디지털 증거(Digital evidence)와 포렌식(Forensics)

김 봉 수*

현대사회에서 디지털문화는 이동통신 및 E-mail 등을 통해서 일상생활영역에까지 깊숙이 뿌리를 내리고 있기 때문에, 인간의 행위 역시 디지털정보 또는 전자적 데이터 등으로부터 자유로울 수 없다. 그리고 이러한 법현실은 인간행위를 규범적으로 평가하는 법영역에서도 예외가 아니다. 따라서 인간행위의 법위반 내지 범죄성립여부를 다루는 민·형사소송에서도 디지털정보 및 데이터는 이제 인간행위에 대한 법적 평가를 둘러싸고 벌어지는 다툼과 관련하여 사실관계의 진위여부를 입증해 주는 증거로서 중요한 의미를 가진다.

하지만 디지털 증거(Digital evidence)는 기존의 물리적 증거와 구별되는 특성(매체독립성, 불가시성, 전문성, 대량성, 취약성 등)을 가지고 있기 때문에, 이를 증거로 활용하기 위해서는 증거의 수집과 분석 그리고 법정에 증거로 제출하기까지 철저한 절차적 통제와 세심한 취급을 요한다. 바로 이러한 특별한 취급과 절차적 매뉴얼의 필요성에 따라 등장한 것이 '디지털 포렌식(Digital Forensics)'이라고 할 수 있다. 하지만 '디지털 증거' 또는 '디지털 포렌식'의 개념 및 필요성에 대한 인식이 아직까지는 우리나라의 소송절차(특히 형사소송절차)에 적극적으로 반영되어 있지 않기 때문에 '디지털 증거'와 이를 위한 '디지털 포렌식'이 하나의 법문화로 정착하기 위해서는 지속적인 연구와 국가적 차원에서의 지원이 필요하다고 사료된다.

* 서울대학교 박사후과정 연구원, idi21@naver.com

목 차

Ⅰ. 서론 – 『아날로그』와 『디지털』이 혼합된 현재(**現在**)

「아날로그」와 「디지털」이라는 단어는 흔히 '과거 vs 현재' 또는 '구식 vs 신식'을 나타내는 대립개념 내지 상반된 의미의 수식어로써 사용되어졌다. 하지만 근래에 들어와서는 현대사회 속에서의 삶의 방식을 의미하는 용어로까지 그 의미가 확대되었다. 예컨대, '아나디지' 혹은 '디지로그'와 같은 합성어가 바로 그것이다. 먼저 「아나디지(AnaDigi)」는 아날로그적인 감성 및 상상력, 인간적인 요소들을 근간으로 디지털의 발전된 기술을 활용하는 사회를 나타내는 말이며, 이른바 아날로그시대에 디지털적인 도구를 이용하는 것을 표현하는 신조어이고, 반면에 「디지로그(DigiLog)」는 디지털이 근간이 된 사회에서 디지털 사회에서 부족할 수 있는 아날로그적인 감성(예컨대 인간미, 감성 등)으로 보충하는 것을 의미한다. 따라서 양자의 개념은 주된 기반을 어디에 두느냐에 따라 방향성을 달리하는 개념이라 할 수 있다. 즉 전자는 아날로그적인 삶에 기반을 두고 디지털을 이용하는 것인 반면, 후자는 디지털 세계를 바탕으로 하면서 아날로그를 가미하는 방식을 의미한다. 하지만 두 개념 모두 「아날로그」와 「디지털」의 혼합 혹은 융합적인 삶의 형태 내지 방식을 의미함으로써, '현대적 삶'의 모습을 함축적으로 표현하고 있다는 점에서 본질적으로 의미의 동질성을 갖는 유개념(類槪念)이라고 평가할 수 있다. 그리고 이는 현대적 삶 또는 생활방식의 특성을 정확하게 나타내고 있는 현시대의 '키워드(Keyword)'이기도 하다.

상황이 이렇다보니, 새삼스레 이처럼 우리의 일상적인 생활 속에 깊이 스며들어와 있는 '디지털'이 법적으로 가지는 의미는 무엇인지 궁금해진다. 바꾸어 말하면 '디지털화'되고 있는 개인의 삶 또는 특정한 행위들에 대해서 만약 법적인 판단을 내려야 한다면, 과연 기존의 법적 판단방식 내지 접근방법으로 가능한 것인지, 다르다고 한다면 무엇이 다르고, 또 어떻게 이 문제를 취급하는 것이 바람직한 것인지 고민하지 않을 수 없다.

따라서 이 글에서는 디지털기술의 발전과 그로 인한 현대사회의 변화들을 법적 관점에서 어떻게 바라볼 것인지에 관한 문제를, '디지털 증거의 등장'이라는 법영역에서의 새로운 변화를 중심으로 하여 규범적(특히 형사법적)인 시각에서 접근해 보고, 빠르게 디지털화되어 가고 있는 사회변화 속에서 법규범(특히 형사법)이 수용해야 하는 변화의 방향성을 짚어보고자 한다.

