情 報 保 護 學 會 誌
第18卷 第3號, 2008. 6

현행 증거법에 적합한 디지털 포렌식 절차

이 광 열*, 최 윤 성**, 최 해 랑**, 김 승 주**, 원 동 호**

요 약

디지털 매체의 증가로 인해 범죄의 상당한 부분이 디지털매체로 이루어지고 있다. 따라서 디지털 증거는 수사, 재판 과정에서 그 중요도가 점차 증가하고 있다. 그러나 형사소송법은 증거의 일반적인 규정만 하고 있을 뿐 디지털 증거에 관해서는 따로 규정하고 있지 않다. 또한 디지털 포렌식 절차에 대한 대부분의 연구는 범죄수사의 시간의 흐름에 따른 연구만 이루어질 뿐, 궁극적으로 법정에서 증거로 사용되기 위해 어떠한 절차를 따라야 하는지에 대한 연구는 이루어지지 않고 있다. 따라서, 현행 증거법에 맞게 디지털 포렌식 절차를 연구할 필요가 있다. 본 논문에서는 현행 증거법의 내용을 분석하고 현행 증거법에 적합한 디지털 포렌식 절차를 소개한다.

Ⅰ. 서 론

현대사회는 정보화 사회로 수많은 디지털 기기가 사용되고 있다. 컴퓨터, 휴대폰, PDP 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 늘어가고 있다.

디지털 포렌식은 디지털 범죄가 발생하였을 때, 증거를 확보하고 분석하여 유죄의 증거로 사용하는 것을 말한다. 그러나 현행 증거법에서는 모든 물건, 문서, 증언을 증거로 사용할 수 있지는 않다. 즉, 형사소송법에서는 '사실인정은 증거에 의하여야 한다'는 증거재판주의를 규정하고 있고, 이는 증거능력(사실인정 할 수 있는 법률상의 자격)있고 적법한 증거조사를 거친 증거에 의해서 사실을 인정할 수 있다는 것으로 해석된다. 따라서 디지털 포렌식에 의해 얻어진 증거도 증거능력이 있어야 하고, 증거조사를 거쳐야 한다. 또한 증거능력이 인정된다하여 바로 사실인정을 하는 것이 아니라 법관이 자유심증으로 사실을 인정할지 결정하게 되는데 이것이 증명력의 문제이다. 증명력의 경우는 증거의 정확성, 신뢰성을 확보하는 것이 중점이 된다.

디지털 포렌식의 궁극적인 목적은 증거로 사용하는 것에 있으므로, 현행 증거법에 관한 연구와 현행 증거법에 맞는 디지털 포렌식 절차의 분석이 필요하다.

따라서 본 논문의 2장에서는 디지털 포렌식의 정의 및 특징, 포렌식 절차 및 법률 연구, 표준화 현황 등의 동향에 대해서 서술한다. 3장에서는 우리나라의 형사소송법에 대해서 살펴보면서 증거법의 증거능력과 증명력이 무엇인지 알아본다. 4장에서는 분석한 내용을 바탕으로 디지털 포렌식 절차를 시간순서가 아니라, 디지털 증거에 대한 증거능력과 증명력 확보를 위한 포렌식의 절차를 알아본다. 즉, 디지털 포렌식 절차를 시간 순으로 고찰하는 방식이 아닌 증거의 신뢰성, 위법수집증거 배제법칙, 전문법칙의 예외, 증명력 확보를 기준으로 하여 디지털 포렌식 절차를 분석하고 제안한다.

Ⅱ. 디지털 포렌식 연구동향

2.1 디지털 증거의 특성

디지털 증거의 특성에 관해 육안으로 식별되지 않는 특성(잠재성)과 0,1의 조합으로 이루어진 특성을 말하는 이진성, 매체의 용량이 커지므로 증거확보에 절대적 시간과 에너지를 소진시키는 방대성, 전원이 끊어지면

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-C1090-0801-0028)
* 성균관대학교 정보통신공학부 (lky9419@naver.com)
** 성균관대학교 정보통신공학부 정보보호연구소 (yschoi, hlchoi, skim, dhwon)@security.re.kr

데이터가 날아가는 휘발성이 있다. 또한 디지털 증거는 불가시성, 변조나 위조가 쉽고 찾아내기 어려운 취약성, 디지털, 대량성, 국경초월성의 특징이 있다. 이와 같이 디지털 증거는 오직 하나만 존재할 수 있는 일반적인 증거물과 구별되는 특징적인 차이점을 가지고 있다[1].

