화와 다양한 디지털 자료를 생성하는 기기 등의 출현으로 컴퓨터 매체나 그 출력물에 대한 관심에서 벗어나 그 본래 소스인 디지털 증거 자체에 연구의 초점이 맞추어 지면서 디지털 포렌식으로의 명칭이 변화되기 시작하였고, 2001년 8월 미국 대학 연구진들과 컴퓨터 포렌식 전문가들이 뉴욕주 유티카에서 '디지털 포렌식 연구 워크숍(Digital Forensic Research Workshop)'을 개최하면서 정식으로 디지털 포렌식이라는 용어가 사용되기 시작하였다(탁희성·이상진,

9) 위키피디아 https://ko.wikipedia.org/wiki

2006).

포렌식(forensic)의 어원은 고대 로마시대의 “Forum”이라는 라틴어에서 유래한 것으로 많은 사람이 모여 상거래를 하거나 논쟁을 하는 장소였는데, 근래 “법정의”, “공개토론이나 변론에 사용되는”, “수사와 법정에서의 증거 또는 사실관계를 확정하기 위하여 사용하는 과학이나 기술에 관한”, “범죄와 관련된 증거물을 과학적으로 조사하여 정보를 찾아내기 위한”이라는 의미를 갖는 형용사이며, 일반적으로 법정변론을 위하여 사용되는 과학, 즉 법정과학 또는 법과학이란 개념으로 이해된다(유영찬, 2002).

대검찰청 예규인 「디지털 포렌식 수사관의 증거 수집 및 분석 규정」제2조(정의) 제2호에서 "디지털포렌식"이란 디지털 증거를 수집·분석 또는 보관하거나 현출하는데 필요한 기술 또는 절차를 말한다고 정의한다.

디지털 포렌식은 수사관에게 디지털 긎거를 수집하는 과정에서 합법적이고, 과학적인 범죄 입증절차를 제시하고 있으며, 과학적인 절차에 의해 수집된 증거를 최종적으로 법원에 제출함으로써 범죄사실의 증명을 한층 강화하고 있다. 즉, 포렌식은 수사과정에서 과학적이고 체계적인 증거확보 절차에 따라 합법적인 증거를 산출해냄으로써 범죄자 색출 및 범죄사실의 증명을 통한 실체적 진실의 발견에 크게 기여하고 있다. 따라서 디지털 포렌식은 단순히 디지털 증거 수사를 위한 과학적인 방법 및 절차를 연구하는 학문에서 한발 더 나아가 디지털 증거의 증거능력을 부여하기 위한 소송법적 영역의 한 분야를 이루는 학문이다(곽병선, 2011)

2. 디지털 포렌식의 기본원칙

2.1. 적법절차의 준수

적법절차의 준수는 수사 전반에 걸쳐 적용되는 원칙이다. 디지털 포렌식 수사도 위 원칙에 의거 필요 한도 내에서 최소한의 증거 수집을 해야 하며, 일반적인 형사소송법 원칙을 준수하여야 한다.

이에 따라 대검예규인 「디지털 포렌식 수사관의 증거 수집 및 분석 규정」을 보면, 제12조(과잉금지 원칙 준수)에서 “디지털 증거를 압수수색·검증 할 때에는 수사에 필요한 최소한의 범위에서 실시하여야 하고, 모든 과정에서 적법절차를 엄격히 준수하여야 한다.”고 규정되어 있고, 제13조(디지털 포렌식 수사관에 의한 압수수색·검증)에서 “디지털 포렌식 수사관 또는 대검찰청에서 실시한 디지털 증거 압수수색 실무교육을 받은 수사관이 하여야 한다. 다만 긴급을 요하는 등 부득이한 사유가 있는 경우에는 다른 수사관이 이를 대신할 수 있으며, 이 경우 디지털수사과장 등에게 그 사실을 통보하고 협조를 구해야 한다.”고 규정하고 있다.

경찰청 훈령「디지털 증거 수집 및 처리 등에 관한 규칙」에서도 제3조(인권보호 원칙)에서 “디지털 증거의 수집, 운반, 분석 및 보관 업무를 수행하는 자는 개인의 인권을 존중하고 사건 관계인의 명예를 훼손하지 않도록 주의하여야 하며, 직무상 알게 된 비밀을 지켜야 한다.”라는 조항이 있고, 제8조(과잉금지의 원칙)에서 “디지털 데이터의 수집은 수사목적을 달성하는데 필요한 최소한의 범위에서 이루어져야 한다.”고 규정되어 있다.

2.2. 원본증거의 절대적 보존

디지털 증거는 그 특성상 조작 또는 훼손 가능이 물리적 증거보다 용이하므로 실체적 진실 발견을 위한 법절차에서 디지털 증거의 진정성과 무결성의 문제는 대단히 중요하다.

진정성(authenticity) 문제는 특정인의 행위의 결과가 정확히 표현되도록 만들어졌는지에 관한 최초의 성립(작성)과정의 순수성을 주로 다루는 것이고, 또한 이후 자료의 저장, 수집, 보존, 제출 과정에서 오류가 발생

하였는지 여부를 다루는 문제인 반면, 무결성(integrity)은 저장, 수집된 이후 증거의 변경이나 훼손 여부를 다룬다는 점에서 차이가 있는데 간단히 진정성은 최초의 증거와 법정에 제출된 증거가 일치한다는 성질을 밝히는 것이고, 무결성은 디지털 증거의 수집, 관리 등의 절차적 측면에 초점을 맞춘 의미이다(한명훈, 2015). 무결성의 문제는 증거처리의 전반적 과정에서 문제가 되므로 무결성이 바로 진정성을 의미한다고 보아야 하기 때문에 굳이 이를 구별하여 설명할 필요는 없어 보인다(전명길, 2011).

대검찰청 예규인 「디지털 포렌식 수사관의 증거 수집 및 분석 규정」제4조 (디지털 증거의 무결성 유지)에서 디지털 증거는 압수·수색·검증한 때로부터 법정에 제출하는 때까지 훼손 또는 변경되지 아니하여야 한다고 규정되어 있고, 경찰청 훈령인「디지털 증거 수집 및 처리 등에 관한 규칙」제4조(증거수집 및 처리의 원칙)에서 ① 출력·복사·복제된 디지털 증거는 원본과 동일성이 유지되어야 한다. ② 디지털 증거는 압수 시부터 송치 시까지 변경 또는 상실되지 않도록 주의하여야 한다고 규정되어 있어 디지털 증거의 무결성, 동일성을 유지하면서 디지털 포렌식 업무를 수행하여야 한다는 점을 강조한다.

2.3. 분석자와 도구의 신뢰성 확보

디지털 포렌식 수행은 사람에 의하여 이루어지며 분석한 결과에 대하여 증거로서의 신뢰와 가치를 가지기 위해서는 전문적인 자격을 가진 분석관에 의하여 도출된 결과임을 증명할 필요가 있다. 우리나라의 검찰과 경찰의 디지털 포렌식 관련 규정[10]을 보면 디지털 포렌식 수사관 등의 자격과 임명을 엄격히 정하고 있다.

디지털 포렌식은 실행과정에서 다양한 소프트웨어와 기기들이 사용

10) 대검찰청 예규 제805호 디지털 포렌식 수사관의 증거수집 및 분석규정 제6조, 경찰청 훈령 제766조 디지털 증거 수집 및 처리 등에 관한 규칙 제5조

되어 지는데 신뢰성 확보 면에서는 디지털 포렌식에 사용되는 검증된 소프트웨어 사용이 가장 중요한 부분을 차지하며, 제3자 어느 누가 분석하더라도 동일한 결과가 얻어져야 한다. 미국의 경우 법무부 산하 국가표준기술연구소(NIST ; National Institute of Standard and Technology)에서 CFTT(Computer Forensic Tool Testing) 프로젝트를 주관하며 이는 디지털 포렌식 분석자가 정확한 결과를 산출하는데 사용하는 도구(Tool)이 적정한지 판단하고 보장해 주는 기능을 담당하며 CFTT의 테스트 결과는 툴개발자에게 툴에 대한 개선점을 피드백 하는 역할을 한다(양근원, 2006).

국내 관련 규정으로 대검찰청 예규인 「디지털 포렌식 수사관의 증거수집 및 분석 규정」제6조 (디지털 포렌식 수사관의 임명)에서 디지털 포렌식 수사관 임명에 대하여 엄격한 자격을 요구하며, 디지털 포렌식 수사관으로 임명된 자는 전문성 향상을 위하여 매년 대검찰청 디지털수사과나 국내외 국가기관, 전문교육기관 또는 학회에서 실시하는 디지털 포렌식 관련 교육을 이수하도록 요구함을 볼 수 있고, 제5조 (디지털 증거의 신뢰성 유지)에서 디지털 증거는 그 수집 및 분석 과정에서 이용된 도구와 방법의 신뢰성이 유지되어야 한다고 규정되어 있다.

또한 경찰청 훈령인 「디지털 증거 수집 및 처리 등에 관한 규칙」에서 제5조(증거분석관의 자격 및 선발)에서 경찰 교육기관의 디지털 포렌식 관련 전문교육을 수료한 자, 국가 또는 공공기관의 디지털 포렌식 관련 분야에서 3년 이상 근무한 자, 디지털 포렌식, 컴퓨터공학, 전자공학, 정보보호공학 등 관련 분야 대학원 과정을 이수하여 석사 이상의 학위를 소지한 자, 디지털 포렌식, 컴퓨터공학, 전자공학, 정보보호공학 등 관련 분야 학사학위를 소지하고, 해당 분야 전문교육 과정을 수료하거나 자격증을 소지한 자 중 어느 하나의 조건에 해당되어야 증거분석관으로 선발될 요건이 된다.

2.4. 디지털 포렌식에 대한 기본 원칙을 밝힌 판례 및 규정

‘일심회’관련 대법원 판례[11]에서, 압수물인 디지털 저장 매체로부터 출력한 문건을 증거로 사용하기 위해서는 디지털 저장 매체 원본에 저장된 내용과 출력한 문건의 동일성이 인정되어야 하고, 이를 위해서는 디지털 저장 매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았음이 담보되어야 한다. 특히 디지털 저장 매체 원본을 대신하여 저장 매체에 저장된 자료를 하드카피 또는 이미징한 매체로부터 출력한 문건의 경우에는 디지털 저장 매체 원본과 하드카피 또는 이미징한 매체 사이에 자료의 동일성도 인정되어야 할 뿐만 아니라, 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다고 판시하였다.

또한 관련 규정으로는 형사소송법 제292조의3[12] 에서 정보를 담기 위하여 만들어진 물건으로서 문서가 아닌 증거의 조사에 관하여 필요한 사항을 대법원규칙으로 정하도록 하는 규정에 따라, 형사소송규칙 제134조의7(컴퓨터용디스크 등에 기억된 문자정보 등에 대한 증거조사)에서 ① 컴퓨터용디스크 그 밖에 이와 비슷한 정보저장매체(다음부터 이 조문 안에서 이 모두를 “컴퓨터디스크 등”이라 한다)에 기억된 문자정보를 증거자료로 하는 경우에는 읽을 수 있도록 출력하여 인증한 등본을 낼 수 있고 ② 컴퓨터디스크 등에 기억된 문자정보를 증거로 하는 경우에 증거조사를 신청한 당사자는 법원이 명하거나 상대방이 요구한 때에는 컴퓨터디스크 등에 입력한 사람과 입력한 일시, 출력한 사람과 출력한 일시를 밝혀야 하며 ③ 컴퓨터디스크 등에 기억된 정보가 도면 사진 등에 관한 것일 때에는 제1항과 제2항의 규정을 준용한다고 규정하고 있다. 그리고

11) 대법원 2007. 12. 13. 선고 2007도7257

12) 형사소송법 제292조의3(그 밖의 증거에 대한 조사방식) 도면 사진 녹음테이프 비디오테이프 컴퓨터용디스크, 그 밖의 정보를 담기 위하여 만들어진 물건으로서 문서가 아닌 증거의 조사에 관하여 필요한 사항은 대법원규칙으로 정한다.

앞서 살펴보았듯이 대검찰청 예규인 「디지털 포렌식 수사관의 증거 수집 및 분석 규정」와 경찰청 훈령 「디지털 증거 수집 및 처리 등에 관한 규칙」에서도 디지털 포렌식 기본원칙 준수에 대하여 규정함을 볼 수 있다.

3. 디지털 포렌식 유형[13)]

국내 디지털 포렌식 관련 서적과 논문 등에는 디지털 포렌식 유형에 대하여 일반적으로 디스크 포렌식, 네트워크 포렌식, 인터넷 포렌식, 데이터 베이스 포렌식, 모바일 기기 포렌식, 암호 포렌식 등으로 나누는 것을 볼 수 있다. 이런 유형은 디지털 기기의 발전 상황에 따른 분류이며 아래의 분류방법은 디지털 포렌식의 실무적인 시점에서 디지털 포렌식 유형을 세분화한 분류방법이다.

3.1. 컴퓨터 포렌식

컴퓨터 포렌식은 디지털 포렌식을 구성하는 전통적인 영역이며 실무자들이 상당한 비중을 두는 영역이라고 할 수 있다. 컴퓨터는 사건에서 유용하게 활용될 수 있는 다양하고 방대한 정보를 담고 있는 경우가 많다. USB나 휴대전화, 디지털 카메라, 외장형 하드드라이버 등은 메인 컴퓨터와의 연결이 빈번이 발생되므로 그 내용이나 접속기록이 컴퓨터에는 지문처럼 남게 되어 사건의 실마리가 될 수 있다. 컴퓨터 포렌식은 사용자계정, 로그파일, 타임스탬프, 이미지파일, 이메일 등을 분석하거나 컴퓨터 내 저장장치에 존재하는 데이터 등을 분석하는 것이 중요한 목적이다.

---

13) Larry E. Daniel, Lars E. Daniel, Digital Forensics for Legal Professionals 한국어 번역판, BJ퍼블릭, p.22 ~ 29 인용

3.2. 사고 대응(Incident Response)

디지털 포렌식 전문가들은 사고대응이라는 개념을 디지털 포렌식의 세부적 분야로 보기도 하며 디지털 포렌식의 한 유형 즉 네트워크 포렌식이라고 한다. 여기서 사고(Incident)라는 의미는 네트워크에 대한 보안 침해 상황을 말하며 네트워크 보안, 해킹, 악성코드 등 다양한 상황이 포함된다. 전문가들은 네트워크 공격 파악, 악성 코드 전파 여부 및 침입 경로 확인, 악성 코드 제거 등의 역할을 하며 감염된 데이터를 복구하는 작업을 하기도 한다.

3.3. 휴대폰 포렌식

휴대폰 포렌식은 급증하는 휴대전화 사용자와 휴대전화 내 저장된 정보의 중요성으로 인하여 통화기록, 문자메시지, 사진이나 비디오, 오디오 기록, 이메일을 통한 분석이 사건을 해결하는 중요한 방법이 되고 있고 관련 증거의 확보가 수사의 성패를 가를 만큼 중요하고 필수적인 분야로 인식되고 있다.

3.4. 위치정보(GPS)포렌식

GPS 장비를 확인하여 사람이나 자동차가 이동한 상황을 확인할 수 있고 최근 방문위치, 자주 방문하는 장소, 주소나 전화번호를 검색한 자료 등 다양한 정보를 얻을 수 있다.

3.5. 미디어 장치 포렌식

미디어 장치란 디지털 오디오 녹음기, 디지털 뮤직 플레이어,

PDA(Personal Data Assistants), USB, 외장형 하드 드라이버 등을 일컫는다. 기기 내 존재하는 파일을 추출하거나 삭제된 파일을 복구하여 가치있는 증거로서의 자료를 확보한다. 이런 미디어 장치가 컴퓨터와 연결될 시 전송된 파일과 전송이 일어난 일자 등의 정보를 컴퓨터에 남기게 된다.