Ⅱ. 디지털시대로의 전환이 갖는 법적 의미
-'디지털 증거'의 등장으로 인한 증거법분야에서의 변화를 중심으로

벌써 2년 전 이야기가 되어버린 「신정아」 사건을 비롯해서 최근 사회적 물의를 일으키고 있는 「신영철 대법관의 재판개입」 사건은 당사자들 간에 오고간 E-mail이 범죄수사의 단서 및 유죄입증의 결정적인 증거가 되어서 법의 심판을 받게 된 대표적인 사례이다. 바로 여기서 등장하는 E-mail과 같은 것이 '디지털 증거'라고 할 수 있다. 이처럼 '디지털'이라는 용어는 이미 우리의 법현실 속에 깊숙이 들어와 있고, 이러한 법현실의 변화에 민감할 수밖에 없는 법영역, 즉 '증거법' 분야에서는 사실상 증거의 '질적 변화'를 가져오고 있다.

즉 과거에는 문서, 시각매체 및 증언 등과 같은 유형적 증거가 주된 형태였고, 이후에는 아날로그적 기술의 발전으로 오디오테이프 또는 비디오테이프, 엑스레이 등의 영상 등이 증거로 활용되었다. 하지만 이 역시 증거의 속성 내지 성질상 유형적 증거로서 평가할 수 있다. 그러나 현재에는 디지털기술을 통한 정보저장기술이 발전하여

기존에 문서 혹은 테이프, CD 등과 같은 아날로그적 저장매체가 설 자리를 잃게 되면서, 디지털저장방식으로 저장되어 있는 정보 자체가 증거로서의 가치를 가지고 법영역에 등장하고 있다. 바로 기존의 아날로그적 성격의 물리적 증거와 구별하여 이를 '전자증거(e-evidence)' 내지 '전자적 증거(electronic evidence)'[1] 또는 '디지털 증거(digital evidence)'[2]라고 하는 것이다.[3]

1. 『디지털 증거(digital evidence)』의 개념

그렇다면 법현실 속에서 이미 등장한 '디지털 증거(digital evidence)'를 어떻게 정의할 것인지가 문제되는데, 아쉽게도 아직까지 이에 대한 정확한 개념정립은 이루어지지 않고 있는 것으로 보인다. 다만 1995년 창설된 IOCE(International Organization on Computer Evidence: 컴퓨터증거에 관한 국제조직)과 1998년 SWGDE(Scientific Working Group on Digital Evidence: 디지털 증거에 관한 과학실무그룹)의 디지털 증거에 대한 정의는 참고해 볼만하다. 먼저 IOCE는 '2진수 형태로 저장 혹은 전송되는 것으로서 법정에서 신뢰할 수 있는 정보'[4]를, 그리고 SWGDE는 '디지털 형태로 저장·전송되는 증거가치 있는 정보'[5]를 각각 디지털 증거로 개념정의하고 있다.

그리고 이러한 개념 정의에 따라서 '디지털 증거'를 '전자적 증거(electronic evidence)'와는 다른 층위의 개념으로 구별하여 사용하려는 것이 일반적이다.[6] 즉 전자적 증거는 아날로그방식[7] 또는 디지털방식[8]으로 저장된 정보 내지 데이터를 총체적으로 의미

1) 탁희성(2004), p.8.
2) 안경옥(2005), p.155.
3) Howard L. Nations(2007). 이 외에도 '컴퓨터에 의해 생성된 증거(computer-generated evidence)' 또는 '첨단증거(hi-tech evidence)' 등의 용어도 사용되고 있다(이규호(2007), p.153).
4) http://www.ioce.org/G8_proposed_principles_for_forensic_evidence.html에서 "G8 Proposed Principles For The Procdures Relating To Digital Evidence" 참조 [양근원(2006), p.136에서 재인용].
5) http://www.fbi.gov.hq/lab/fsc/backissu/april2000/swgde.html 참조 [양근원(2006), p.136에서 재인용].
6) 양근원(2006), pp.135~136; 이규호(2007), p.154.
7) 아날로그방식은 연속으로 변화하는 양을 그대로 표현하는 방식으로써, 동종의 기기나 매체를 벗어나서는 호환이 어려울 뿐만 아니라 다른 매체에 복사하거나 이동되면 반드시 전자적 혹은 물리적으로 양적·질적인 손실이 생기기 때문에 데이터의 동일성이 인정되지 않는다.

하는데 반해서, 디지털 증거는 이 중에서 후자의 방식으로 저장된 정보 및 데이터만을 의미한다는 것이다. 요컨대, 정보저장방식의 관점에서 볼 때, 디지털 증거는 전자적 증거보다는 좁은 개념으로 이해할 수 있다.

하지만 이러한 전자적 증거와 디지털 증거의 개념적 구분만으로는 '디지털 증거' 개념의 어렴풋한 윤곽만을 확인할 수 있을 뿐이고, 따라서 보다 적극적인 개념정의가 필요하다고 본다.

2. 디지털 증거의 특성

일반적으로 디지털 증거가 기본의 물리적 증거와 구별되는 차이 내지 특성으로, 매체독립성, 대량성, 원본과 사본의 구별 곤란성, 변조용이성, 비가시성 내지 비가독성, 전문성 등이 거론되어진다.[9)]