2.2 디지털 포렌식 연구 동향

디지털 포렌식이란 컴퓨터, 핸드폰 등의 디지털기기를 이용한 범죄에 있어 디지털화된 증거를 확보하고 이를 보존, 분석하는 기술로 다양하게 연구되고 있다.

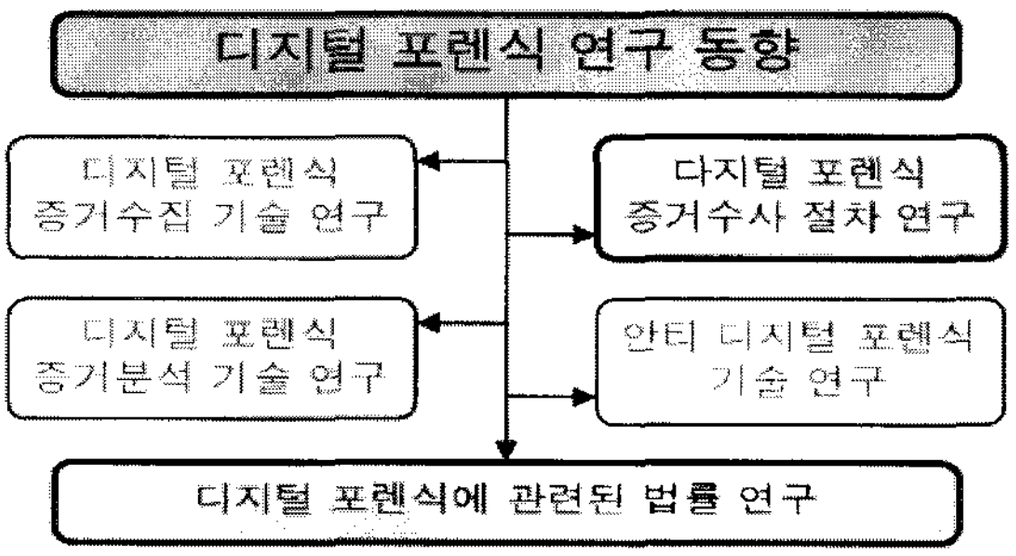
디지털 포렌식 수사절차에 대한 연구는 디지털 증거처리 및 분석과정의 표준화된 절차를 분석하거나, 디지털 증거의 무결성 확보를 위한 수사현장의 연계관리 방법 연구하며, 디지털 증거수사의 효율적 방안 및 절차 모델을 연구하고 있다.

디지털 포렌식 증거 수집 기술에 대한 연구는 삭제된 디지털 증거의 효율적인 복구 방식을 분석하거나, 물리적 복구 방법을 분석하여 포렌식에 활용하는 방안을 연구하며, 모바일 기기나 활성화된 기기에서 무결성을 보장하며 증거를 수집하는 방식을 연구하고 있다.

디지털 포렌식 증거 분석 기술에 대한 연구는 메모리 정보 분석 및 HTML 파일의 분석 방식을 연구하거나, 네트워크상의 증거를 분석하는 방식과 휴대폰 기기 내의 정보를 분석하여 증거로 사용하는 방안, 디지털화 된 회계증거를 분석하는 방식을 연구하고 있다.

안티 디지털 포렌식 기술에 대한 연구는 일반적인 안티 포렌식 기술을 분석하고 그에 대한 대응 방향을 연구하거나, PE 파일형식에서 정보은닉 등을 통해 증거수집을 방해하는 방안을 연구하고, 안티 포렌식 기법을 이용해서 개인의 프라이버시를 보호하는 방안을 연구하고 있다.

그리고 디지털 포렌식에 관한 법률 연구는 국내외 디지털 포렌식 법제 현황을 조사하거나 법정에서 디지털 증거가 범죄의 증거로써 사용되기 위해 필요한 요건을 연구하고 있다.