3.6. 소셜 미디어(Social Media) 포렌식

트위터, 페이스북, 카카오톡과 같은 소셜 네트워크를 사용하지 않는 사람이 거의 없을 정도로 보편적인 생활의 도구가 되어 왔다. 이런 소셜 미디어는 기존의 이메일보다 사람들 간의 의사소통의 역할을 담당하고 있어 하드드라이버나 휴대폰에 남겨진 관련 데이터를 발견하여 사건해결에 도움을 줄 수 있다.

3.7. 디지털 비디오 및 사진 포렌식

사진은 정지 이미지(Still Image)이고 비디오는 정지 이미지의 연속된 장면이다. 디지털 비디오 및 사진 포렌식은 이러한 개별적 정지 이미지에 대한 분석을 하고 이미지의 해상도나 선명도, 화질 등을 향상시키는 개선작업 기법이라고 할 수 있다.

3.8. 디지털 카메라 포렌식

고전적인 필름 카메라는 거의 디지털 카메라로 대체되었다. 필름 카메라는 사진만 남기지만 디지털 카메라는 사진 그 자체 외 사진에 대한 많은 정보 즉 메타데이터를 남기는데 이를 통하여 증거가치가 있는 데이터를 수집할 수 있다.

3.9. 디지털 오디오 포렌식

디지털 음성 녹음 장치에서 만들어진 음성 데이터를 분석하고 녹음된 음질을 개선하는 기법을 말한다. 이 기법을 활용하여 녹음된 음성의 무결성을 확인하거나 음성의 훼손 여부를 확인할 수 있다.

3.10. 멀티미디어 게임 포렌식

최근 가장 인기가 많은 게임은 멀티플레이어 게임이며 특히 다중 접속 온라인 역할 게임(MMORPGs ; Massively Multiplayer Online Role Playing Games)은 전 세계적으로 수많은 사람들이 장시간 이 게임을 즐기고 있다. 접속자가 선택한 캐릭터가 게임 속 세상을 탐험하면서 해당 역할을 수행하면서 획득한 점수에 따라 캐릭터의 레벨이 올라가며 게임에 가입된 캐릭터들의 단체나 씨족에 가입하는 방식이다. 멀티플레이어 게임에서 생성된 기록은 타임라인을 수립하거나 알리바이 확인 또는 게임 중 채팅한 내용을 확인하여 이를 활용할 수 있다.

3.11. 게임 콘솔(Game Console) 포렌식

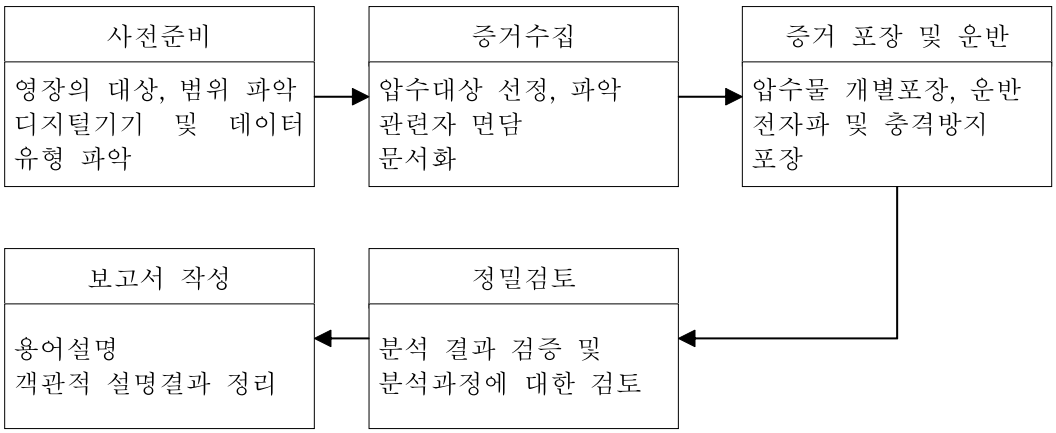
소니의 플레이스테이션(Sony Playstation), 닌텐도 위(Nintendo Wii) 등의 게임 콘솔은 기본적인 기능은 컴퓨터와 유사하다. 운영체제를 가지며 하드 드라이브가 포함되어 있다. 그래서 게임 뿐만 아니라 인터넷을 검색하거나 영화를 보는 데 이용되기도 하여 게임 콘솔에도 증거로 활용될 수 있는 데이터가 남으므로 이를 활용할 수 있다.

4. 디지털 포렌식 절차

미 법무부 산하 국립사법연구원(NIS ; National Institute of Justice)는 법집행기관 포렌식 전문가, 학자, 변호사 등을 구성원으로 하는 디지털 증거분석 기술연구 그룹(TWGEDE ; Technical Working Group for the Examination of Digital Evidence)을 설치하여, 2004년 '디지털 증거분석 지침(Forensic Examination of Digital Evidence : A Guide for Law Enforcement)[14]'을 제시하였다.

이 지침에서 디지털 포렌식 절차를 보면, 증거 평가(Evidence Assessment), 증거 획득(Evidence Aquisition), 증거 분석(Evidence Examination), 기록 및 보고(Document and Reporting)순으로 수행된다(양근원, 2006). 이를 실무적으로 세분화하여 설명하면 아래 <그림 2-1>과 같은 과정으로 구성된다.

<그림 2-1> 디지털 포렌식 절차



* 이상식(2010), 디지털 포렌식 개론,

14) https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

국내에서 디지털 포렌식 세부 절차에 대한 규정으로는 대검찰청의 디지털 포렌식 수사관의 증거수집 및 분석규정(대검찰청 예규 제805호, 2015. 7. 16. 일부개정) 과 경찰청의 디지털 증거 수집 및 처리 등에 관한 규칙(경찰청훈령 제766호, 2015. 5. 22. 제정)이 있다.

4.1. 대검찰청의 디지털 포렌식 수사관의 증거수집 및 분석규정

제1장 총칙에서 목적, 적용범위, 정의, 디지털증거의 무결성 유지, 디지털 증거의 신뢰성 유지, 디지털 포렌식 수사관의 임명, 거점청 디지털 포렌식팀 설치 및 운영, 디지털 포렌식 수사관의 배치, 제2장 디지털 증거의 수집·분석 지원요청에서 지원요청, 협조의무, 정보보고에 대한 규정이 있고, 제3장 디지털 증거의 압수·수색·검증에서 과잉금지원칙 준수, 디지털포렌식 수사관에 의한 압수·수색·검증, 사전준비, 정보저장매체 등의 압수·수색·검증, 정보저장매체의 운반, 복귀 및 보고에 대한 내용이 있고, 제4장 디지털 증거의 등록에서 이미지 파일의 등록, 정보저장매체 등의 등록 및 책임자등의 참여가 있고, 제5장 디지털 증거의 분석에는 분석보고서 작성, 분석결과 통보 등으로 구성되어 있다.

4.2. 경찰청의 디지털 증거 수집 및 처리 등에 관한 규칙

제1장 총칙에서 목적, 정의, 인권보호 원칙, 증거수집 및 처리의 원칙, 증거분석관의 자격 및 선발, 디지털 증거 분석의 체계, 다른 법령과의 관계, 제2장 디지털 증거의 수집에서 과잉금지의 원칙, 지원 요청 및 처리, 영장 집행의 준비, 영장 집행의 방법, 압수절차, 임의제출, 제3장 증거분석 의뢰, 증거분석 접수, 신뢰성 확보 조치, 디지털 증거의 분석, 증거분석실 등의 출입제한, 결과보고서 작성, 필요적/임의적 기재사항, 분석결과 통보, 보관 및 반환, 디지털 증거의 보관 및 삭제·폐기로 구성된다.

4.3. 검찰과 경찰의 디지털 증거수집 등에 대한 규정의 차이점

검찰과 경찰의 디지털 증거수집과 분석, 처리 등에 대한 규정은 그 절차와 방법 면에서 내용이 유사하나 검찰의 경우를 보면, 제18조 정보저장매체 등에 기억된 정보를 이미지 파일로 복제한 경우에는 이를 디지털수사통합업무관리시스템[15]에 등록하며, 제22조 디지털 증거의 분석은 디지털수사통합업무관리시스템에 등록된 이미지 파일로 한다. 다만, 이미지 파일로 복제하는 것이 곤란한 경우에는 압수 또는 복제한 정보저장매체 등을 직접 분석할 수 있으며, 이 경우에는 정보저장매체 등의 형상이나 내용이 훼손·변경되지 않도록 적절한 조치를 취하여야 한다고 규정되어 디지털통합업무관리시스템을 통하여 디지털 정보의 수집과 분석을 일률적으로 운영함을 볼 수 있다.

15) 대검찰청 예규 제805호 디지털 포렌식 수사관의 증거수집 및 분석규정 제3조(정의)에서 “디지털수사통합업무관리시스템”이란 디지털 증거의 수집 및 분석에 관한 사항과 디지털 증거의 보관에 관한 이력 등을 관리하는 전산시스템을 말한다.

제 3 절 디지털 포렌식의 필요성

1. 사이버 범죄의 증가

컴퓨터, 임베디드 기기 등 디지털 디바이스 사용의 폭발적 증가와 그로 인한 인터넷, 소셜 네트워크 등의 사용 증가에 비례하여 사이버 범죄는 늘고 있다. 이런 정보통신기술의 발달은 범죄자들에게 새로운 범죄의 기회를 제공하고 있다. 사기, 명예훼손, 모욕, 지적재산권 침해 등 기존의 범죄 유형이 정보통신기술을 주된 또는 보조적 도구로 사용하는 실정이다. 또한 사이버 범죄 뿐 아니라 일반적인 범죄에서도 중요한 단서가 되는 증거가 피의자와 관련되는 일반 디지털기기 내에 보관되어 있는 경우가 증가하고 있는 실정이다. 경찰청 사이버안전국 사이버범죄 통계인 <표 2-1>을 보면, 국내 사이버범죄는 지속적으로 증가하고 있음을 볼 수 있다.

<표 2-1> 경찰청 사이버안전국 사이버범죄 현황

구 분	총 계			사이버테러형 범죄			일반사이버 범죄		
	발생	검거		발생	검거		발생	검거	
		건수	인원		건수	인원		건수	인원
2004	77,099	63,384	70,143	15,390	10,993	11,892	61,709	52,391	58,251
2005	88,731	72,421	81,338	21,389	15,874	17,371	67,342	56,547	63,967
2006	82,186	70,545	89,248	20,186	15,979	17,498	62,000	54,566	71,750
2007	88,847	78,890	88,549	17,671	14,037	15,302	71,176	64,853	73,247
2008	136,819	122,227	128,635	20,077	16,953	17,649	116,742	105,274	110,986
2009	164,536	147,069	160,656	16,601	13,152	13,619	147,935	133,917	147,037
2010	122,902	103,809	111,772	18,287	14,874	16,777	104,615	88,935	94,995
2011	116,961	91,496	95,795	13,396	10,299	11,399	103,565	81,197	84,396
2012	108,223	84,932	86,513	9,607	6,371	7,239	98,616	78,561	79,274
2013	155,366	86,105	92,621	10,407	4,532	5,514	144,959	81,573	87,107

* 내사종결도 사이버범죄의 변화추이를 분석할 수 있다는 점에서 포함

<표 2-2> 사이버 범죄의 유형

구분	총 계			정보통신망침해범죄			정보통신망이용범죄			불법컨텐츠범죄		
	발생	검거		발생	검거		발생	검거		발생	검거	
		건수	인원		건수	인원		건수	인원		건수	인원
2014	110,109	71,950	59,220	2,291	846	1,171	89,581	56,461	38,579	18,299	14,643	19,470
2015	144,679	104,888	75,250	3,154	842	1,098	118,362	86,658	50,777	23,163	17,388	‘23,375

* ’14. 7.부터 사이버 新범죄유형 통계를 적용하여 舊유형과 新유형간 비교는 어려움.

’14년 누적통계는 ’14년 상반기 KICS 소급입력자료’ 반영

특히 2014년과 2015년의 정보통신망 이용 범죄의 통계를 보면, 사건발생 비율이 전년 대비 32.1 %, 검거인원은 전년대비 31.6 % 증가되어 인터넷 사기, 사이버 명예훼손 등의 정보통신망 이용 범죄는 급증하고 있음을 보여준다.

2. 전통적 범죄에 있어 디지털 정보기술 활용 증가

전통적인 범죄 그 중 개인 간에 빈번히 발생하는 상해, 폭행, 살인, 성범죄, 재산 범죄 등의 최근 유형에 있어 범행 행위자가 그 범죄의 도구로 다양한 디지털 기기 또는 정보통신망 등 디지털 정보기술을 이용하여 위 유형의 범죄를 발생시키는 경우가 많아지고 있다. 그러므로 이런 유형의 범죄에 대한 수사방법은 사용된 디지털 기기 또는 정보통신망에 대한 디지털 포렌식 수사가 필수이며 범죄자 등이 범죄 실행의 도구로 사용하는 컴퓨터, 스마트폰, 이메일, IT기기 등에 저장된 디지털 자료에 대한 분석뿐만 아니라, 범죄자 자신이 의식하지 못하는 사이 디지털 정보매체에 노출되었을 가능성이 크므로 전자적 증거를 추적하여 얻어진 다양한 디지털 정보가 범죄 수사 해결의 실마리를 제공하여 준다.

3. 미국 e-Discovery 제도의 도입

3.1. e-Discovery의 개념

e-Discovery는 electronic Discovery의 약자로 ESI(Electronically Stored Information)에 대한 증거개시(Discovery)를 말한다.

e-Discovery의 대상인 ESI에 대하여 문구 그대로 해석하면 전자적으로 저장된 정보를 말하는데, 컴퓨터 하드웨어나 소프트웨어에 사용하기 위해 디지털 형태로 생성 및 사용되는 정보를 지칭하며, 컴퓨터 등의 디지털 정보기기를 통하여 생성되고 검색 가능한 형태로 저장 된다(탁희성, 2011). 최근 판례와 법정에서 요구하는 증거의 요건에 대한 측면에서 디지털 포렌식에서 말하는 디지털 증거(Digital Evidence)의 개념과 거의 일치한다고 볼 수 있고, 증거개시(Discovery)란 소송상대방의 요청으로 소송과 관련된 정보를 의무적으로 공개하는 절차로서 재판과 관련된 소송 당사자 또는 당사자들이 서로 특정한 상황과 관련된 사실을 찾는 법적 절차를 말한다(유정호·박영수, 2014).

Discovery 제도는 일찍이 영국의 형평법(Equity)에서도 발견되는데 현대적인 의미의 Discovery 제도는 19세기 보통법(Common Law)과 형평법의 통합이 있은 후에야 시작되었고(서동희, 2005), 사실상의 법제화는 미국에서 1938년 제정된 연방민사소송규칙(The Federal Rules of Civil Procedure, FRCP)에 증거개시제도를 규정되었는데, 어떤 증거가 있으며 그 증거를 활용할 수 있는지를 상대방이 평가하여 쟁점을 명확히 하고 시간낭비를 줄일 수 있는 소송의 사전 개시절차인 조사 단계에서 이루어진 절차라고 할 수 있으며 당사자의 증거개시 요청을 상대방이 거부해 분쟁이 생기면 법원이 개입한다[16]. 즉 법원에서 공개재판(trial)이 시작되기 전인 소송 전 단계에서 양 당사자 또는 제3자가 보관하고 있는 소송 관련 증거를 공개하는 절차를 말하며 법원은 당사자에게 증거를 보

16) 한국 EMC 컨설팅, CEO E-DISCOVERY를 고민하다, 2011, 전자신문사, p.13

존할 것을 명령하고 그 증거를 공개하도록 하는 것이 이 제도의 핵심이라 할 수 있다.