첫째, '①매체독립성'[10)]은 앞서 설명한 바와 같이 디지털저장방식의 특성에서 비롯된 것으로써, 저장매체나 매개체의 특성에 따른 영향을 받지 않는다. 즉 저장되는 매체의 성질에 좌우되지 않고, 항상 일정한 정보의 값을 유지한다는 것이다. 따라서 디지털정보는 복사 또는 기타 방법을 통한 정보의 생산과 이전 등이 자유롭기 때문에 원본 및 사본의 대량생산이 가능하고(②대량성),[11)] 그로 인해 디지털 증거에 있어서 '③원본과 사본의 구별 곤란성'을 초래하게 된다. 즉 반복된 복사과정을 거치더라도 디지털정보의 값 혹은 가지가 동일하게 유지되지 때문에 질적인 측면에서 원본과 사본의 구별되지 않게 된다.[12)] 바로 이러한 특성은 후술하는 디지털 증거의 증거능력과 관련하여 어려운 문제를 초래한다. 그리고 위의 2가지 특성을 고려해 볼 때, 결국 디지털 증거는 '가변적인' 증거로서 간단한 조작만으로도 위조 내지 변조가 가능하고,

8) 한편 디지털방식은 데이터를 0과 1을 조합하여 표현하는 방식으로써, 데이터를 디지털로 저장하는 경우 매체와 기기에 상관없이 동일한 값이면 동일한 가치를 갖는다.
9) 양근원(2006), pp.137~139; 노명선(2008), p.78; 박수희(2007), pp.130~131.
10) 원혜욱(2000), p.32; 양근원(2006), p.137.
11) 안경옥(2005), p.157.
12) 이성진 외(2002), p.150.

정보일부의 삭제 내지 변경이 용이하다는 점에서, 증거로서 '④취약성'의 한계를 갖는다.

뿐만 아니라 디지털 증거는 전자적 정보의 형태로 기록·저장되어지기 때문에 인간의 오감으로는 직접 정보의 내용을 인지할 수 없다는 점에서 '⑤비가시성 내지 비가독성'의 특징을 갖는다.[13] 따라서 디지털 증거를 재판에서 증거로 활용하기 위해서는, 디지털형태로 저장된 정보를 다시 현시적인 증거로 가시화하는 변환과정이 필수적으로 요구된다. 그리고 이 변환과정에는 디지털저장과 관련한 프로그램 및 기술들이 동원되어야 하기 때문에 이에 관한 전문가의 참여가 필요하게 되고,[14] 따라서 디지털 증거는 판독하는 '⑥전문성'을 띄게 된다.

3. 디지털 증거의 법적 취급과 활용에 있어서의 문제점

위와 같은 특성들로 인해서 법적으로 디지털 증거에 의미를 부여하기 위해서는, 기존의 물리적 증거와는 수집과 활용에 있어서의 다양한 문제들이 발생한다.

먼저 [디지털 증거의 수집과정]과 관련해서는, 디지털 증거의 비가시성 내지 비가독성 때문에 직접적인 인지 내지 판독이 불가능하고, 따라서 필수적으로 전문가의 참여와 가시화를 위한 변환절차가 요구된다. 하지만 디지털 증거의 취약성 때문에 이 과정에서 증거의 왜곡, 증거내용의 변경 및 훼손, 더 나아가서는 조작가능성의 문제 등이 발생하게 된다. 그리고 증거로서 의미를 가지는 전자적 정보가 디지털방식으로 저장되어 있는 것이 디지털 증거이기 때문에, 이러한 디지털 증거의 수집과 확보를 위해서는 저장매체에 대한 압수 및 수색 등이 필수적인 절차로 동반되어지는데, 이 과정에서 법적 문제가 발생하게 되면 형사소송법 개정을 통해 명문화된 위법수집증거배제법칙과 관련하여 복잡한 문제가 발생할 소지가 있다.[15] 그러므로 디지털정보를 법적 증거로 활용하기 위해서는 수집과정에 대한 매우 엄격한 통제와 정교한 절차적 매

13) 노명선(2008), p.79.

14) 양근원(2006), p.139; 노명선(2008), p.78.

15) 이은모(2005), pp.156~175; 이 철(2004), pp.265~291; 노명선(2008), pp.74~125; 원혜욱(2003), pp.165~191; 이종상(2001), pp.327~389.

뉴얼이 필요하다. 더욱이 이는 디지털 증거의 증거능력과 관련하여 '무결성(無缺性)' 요건의 충족여부와 직결되기 때문에, 물리적 증거의 수집과 비교할 때보다 세심한 주의가 요구된다.

한편 [디지털 증거의 활용]과 관련해서는, 디지털 증거도 증거이기 때문에 증거능력 인정을 위한 기본적인 조건을 갖추어야 한다. 즉 증거로서의 '진정성' 및 '무결성'의 요건을 충족해야만 디지털 증거를 형사소송에서의 증거로 활용할 수 있는 것이다. 여기서 증거능력의 요건으로 등장하는 '진정성' 요건은 물리적 증거의 증거능력에서 말하는 형식적·실질적 진정성립과 논의의 맥을 같이 한다. 즉 디지털 증거의 진정성 역시 특정의 행위로 생성된 결과물이고, 그 저장 및 수집과정에서 오류가 없는 경우에 한하여 인정될 수 있다.[16] 반면 '무결성' 요건은 수사 및 재판을 위한 사후과정, 즉 디지털 증거의 수집·분석·보관·처리·법정제출 전 과정에서 최초의 원본성이 훼손되거나 오염되지 않았는지를 평가하는 요건이라고 할 수 있다.

이와 같이 디지털 증거를 물리적 증거와 같이 형사소송에서 증거로 활용하기 위해서는, 행위자에 의한 원본의 생성에서부터 수사과정에서의 수집 및 분석 그리고 이를 법정에 증거로 제출하기까지 취급상 특별한 주의를 요하고, 이를 뒷받침해줄 제도적 장치로서의 세심한 절차 마련이 선결문제로서 중요한 의미를 갖게 되는데, 이러한 필요성에 의해서 등장한 것이 '디지털 포렌식(Digital Forensics)'이다.