〔그림 1〕 디지털 포렌식 연구동향

2.3 디지털 포렌식 증거수사 절차 연구 분석

디지털 포렌식 절차는 전문 인력과 포렌식 도구의 활용방안 수립과 보관의 연속성 방안을 수립하고 데이터 무결성 유지방안 수립하는 증거 수집 전 단계, 휘발성 증거를 수집하고 전원차단여부를 결정하며 증거를 수집하는 증거 수집 단계, 데이터 복구 및 증거 분석과 결과 보고서를 작성하는 증거분석 단계의 세 단계로 나눌 수 있다[2]. 그리고 디지털 포렌식 절차는 증거물 획득, 증거물 분석, 증거물 보관, 보고서 작성으로 나누어 연구하기도 한다[3]. 또한 디지털 포렌식 절차는 증거의 순서를 기준으로 하여 증거확보, 증거입증, 증거분석, 증거제출로 나눌 수 있으며[4], 디지털 수사의 전반적인 절차를 기준으로 하여 수사준비, 증거물획득, 증거물의 인증, 증거물의 보관 및 이송, 증거물의 분석, 보고서 작성으로 나눌 수 있다[1].

이렇게 현재까지 디지털 포렌식 절차에 관한 연구는 수사 단계에서 시간의 흐름에 따른 절차를 분석하고 단계를 세분화하는 방식으로 진행되고 있다. 하지만 범죄 수사의 단계 별 수사방식 및 절차에 대한 연구가 대부분이어서 각 절차의 법적 효력을 알기 어려우므로, 디지털 증거가 법적으로 인정받기 위해서는 어떠한 절차를 따라야 하는지에 대한 연구가 필요하다.

2.4 디지털 포렌식과 관련된 법률 연구 분석

디지털 포렌식에 관한 법률의 연구에는 국내외 디지털 포렌식 법제 현황을 조사하여 비교하는 분야가 있다. 국가 디지털 포렌식 법률 체계를 제시하고 각각의 구성요소들에 대해 살펴본 후 이를 기반으로 하여 미국의 법제 현황과 국내 법제 현황을 비교하며, 디지털 포렌식 수행 절차에 대한 법적 요구사항들을 정의하고 포렌식 기술 활성화 방안을 제시하고 있다[5].

하지만 형사소송법상의 디지털 증거에 대한 언급이 부족하여, 실제 법정에서 디지털 증거가 사용되기 위한 방법에 대해 연구가 필요하다.

디지털 포렌식과 관련된 법률 연구 중에는 디지털 증거의 법적효력에 대해서 연구하는 분야가 있다. 법정에

서의 디지털 증거가 법적 효력을 가지기 위해서 증거에 대한 전문법칙을 분석하여 디지털 증거를 허용하기 위한 일정 예외요건 및 별도의 디지털 증거의 증거능력 허용요건을 연구하고 있다[6]. 이외에도 특정판례를 분석하여 디지털 증거의 증거능력과 관련된 무결성, 신뢰성에 대한 문제를 분석하고 디지털 증거의 확보 및 분석, 법정제출 과정에서 요구되는 기준을 제시한다[7]. 또한 디지털 증거의 특성을 연구하여 디지털 증거가 법정에서 증거로 인정받기 위한 조건을 기술하고, 디지털 증거 획득의 표준 절차 및 디지털 포렌식 시스템의 요구사항을 연구하고 있다[8].