제도가 도입될 당시는 증거개시의 대상이 오프라인 상 유형물로 국한하였으나 컴퓨터 등의 기기의 개발과 정보통신기술의 발달로 인하여 디지털 증거물의 비중이 날로 커지고, 기존의 종이문서를 주 대상으로 하던 증거개시절차가 디지털 자료로 대상이 옮겨감에 따라 이를 제대로 규율하기 어려운 문제가 발생하게 됨에 따라 2006년 12월 1일 개정, 발효된 연방민사소송규칙에 e-Discovery에 대한 개념과 내용이 들어가게 된다. 이런 전자증거개시(e-Discovery)제도는 증거개시제도와 다른 별개 제도가 아니라 그 대상에 있어 전자적으로 저장된 정보(ESI)인 증거개시제도를 의미하는 것이다. 전자적으로 저장된 정보를 대상으로 하기에 디지털 데이터의 특수성에 맞추어 관련 규정을 찾아볼 수 있다. 그것은 증거개시 대상인 전자적 자료(Electronical Stored Information, ESI)는 기존의 종이문서와 다르게 취급돼야 하며, 각 당사자는 전자적 자료의 보존 의무를 부담하고, 특권면책사유가 존재하는 전자적 자료에 대해는 증거개시의무가 면제되며, 전자적 자료는 합리적으로 접근할 수 있는 자료와 그렇지 않은 자료로 나누어 이원적으로 취급돼야 하고, 증거의 악의적·고의적 훼손에 대해는 제재를 받아야 하지만, 선의인 경우에는 법원의 제재를 면할 수 있다는 내용을 찾아볼 수 있다[17].

미국의 민사소송 구조는 사전 개시 절차와 본안 절차의 2단계 구조로 이루어지며 사건의 90% 이상이 사전 개시 절차에서 화해 등으로 종결되고 있는 실정이다(최득신, 2008). 합의를 통하여 사건을 조기에 종결하기도 하고 실제 공판 절차에서도 다투어야 하는 쟁점을 줄여 신속하게 재판을 끝낼 수 있다.

17) 한국지적재산권보호협회, 국제IP분쟁 이슈보고서(2분기), 2013, p.90 ~ 93

3.2. 미국에서의 e-Discovery 주요 사례

좁은 국내 시장을 벗어나 글로벌화하고 있는 우리나라 기업과 관련된 미국에 있어 주요 소송 사건을 통하여 E-Discovery에 대한 중요성을 인식하여 우리 기업과 법률시장은 이에 제대로 대처할 필요성이 커지고 있는 실정이다.

3.2.1. 듀퐁 vs 코오롱 사례

코오롱의 자회사인 코오롱인더스트리는 2005년 아라미드[18] 슈퍼섬유인 '헤라크론' 브랜드를 개발하였는데 2009년 미국 화학회사인 듀퐁이 코오롱이 자사의 아라미드 섬유 '케블라'의 영업 비밀을 빼내갔다고 주장하면서 미국 버지니아 동부법원에 소송을 제기하였다. 소송 진행 중 보존의무가 있는 사건 관련 이메일에 대하여 코오롱의 임직원들이 고의로 이메일을 삭제하였다는 이유로 코오롱이 제재를 받았다. 미국의 소송에서 고의로 증거를 인멸하면 인멸 정도에 따라서 최고 패소판결까지 받을 수 있는데, 코오롱 임직원들이 고의, 악의로 증거를 삭제하기는 하였지만, 코오롱이 회사 차원에서 광범위하게 증거를 인멸하지는 않았고, 임직원들에게 증거를 보전하라는 지시를 적시에 내렸기 때문에 가장 강력한 제재는 피할 수 있어 패소 판결까지 내려지지는 않았지만 불리한 추정(adverse inference)의 결과로 버지니아 동부법원은 코오롱에 9억1,990만 달러(약 1조원)의 배상 판결을 내렸다[19]. 이후 항소심에서 1심 재판부를 교체하고 코오롱 측의 유리한 증거를 채택하지 않은 이유로 파기 환송하였으며, 2015년 4월 코오롱이 민사 합의금 2억7500만 달러와 형사 벌금 8,500만 달러를 각각 납부하기로 하여 사건을 종결되었다[20].

---

18) 총알도 뚫지 못하는 강도, 500℃의 불 속에서도 타거나 녹지 않는 내열성 그리고 아무리 힘을 가해도 늘어나지 않는 뛰어난 인장강도를 가진 섬유이다.(위키백과)

19) http://www.boannews.com/media/view.asp?idx=40243&kind=1

20) http://www.hankookilbo.com/v/dd46b0064be8422ab7f93f723f1f9c53

3.2.2. 애플 vs 삼성 사례

2011년 4월 이어 2012년 2월 두 차례에 걸쳐 애플은 삼성전자를 상대로 애플의 디자인, 기능 등이 침해당했다는 취지로 법원에 제소하였다[21]. 이에 맞서 2012년 4월 삼성 또한 애플을 자사의 특허 침해로 소송을 제기하게 된다. e-Discovery 절차에서 상대방에 대한 자료요구권을 행사할 수 있어 각 회사는 상대방에게 관련 자료를 요구하여 방대한 자료를 확보하였다.

소송 과정에서 눈여겨 볼만한 점은 2012년 8월에는 1차 소송에 대한 1심 배심원 평결이 있었는데 배심원들은 삼성이 애플의 디자인 특허와 실용 특허, 그리고 애플의 트레이드 드레스(Trade Dress)[22]를 고의적으로 침해했다고 평결하면서 삼성이 애플에게 10억 4900만 달러를 배상하라고 평결하였으나 애플은 삼성에게 배상할 필요가 없다고 평결하였다.

삼성전자가 미국 법원에서 열린 특허 소송에서 애플에 패한 원인을 두고 미국 배심원제도의 문제점부터 삼성 변호인단의 미숙한 대응, 심지어 배심원의 애국심까지 거론되었다. 그러나 무엇보다 배심원들의 결정에 가장 결정적 영향을 미친 것은 다름 아닌 삼성전자에서 나온 내부 문서와 이메일 증거였다는 것이 전문가들의 대체적인 의견이며 미공개 재판기록 증거와 기존 공개된 증거들에서, 삼성의 내부 이메일과 구글의 “너무 비슷하니 좀 고쳐라”는 취지의 경고, 이른바 ‘벤치마킹’이라는 명

---

21) 미국에서 1차 소송을 디자인소송, 2차 소송을 기능소송이라 부르며, 1차 소송은 1심에서 삼성이 애플에 9억3,000만 달러 배상을 판결, 항소심에서는 삼성이 애플에 5억 4,000만 달러 배상을 판결하여 일단 삼성이 애플에 배상금을 지불한 뒤 대법원에 상고하였으며, 2차 소송은 1심에서 삼성의 특허침해 3건을 인정하고 1억1,900만 달러 배상을 판결하고 애플도 특허침해 1건 인정하여 15만8,400달러 배상을 선고하였다. 그러나 항소심에서는 삼성의 특허침해 건을 무효로 하고 애플의 삼성 특허 침해 1건을 그대로 유지하는 판결을 하고, 애플은 상고하여 사건은 대법원으로 넘어가게 되었다.(이경진, MK뉴스 2016. 2. 28)

22) 지적재산권 용어로 제품의 고유한 이미지를 형성하는 색채・크기・모양 등을 뜻하며 제품의 실루엣이나 전체적인 분위기를 지적재산권으로 본다.(위키백과)

목으로 아이폰의 모든 기능을 하나하나 비교하면서 지적한 내부 문서 등은 배심원들에게 '알면서도 고의적으로 베꼈다'는 결론을 내리는 데 결정적 영향을 미쳤다. 이러한 증거들은 삼성전자와 애플이 서로 증거를 수집할 수 있도록 상대방 메일 서버를 열람할 수 있도록 하는 미국 법원의 명령에 의해 상호 조사과정에서 나온 것들이다[23].

3.2.3. e-Discovery제도에 대한 철저한 인식과 대비 필요

우리나라는 아직 e-Discovery에 대한 인식과 이에 대한 대응 시스템이 아주 부족한 실정이다. 앞에서 설명한 예와 같이 국제적 특허 등 법률분쟁에 휘말리는 기업은 자사의 법무팀이나 대형로펌에 전적으로 일을 맡기고 기업 경영진은 e-Discovery에 무지하며 대비의 필요성을 느끼지 못하고 있는 실정이다. 평소 법률적 분쟁에 대비하여 소송의 상대방이 요구할 수 있는 기업 내 메일, 방대한 전자적 자료 등에 대한 관리가 필수적이다. 기업 경영진이 이런 시대적 흐름에 대처하지 못한다면 기업과 국가의 경쟁력은 뒤처질 수밖에 없을 것이다.

4. e-Discovery가 일부 적용된 국내 제도

4.1. 민사소송법 관련 e-Discovery 제도

우리나라 민사소송법에는 미국의 민사소송절차처럼 증언, 질문서의 교환, 자백요구서, 문서열람조사, 신체정신검사 등을 통해 당해 사건에 관련된 전체 사정을 법관의 관여 없이 알아낼 수 있는 당사자의 정보 수집권 보장이라는 의미의 전형적인 증거개시제도는 없으며, 다만 민사소송법상의 문서제출명령제도[24]가 일정 부분 미국의 증거개시제도의 기능을

23) 봉성창, ZD Net Korea, 2012. 8. 29.
24) 민사소송법 제343조 내지 제350조

제4절 서증
제343조(서증신청의 방식) 당사자가 서증(書證)을 신청하고자 하는 때에는 문서를 제출하는 방식 또는 문서를 가진 사람에게 그것을 제출하도록 명할 것을 신청하는 방식으로 한다.
제344조(문서의 제출의무) ① 다음 각호의 경우에 문서를 가지고 있는 사람은 그 제출을 거부하지 못한다.
1. 당사자가 소송에서 인용한 문서를 가지고 있는 때
2. 신청자가 문서를 가지고 있는 사람에게 그것을 넘겨 달라고 하거나 보겠다고 요구할 수 있는 사법상의 권리를 가지고 있는 때
3. 문서가 신청자의 이익을 위하여 작성되었거나, 신청자와 문서를 가지고 있는 사람 사이의 법률관계에 관하여 작성된 것인 때. 다만, 다음 각목의 사유 가운데 어느 하나에 해당하는 경우에는 그러하지 아니하다.
가. 제304조 내지 제306조에 규정된 사항이 적혀있는 문서로서 같은 조문들에 규정된 동의를 받지 아니한 문서
나. 문서를 가진 사람 또는 그와 제314조 각호 가운데 어느 하나의 관계에 있는 사람에 관하여 같은 조에서 규정된 사항이 적혀 있는 문서
다. 제315조제1항 각호에 규정된 사항중 어느 하나에 규정된 사항이 적혀 있고 비밀을 지킬 의무가 면제되지 아니한 문서
②제1항의 경우 외에도 문서(공무원 또는 공무원이었던 사람이 그 직무와 관련하여 보관하거나 가지고 있는 문서를 제외한다)가 다음 각호의 어느 하나에도 해당하지 아니하는 경우에는 문서를 가지고 있는 사람은 그 제출을 거부하지 못한다.
1. 제1항제3호나목 및 다목에 규정된 문서
2. 오로지 문서를 가진 사람이 이용하기 위한 문서
제345조(문서제출신청의 방식) 문서제출신청에는 다음 각호의 사항을 밝혀야 한다.
1. 문서의 표시
2. 문서의 취지
3. 문서를 가진 사람
4. 증명할 사실
5. 문서를 제출하여야 하는 의무의 원인
제346조(문서목록의 제출) 제345조의 신청을 위하여 필요하다고 인정하는 경우에는, 법원은 신청대상이 되는 문서의 취지나 그 문서로 증명할 사실을 개괄적으로 표시한 당사자의 신청에 따라, 상대방 당사자에게 신청내용과 관련하여 가지고 있는 문서 또는 신청내용과 관련하여 서증으로 제출할 문서에 관하여 그 표시와 취지 등을 적어 내도록 명할 수 있다.
제347조(제출신청의 허가여부에 대한 재판) ① 법원은 문서제출신청에 정당한 이유가 있다고 인정한 때에는 결정으로 문서를 가진 사람에게 그 제출을 명할 수 있다.
②문서제출의 신청이 문서의 일부에 대하여만 이유 있다고 인정한 때에는 그 부분만의 제출을 명하여야 한다.
③제3자에 대하여 문서의 제출을 명하는 경우에는 제3자 또는 그가 지정하는 자를 심문하여야 한다.
④법원은 문서가 제344조에 해당하는지를 판단하기 위하여 필요하다고 인정하는 때에는 문서를 가지고 있는 사람에게 그 문서를 제시하도록 명할 수 있다. 이 경우 법원은 그 문서를 다른 사람이 보도록 하여서는 안된다.
제348조(불복신청) 문서제출의 신청에 관한 결정에 대하여는 즉시항고를 할 수 있다.
제349조(당사자가 문서를 제출하지 아니한 때의 효과) 당사자가 제347조제1항·제2항 및 제4항의 규정에 의한 명령에 따르지 아니한 때에는 법원은 문서의 기재에 대한 상대방

담당한다고 볼 수 있다(최신득, 2008). 일방 당사자가 문서를 소지하고 있지 않는 경우 법원에 문서제출명령을 신청하거나 송부촉탁을 신청하는 방법이 있다. 그러나 그 대상이 전자자료 등에 대한 언급 없이 서증에 국한된다는 것이 현행법의 한계이다.

4.2. 형사소송법 관련 e-Discovery 제도

2008년 개정·시행 전의 형사소송법에서는 수사기관에서 수사 중인 수사서류와 증거물에 대하여 원칙적으로 열람·등사가 허용되지 않았고 소송 계속 중의 관계서류 또는 증거물을 열람 또는 등사할 수 있다고만 규정되어 구체적인 열람·등사의 대상과 범위는 법률에 규정되지 않아 논란의 대상이 되어 왔다.

이에 헌법재판소는 형사확정기록에 대하여 이를 국민이나 사건 당사자에게 공개할 것인지에 관하여 명문의 법률규정이 없다고 하더라도 표현의 자유에 포함되는 알 권리의 기본권 보장 법리에 의할 때 이에 대한 열람이나 복사는 원칙적으로 정당한 이익 있는 국민에게 인정된다 할 것이고, 따라서 특단의 사정이 없는 한 사건 당사자에 대하여 검찰청이 보관하고 있는 형사확정소송기록에 대한 접근의 자유가 보장되어야 할 것이라고 하였다[25].

그리고 국가보안법 위반의 한 사건에서 검사가 공소제기 후 수사기록에 대한 변호인의 열람·등사신청을 거부한 처분에 대하여 헌법소원이 제기되어 이에 대하여 헌법재판소는 위헌결정을 하였다[26].

헌법재판소는 ①수사기록에 대한 변호인의 열람등사는 검사가 보관하

의 주장을 진실한 것으로 인정할 수 있다.
제350조(당사자가 사용을 방해한 때의 효과) 당사자가 상대방의 사용을 방해할 목적으로 제출의무가 있는 문서를 훼손하여 버리거나 이를 사용할 수 없게 한 때에는, 법원은 그 문서의 기재에 대한 상대방의 주장을 진실한 것으로 인정할 수 있다.
25) 헌법재판소 1991. 5. 13. 90헌마133 결정
26) 헌법재판소 1997. 11. 27. 96헌마60 결정

고 있는 수사기록에 대한 변호인의 열람·등사는 실질적 대등을 확보하고 신속 공정한 재판을 실현하기 위하여 필요 불가결한 것이며 그에 대한 지나친 제한은 피고인의 신속 공정한 재판을 받을 권리를 침해한 것이다. ②변호인의 조력을 받을 권리는 변호인과의 자유로운 접견교통권에 그치지 아니하고 더 나아가 변호인을 통하여 수사서류를 포함한 소송관계서류를 열람·등사하고 이에 대한 검토 결과를 토대로 공격과 방어의 준비를 할 수 있는 권리도 포함된다고 보아야 할 것이므로 변호인의 수사기록 열람·등사에 대한 지나친 제한은 결국 피고인에게 보장된 변호인의 조력을 받을 권리를 침해하는 것이라고 하였다.