Ⅲ. 디지털 포렌식(Digital Forensics)과 관련한 법적 문제

1. 디지털 포렌식의 개념과 필요성

본래 '포렌식(forensic)'은 법의학에서 사용하는 용어로써, 사체를 조사해 수사에 도움이 될 수 있는 증거를 찾아 이를 수집·분석하여 그 조사결과를 법정에 제출하는 일련의 과정을 말한다. 따라서 '디지털 포렌식(digital forensics)'은 이러한 포렌식의

16) 양근원(2006), p.143.

개념을 디지털영역에 접목한 용어로써, '법정 제출용 디지털 증거를 수집하여 분석하는 구체적인 기술 내지 일련의 절차'를 의미한다.

그리고 전술한 바와 같이 디지털 증거수집 및 분석과정은 기술적 복잡성을 가진 분야이기 때문에 수집 및 분석과 관련하여 전문성이 요구되고, 따라서 체계적인 디지털 포렌식의 확립과 지속적인 발전은 곧 디지털 증거의 진정성 및 무결성 그리고 당해 정보 및 데이터에 대한 신뢰성과 직결된다는 점에서 아주 중요한 의미를 가질 뿐만 아니라 더 나아가서는 사법기관의 인권보호 및 사법적 정의구현에도 기여할 수 있다는 점에서 보다 많은 관심과 연구가 필요한 영역이라고 평가할 수 있다.

2. 디지털 포렌식의 유형

전술한 바와 같이 디지털 포렌식은 증거의 수집, 보존, 분석, 문서화, 그리고 재판과정에 증거로 제출하기까지의 모든 과정을 포함한다. 하지만 디지털저장기술의 발전으로 인해서 디지털 포렌식의 적용대상으로서의 현실에도 많은 변화가 이루어지고 있다. 즉 과거의 컴퓨터 하드디스크 검사와 같은 단순한 기술을 넘어서 현재에는 네트워크, 인터넷, 데이터베이스, 모바일 기기, 휘발성 메모리 등에 대한 다양하고 복잡한 정보수집기술 및 분석작업이 요구되고 있다. 따라서 이러한 법현실의 빠른 변화에 대응하기 위해서, 디지털 포렌식의 방식 및 유형도 다양화되고 있는데, 이를 유형화 또는 분류해 보면 다음과 같다.

(1) 디지털정보의 수집 및 사용목적에 따른 분류

먼저 데이터 및 디지털정보의 수집과 사용용도 및 목적에 따라 디지털 포렌식을 유형화하면, 크게 '정보추출형'과 '사고대응형'으로 나누어 볼 수 있다.

1) 정보추출 포렌식(Information extraction forensics)

먼저 '정보추출형' 포렌식은 디지털 저장매체에 기록되어 있는 데이터를 복구하거나 검색하여 찾아내고, 회계 시스템에서 필요한 계정을 찾아 범행을 입증할 수 있는 수치 데이터를 분석하거나 이메일 등의 데이터를 복구 및 검색하는 과정을 통해서 범

행 입증에 필요한 증거를 발견 및 확보하는 것을 목적으로 하는 포렌식의 유형이다.

2) 사고대응 포렌식(Incident response forensics)

한편 '사고대응형' 포렌식은 해킹과 같은 침해행위로 인해 손상된 시스템의 로그, 백도어, 루트킷 등을 조사하여 침입자의 신원, 피해내용, 침입경로 등을 파악할 목적으로 이루어지는 디지털 포렌식의 유형으로서, 네트워크 기술과 서버의 로그 분석기술, 유닉스, 리눅스, 윈도우즈 서버 등 운영체제에 관한 전문적 지식과 기술 등이 요구된다.

(2) 수집 및 분석대상(저장매체의 특성)에 따른 분류

한편 디지털 증거의 분석대상을 기준으로 분류해보면, 아래와 같이 휘발성증거에 대한 포렌식, 디스크 증거에 대한 포렌식, 네트워크 증거에 대한 포렌식, 프로그램 소스 분석 등으로 나누어 볼 수 있다.[17]

1) 휘발성 증거에 대한 포렌식

이는 예컨대, 레지스터(Registers) 및 캐쉬(Cache), 메모리(Memory)의 내용이나 네트워크 연결상태(State of network connections), 실행중인 프로그램상태, Swap파일 시스템의 내용, 기타 하드디스크에 저장된 파일 및 디렉토리에 대한 시간속성정보들과 같이 생성 및 접근과정에서 본래의 정보 및 데이터가 쉽게 변하거나 훼손되는 휘발성정보를 수집하는 경우에 요구되는 수집방식 및 절차를 말한다. 즉 휘발성 정보 및 데이터에 대한 포렌식은 디스크 이미지 복사 등을 사용하여 수집하는데 한계가 있기 때문에, 원본성 및 무결성을 입증하는데 특별한 기술적 조치를 요한다.

2) 디스크 증거에 대한 포렌식

이는 소위 하드디스크, 플로피 디스크, 콤팩트 디스크(CD), DVD, USB메모리 등과 같이 비휘발성 저장매체로부터 디지털정보 및 데이터를 획득·분석하는 작업을 말한다. 이러한 저장매체와 관련한 디지털 증거의 경우에는 주로 저장매체의 압수 및 복제 혹은 이미지 복사 등의 방법을 통해서 구체적인 정보 및 데이터를 확보·분석하는 것

17) 양근원(2006), pp.219~223.