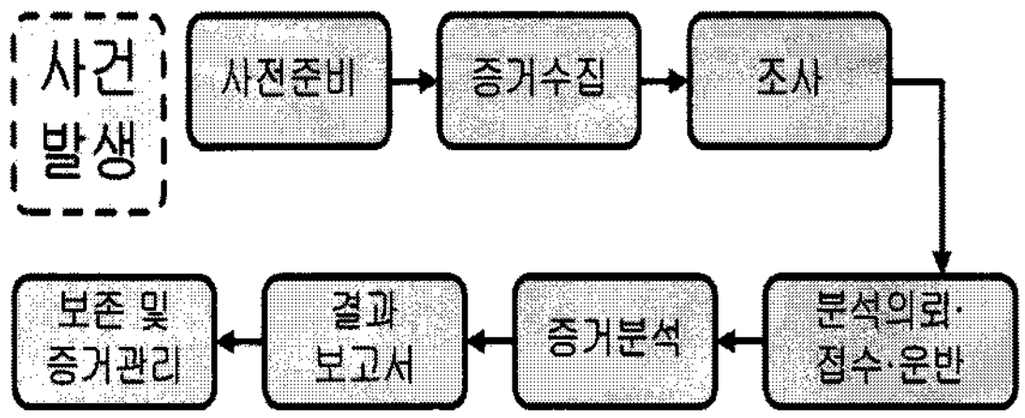
하지만 지금까지의 연구는 증거능력에 관한 내용 중 전문법칙에 대해서만 언급하거나 특정판례 상의 내용을 바탕으로 하여 디지털 증거의 증거능력을 보여주기 때문에, 법률상에서 디지털 증거가 증거로 인정받기 위해 필요한 전체적인 요구사항에 대한 연구가 필요하다. 그리고 법률상의 디지털 증거에 대한 언급 없이 디지털 증거처리 표준절차 및 디지털 포렌식 시스템의 요구사항을 기술하고 있으므로, 제시한 사항의 실제적 법적 효용성에 대한 연구가 필요하다.

2.5 디지털 포렌식 표준화 동향

경찰청은 대한상공회의소에서 개최한 '국제 사이버테러대응 공동 심포지엄'에서 디지털 증거처리 가이드라인과 증거분석 표준절차에 대해 공개발표를 하였다. 이 가이드라인은 경찰청과 한국디지털포렌식학회가 공동으로 연구해온 것으로, 디지털 증거의 수집 및 운반, 분석, 보고서 작성, 증거물 관리 절차와 방법을 상세하게 규정하여 수사기관들이 디지털 증거를 이용해 사실관계를 입증하고 결과의 신뢰성 여부를 판단하는데 중요한 지침이 되도록 하고 있다[9].

[그림 2]에서는 디지털증거처리 표준가이드라인에서 제시한 7단계 절차를 보여주고 있으며, 그 절차는 사전준비, 증거수집, 조사, 분석의뢰 · 접수 · 운반, 증거분석, 결과보고서, 보존 및 증거관리로 나누어진다.

디지털증거처리 표준가이드라인에서는 사전준비 프로세스의 기본원칙으로 적법절차 준수, 원본의 안전한 보존, 증거의 무결성 확보에 대해 명시하고 있다, 그리고 증거수집 프로세스에서는 증거수집 절차에 관해 기술하며 사진촬영이나 증거현장을 스케치하고, 휘발성증거인 경우에는 현장에서 수집하고 휘발성증거가 아니라면 전원을 내린 후에 수집대상이 무엇인지(하드디스크인지, 주변장치인지 등) 파악한 후 증거물을 포장하고 목록장성 후 입회인의 서명, 사용자 질의서 작성 할 것 등을 기술한다. 또한, 증거분석 단계에서는 4대 기본원칙을 정의하고 있는데, 증거원본의 안전한 보존 및 무결성 확보, 증거기법과 도구의 신뢰성확보 방안, 증거분석 과정의 기록 방법, 증거분석의 신뢰성확보에 대해 정의하고 있다. 그리고 증거분석단계에서는 디지털 증거의 유형을 디스크 포렌식, 네트워크포렌식, 웹 포렌식, 전자우편 및 메신저 포렌식, 해킹 및 악성코드 포렌식, 암호포렌식 등으로 분류하고 있다. 증거물의 분석의뢰 · 접수 · 운반 증거분석 프로세스는 수시기관 및 포렌식 전문기관 사이의 이송 시 무결성을 준수하기 위한 것으로 수사관과 전문 증거분석관과의 역할 정의를 하고 있다. 마지막으로 결과보고서 단계서는 결과보고서 작성에 관한 원칙을 서술하고 있다[10].