그러나 수사기록에 대한 열람·등사권이 이러한 신속·공정한 재판을 받을 권리와 변호인의 조력을 받을 권리로부터 보장되는 것이라고 하더라도 이는 무제한적인 것은 아니며 헌법상 보장된 다른 기본권과의 사이에 조화를 이루어야 한다고 하였다. 이에 따라 변호인의 수사기록에 대한 열람·등사권도 기본권 제한의 일반적 법률유보 조항인 국가안전보장, 질서유지 또는 공공복리를 위하여 제한되는 경우가 있을 수 있으며, 검사가 보관 중인 수사기록에 대한 열람·등사는 당해 사건의 성질과 상황, 열람·등사를 구하는 증거의 종류 및 내용 등 제반 사정을 감안하여 그 열람·등사가 피고인의 방어를 위하여 특히 중요하고 또 그로 인하여 국가기밀의 누설이나 증거인멸, 증인협박, 사생활 침해, 관련사건 수사의 현저한 지장 등과 같은 폐해를 초래할 우려가 없는 때에 한하여 허용된다고 하였다.

이러한 헌법재판소의 결정은 당시의 원칙적 개시, 예외적 불개시의 실무 관행에서 한 걸음 더 나아가 공소제기 후 검사가 보관 중인 수사기록에 대한 변호인의 열람·등사를 검사의 시혜적 사항이 아니고 일종의 권리의 차원으로 선언한 점에서 큰 의미가 있으며 그 권리는 무제한한 것이 아니므로 예외적으로 열람·등사가 허용되지 않는 경우도 있을 수 있다는 점을 인정한 점에서는 기존의 원칙적 개시, 예외적 불개시라는 실무 관행을 타당성을 인정하고 있다. 다만, 변호인의 열람·등사가 하나의

권리로 인정되는 이상 예외적 불개시의 경우에도 불개시를 인정할 만한 일정한 사유가 있어야 한다는 점이 추가되었다고 본다(이완규, 2007).

이런 연유로 피고인의 방어권 보장과 신속한 재판을 위하여 증거개시 제도를 도입한 형사소송법(2008년 1월 1일 시행)을 살펴보면, 제266조의3 및 제266조의4에서 피고인 또는 변호인이 공소 제기된 사건에 관한 서류 또는 물건의 열람 등사 등을 신청할 수 있도록 하고 제266조의11에서는 검사가 피고인 또는 변호인에게 증거개시를 요구할 수 있도록 하였다[27]. 그리고 민사소송법의 문서제출명령에서 서증에 국한된 규정과 달

27) 형사소송법
제266조의3(공소제기 후 검사가 보관하고 있는 서류 등의 열람·등사) ① 피고인 또는 변호인은 검사에게 공소제기된 사건에 관한 서류 또는 물건(이하 "서류등"이라 한다)의 목록과 공소사실의 인정 또는 양형에 영향을 미칠 수 있는 다음 서류등의 열람·등사 또는 서면의 교부를 신청할 수 있다. 다만, 피고인에게 변호인이 있는 경우에는 피고인은 열람만을 신청할 수 있다.
1. 검사가 증거로 신청할 서류등
2. 검사가 증인으로 신청할 사람의 성명·사건과의 관계 등을 기재한 서면 또는 그 사람이 공판기일 전에 행한 진술을 기재한 서류등
3. 제1호 또는 제2호의 서면 또는 서류등의 증명력과 관련된 서류등
4. 피고인 또는 변호인이 행한 법률상·사실상 주장과 관련된 서류등(관련 형사재판확정기록, 불기소처분기록 등을 포함한다)
②검사는 국가안보, 증인보호의 필요성, 증거인멸의 염려, 관련 사건의 수사에 장애를 가져올 것으로 예상되는 구체적인 사유 등 열람·등사 또는 서면의 교부를 허용하지 아니할 상당한 이유가 있다고 인정하는 때에는 열람·등사 또는 서면의 교부를 거부하거나 그 범위를 제한할 수 있다.
③검사는 열람·등사 또는 서면의 교부를 거부하거나 그 범위를 제한하는 때에는 지체없이 그 이유를 서면으로 통지하여야 한다.
④ 피고인 또는 변호인은 검사가 제1항의 신청을 받은 때부터 48시간 이내에 제3항의 통지를 하지 아니하는 때에는 제266조의4제1항의 신청을 할 수 있다.
⑤검사는 제2항에도 불구하고 서류등의 목록에 대하여는 열람 또는 등사를 거부할 수 없다.
⑥제1항의 서류등은 도면·사진·녹음테이프·비디오테이프·컴퓨터용 디스크, 그 밖에 정보를 담기 위하여 만들어진 물건으로서 문서가 아닌 특수매체를 포함한다. 이 경우 특수매체에 대한 등사는 필요 최소한의 범위에 한한다.
제266조의11(피고인 또는 변호인이 보관하고 있는 서류등의 열람·등사) ① 검사는 피고인 또는 변호인이 공판기일 또는 공판준비절차에서 현장부재·심신상실 또는 심신미약 등 법률상·사실상의 주장을 한 때에는 피고인 또는 변호인에게 다음 서류등의 열람·등사 또는 서면의 교부를 요구할 수 있다.
1. 피고인 또는 변호인이 증거로 신청할 서류등
2. 피고인 또는 변호인이 증인으로 신청할 사람의 성명, 사건과의 관계 등을 기재한 서면
3. 제1호의 서류등 또는 제2호의 서면의 증명력과 관련된 서류등

리 형사소송법 제266조의3 제6항에서 “제1항의 서류 등은 도면·사진·녹음테이프·비디오테이프·컴퓨터용 디스크, 그 밖에 정보를 담기 위하여 만들어진 물건으로서 문서가 아닌 특수매체를 포함한다. 이 경우 특수매체에 대한 등사는 필요 최소한의 범위에 한한다.”라고 규정되어 전자적 정보자료에 대한 규정도 명문화하였다.

5. e-Discovery와 디지털 포렌식 관계

e-Discovery와 디지털 포렌식은 취급 대상이 디지털 데이터(디지털 증거)이므로 많은 공통점이 있다. 둘 다 증거를 취급하는 절차를 다루며 증거가 증거능력을 가져야 한다는 점이다. 디지털 데이터는 특성상 수정, 복사 및 삭제가 용이하다. e-Discovery를 수행하는데 있어 디지털 데이터의 위 특성으로 인하여 증거를 발견하는 과정에서 훼손 또는 삭제로 인하여 증거로서의 가치를 인정받지 못할 위험성이 있다. 이런 위험에 빠지지 않기 위하여 디지털 포렌식은 주로 형사 소송 절차에서 다루어지는 디지털 증거의 검색과 복구, 분석을 통하여 소송의 해결에 필요한 증거를 찾는 과정, 그 증거에 대한 증거 능력을 유지하는 절차에 대한 개념으로 발전되어 왔으며, 전자적으로 저장된 정보(ESI)를 다루는 E-Discovery 절차에 그대로 적용될 수 있어, 수집되고 선별과정을 거쳐 분석, 보관, 생산되는 일련의 ESI는 디지털 포렌식 절차에 맞게 취급되어져야 한다(유정호·박영수, 2014).

---

4. 피고인 또는 변호인이 행한 법률상·사실상의 주장과 관련된 서류등
②피고인 또는 변호인은 검사가 제266조의3제1항에 따른 서류등의 열람·등사 또는 서면의 교부를 거부한 때에는 제1항에 따른 서류등의 열람·등사 또는 서면의 교부를 거부할 수 있다. 다만, 법원이 제266조의4제1항에 따른 신청을 기각하는 결정을 한 때에는 그러하지 아니하다.
③검사는 피고인 또는 변호인이 제1항에 따른 요구를 거부한 때에는 법원에 그 서류등의 열람· 등사 또는 서면의 교부를 허용하도록 할 것을 신청할 수 있다.
④제266조의4제2항부터 제5항까지의 규정은 제3항의 신청이 있는 경우에 준용한다.
⑤제1항에 따른 서류등에 관하여는 제266조의3제6항을 준용한다.

우리나라의 경우 디지털 포렌식은 검찰, 경찰 등 수사기관을 중심으로 발전되었고 e-Discovery는 기업, 법무법인 등의 사적 분야의 필요로 발전되다보니 학문적, 실무적 교류가 극히 미미한 것 같다. 목적, 개념 등의 유사함으로 인해 두 분야에 공통적으로 활용 가능한 지식의 이용과 응용이 필요하며 이런 외적인 한계를 극복하여 분야를 아우르는 융합적 연구가 필요하다고 본다.

6. e-Discovery제도의 국내 도입가능성

앞서 현행 민사소송법에서 일정 부분 미국 Discovery 제도의 역할을 하는 문서제출명령이 Discovery 제도와 특히 다른 점은 Discovery 제도에서는 실질적 제재(Sanction)가 있다는 것으로, 소송 당사자가 증거에 대한 보존의 의무를 준수하지 못하여 상대방이 요구한 증거를 제출하지 못하였거나 제출하지 못한 사유가 있을 경우에는 법원에 그 정당한 사유를 밝혀야 하나 이유를 밝히지 못할 경우 고의적인 은폐로 간주되어 소송에서 가혹한 제재가 가해질 수 있고 심하면 패소할 가능성도 크다.

이런 실질적인 처벌제도가 있으므로 현대형 소송에서는 현행 민사소송법의 문서제출명령에서 더 나아가 Discovery 제도의 도입이 절실히 필요하다. 현대형 소송이란 신기술의 개발능력이 있는 거대 기업이 인류가 일찍이 경험하지 못하였던 해악을 생활속에 창출하게 되고, 그 결과로 사람의 신체 및 생활환경에 심각한 피해를 미치게 됨으로써, 피해자들이 집단적으로 거대 조직에 대하여 손해배상청구를 하는 구조를 갖게 되는데, 그 배경이 된 분쟁 자체가 현대적이라는 점에서 현대형 소송이라고 불리어 진다(서동희 2005). 공해 소송, 제조물 소송, 의료 소송 등이 그 예로 들 수 있다. 차량 급발진 사건의 경우와 같이 제조물 소송에서 관련 증거는 제조 기업에 편중되어 있고 의료 소송에 있어 의료 지식 전문가인 의사에게 편재되어 있는 상황에서, 일반 소비자인 원고가 관련 증거를 확보하여 승소하기에는 일반적인 민사절차로서는 한계가 있는 것

이 당연하다.

미국에서 1960년대 이후 흑인을 비롯한 소수 인종의 인권, 여성의 권익, 환경오염의 방지, 대기업의 소비자에 대한 횡포, 증권회사의 개인에 대한 무책임한 행동 등에 대한 증거개시제도를 통한 정의실현을 이루어 왔는데 이런 결과물은 증거개시제도가 없었다면 불가능하였을 것이라는 점에 대하여는 이론의 여지가 없다(변진석 2012).

최근 대법원이 사실심 충실화 마스터플랜 보도자료(2014. 11. 28.)를 통하여 아래와 같은 내용으로 한국형 Discovery 제도 도입을 추진한다는 내용으로 발표하였다.

법원도 사건에 대한 재판 전 조정 및 화해를 위하여 사실상 형식적으로 운영되어 왔던 디스커버리 제도의 성격을 가지는 문서제출명령제도를 미국식의 디스커버리 제도로 활용하는 의미에서 불이행에 대한 제재를 강화하여 이를 실용적으로 활성화함으로 소송의 신속화, 경제화를 위한 노력을 찾아볼 수 있다.

한국형 디스커버리 제도 도입 등 증거 수집과 제출 기회의 충분한 보장 및 심리 충실화

(방안) 민사・행정소송에서 본안전 증거조사절차(한국형 디스커버리 제도)도입
- 당사자의 증거수집 확보 수단이 부족하여 사실심 심리가 부실화되는 문제, 정보편중에 의한 절차적 불평등 야기의 문제를 해결하기 위한 방안
- 영미식 디스커버리, 독일식 독립적 증거조사절차를 참조하여 본안전 증거조사절차(한국형 디스커버리 제도)의 도입을 추진하고, 문서제출명령 불이행의 제재를 강화하여 증거수집절차의 실질화를 구현함
- 소송계속 여부 및 증거보전 필요성 유무와 무관하게 오로지 증거수집을 목적으로 증인신문・검증・감정 등뿐 아니라 문서제출명령까지 독립된 절차로 신청하는 제도를 도입함
- 본안 전에 조사된 증거는 본안소송에서 그대로 증거로 사용하도록 함
- 문서제출명령을 불이행할 경우, 문서로써 증명하려고 한 주장까지도 진실한 것으로 추정할 수 있도록 함

* 현재는 문서의 성질과 내용을 구체적으로 알기 어려운 경우에는 상대방이 문서제출명령을 불이행해도 제출대상 문서로써 증명하려는 주장을 인정받기 어려웠으나, 이러한 경우에도 개선안 시행 이후에는 당사자의 주장 자체를 진실하다고 추정할 수 있도록 하여, 문서제출명령의 실효성을 더욱 강화하는 방안임

- 본안전 증거조사결과를 토대로, 조정·화해를 시도하여 조기에 화해적 분쟁해결도 도모함

제 3 장 디지털 포렌식 전문가 현황 및 프로그램

제 1 절 국내외 디지털 포렌식 관련 기관

1. 국내 디지털 포렌식 업무 수행관련 기관

디지털 포렌식 업무 수행관련 국내 국가기관으로서 검찰청, 경찰청, 국가정보원, 국방부, 관세청, 공정거래위원회, 한국저작권위원회 등을 들 수 있고, 자체적인 조직과 인원을 가지고 디지털 포렌식 관련 조사, 연구개발 등의 업무를 수행하고 있다. 국내 대표적인 수사기관인 검찰과 경찰의 디지털 포렌식 수행 기관에 대하여 알아보기로 한다.

1.1. 검찰청

검찰청에서는 2008년 대검찰청 산하에 디지털포렌식센터(DFC : Digital Forensic Center)를 개관하여 디지털 증거, 마약, 유전자, 영상 등 증거물 감정 및 감식 업무를 담당하였고 2011년 사이버범죄수사단을 창설하였으며, 2012년 본 센터는 국가디지털포렌식센터(NDFC)로 명칭을 변경하였다. 대검 예규인 「국가디지털포렌식센터 운영에 관한 규정[28]」 제3조 국가디지털포렌식센터의 업무를 보면, 감정·분석 등 업무, 그와 관련된 연구·개발 및 교육에 관한 사항, 감정·감식·분석기법과 관련된 국내·외 교류협력 및 정보의 수집·분석에 관한 사항, 그 밖에 공익적 업무를 수행하는 국가기관 등 공공기관에 대한 감정·감식·분석 및 그 지원에 관한 사항을 규정하고 있다.

---

28) 대검예규 제812호(2015. 11. 1. 제정)

다음의 <표 3-1>은 디지털포렌식센터 구성 및 주요업무 현황을 나타내고 있다[29].

<표 3-1> 검찰청 디지털포렌식센터 구성 및 주요업무

구성	주요업무
디스크 분석팀	서버, 데스트톱, 노트북, 외장하드 등 디지털 저장매체에 대한 압수수색 및 복구분석을 실시하여 디지털 증거 수집,분석
DB 분석팀	기업 등 조직을 대상으로 하는 수사에 있어 그 조직의 업무 시스템에 활용되고 있는 각종 데이터베이스를 수색, 분석
모바일 분석팀	휴대폰, PDA 등 이동형 디지털 기기에 대한 분석
통화/계좌 분석팀	전화통화 및 금융거래 계좌내역 자료를 데이터베이스화한 후 정보 분석
사이버팀	해킹 등 사이버 범죄에 대응하기 위한 추적, 분석
교육연구팀	디지털 포렌식 전문가 양성 과정 및 디지털 수사관 교육

대검찰청 과학수사부 디지털수사과에서 일선 수사팀의 디지털포렌식 지원요청을 총괄 담당하고 있고 현장밀착형 수사지원을 위하여 아래 표와 같이 서울고검 등 10곳에 거점청 디지털포렌식팀을 운용하고 있다[30]. 각 팀마다 관할지역 내 수사지원이 원칙이나 대검 디지털수사과에서는 일선 수사팀의 수사지원 요청 접수 시 사건의 중요성, 지원 규모 및 필요인력, 거점청별 유휴인력 등을 종합적으로 고려하여 필요시 관할지역 외 업무지원을 할 수 있도록 조정·배정하는 등 탄력적으로 운용하고 있다[31].