이 보통이다.

3) 네트워크 증거에 대한 포렌식

이는 네트워크상에서 전송중인 디지털 증거를 획득·분석하는 작업을 의미하는데, 전송중인 패킷의 헤더를 분석하거나 통신내용을 분석하는 방법이 주로 사용되고, 이와 관련해서는 통신비밀보호법의 엄격한 제한 및 절차적 통제를 받는다.

4) 프로그램 소스(Source) 분석

이는 확보된 프로그램 원시코드를 분석하거나 원시코드가 없을 경우 리버스엔지니어링(Reverse Engineering) 등의 기법을 통해서 디지털 증거로 확보된 프로그램의 작동방식 및 결과를 분석하는 과정을 말한다.

3. 디지털 포렌식의 원활한 활용을 위한 단계적 고찰

(1) 증거수집 전단계 - 전문인력 양성과 절차적 매뉴얼 확립의 필요성

디지털 포렌식을 적극적으로 활용하기 위해서는, 다양한 운영체제 및 파일 시스템, 네트워크, 데이터베이스, 회계 시스템 등에 대한 지식과 기술을 가진 전문인력의 양성과 확보가 무엇보다 필요하고, 다양한 디지털 증거에 대한 다각적인 접근과 분석이 가능하도록 전문적인 디지털 포렌식의 도구개발 등 활발하게 이루어질 필요가 있다. 이를 위해서는 디지털관련 분야 및 전공인력들의 지속적인 관심 및 적극적인 참여 그리고 국가의 정책적·재정적 지원과 전문기관의 설립 등과 같은 기본적인 인프라의 구축이 절실히 필요하다고 볼 수 있다.

그리고 디지털 증거의 폭넓은 활용을 위해서는, 증거의 연속성 및 무결성을 유지하기 위한 절차적 매뉴얼을 작성하여 활용하는 것이 필요하다. 즉 증거를 소유한 사람 또는 가져간 시간, 돌려준 시간, 소지한 이유 등을 정확히 기록하게 하여 증거가 훼손되거나 손실되지 않도록 세심하고 철저한 절차적 지침을 마련하는 것이 중요하다.

(2) 증거수집단계 - 디지털 증거의 종류에 따른 수집방법의 다양화

디지털 포렌식의 유형 또는 분류에서 살펴본 바와 같이, 수집대상인 디지털 증거의

성격 또는 해당 저장매체의 특성과 종류에 따라 다양한 수집방법 및 포렌식 도구의 활용이 필요하다. 따라서 디지털 포렌식을 진행할 때, 우선적으로 휘발성 증거에 대한 수집이 먼저 이루어져야 할 것이다. 즉 증거수집시에 메모리나 프로세스, 화면에 있는 정보 등 소멸 가능성이 많은 증거부터, 예컨대 레즈스트리와 캐쉬, 라우팅 테이블, ARP 캐쉬, 프로세스 테이블, 커널 정보와 모듈, 메인메모리, 임시 파일, 보조 메모리, 라우터 설정 정보, 네트워크 위상(Topology)과 같은 순으로 디지털 증거의 수집이 이루어져야 할 것으로 판단된다.

또한 문서의 작성, 수정 등의 정보가 문제가 될 때에는 가급적이면 전원을 차단하고 전문가에게 분석을 의뢰하여야 하며, 네트워크에 연결되어 있는 경우에는 수시로 접속하여 데이터의 삭제가 가능하기 때문에 사전에 네트워크 단자를 제거하는 등의 조치를 취해야 한다. 그리고 증거 수집 과정에서 사용한 도구의 이름, 버전, 분석과정, 시간, 산출 결과 등 전 과정도 기록하도록 하여 수집과정의 신뢰성 및 무결성을 입증하는 자료로서 활용하고 분석과정에서도 이를 참고할 수 있도록 기록화를 의무화하는 것이 필요하다. 그리고 다수의 사용자가 접속하는 대형 시스템의 경우에는 선의의 피해자가 생기지 않도록 필요한 데이터를 현장에서 추출하고 별도의 저장장치에 복사하거나 양이 적은 경우는 프린터로 출력하여 수집하는 등 디지털 증거의 종류 및 저장상태 등에 따른 신속하고 적절한 대응방안들이 꼼꼼히 마련되어야 한다.

⑶ 증거분석단계 - 디지털 증거의 원본성과 무결성의 확보방안 모색

디지털 증거가 궁극적으로 재판상 증거로서 활용되기 위해서는, 앞서 살펴본 바와 같이 원본성과 무결성을 필수적으로 갖추어야 한다. 이는 증거의 수집과정에서부터 운반 및 분석과정에 이르기까지 가능한 한 디지털 증거 원본의 훼손 및 변형을 방지하여 디지털 증거의 원본을 절대적으로 보존해야 함을 의미한다.[18] 따라서 증거수집 후에도 봉인을 해서 운반하고, 분석할 때에도 원복을 복제하여 복제본을 사용하게 함으로써 되도록 원본사용을 억제할 필요성이 있다.

18) 양근원(2006), p.217.

또한 디지털 증거를 추출할 때에는 다양한 포렌식 도구(암호 복구, 데이터복구, 키워드 검색 및 정보 추출, MAC Time 분석 등)를 사용하여 증거물을 과학적이고 기술적으로 분석하여야 하고, 그 과정과 절차를 반드시 기록하도록 해야 한다.