〔그림 2〕 디지털증거처리 표준가이드라인의 7단계 절차

2.6 디지털 포렌식 연구 분석

현재 디지털 포렌식에 대한 연구는 앞에서 살펴본 것과 같이 디지털 포렌식의 의의 및 종류를 정의하거나 디지털 증거의 특성을 파악하는 방식으로 이루어지고 있다. 그리고 디지털 증거에 적합한 수사절차를 제시하거나 이를 바탕으로 디지털 증거에 대한 처리방식을 표준화하는 연구가 이루어지고 있다.

하지만 이러한 연구에서는 국내 증거법에 따라 궁극적으로 증거로 사용되기 위해서 어떠한 절차를 따라야 하는지에 대해서는 명시되고 있지 않다. 즉, 시간의 흐름에 따른 분석방식에 대한 연구는 이루어지고 있으나 어떠한 단계에서 증거능력과 증명력 등이 문제되는 지는 기술되어있지 않다. 따라서 디지털 포렌식 절차에서 증거의 증거능력과 증명력을 인정받을 수 있는 방안에 대해서 연구할 필요가 있다.

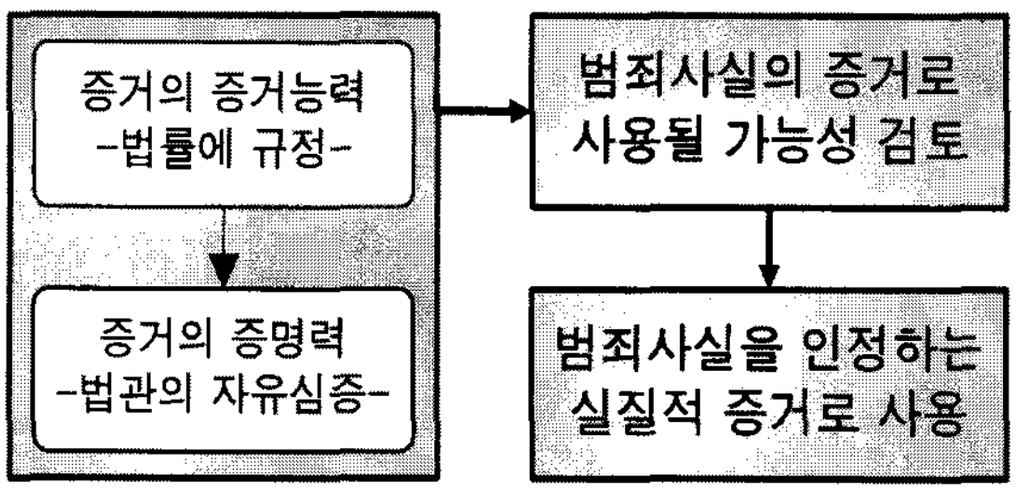
Ⅲ. 형사소송법상의 증거

3.1 국내 소송절차에서의 증거

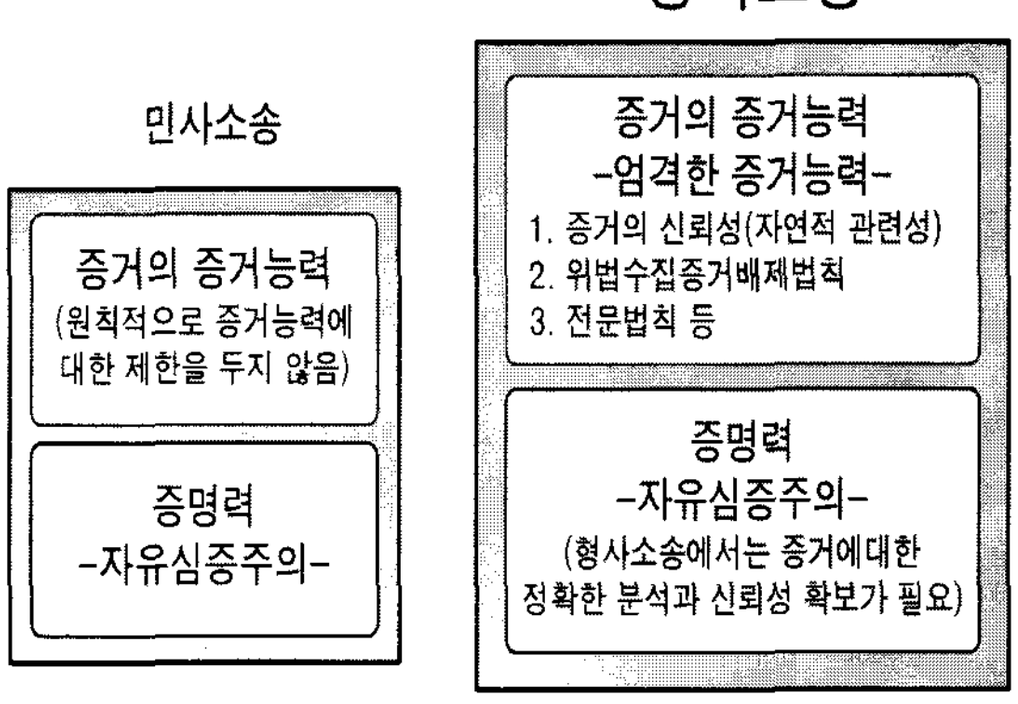
증거란 사실인정의 근거가 되는 자료를 말하는데, 증거로 사실인정을 하기 위해서는 증거가 될 수 있음을 뜻하는 증거능력과, 증거의 실질적 가치를 의미하는 증명력이 있어야 한다. 증거능력은 미리 법률에 규정되어 있지만 증명력은 법관의 자유심증에 맡겨져 있다. 아무리 증거가 가치 있는 것이라도 증거능력이 없으면 사실인정을 할 수 없고, 공판정에 제출하여 증거조사를 할 수도 없다. 즉, 증거능력이 있어야 비로소 증거의 가치를 판단하게 되므로 증거능력의 판단이 증명력 판단 이전의 문제라고 할 수 있다.