29) 대검찰청, 차세대 디지털 포렌식 기술 및 사이버범죄 대응 기술 연구, 2012
30) 대검찰청 과학수사부 디지털수사과 디지털포렌식 Q&A, 2015.
31) 대검찰청 예규 제805호「디지털 포렌식 수사관의 증거 수집 및 분석규정」 제7조 (거점청 디지털포렌식팀 설치 및 운영)① 각 고등검찰청 또는 지방검찰청에 별도의 기구로 디지털포렌식팀을 설치할 수 있다.
② 거점청 디지털포렌식팀은 디지털포렌식 수사관으로 구성한다.

<그림 3-1> 검찰청 디지털포렌식팀 조직 및 인원 현황

<table>
<tr><td colspan="5">대검찰청 디지털수사과(15명)</td></tr>
<tr><td>서울고검
8명</td><td>부산고검
8명</td><td>대구고검
5명</td><td>광주고검
7명</td><td>대전고검
5명</td></tr>
<tr><td>서울중앙지검
10명</td><td>창원지검
2명</td><td colspan="3" rowspan="4"></td></tr>
<tr><td>서울남부지검
5명</td></tr>
<tr><td>인천지검
4명</td></tr>
<tr><td>수원지검
4명</td></tr>
</table>

* 2015년 10월 현재

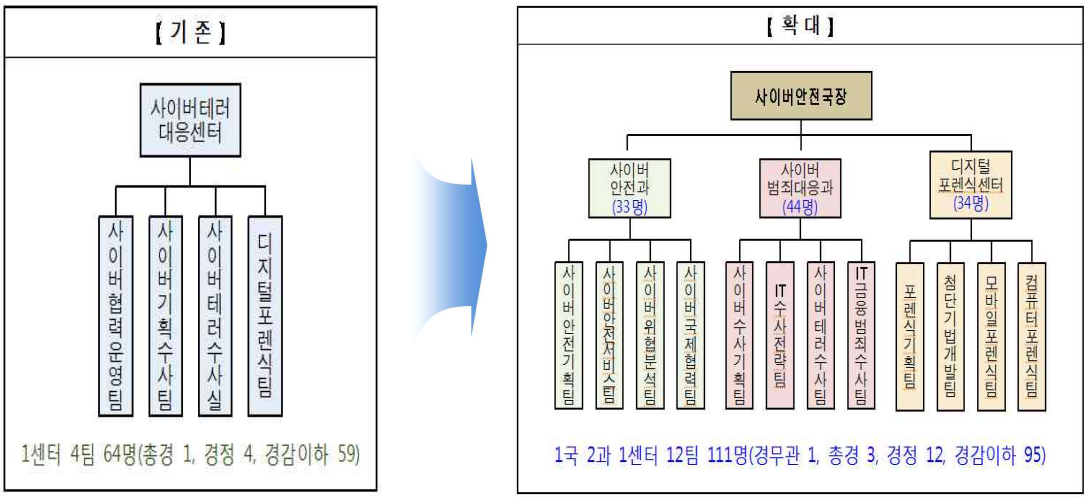
1.2. 경찰청

경찰청은 1997년 컴퓨터범죄수사대, 1999년 사이버범죄수사대를 설치하였고 이어 2000년 사이버테러대응센터를 창설하였다. 경찰청 수사국 내 1과 4팀 64명의 직원으로 조직된 사이버대응센터는 해킹, 바이러스 유포, 인터넷 사기, 사이버 명예훼손 등의 사이버 범죄수사 및 사이버 치안 유지의 업무를 담당하다가, 2013년 3. 20. 방송 및 금융망 사이버테러와 6. 25. 정부기관 등에 대한 사이버테러 사건을 계기로 사이버공격이 국가차원의 위협으로 대두됨에 따라, 2014. 6. 11. 아래 표와 같이 사이버안전국을 신설하면서 사이버안전국장과 2과 1센터 12팀 111명으로 확대, 개편하였다[32].

③ 각 거점청 디지털포렌식팀은 해당 고등검찰청 또는 지방검찰청 관할구역내의 디지털 증거 수집 및 분석 업무를 전담한다. 다만, 대검찰청 디지털수사과장이 각 거점청 디지털포렌식팀의 관할외의 업무 지원을 조정할 수 있다.

32) 경찰청 사이버안전국 출범 보도자료, 2014. 6. 11.

<그림 3-2> 경찰청 사이버안전국 조직도



<표 3-2> 사이버안전국 과·팀별 업무

과	팀별 임무
사이버안전과	▸ 사이버안전기획팀 : 사이버안전 종합대책 수립, 인력관리, 예산, 장비 ▸ 사이버안전서비스팀 : 사이버범죄 신고·상담, 사이버안전정보 제공 ▸ 사이버위협분석팀 : 사이버위협정보 수집·분석 및 측정 ▸ 사이버국제협력팀 : 국제기구 및 외국과의 협력 및 공조활동
사이버범죄 대응과	▸ 사이버수사기획팀 : 사이버범죄 수사지휘(지도) 및 대책 수립 ▸ IT수사전략팀 : 신종 사이버범죄, 사이버테러 대응 전략 기획 ▸ 사이버테러수사팀 : 해킹, 디도스 공격 등 중요 사이버범죄 수사 ▸ IT금융범죄수사팀 : 피싱, 파밍 등 신종 금융범죄 수사
디지털포렌식 센터	▸ 포렌식기획팀 : 디지털포렌식 정책기획 및 지도 ▸ 첨단기법개발팀 : IT 환경분석 및 신규 추적기법·도구 개발 ▸ 모바일포렌식팀 : 스마트폰 등 모바일기기 확장분석 기법 개발 ▸ 컴퓨터포렌식팀 : 악성코드 등 디지털기기 증거분석 기법 개발

또한 국민과 기업이 안심하고 이용할 수 있는 사이버공간의 안전 확보를 비전으로 6개 분야 20개 실천과제로 구성한 '사이버안전 확보 기본계획'을 발표하였는데 그 분야별 내용을 간단히 보면, 예방중심의 사이버 안전 서비스제공, 범죄 정보 조기 분석을 통한 선제적 대응, 수사역량강화를 통한 사이버범죄 강력 단속, 국내외 협력강화를 통한 사이버 치안 역량 강화, 사이버범죄 대응 요원의 전문성 강화에 대한 방안으로 사이버범죄 대응 요원 중 IT전공자 비율을 현 30%에서 2018년까지 50%로 확대하고, 디지털 포렌식·악성코드 등 분야별 교육프로그램을 내실화하며, 민간 디지털증거분석 전문가를 지속적으로 특채하고, 한국경찰을 대표하는 국제 사이버범죄 전문가를 양성하는 등 전문성을 강화(2013년 말 현재 사이버수사요원 1,038명 중 IT전공자 310명으로 30%), 조직 개편 및 연구 개발로 변화에 능동적 대처방안으로 증가하는 사이버범죄 추세에 맞추어 경찰관 2만명 증원 계획과 연계하여 향후 5년간 사이버요원을 지속 증원하고, 연차적으로 지방청 사이버수사대를 사이버안전과로 전환해 나가는 등 사이버안전활동 대응 인력과 조직을 확충하고, 국립과학수사연구원과 유사한 '디지털 증거 연구소' 설립을 추진하고, 국민 편의를 위해 '사이버범죄신고 종합 접수·대응 센터'와 '사이버범죄 예방교육 총괄 전담기구'를 추진하는 등 발전적으로 조직을 개편하며, 경찰대학 '국제사이버범죄 연구센터'를 사이버안전 연구·개발(R&D) 전담조직으로 확대 개편하고, 사이버범죄/포렌식 분야 연구를 국가 R&D 과제로 격상 등을 살펴볼 수 있는데, 경찰이라는 거대한 국가조직의 사이버범죄에 대한 대응과 디지털 포렌식 분야에 대한 관심과 노력을 눈여겨 볼 수 있다.

2. 미국 디지털 포렌식 업무 수행관련 기관

2.1. 미국에서의 포렌식랩(Forensic Lab)

디지털 포렌식은 전통적인 법과학의 의미를 가지는 포렌식의 한 분야

로 발전되어 온 것은 주지의 사실이고 범죄수사와 형사재판뿐만 아니라 민사 재판에서도 실체적 진실을 보여주는 중요한 도구이다.

수사과정에서 실체적 진실에 접근하기 위한 필요에 의하여 법과학(Forensic Science)이 요구된다. 법집행 기관의 필요성에 의하여 시작되나 수사기관의 특정적 목적에서 벗어나 과학적 분석의 필요성이 대두되고 이에 독자성을 갖춘 분야로 인식되어 발전되어 왔다. 그리하여 법과학은 포렌식랩[33]을 중심으로 발전되어 왔다. 미국에서는 1923년 로스앤젤레스 경찰국(LAPD ; Los Angeles Police Department)에서 최초의 포렌식랩이 설치되고 이어 1932년 연방수사국(FBI)에도 포렌식랩이 설치된다[34].

이런 포렌식랩들은 연방정부기관 및 주정부기관, 각 지방 기관 등에 필요성에 따라 다양하게 존재하게 된다. 그리하여 각 포렌식랩에 대한 자격이나 인증의 문제가 중요하게 부각된다. 미국 포렌식랩에 대한 인증은 미국 법과학시험기관장/시험기관 인증위원회(ASCLD/LAB ; American Society of Crime Laboratory Directors/Laboratory Accreditation Board) 프로그램이 대표적이다. 2016년 4월 현재 미국에서 32개의 연방기관 포렌식랩, 186개의 주정부 포렌식랩, 130개의 지방 포렌식랩, 18개의 외국 포렌식랩, 25개의 사설 포렌식랩이 ASCLD/LAB에 의하여 인증되었다[35].

디지털 포렌식 분야를 보면, 초창기 일선 법집행기관에서는 수사관들에 의하여 직접 수행되던 디지털 증거 관련 업무가 점차 디지털 포렌식랩(Digital Forensic Lab)으로 무게중심이 옮겨지고 있다. 미국은 컴퓨터의 개발 및 활용에 있어 선구자적 입장에 걸맞게 디지털 포렌식에 대한

33) 포렌식랩(Forensic Laboratory)은 Crime Laboratory라고도 하며 국내에서 법과학기관, 법과학 연구실 등의 명칭으로 해석될 수 있으며 대부분의 국가에서 공적인 목적 형태로 운영되며 대학의 연구실 등에도 위 명칭을 사용하기도 한다. 국립과학수사연구원은 국내 대표적이며 독보적인 포렌식랩이라고 할 수 있다.

34) https://www.fbi.gov/about-us/lab

35) http://www.ascld-lab.org/accredited-laboratory-index/

연구와 교육에 힘써왔고 디지털 포렌식랩을 중심으로 수사와 연구 개발을 수행하고 있다.

2.2. 디지털 포렌식랩 기관

미국에서는 기관의 성격과 운영방식에 따라 그 운영 형태는 디지털 포렌식랩이 독립적으로 운영되는 경우, 일반 포렌식랩의 하위 조직으로 운영되는 경우, 별도의 디지털 포렌식랩을 운영하지 않고 수사기능에서 사이버수사의 일부분으로서 랩을 운영하는 형태 등으로 나타나고 있다.

미국 연방기관 내의 디지털 포렌식랩은 연방수사국(FBI)의 CART(Computer Analysis Response Team), 마약수사국(DEA)의 DEL(Digital Evidence Laboratory)을 포함하여 국토안보부 산하 비밀경호국(Secret Service), 각 군 수사기관 등에 독립적인 디지털 포렌식랩을 운영하고 있다.

미국 FBI는 2002년 지방 법집행 기관을 위한 디지털 증거 검사, 압수 지원, 훈련 등을 담당하는 RCFL(Regional Computer Forensics Laboratory)을 설립한다. 지방 법집행 기관이 비싼 비용 문제로 인하여 자체적으로 포렌식랩을 설치하지 않고 연방차원에서 포렌식랩을 설립하여 각 지방 법집행 기관이 공동 이용하는 방법이다. RCFL은 범죄 유형을 테러, 아동포르노범죄, 폭력범죄, 산업기술 유출범죄, 지적재산권 범죄, 금융범죄, 재산범죄, 인터넷범죄, 사기 등 9개의 분류로 나누어 디지털 증거를 활용한 범죄 해결에 이바지 하고 있다. FBI의 자체 수사에 이용되는 CART와는 달리, RCFL는 지방 모든 법집행 기관에서 참여, 활용할 수 있다.

제 2 절 디지털 포렌식 교육과정에 대한 연구

1. 국내 디지털 포렌식 교육 프로그램

1.1. 검찰 디지털 포렌식 전문가 양성 프로그램

검찰청에서는 검찰수사관을 대상으로 하는 디지털 포렌식 전문가 양성 프로그램을 운영하고 있다[36].

<표 3-3> 검찰 디지털 포렌식 교육생 선발 기준 및 교육내용

구분	평가 항목	비율(100)	가점 부여 사항	비고
경력사항	수사 경력	10	수사경력을 참조하여 기간이 길수록 가점 부여	신청서
	조직기여도	10	포상 및 공적 사항	신청서
추천사항	공식 추천	10	일선청 공식 추천자 가점 부여	공문
자격사항	IT 전문 자격증	10	CISA, CISSP, CIA, OCP, CCNA, MCSE, 정보처리기사, 정보처리산업기사 등 소지자 가점 부여	신청서 증빙서류
	정보화 관련 자격증	5	사무자동화기사, MOUS, 워드프로세스 등 오피스 관련 자격증 소지자 가점 부여	신청서 증빙서류
교육훈련	IT관련 학과	5	컴퓨터 공학, 전산공학 등 IT관련 학과 졸업자 가점 부여	신청서 증비서류
	포렌식 관련 단기 교육 이수	5	포렌식 관련 검찰 내/외부 단기 교육 수료자 가점 부여	신청서
복무태도	근무 성실도	20	소속청의 평판 등을 간접적으로 조사하여 그 결과에 따라 가점 부여	타과협조
신청사항	자기소개서	20	신청서에 첨부된 자기소개서의 기재 내용의 평가에 따라 가점 부여	신청서
기타사항	해당 기수별 특이사항	5	외국어 능통자 당해 연도 교육 수요 해당 여부	증빙서류 기타

36) 대검찰청 제30기 디지털포렌식 전문가 양성 교육생 추천 협조 공문, 2016. 4. 4.

<표 3-4> 검찰청 디지털 포렌식 교육내용

단계	기간	과정명 (13개)	교육 과목 (36개)
1	5일	컴퓨터 구조 및 시스템 이해	컴퓨터 하드웨어 구조 이해 (2일) 컴퓨터 시스템 이해 (2일) 시스템 백업/복원 (1일)
	5일	윈도우 및 MAC	Windows XP (1일) Windows 7&8 (2일) MAC OS (2일)
	5일	리눅스 일반	리눅스 시스템의 구성 및 동작 원리 (2일) 리눅스 명령어 (2일) 리눅스 아티팩츠 (1일)
	5일	데이터베이스 일반	My SQL/PHP (2일) MS SQL (2일) Oracle (1일)
	5일	모바일 일반	모바일 포렌식 개론 및 기기별 특성 (2일) iPhone 소개 (1일) Android 소개 (1일) 모바일 앱 소개 및 분석 (1일)
2	2일	디지털포렌식 입문	디지털포렌식 개론 (1일) 이미징 기법 (1일)
3	5일	파일시스템 Ⅰ	디스크 구조 (1일) FAT File System (2일)
		파일시스템 Ⅱ	NTFS (2일)
4	5일	디지털포렌식도구	Encase 6&7 (4일) CFT (1일)
5	3일	윈도우 포렌식	윈도우 아티팩트 Ⅰ (1일) 윈도우 아티팩트 Ⅱ (1일) 레지스트리 포렌식 (1일)
6	9일	특수 포렌식	MAC 포렌식 (1일) DB 포렌식 (3일) Mobile 포렌식 (3일) D-NET망 소개(0.5일) 통화, 계좌분석 (0.5일) 저장매체 수리 이해 (0.5일) MFA 소개 (0.5일)
7	4일	주제발표	주제발표 (4일)
8	3일	평가	1차 평가 2차 평가 주제발표 평가
9	52일	실무훈련	압수수색 및 증거분석

이는 디지털 증거 압수·수색 및 분석 업무를 수행하기 위한 디지털 포렌식 전문 수사관을 양성하는 과정으로 교육 장소는 대검찰청 국가디지털포렌식센터 전용 교육장에서 이루어지며, 6개월의 교육과정 중 3개월은 컴퓨터 기반의 디지털 포렌식 이론 및 실무 교육과 3개월은 현장 실습 위주로 편성되어 있다.