그리고 이러한 수집 및 분석 등 모든 과정에 대해서는 기록과 문서화를 의무화 함으로써[19] 이를 재판과정에서 디지털 포렌식의 결과물에 대한 신뢰성 및 무결성을 입증할 수 있는 근거자료로 활용할 수 있도록 절차화하는 것이 필요하다.

Ⅳ. 디지털 증거의 수집·분석과 관련한 형사소송법적 쟁점

1. 압수·수색과 관련한 문제점

(1) 압수의 대상성에 관하여

디지털정보 또는 데이터가 물리적 증거의 확보수단인 압수의 대상이 될 수 있는지에 관해서는 형사소송법의 해석과 관련하여 긍정설과 부정설의 견해대립이 존재한다.

압수와 관련하여 우리 형사소송법은 제106조 제1항에서 "법원은 필요한 때에는 증거물 또는 몰수할 것으로 사료하는 물건을 압수할 수 있다"고 규정하고 있고, 여기서의 '증거물'을 '물리적으로 관리가능한 유체물'로 보는 것이 일반적인 해석론이다. 따라서 디지털 정보 내지 데이터가 여기서 말하는 압수할 수 있는 '유체물'로 볼 수 있는지가 문제된다.

먼저 이를 긍정하는 견해로는, ⅰ) 민법상의 물건개념을 유추적용하는 견해,[20] ⅱ) 미연방형사소송규칙 제41조 (h)항의 규정해석과 관련하여 이를 한시적 열거규정으로 보지 않고 예시적 규정으로 해석하여 압수대상물은 유체물에 한정되지 않는다고 판시한 미국법원의 United States v. New York Telephone Co. 판결을 논거로 하여 디지털 정보 및 데이터의 압수를 인정하는 견해,[21] ⅲ) 전자기록 등에 대한 일부 폐기규정

19) 양근원(2006), p.218.
20) 노승권(2000), p.280.
21) 박문수(2003), pp.362~363; 원혜욱(2003), pp.174~175; 이종상(2001), pp.350~351.

을 신설하여 데이터 자체의 몰수근거를 명시한 형법 제48조 제3항을 논거로 제시하는 견해,[22] iv) 현행 형사소송법상의 법규정 흠결을 인정하고, 사이버범죄의 규제라는 형사정책적 측면에서 엄격한 영장주의 하에서 제한적으로 압수를 인정해야 한다고 보는 견해[23] 등이 존재한다.

반면에 이를 부정하는 주장으로는, ⅰ) 유체물의 물리적 성격을 강조하여 현실적인 압수가능성 자체를 부정하는 견해,[24] ii) 무체물에 해당하는 디지털 정보 내지 데이터는 인쇄 등을 통해서 유체물인 기록매체에 수록되어야 증거로서 활용이 가능하기 때문에, 실제로 무체물인 정보 자체만을 압수하는 것은 생각하기 어렵다고 보는 견해[25] 그리고 정보저장매체와 분리된 정보자체만을 압수할 수는 없으며, 컴퓨터 자체나 출력된 정보 또는 복사된 파일만이 압수의 대상물이 될 수 있다고 해석하는 견해[26] 등이 있다.

하지만 현행 형사소송법의 해석론상 무체물인 데이터 내지 정보 자체를 압수의 대상물로 해석하는 것은 불리한 유추해석 내지 확장해석에 해당하여 문제가 발생할 수 있다.[27] 따라서 전자적 정보 내지 디지털 데이터를 포함할 수 있도록 조속히 입법적인 정비를 하는 것이 바람직하다고 판단된다.

⑵ 압수대상 및 수색장소의 특정에 관하여

우리나라 헌법과 형사소송법은, 강제처분인 압수·수색을 할 경우에 영장주의에 따라서 압수 및 수색영장에 의한 집행을 원칙으로 하고 있고(헌법 제12조 제3항, 형사소송법 제113조), 압수·수색영장에는 피고인의 성명, 죄명, 압수할 물건, 수색할 장소, 신체, 물건, 발부년월일, 유효기간과 그 기간을 경과하면 집행에 착수하지 못하여 영장을 반환하여야 한다는 취지 기타 대법원규칙으로 정한 사항을 기재하고 재판장

22) 김기준(2001), pp.169~170.
23) 탁희성(2004), pp.36~37.
24) 오기두(1997), p.73.
25) 이 철(2004), pp.270~271.
26) 안경옥(2004), p.114.
27) 탁희성(2004), p.32.

또는 수명법관이 서명날인하여야 한다고 밝힘으로써, 압수·수색영장의 방식에 관하여 아주 상세하게 규정하고 있다(형사소송법 제114조).

하지만 이러한 압수·수색영장과 절차에 대한 형사소송법의 규정은 원칙적으로 물리적 증거의 수집을 염두에 두고 만들어진 법규정이기 때문에, 동 규정을 이 글의 전반부에 설명한 것처럼 '매체독립성' 및 '취약성' 그리고 '불가시성' 등의 특성으로 인해서 물리적 증거와는 다른 취급이 요구되는 디지털 증거의 수집에도 그대로 적용할 수 있는지가 문제된다. 특히 디지털 증거는 '불가시성 내지 불가독성'의 특성 때문에 외부에서 직접적으로 인지하는 것이 불가능하고, 당해 디지털 정보 내지 데이터가 저장되어 있는 매체를 대상으로 압수나 수색을 해야 하는 현실적인 한계가 존재하는데, 문제는 해당 저장매체(예컨대, 컴퓨터 하드디스크, 서버 등) 안에 들어있는 범죄와 무관한 타인의 개인정보 및 데이터들까지도 사실상 압수·수색의 대상이 됨으로써, 개인의 비밀 및 권리침해가 발생할 위험성이 높다는 점이다.

바로 이러한 압수·수색의 집행과정상의 한계와 문제점 때문에, 압수·수색영장의 적용범위, 즉 '압수할 물건' 및 '수색할 장소'의 특징이 중요한 문제이다.

하지만 집행과정상의 사실상 혹은 현실적인 한계에도 불구하고, 나날이 증가하는 사이버범죄 내지 기타 디지털 증거관련 범죄 등을 억제하기 위해서는 압수·수색과 같은 강제수사가 불가피하기 때문에, 형사정책적인 관점에서 접근할 필요성이 있다고 본다. 따라서 디지털 증거의 특성상 압수 및 수색범위에 대한 특정이 물리적 증거에서만큼 구체화되는 것은 현실적으로 어렵다하더라도 최소한 헌법 및 형사소송법상의 영장주의를 형해화하지 않는 수준까지의 특정은 이루어져야 한다고 생각한다.[28)]

2. 증거법상의 증거능력과 관련한 문제점

(1) 디지털 증거의 증거능력과 증거법상의 2가지 원칙

디지털 증거의 증거능력과 관련해서는 크게 2가지의 접근방법이 존재한다. 먼저

28) 이은모(2005), p.160; 탁희성(2004), p.28.

'비가시성 및 불가독성'의 특성을 갖는 디지털 증거의 경우에는 소위 '포렌식 조사관'에 의해 그 내용을 가시화하는 작업(예컨대 인쇄 등의 작업을 통한 서면화 등)이 필요하게 되는데, 이렇게 해서 생성된 서류 등이 '과연 전문증거배제법칙과 관련하여 증거능력을 획득할 수 있는지'의 관점에서 디지털 증거의 증거능력 문제를 접근하는 견해[29]가 있고, 이와 달리 디지털 증거는 전술한 특성들로 인해서 그 수집 및 분석 그리고 법정제출에 이르기까지 세심한 주의와 엄격한 절차적 통제가 필요한 증거법의 특수한 영역이기 때문에, 헌법 및 형사소송법상의 적정절차 및 영장주의 그리고 2007년 개정 형사소송법을 통해서 명문화된 위법수집증거배제법칙에 따라 증거능력 인정여부를 판단해야 한다고 보는 견해[30]가 존재한다.

⑵ 디지털 증거의 실질적 내용과 증거가치의 고려

위의 2가지 접근방법에서 거론하고 있는 '전문증거 배제법칙'과 '위법수집증거 배제법칙'은 형사증거법상의 대원칙으로써, 디지털 증거의 증거능력 인정여부를 결정할 때 반드시 검토되어야 하는 문제이다. 하지만 전술한 2가지의 접근방법론 중에서 전자와 같이 서면화된 디지털 증거를 무조건 전문증거로 평가하거나, 기계적으로 동 원칙을 적용하는 것은 문제가 있다고 사료된다. 왜냐하면 전문증거 배제법칙은 원칙적으로 진술증거의 증거능력과 관련한 증거법상의 원칙으로서, 문제된 디지털 증거의 내용이 진술과 관련된 경우에는 전문증거로서 동 원칙에 따라 취급할 수 있지만, 디지털 증거가 요증사실에 대한 물리적 증거로서 증거가치를 가지는 경우에는 전문증거 배제법칙은 적용되지 않는다고 보는 것이 타당하다고 생각한다. 따라서 전문증거 배제법칙 및 위법수집증거 배제법칙에 의한 증거법상의 효율적인 제한과 통제를 위해서는, 디지털 증거의 실질적인 내용과 성격 및 증거로서 활용목적 그리고 디지털 증거만의 특성 및 증거수집·분석·활용상의 특수성과 한계 등을 고려하여 유연한 접근과 문제해결방식이 마련되어야 할 것으로 생각한다.

---

29) 하태훈·강동범(1998), p.317; 원혜욱(2000), pp.33~34; 오기두(1997), p.219.
30) 박수희(2007), pp.148~149.

Ⅴ. 결 론

지금까지 살펴본 바와 같이 현대사회에서 디지털문화는 이동통신 및 E-mail 등을 통해서 일상생활영역에까지 깊숙이 뿌리를 내리고 있기 때문에, 인간의 행위 역시 디지털정보 또는 전자적 데이터 등으로부터 자유로울 수 없다. 그리고 이러한 법현실은 인간의 행위를 규범적으로 평가하는 법영역에서도 예외가 아니다.

따라서 인간행위의 법위반 내지 범죄성립여부를 다루는 민·형사소송에서도 디지털정보 및 데이터는 이제 인간행위에 대한 법적 평가를 둘러싸고 벌어지는 다툼과 관련하여 사실관계의 진위여부를 입증해 주는 증거로서 중요한 의미를 가진다.