현재 30기 교육이 실시되고 있으며, 교육생 선발 기준과 교육내용을 살펴보면 <표 3-3>과 <3-4>와 같다.

주요 내용을 살펴보면, 경력, 추천, 자격, 교육훈련, 복무태도, 신청사항 기타사항의 7가지 항목에서 각각의 평가항목에 따라 평가되며, 디지털 포렌식 교육훈련을 위한 기본적인 역량을 근거로 가점이 부여된다.

<표 3-5> 검찰청 디지털 포렌식 교육 평가방법

구분		평가항목		배점 (200점)	비고
이론 교육	1차시험	컴퓨터 일반과목	컴퓨터/윈도우/MAC, 운영체제론, 리눅스, 데이터베이스 일반, 모바일기본과정 등	40	필기
		디지털포렌식 개론, 이미징 기법, 디스크 구조		10	필기
	2차시험	FAT, NTFS , EnCase V6, V7		30	필기
		CFT, 윈도우 포렌식, 레지스트리 포렌식		20	필기
실무 훈련	과제제출	분석보고서 및 주제발표 (주제발표는 포렌식 관련 논문 제출 및 PT, A4지 10장 내외)		각 50	보고서 논문
	실무수습	실무수습일지		70	실 무 평 가
		실무수습태도		30	실 무 평 가
복무	교육태도	출근점검부 및 법무연수원 평가관리 규정		벌점제	28기부터 추가
포렌식 자격증		EnCE(EnCase Certified Examiner)		취득 (1개 이상)	
		디지털 포렌식 전문가 2급(한국포렌식학회)			

또한, 위 교육과정의 수료 후 <표 3-5>와 같은 교육 평가를 하며, 28기 교육생 이후부터 EnCE(EnCase Certified Examiner), 디지털 포렌식 전문가 2급(한국포렌식학회) 자격증 중 1개 이상을 취득해야 하는 조건이 있다.

교육 수료 후 조직 내 관리 사항을 보면, 교육 수료자는 디지털 포렌식 전문 수사관 DB 등재 등 이력 관리함과 교육 수료 후 원소속청 복귀 수사관은 거점청 디지털 포렌식 예비수사관으로 편성되어 디지털 포렌식 수사관 결원 발생 시, 우선 선발 기회 부여한다.

검찰 디지털 포렌식 전문가 양성 프로그램 수료 후 취득하여 하는 자격증인 사단법인 한국포렌식학회 주관 디지털 포렌식 검정시험[37]에 대한 내용은 아래와 같다.

<표 3-6> 디지털 포렌식 전문가 응시자격 및 면제

	1급 시험	2급 시험
응시자격	1. 디지털 포렌식 전문가 2급 자격을 보유하고, 2년 이상 유관경력이 있는 사람 (다만, 자격 취득 후 당 학회 주관의 보수교육을 매년 8시간 이상 이수한 경우에 한함) 2. 석사 이상의 유관학력을 취득한 후 2년 이상의 유관경력이 있는 사람 3. 변호사나 변리사, 공인회계사로서 3년 이상의 유관경력이 있는 사람 4. 유관자격을 보유한 사람으로 유관경력 3년 이상인 사람 제한없음	제한없음
필기시험 면제	1. 필기시험에 합격한 자는 신청에 의하여 실시하는 필기시험 3회에 한하여 시험면제 2. 민간자격 시험에 합격한 자는 필기시험면제, 실기시험만 응시하여 합격하면 국가공인자격으로 갱신(민간자격시험 필기, 실기 모두 합격한 자)	

37) http://www.forensickorea.org/forensic/information.asp

<표 3-7> 출제기준 및 범위(1급)

<table>
<tr><th colspan="2" rowspan="2">자격종목</th><th rowspan="2"></th><th rowspan="2">시험과목</th><th colspan="3">검정방법</th></tr>
<tr><th>검정시간</th><th>시험문항수/배점</th><th>문제유형</th></tr>
<tr><td rowspan="10">1급</td><td rowspan="6">1차 필기 (3과목)</td><td>기본</td><td>디스크 포렌식</td><td rowspan="6">180분</td><td>4문항/200점</td><td>단답형/주관식/서술형</td></tr>
<tr><td rowspan="4">선택 1</td><td>DB 포렌식</td><td rowspan="4">2문항/100점</td><td rowspan="4">단답형/주관식/서술형</td></tr>
<tr><td>네트워크 포렌식</td></tr>
<tr><td>모바일 포렌식</td></tr>
<tr><td>침해사고 대응 포렌식</td></tr>
<tr><td>기본</td><td>증거법</td><td>4문항/200점</td><td>단답형/주관식/서술형</td></tr>
<tr><td rowspan="4">2차 실기 (2과목)</td><td>기본</td><td>디스크 포렌식</td><td colspan="3" rowspan="4">• 검정시간 : 240분
• 실기문항 수 :
디스크 포렌식 2문항/50점
선택과목 2문항/50점</td></tr>
<tr><td rowspan="3">선택 1</td><td>DB 포렌식</td></tr>
<tr><td>네트워크 포렌식</td></tr>
<tr><td>모바일 포렌식</td></tr>
<tr><td></td><td></td><td></td><td>침해사고 대응 포렌식</td><td colspan="3"></td></tr>
</table>

<표 3-8> 출제기준 및 범위(2급)

<table>
<tr><th colspan="2" rowspan="2">자격종목</th><th rowspan="2">시험과목</th><th colspan="3">검정방법</th></tr>
<tr><th>검정시간</th><th>시험문항수/배점</th><th>문제유형</th></tr>
<tr><td rowspan="6">2급</td><td rowspan="5">1차 필기</td><td>컴퓨터구조와 디지털저장매체</td><td rowspan="5">180분</td><td>15문항/15점</td><td>선다형</td></tr>
<tr><td>파일시스템과 운영체제</td><td>15문항/15점</td><td>선다형</td></tr>
<tr><td>응용 프로그램과 네트워크의 이해</td><td>15문항/15점</td><td>선다형</td></tr>
<tr><td>데이터베이스</td><td>15문항/15점</td><td>선다형</td></tr>
<tr><td>디지털포렌식 개론(기초실문 + 법률이론)</td><td>15문항/15점</td><td>선다형</td></tr>
<tr><td>2차 실기</td><td>디지털 포렌식 기초실무</td><td colspan="3">• 검정시간 : 240분
• 실기문항 수 : 5문항/100점</td></tr>
</table>

1.2. 대학의 디지털 포렌식 교육과정

디지털 포렌식 분야 전문인력 양성 필요성으로 인해 국내 대학에서도 관련 학부나 대학원과정이 늘어나고 있다. 아래 표에서 현재 국내 디지털 포렌식 과정을 개설한 대표적인 대학의 내용 및 특징, 그리고 주요 커리큘럼을 정리하였다.

<표 3-9> 국내 주요대학 디지털포렌식 교육과정

대학	내용 및 특징	주요 커리큘럼
서울대학교	- 사이버 범죄 대응 인력 및 차세대 리더 양성을 목표 - 융합과학기술대학원 수리정보과학과 디지털포렌식 석사과정(2년) 개설	- 컴퓨터학 - 암호학 - 컴퓨터구조 - 파일시스템 - 디지털증거법 - 정보보호법 - 안티포렌식 - 디지털포렌식 관련 실습
고려대학교	- 사이버 범죄에 대비한 정보보안 분야의 전문가 양성을 목표 - 정보보호대학원 디지털포렌식학과 등 정보보호 관련 다양한 계약학과 개설 - 정보보호연구원 산하 디지털포렌식연구센터 설립, 운영	- 정보보호이론 - 사이버범죄학 - 디지털증거법 - 디지털법과학 - 디지털포렌식 기술 - 사이버법률 - 역공학 및 악성코드분석
군산대학교	- 학부과정 - 디지털 포렌식 전문가 양성목적의 다양한 분야의 강좌를 개설 - 민법총론, 형법총론, 민사소송법을 이수 교과목으로 지정 - 한국포렌식학회 주관 디지털 포렌식 전문가 자격증 취득 및 정보보안 관련 자격증 취득 목표	- 디지털포렌식 개론 - 컴퓨터구조와 저장매체 - 디지털범죄 - 포렌식절차/증거법 - 파일시스템과 운영체제 - 응용프로그램과 네트워크 - 포렌식 DB 이해 - 정보보안관리 및 법규 - 네트워크 및 APP보안 - 시스템 포렌식 - 디지털 증거 분석

동국대학교	- 사이버범죄에 대응하기 위한 사이버포렌식 전문가 양성 목표 - 국제정보보호대학원 정보보호학과 사이버포렌식 전공	- 사이버포렌식 총론 - 포렌식과 증거법 - 파일시스템 - 포렌식 소송절차 - 포렌식 윤리 - 안티포렌식 기술 - 네트워크/시스템포렌식 - 저작권/금융/감사/의료/회계/모바일포렌식
연세대학교	- 사이버 범죄 대응 인력 및 차세대 리더 양성을 목표 - 정보대학원 내 디지털포렌식 석사과정(1년 6월) 개설	

국내 대학의 주요 디지털 포렌식 관련 과정은 사이버 범죄에 대응하기 위한 전문가 양성을 목표로 군산대학교 외 석사과정으로 디지털 포렌식 프로그램을 운영하고 있다. 커리큘럼을 살펴보면, 디지털 포렌식이라는 학문의 융합적 성격으로 컴퓨터, 정보보안 관련 과목과 법과목이 어우러진 커리큘럼을 볼 수 있다.

2. 해외 디지털 포렌식 교육 프로그램

미국에서는 법과학 교육의 중요성을 인식하고 법무부 산하 국립사법연구원(NIS ; National Institute of Justice)이 2001년 법과학 교육과 훈련을 위한 기술연구 그룹(TWGED ; Technical Working Group for Education and Training in Forensic Science)을 설치하여, 법과학 교육의 질을 향상시키기 위한 목적으로 2004년 '법과학 교육과 훈련 : 포렌식 랩, 교육기관, 학생들을 위한 가이드(Education and Training in Forensic Science : A Guide for Forensic Science Laboratories, Educational Institutions, and Students)[38]'을 제시하였다.

미국 법과학회(AAFS ; American Academy of Forensic Science)에서는 포렌식 분야 대학 및 대학원 과정의 발전과 인증, 그리고 TWGED의 가이드라인에 따른 표준을 제시할 목적으로 2004년 법과학 교육프로그램 인증 위원회(FEPAC ; Forensic Education Programs Accreditation Commission)를 설치하였다. 현재 FEPAC에 의하여 인증된 포렌식 과정을 설치한 미국 내 대학은 40여 개에 이르고 있다[39].

2.1. 디지털 포렌식 분야의 교육과 훈련을 위한 보고서

디지털 포렌식 분야는 TWGED 가이드에 포함되어 있지 않았으나 2007년에 디지털 포렌식 분야의 교육과 훈련을 위한 TWGED(Technical Working Group for Education and Training in Digital Forensics) 보고서를 작성하였다[40].

포렌식랩과 마찬가지로 디지털 포렌식랩도 인증문제가 중요한데 SWGDE(Scientific Working Group on Digital Evidence)[41] 등의 노력으로 2003년 디지털 포렌식랩은 ASCLD/LAB의 인증프로그램에 포함되게 되었다. 오디오 분석, 컴퓨터 포렌식, 디지털 이미지 분석, 비디오 분석 중 어느 하나라도 취급하는 포렌식랩은 디지털 증거를 취급하는 기관으로 인증을 신청해야 한다. ASCLD/LAB이 개별적으로 인증 요건을 정하고 있는 법과학 분야는 통제물질, 독물학, 미세증거, 생물학, 무기와 도구흔, 문서, 잠재지문, 기술지원, 범죄현장 등 분야에 한정되었으나 디지털 포렌식은 정규적 법과학의 한 분야로 인정받는 계기가 되었고 이는 디지털 포렌식에 대한 통일된 표준 및 적격성 등 여러 사항에 대한 연구와

38) https://www.ncjrs.gov/pdffiles1/nij/203099.pdf
39) http://www.fepac-edu.org/accredited-universities
40) https://www.ncjrs.gov/pdffiles1/nij/grants/219380.pdf
41) 디지털 증거에 대한 복구, 보존, 시험 등을 위한 가이드라인과 표준을 정하고 발전시키기 위하여 법집행기관, 학계, 일반기업의 디지털 포렌식 전문가들이 모여 1998년 결성된 단체(위키사전)

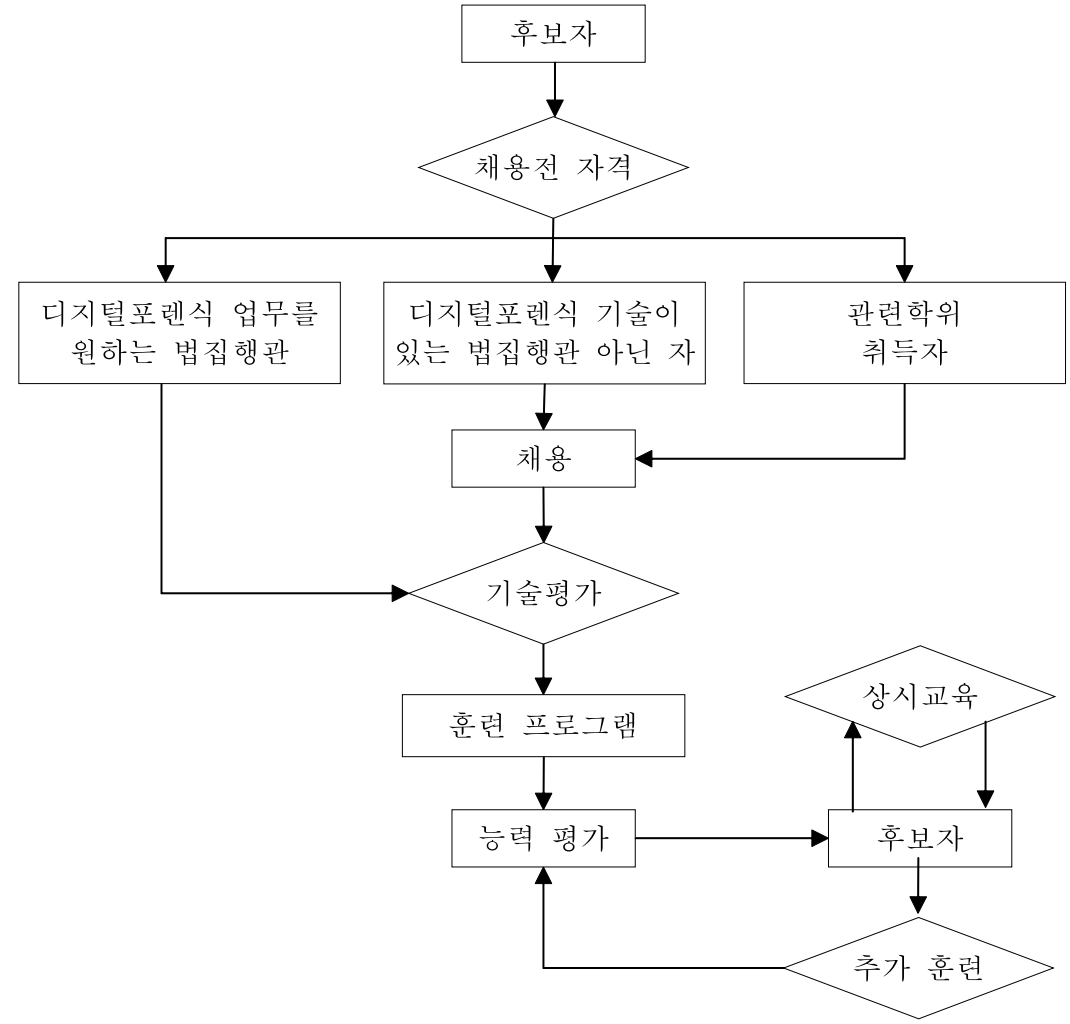
합의가 매우 빠른 시간 내에 이루어 졌다는 것을 의미한다(임종인, 2007).

앞서 기술하였듯이 미국 법무부 국립사법연구소(NIS)의 일반 법과학의 수준을 높이기 위하여 결성된 TWGED(Technical Working Group for Education and Training in Forensic Science)에서 제시한 가이드인 '법과학 교육과 훈련 : 포렌식랩, 교육기관, 학생들을 위한 가이드(Education and Training in Forensic Science : A Guide for Forensic Science Laboratories, Educational Institutions, and Students)'이후 디지털 포렌식 분야에 대한 가이드는 2007년 8월 발표되었다. 디지털 포렌식의 교육과 훈련을 위한 TWGED(Technical Working Group for Education and Training in Digital Forensics) 보고서라는 명칭으로 발표되었다.

이 보고서에서 <그림 3-3>과 같이 디지털 포렌식 실무자의 경력유형과 개발루트를 살펴볼 수 있다.

디지털 포렌식 실무자가 되기 위해서는 위와 같이 디지털 포렌식 업무를 원하는 법집행관, 디지털 포렌식 기술은 있지만 법집행관이 아닌 사람, 그리고 관련 학위 취득자의 3가지 유형이 있다. 3가지 유형의 사람들은 디지털 포렌식 실무를 처리하는 전문가가 되기 위해서는 개인적으로 성실성(Integrity), 정직성(Honesty), 과학적 객관성(Scientific Objectivity)을 갖출 것을 요구한다. 전통적으로 디지털 포렌식 실무자에게는 학위를 요구하지 않았으나 특히 과학 분야의 학사학위를 요구하는 추세로 바뀌고 있다.

<그림 3-3> 디지털 포렌식 경력유형과 개발 루트



그리고 아래 표 <3-10>과 <3-11>은 디지털 포렌식 실무가들에게 요구되는 기술적, 전문적 지식사항이다.

<표 3-10> 기술적 지식사항

컴퓨터 하드웨어 구조(Computer hardware and architecture)
저장 매체(Storage Media)
운영 체제(Operation Systems)
파일 시스템(File Systems)
데이터베이스 시스템(Database Systems)
네트워크 기술과 정보통신 기반(Network Technologies and Infrastructures)
프로그래밍과 스크립팅(Programming and Scripting)
컴퓨터 보안(Computer Security)
암호학(Cryptography)
소프트웨어 툴(Software Tool)
검증과 시험(Validation and Examination)
융합적 분야 인식(Cross Discipline Awareness)

<표 3-11> 전문적 지식사항

비판적 사고(Critical Thinking)
과학방법론(Scientific Methodology)
정량적 추리와 문제해결(Quantitative reasoning and Problem Solving)
의사결정(Decision Making)
랩 실무(Laboratory Practices)
세부사항에 대한 주의(Attention to Detail)
대인기술(Interpersonal Skills)
공석에서 말하기(Public Speaking)
구두와 서면 의사소통(Oral and Written Communication)
시간관리(Time Management)
작업우선 순위결정(Task Prioritization)
디지털 포렌식 절차의 응용(Application of Digital Forensic Procedures)
증거보존(Preservation of Evidence)
수사절차(Investigative Process)
법절차(Legal Process)

<표 3-12> 디지털 포렌식 학사학위 프로그램의 모델 커리큘럼

과목 분류	내용	학점
대학 교양	- 외국어, 인문, 사회과학, 수학, 화술에 관한 과정 - 과학과정 8학점(실험 2학점)(과학적 방법 탐구, 전기와 자기에 관한 기초적 지 식 포함)	36 ~ 40
컴퓨팅과 정보과학	- 컴퓨터와 저장 매체 - 응용 파일시스템과 운용체제 - 기초 컴퓨터 네트워킹, 네트워크 보안 - 컴퓨터 프로그램밍 - 컴퓨터 구조학 - 데이터베이스 및 그 활용 - 정보보안 - 이산수학	24
법과학	- 법과학 개론 - 법과학 실습(법윤리, 증언, 증거의 무결성과 진정성, 연계 보관성(chain of custody) 포함)	6
추가 필수 과정	- 기본 법률 쟁점 - 수사기법 - 화술 - 작문 - Capstone Project - 디지털 포렌식 주요 논점(세미나 1학점)	16
디지털 포렌식랩(Lab) 실습	- 기초 컴퓨터 포렌식(3학점 + 랩실습 1학점) - 파일시스템, OS 자료 복원, 시험(3학점 + 랩실습 1학점) - 디지털 매체 분석, 저장 장치와 그 활용	12
고급 디지털 포렌식 과정		
고급 디지털 포렌식	- 고급 컴퓨터 포렌식(3학점 + 랩실습 1학점) - 네트워크 포렌식(3학점 + 랩실습 1학점) - 저장 시스템(3학점)	11
선택과목	- 개인전자 기기(PED) 포렌식(3학점 + 랩실습 1학점) - 임베디드 기기(Embedded Device) 포렌식(3학점 + 랩실습 1학점) - 역공학 기법과 대책(3학점) - 멀티미디어 포렌식(3학점) - 통계학(3학점) - Independent Study(3학점) - 고급 디지털 포렌식 법률 쟁점(3학점) - 민법 쟁점(3학점)	9
총 이수 학점 : 120 ~ 124		

<표 3-13> 디지털 포렌식 석사학위 프로그램의 모델 커리큘럼

연구 분야	내용
디지털 포렌식 방법 개발	- 단순 또는 복합적 디지털 기기, 시스템을 포함한 복잡한 디지털 포렌식 시나리오를 제시하고, 해결 방법을 제안, 개발
고급 운영체제 분석	- 실시간(Real-time) 시스템[42] - 거래처리(Transaction Processing) 시스템[43]
디지털 포렌식 관리	- 범죄현장 관리 - 디지털 포렌식 랩 관리 - 케이스(case) 관리 - 품질 보증 - 윤리와 직업적 책임
디지털 증거 보존	- 통제와 검증 과정 - 디지털 증거의 보전과 복원에 대한 자연, 인간, 기구와 시간의 효과
형사와 민사의 법률 쟁점	- 법정 증언 - 법정에서의 증거 제출 - 고급 법률 논점 - 컴퓨터 압수/수색 - 모의 법정 - 전자적 증거 - 증거법
복잡한 데이터 분석	- 링크 해석(Link Analysis)[44] - 디지털 증거에서 물리적 증거로의 링크 - 타임라인 분석 : 데이터와 관련된 일자 연관성 - 데이터 구조 이해
복잡한 케이스(Case) 연구/시뮬레이션	- 다양한 케이스에서 연관성 있는 디지털증거 비교 - 대용량 데이터베이스 분석 - 엔터프라이즈 시스템(Enterprise System)[45] - 증거에 대한 국가 관할권과 국제적 수사 문제
데이터 통신 및 네트워크 시스템	- 패킷과 프레임 분석 - 네트워크 보안 이해 - 통신망 트래픽 복원과 추적

42) 컴퓨터에 의한 정보 처리방식으로 데이터가 발생한 시점에서 필요한 계산처리를 즉석에서 처리하여 그 결과를 데이터가 발생한 곳에 되돌려 보내는 방식이다. 예약 시스템, 예금 업무, 재고관리, 대공방위 시스템 등에 응용되며 소프트웨어와 하드웨어의 좋고 나쁨이 큰 영향을 끼친다. 리얼타임 시스템, 온라인 처리 시스템, 또는 즉시처리 시스템이라고도 한다. 이 방식의 주된 응용 면은 항공기나 철도의 좌석 예약 시스템, 은행의 예금업무, 제조업에서의 재고관리 ·공정관리

그리고 보고서에는 디지털 포렌식 관련 학위 교육 과정에 대한 모델을 제시하였는데, 2년 과정 준학사(Associate Degree Program in Digital Forensics), 4년 과정 학사(Baccalaureate Degree Program in Digital Forensics), 석사(Graduate Degree Program in Digital Forensics) 과정과 자격증(Academic Certificate Program in Digital Forensics) 과정 프로그램, 디지털 포렌식 실무가로서 훈련 및 상시 교육에 대한 요구사항과 커리큘럼 등을 상세히 제시하였다. <표 3-12>와 <표 3-13>은 디지털 포렌식 학사 및 석사 과정에 대한 커리큘럼이다.

2.2. 미국 대학

2.2.1. 로드아일랜드 대학교

로드아일랜드 대학교(University of Rhode Island)에서는 교내 설치된 '디지털 포렌식 사이버 보안 센터(DFCSC ; Digital Forensics and Cyber Security Center)'에서는 디지털 포렌식과 사이버 보안 분야에서 교육, 연구, 훈련, 디지털 포렌식 업무 지원 등을 담당하고 있으며, 2012

등을 들 수 있다. 또 대공방위(對空防衛) 시스템(미국의 SAGE 시스템 등)은 국가적인 규모의 실시간처리 시스템이다. 실시간처리 시스템의 구성에서는 컴퓨터 본체에 접속하는 외부기억장치, 개개의 적용업무에 따른 단말입출력장치, 단말장치와 컴퓨터 본체를 잇는 통신제어장치 등이 중요하다.(두산백과)

43) 거래처리 시스템이란 기업에서 일상적이고 반복적으로 수행되는 거래를 손쉽게 기록하고 처리하는 정보 시스템으로 기업 활동의 가장 기본적인 역할을 지원하는 시스템을 말한다. MIS의 하위 시스템으로는 컴퓨터를 이용하여 제품의 판매 및 구매와 예금의 입출금・급여계산・항공예약・물품선적 등과 같은 실생활에서 가장 일상적이고 반복적인 기본 업무를 능률적으로 신속하고, 정확하게 처리해서 데이터베이스에 필요한 정보를 제공해 준다. 거래처리 시스템의 주목적은 많은 양의 데이터를 신속하고 정확히 처리하는 것에 있다.(매일경제용어사전)

44) 링크 해석은 네트워크 이론에서 마디(nodes) 사이의 관계-조직, 사람, 거래를 포함하는 다양한 형태의 마디에서 관계가 인식이 된다-를 평가하는 데이터분석 기술이다. 링크 해석은 범죄수사(사기 탐지, 대테러 활동, 정보수집), 컴퓨터 보안 분석, 검색 엔진 최적화, 시장조사, 의학연구, 예술 등의 분야에서 사용되어 왔다.(https://en.wikipedia.org/wiki/Link_analysis)

45) 기업 등 다양한 운영 체제가 혼재하는 환경에서, 메인 프레임에서 PC까지의 모든 시스템을 관리 하는 것(컴퓨터인터넷IT용어대사전)

년 미국 국가정보국(National Secyrity Agency)과 국토안보부(Department of Homeland Security)에서는 로드아일랜드 대학교를 정보보안 교육분야에서 우수교육기관(National Center of Academic Excellence)으로 선정하였다[46]. DFCSC에서는 아래와 같이 다양한 과정의 디지털 포렌식 및 사이버 보안 프로그램[47]을 운용하고 있다.

위 프로그램 중 사이버 보안 전공 전문 이학 석사과정(Professional Science Master Degree in Cyber Security)을 살펴보면, 본 과정은 온라인 프로그램으로 구성되며 코스 지원자는 학사학위 소지자로 한정되고 핵심코스 과목을 습득하고, 포렌식 트랙(Forensics track) 또는 보안 트랙(Security Track) 중 하나의 트랙을 선택하여야 한다. 36학점 취득이 필요하며 논문은 요구되지 않고 최종적으로 파트너 기관과의 인턴쉽을 거쳐 대학원 수준의 연구 프로젝트를 완성하기를 요구한다.

<표 3-14> 로드 아일랜드 대학 교육 커리큘럼

프로그램	특징
학부 부전공 과정(undergraduate minor)	- 학부과정(전공에 관계없음)에 있는 학생이 디지털 포렌식이나 사이버 보안을 부전공으로 선택하는 과정
전문 자격 과정(Professional Certificate)	- 학사학위가 없는 직장인을 대상 - 온라인 교육
준 석사 과정(Graduate Certificate)	- 학사학위가 있는 직장인을 대상 - 온라인 교육
전문 이학 석사 과정(Professional Science Masters Degree)	- 학사학위가 있는 직장인을 대상 - 온라인 교육
석사 집중 과정(Masters Degree with a Concentration)	- 컴퓨터과학 석사과정을 하면서 디지털 포렌식 또는 사이버 보안에서의 준석사 학위를 취득하는 과정
박사 집중 과정(PhD with a Concentration)	- 컴퓨터과학 박사과정을 하면서 디지털 포렌식 또는 사이버 보안에서의 준석사 학위를 취득하는 과정

46) http://news.uri.edu/releases/?id=6235
47) http://dfcsc.uri.edu/academics

<표 3-15> 로드 아일랜드 대학 핵심코스 커리큘럼

과목	학점
정보보호 개론(Introduction to Information Assurance)	4
네트워크와 시스템 보안 개론(Introduction to Network and System Security)	4
사이버보안 전문 기술(Professional Skills for Cyber Security)	4
사이버보안 인턴쉽(Cyber Security Internship)	4

<표 3-16> 포렌식 & 사고 대응(Forensics & Incident Response) 커리큘럼

과목	학점
디지털 포렌식 1(Digital Forensics 1)	4
고급 디지털 포렌식(Advanced Digital Forensics)	4
디지털 포렌식 분석(Digital Forensics Analysis)	4
고급 사고 대응(Advanced Incident Response)	4

<표 3-17> 보안(Security) 커리큘럼

과목	학점
고급 네트워크 및 시스템 보안 토픽(Advanced Topics in Network and System Security)	4
디지털 포렌식 1(Digital Forensics 1)	4
고급 사고 대응(Advanced Incident Response)	4
고급 침입 탐지와 방어 또는 고급 디지털 포렌식(Advanced Intrusion Detection and Defence or Advanced Digital Forensics)중 선택1	4

2.2.2. 퍼듀 대학교

또한 미국의 대학에서 디지털포렌식 전공을 위한 유명한 과정은 퍼듀 대학교(Purdue University)의 사이버포렌식에 특화된 컴퓨터정보학 석사 과정(M.S. in CIT(Computer in Information Technology) with a Specialization in Cyber forensics)을 들 수 있다. 입학 조건은 컴퓨터학이나 정보공학 등의 학부과정을 마친 자가 지원하는 것이 바람직하나 이 조건은 필수는 아니다. 이 과정은 몇 가지 옵션(논문을 요하지 않는 과정)이 있으나 박사과정 진학이 가능한 코스는 아래표[48]와 같은 커리큘럼을 가지며 석사취득에 필요한 학점은 33학점 이상이며 논문을 필요로 한다.