하지만 디지털 증거(Digital evidence)는 기존의 물리적 증거와 구별되는 특성(매체독립성, 불가시성, 전문성, 대량성, 취약성 등)을 가지고 있기 때문에, 이를 증거로 활용하기 위해서는 증거의 수집과 분석 그리고 법정에 증거로 제출하기까지 철저한 절차적 통제와 세심한 취급을 요한다. 바로 이러한 특별한 취급과 절차적 매뉴얼의 필요성에 따라 등장한 것이 '디지털 포렌식(Digital Forensics)'이라고 할 수 있다. 하지만 아직까지는 '디지털 증거' 또는 '디지털 포렌식'의 개념 및 필요성에 대한 인식과 공감대가 광범위하게 형성되어 있지 않아서 빠르게 변화하는 디지털시대의 사회변화에 적절하게 대응하지 못하고 있고, 이미 본문에서 살펴본 바와 같이 아직까지 우리나라의 소송절차(특히 형사소송절차)는 물리적 증거를 전제로 규정되어 있기 때문에 '디지털 증거'와 이를 위한 '디지털 포렌식'이 하나의 법문화로 정착하기 위해서는 지속적인 연구와 국가적 차원에서의 지원이 필요하다고 사료된다. 따라서 이러한 법문화의 정착과 디지털 증거의 수집·분석 및 재판상 증거로서의 적극적인 활용을 위해서는, 디지털 포렌식 전문조사관의 양성과 포렌식절차에 대한 상세한 절차적 매뉴얼 마련 그리고 민·형사소송법영역에서의 제도적 개선 및 혹은 절차규정의 정비가 무엇보다도 선행되어야 할 것으로 생각한다.

참고자료

강동욱(1996), “컴퓨터관련범죄의 수사에 있어서의 문제점에 대한 고찰”, 현대형사법론(죽헌 박양빈교수화갑기념논문집).

경찰청(2005), 디지털 증거분석, 경찰청, 2005. 7.

김기준(2001), “전자우편에 대한 증거수집과 관련된 문제점”, 해외연수검사연구논문집 제17집(Ⅱ).

노명선(2008), “전자적 증거의 수집과 증거능력에 관한 몇 가지 검토”, 형사법의 신동향 통권 제16호, 2008. 10.

노승권(2000), “컴퓨터 데이터 압수·수색에 관한 문제”, 검찰 통권 제111호.

박문수(2003), “미국의 컴퓨터에 관한 압수·수색절차 연구”, 해외연수검사연구논문집 제18집(Ⅰ).

박수희(2007), “전자증거의 수집과 강제수사”, 한국공안행정학회보 제29호.

_____(2004), 전자증거에 관한 연구, 이화여자대학교 박사학위논문.

안경옥(2003), “정보사회의 새로운 수사기법과 개인의 정보보호”, 비교형사법연구 제5권 제1호.

_____(2004), “전자적 증거의 수집과 증거능력”, 고시계, 2004. 1.

_____(2005), “형사재판절차에서 테크놀로지의 활용과 형사소송법적 문제점”, 21세기 형사사법개혁의 방향과 대국민 법률서비스 개선방안(Ⅴ).

양근원(2006), “디지털 증거의 특징과 증거법상의 문제 고찰”, 한국경찰학회보 제12호.

_____(2006), “디지털 포렌식과 법적 문제 고찰”, 형사정책연구 제17권 제2호, 2006. 여름호.

이은모(2005), “전자적 정보에 관한 수사상의 문제점”, 형사법연구 제23호, 2005. 여름.

이 철(2004), “컴퓨터증거의 수집절차상의 문제점”, 형사정책연구 제15권 제2호, 2004. 여름.

이성진 외(2002), 해킹피해시스템 증거물 확보 및 복원에 관한 연구, 한국정보보호진흥원.

이종상(2001), "컴퓨터 압수·수색에 관한 연구", 해외연수검사연구논문집, 제17집(Ⅰ).

원혜욱(2000), "컴퓨터관련증거의 증거조사와 증거능력", 수사연구, 2000. 6.

_____(2002), "컴퓨터기록의 증거능력", 지송 이재상교수화갑기념논문집.

_____(2003), "과학적 수사방법에 의한 증거수집-전자증거의 압수·수색을 중심으로-", 비교형사법연구 제5권 제2호.

오기두(1997), 형사절차상 컴퓨터관련증거의 수집 및 이용에 관한 연구, 서울대박사논문.

오정돈(2004), "미국의 수사과정에서의 컴퓨터 압수·수색 및 전자증거의 획득에 관한 고찰", 해외연수검사연구논문집 제19집(Ⅰ).

정 완(2004), "컴퓨터관련증거의 증거조사와 증거능력", 수사연구, 2004. 4.

전상덕(2006), "디지털 포렌식의 기술 동향과 전망", 정보화정책 제13권 제4호, 2006. 겨울.

탁희성(2002), 형사절차법상 Digital evidence에 관한 연구, 형사정책연구원.

_____(2004), "전자증거의 압수·수색에 관한 일고찰", 형사정책연구 제15권 제1호, 2004. 봄.

하태훈·강동범(1998), "정보사회에서의 범죄에 대한 수사와 재판", 정보사회에 대비한 일반법연구(Ⅱ).

Howard L. Nations(2007), The Rules of Digital Evidence, SN009 ALI-ABA 501.

U.S. DOJ CCIPS(2009), Searching and Seizing Computes and Obtaining Electronic Evidence in Criminal Investigations.

Orin S. Kerr(2005), "Digital Evidence and The New Criminal Procedure", Columbia Law Review Vol. 105-279, 2005. 1.