<표 3-18> 퍼듀 대학 교육과정

학점	분류	학위 요구 조건
3	필수	대학원 수준 통계학 또는 정량적 평가(quantitative methods) 코스
3	필수	대학원 수준 연구 방법 코스(research methods course)
3	필수	파운데이션 코스(승인된 코스에서 선택)
15	필수	사이버 포렌식 핵심 코스
3	필수	선택과목(대학원 위원회 승인)
6	연구	연구 석사 논문(2학기 또는 그 이상의 학기 내 논문연구계획, 논문작성, 논문심사 포함)
33	종합	최소 33학점 이수를 요함

<표 3-19> 학위 요구 조건의 세부 내용

48) http://polytechnic.purdue.edu/degrees/ms-computer-and-information-technology

학위 요구 조건	내용
대학원 수준 통계학 또는 정량적 평가(quantitative methods) 코스	실험통계(Experimental Statistics), 통계방법(Statistical Methods), 산업과 기술에서의 측정과 평가(Measurement and Evaluation in Industry and Technology), 또는 CIT 대학원 프로그램 강좌나 대학원 교육 위원회에서 선승인한 코스 중 하나의 과목이 충족되어야 한다.
대학원 수준 연구 방법 코스(research methods course)	•산업기술 분야 연구 분석(Analysis of Research in Industry and Technology) •기술 연구 방법(Qualitative Research Methods in Technology) •컴퓨팅 기술 방법(Research Methods for Computing) •교육적 연구 개론(Introduction to Educational Research)
파운데이션 코스(승인된 코스에서 선택)	•정보기술(Organizational Impact of Information Technology) 정보기술 경제학(Information Technology Economics) •정보기술 프로젝트 관리(Information Technology Project Management) •정보기술 품질관리(Quality Management in Information Technology) 또는 산업기술에서의 품질과 생산성(Quality and Productivity in Industry and Technology) •고급 네트워크 보안(Advanced Network Security) 또는 기본 사이버포렌식(Basic Cyberforensics) •과학과 공학을 위한 프로그래밍(Programming for Science and Engineering)- 프로그램에 있어 보충교육을 필요로 하는 학생 대상 •CIT 대학원 프로그램 강좌나 대학원 교육 위원회에서 선승인한 과목
사이버 포렌식 핵심 코스	<표 3-20> 참조
관련 선택과목	대학원 위원회(Graduate Committee)의 승인을 필요로 한다.
연구 석사 논문	논문 코스는 2학기 이상 요구된다. •첫번째 학기(1-2학점)에는 논문계획서와 그에 대한 심사가 요구된다. •두번째 학기(5-6학점)에는 논문계획서에 따라 작성된 논문에 대하여 심사가 요구된다. •두 학기는 최소 6학점을 요구한다. 만약 연구가 2학기보다 길어질 경우, 다음 학기에 이수 추가 학점을 등록해야 한다.

학점은 4.0만점에 3.0이상의 학점을 요구하며, B-미만인 과목은 6학점 이내이어야 한다. 위 표에서 사이버 포렌식 핵심 코스(Cyber forensics Core Courses)로 불리기도 하는 15학점이 요구되는 사이버 포렌식 과정

은 <표 3-20>와 같다.

<표 3-20> 퍼듀 사이버 포렌식 핵심 코스

과목명	학점
기초 컴퓨터 포렌식	3
사이버 포렌식 연구 토픽	3
클라우드 및 가상 환경에서의 사이버 포렌식	3
파일 시스템에 대한 사이버 포렌식	3
멀웨어(Malware) 사이버 포렌식	3

2.2.3. 교육 커리큘럼에 있어 국내 과정과의 차이점

디지털 포렌식은 IT와 법학의 융합적인 성격으로 이 두 분야가 적절히 조화된 커리큘럼을 요한다. 그러나 위에서 살펴본 로드아일랜드 대학교와 퍼듀 대학교의 디지털 포렌식 석사과정 커리큘럼은 주로 IT분야의 연구에 치우친 면이 있고, 디지털 포렌식의 교육과 훈련을 위한 TWGED(Technical Working Group for Education and Training in Digital Forensics) 보고서에서 제시된 법학과 관련된 모델 커리큘럼은 법정 증언, 법정에서의 증거 제출, 모의 법정, 컴퓨터 압수/수색 등의 과목을 볼 수 있는데 실무가를 위한 교육 커리큘럼으로 구성되어 있음을 알 수 있다. 이는 IT분야와 법학의 균형적인 커리큘럼을 구성하여 교육하는 국내 디지털 포렌식 석사과정과 차이가 있으며, 더욱이 디지털 포렌식 분야 실무자 보다는 리더 양성을 위한 목적을 가지는 국내 석사과정 프로그램과는 차이가 있다고 볼 수 있다.

제 4 장 결론

제 1 절 전문가 양성 및 교육과정 개발 방안

현대사회가 지식정보의 사회로 발전에 감에 따라 첨단정보기술을 활용한 사이버범죄의 발생은 증가하게 되었고, 디지털 포렌식 전문가 양성에 대한 사회적 요구는 지속적으로 발생하게 될 것이다. 이에 본 연구에서는 디지털 포렌식 및 디지털 포렌식 전문가와 관련된 전반적인 이론연구와 사례연구를 통해 분석한 결과, 디지털 포렌식이 필요한 검찰과 검찰, 민간기관을 중심으로 디지털 포렌식 전문가 양성에 많은 노력을 기울이고 있음에도 불구하고, 앞으로도 양적, 질적 전문가 양성과 개발은 미미한 실정이다.

그 원인을 살펴보면 첫째, 많은 선행연구에서 지적하였듯이 법과 제도적 정비가 되지 않은 것이 원인이 된다. 국가정보·수사기관 및 민영기업에서의 디지털 포렌식 기술의 적절한 활용능력의 확보가 국가와 기업의 경쟁력이 되는 상황에서 디지털 증거의 적법성 확보를 통한 법질서 확립과 정의 구현 및 디지털 증거의 적법성 확보를 통한 경쟁력 강화라는 궁극정인 목적을 달성하기 위해서는 한 두 개의 개별적인 법률의 개정이 아니라, 수사·정보기관, 민간기업, 관련 산업체와 같은 모든 주체들의 참여를 전제로 한 국가 디지털 포렌식 체계에 기반을 둔 관련 법규의 수립과 각 법 요소 간 균형있는 발전이 요구된다(유영현 등, 2009).

둘째, 디지털 포렌식 관련 기관의 연계의 부족으로 현재는 수사기관인 검찰과 경찰조직에서 인재 양성을 위해 많은 노력을 기울이고 있지만, 디지털 포렌식이 필요한 국가정보원, 국방부, 관세청과 국세청, 공정거래위원회, 한국저작권 위원회 등의 기관들이 개별적인 디지털 포렌식 전문가 양성과 개발방안을 제시함으로써 관련기관의 상호협력이 되지 않아

정책과 자원의 효율적 활용이 되지 않는 것이 현실이다.

이에 국가적인 차원에서 각 부처의 업무, 권한과 책임 등을 조율하여 디지털 포렌식 전문인력 개발 협의체를 구성한 후 디지털 포렌식 전문가에 대한 필요인원을 조사·분석하고, 전담인력 부족을 해소하기 위해 디지털 포렌식 기능교육원과 같은 전문교육기관을 설립하고 정보통신기술을 활용한 증거수집과 분석, 증거제출과 관련한 교육지원이 필요하다. 이를 위해 디지털 포렌식과 관련한 기관들이 축적하고 있는 정보와 기술의 공유와 중·장기적 협력강화는 필수적인 요소가 될 것이다.

셋째, 디지털 포렌식의 개념에 대한 이해부족으로, 디지털 포렌식은 법학과 인문학, 컴퓨터공학과 IT기술이 포함된 융복합적 성적을 가지고 있어 다양한 분야의 정보와 지식이 요구되는 분야임에도 불구하고, 현재 국내 교육은 대학과정부터 법률적 지식과 이공계 지식이 분리되어 학습되고 있고, 편향된 지식에 대한 교육이 실시되어 수사과정에서 실체적 진실에 접근하기 위한 증거의 수집, 분석, 제출의 통합적 교육이 진행되고 있다. 따라서 독자적 학문으로 법과학이라는 인식을 통해 디지털 포렌식에 대한 접근이 필요하다.

넷째, 대학 기초교육의 부족으로, 현재는 수사기관의 자체교육과 한국포렌식학회와 사이버포렌식 전문가협회에서 주관하는 자격증을 위한 교육과정, 일부 대학에서 개설된 교육과정에서 디지털 포렌식 전문가 양성과 개발을 하고 있으나 정보기술과 산업사회의 발달의 추세를 반영하기는 어려운 실정이다. 따라서 교육전문기관인 대학을 중심으로 실무 적합형 전문가 양성의 목적을 가진 학부과정과 디지털 포렌식 핵심 전문인력 양성과정인 대학원 과정을 중심으로 우수인재의 양성과 개발에 역량을 집중하여야 한다.

다섯째, 국가차원의 자격제도의 정비가 필요하다. 현재 국내 디지털 포렌식 관련 자격은 한국포렌식학회에서 주관하는 디지털 포렌식 전문가 자격과 사이버 포렌식 전문가 협회에서 인증하는 사이버 포렌식 조사전

문가 자격이 있으며 국제 전문자격으로는 EnCE 디지털 포렌식 수사 자격증과 미국 엑세스데이터의 FTK 포렌식 전문가자격증(ACE)가 있다. 이런 자격제도의 문제점은 자격증을 획득하기 위해 단편적인 지식함양에 집중한다는 점이다. 때문에 디지털 포렌식이 국가와 전체사회를 위한 공익적인 측면의 기술인만큼 국가주도형의 교육 커리큘럼과 전문가를 양성하여 수사 일선에 배치함으로써 디지털 증거에 대한 신뢰성을 확보해야 한다.

여섯째, 디지털 포렌식 전문가 양성을 위해서는 교육 전문인력의 개발이 선행되어야 한다. 법과학이나 디지털 포렌식이 비교적 최근에 활발하게 연구되고 있기 때문에 국내에서는 이론적 지식과 경험적 지식을 갖춘 교육인력이 부족한 실정이다. 따라서 현재 수사기관에서 디지털 포렌식 관련 활동을 한 실무경력자를 중심으로 교육 실무자의 양성이 무엇보다 선행되어야 한다.

제 2 절 연구의 의의 및 시사점

본 연구에서는 연구의 목적인 디지털 포렌식 전문가 양성 및 개발방안을 도출하기 위해 디지털 증거와 디지털 포렌식, 미국의 E-Discovery 제도에 대한 이론연구를 실시하였다. 구체적으로 많은 선행연구를 통해 디지털 증거의 개념과 속성, 유형에 대해 연구하였고, 디지털 포렌식의 개념, 기본원칙, 유형과 절차에 대해 연구하였으며, 현대 사회에서 디지털 포렌식의 필요성과 중요성에 대해서도 연구하였다. 또한 미국의 E-Discovery 제도에 대한 이론연구와 사례연구를 통해 국내 도입가능성에 대해서도 검증하였다.

디지털 포렌식 전문가 양성과 개발을 위해서는 국내외 디지털 포렌식 관련기관의 전문가 현황 및 교육 프로그램에 대한 현황을 조사하였고, 결론에서 디지털 포렌식 전문가 양성 및 교육과정 개발 방안을 제시하였다.

따라서 본 연구는 기존의 선생연구에서 많이 다뤄지지 않은 디지털 증거와 디지털 포렌식, 전문가 양성과 개발이라는 주제로 이론연구와 사례연구를 진행하여, 현대 사회에서 디지털 포렌식의 중요성 및 인력양성의 필요성과 정책적 방향성에 대한 시사점을 제공한다.

또한 앞으로의 디지털 포렌식에 대한 학문적 기틀을 제공하여, 앞으로 지속적인 연구를 통해 디지털 포렌식 전문가를 양성하고 개발하는 다양한 제도와 방법을 개발하는데 많은 역할을 할 것으로 기대한다.

제 3 절 연구의 한계 및 발전방안

본 연구는 많은 시사점을 제공하지만 다음과 같은 한계를 포함하고 있어 이를 보완하기 위한 계속적인 연구가 반드시 필요하다.

첫째, 연구대상의 한계이다. 본 연구에서는 디지털 포렌식과 관련한 다양한 이론연구와 관련 기관의 현황에 대한 연구조사를 진행하려고 하였으나 관련한 자료와 국내외 선행연구가 많이 부족하여 연구의 대상을 검찰과 경찰조직을 중심으로 한정하였고, 보다 포괄적인 연구결과를 제시하지 못하였다. 앞으로 많은 연구자들에 의해 다양한 연구가 진행된다면 선행연구의 부족에서 오는 한계는 극복될 것으로 보인다.

둘째, 연구내용과 관련한 한계이다. 본 연구는 디지털 포렌식 전문가 양성 및 교육 프로그램 개발을 중심으로 연구되었으나 관련한 거시적 환경변화, 공급측면에서의 원인, 수요측면에서의 원인 등의 내용을 포괄적으로 포함시켜 연구되지 못하였고, 연구결과가 다소 명확하지 못하게 도출되었다는 한계를 가지고 있다.

셋째, 연구방법의 한계이다. 본 연구의 목적을 달성하기 위해서는 디지털 포렌식의 발전 과정과 전문인력의 수요와 공급의 변화에 대해 시계열적 분석의 필요성이 존재하지만 제한된 사례분석의 형태를 가지고 있어 실증적인 검증이 없었다는 부분과 횡단적 자료만을 이용하였다는 연구의 한계점을 가진다.

참 고 문 헌

곽병선(2011), 디지털 포렌식 수사의 문제점과 개선방안, 법학연구, 42, 171-191.

권오걸(2011), 디지털 증거의 개념, 특성 및 증거능력의 요건, IT와 법 연구, 5, 291-318.

김교성(2014), 디지털 증거의 진정성 입증방안에 관한 연구, 연세대 법무대학원 석사학위논문

대검찰청(2012), 차세대 디지털 포렌식 기술 및 사이버범죄 대응 기술 연구 디지털 포렌식 로드맵 수립

변진석(2012), 미국 민사소송에서 증거개시의 역할과 한계, 한국에 도입 가능성, 미국헌법연구, 23(3), 130-162

송봉규·장석헌(2013), 경찰의 디지털 포렌식 실태와 개선방안, 한국경찰연구, 12(2), 115-142.

서동희(2005), 미국법상의 Discovery 제도의 도입 필요성, 법학연구, 18, 775-812.

양근원(2006), 디지털 포렌식과 법적 문제 고찰, 형사정책연구, 66, 205-246.

유영찬(2002), 법과학과 수사, 현암사

유영현·송봉규·박상진(2009), 디지털포렌식(digital forensic) 전문 인력 필요성과 양성방안, 한국경찰학회보, 22, 253-284.

유정호·박영수(2014), eDiscovery 이해와 위기관리전략, 인포더북스.

임종인(2007), 경찰의 차세대 디지털 포렌식 기반 구축방안, 고려대 정보경영공학전문대학원 석사학위논문.

이상진(2010), 디지털 포렌식 개론, 이룬.

이완규(2007), 개정 형사소송법의 쟁점, 탐구사.

전명길(2011), 디지털 증거의 수집과 증거능력, 법학연구 41, 317-336

최득신, 디지털 포렌식 관점에서 본 증거개시제도 연구(2008), 고려대 석사학위 논문,

탁희성(2011), 전자증거개시제도(E-Discovery)에 관한 연구, 연구총서, 2011(13), 1-145.

탁희성·이상진(2006), 디지털 증거분석도구에 의한 증거수집절차 및 증거능력확보방안, 연구총서, 2006(1), 13-248.

한성훈(2015), 디지털 증거의 증거능력에 관한 소고, 한양법학, 26(3), 335-356.

Anthony Lang, Masooda Bashir, Roy Campbell, Lizanne DeStefano, "Developing a new digital forensics curriculum", Digital Investigation 11, S76-S84, 2014

Carrie Morgan Whitcomb(2002), An Historical Perspective of Digital Evidence
: A Forensic Scientist's View, International Journal of Digital Evidence, 1(1), 1-9.

Larry E. Daniel, Lars E. Daniel, Digital Forensics for Legal Professionals 한국어 번역판(2012), BJ퍼블릭

Linda Volonino, "Electronic Evidence and Computer Forensics", Communication of the Association for Information systems Vol. 12, Article 27, 2003