증명력은 증거능력이 있음을 전제로 하여 범죄사실을 인정함에 있어서의 실질적 가치를 의미한다. 즉, 증거가 증거능력이 있다하여도 그 증거로 범죄사실을 인정할 것인가는 법관의 자유판단, 즉 자유심증에 달린 것이다. 예를 들어 한 가지 범행사실에 여러 가지의 증거가 있고, 모두 증거능력이 있을 때 그 모두가 범죄사실에 대한 증거로 사용될 수도 있지만, 반대로 증거 모두가 배척되어 범죄사실에 대한 증거로써 사용되지 않을 수 도 있는 것이다. [그림 3]에서는 증거가 범죄사실을 인정하는 실절적인 증거로 사용되는 절차를 보여주고 있다.

사실에는 범죄사실(처벌대상이 되는 범죄행위)이 있고, 그 밖의 사실(예를 들어, 정황사실로 양형참작사유로 피고인이 정신질환이 있다든지, 경제적 사정이 있다는 등)이 있다. 범죄사실에 대한 인정 시에만 증거능력 있는 증거가 필요하고, 그 외의 사실(정황사실)은 증거능력 없는 증거도 무관하다. 이것은 피고인에게 유리하게 해석하여 피고인에게 불리한 범죄사실인 경우에 증거능력과 증거조사를 요구하고, 유리한 정상참작사실은 증거능력이 없더라도 사실을 인정할 수 있게 한 취지이다.



〔그림 3〕 증거가 범죄사실의 인정증거로 사용되는 절차



〔그림 4〕 민사/형사 소송에서의 증거능력과 증명력

국내의 재판절차는 크게 형사소송절차와 민사소송절차로 나눌 수 있다.

민사소송법은 자유심증주의를 택하고 있으므로 원칙적으로 증거능력에 대한 제한은 없다. 판례는 민사절차에서 증거수집과정에서 위법하게 녹음한 테이프의 증거능력에 관해서도 증거능력이 없다고 할 수 없다고 판결하였다[11].

형사소송절차에서는 피고인의 인권 문제와 오판을 방지하기 위해 엄격한 증거능력을 요구하는데, 증거의 신뢰성(자연적 관련성), 위법수집증거배제법칙과, 전문법칙이 대표적이다. 증명력의 경우는 법관의 자유심증에 의하는 것이나, 이때에도 증거에 대한 정확한 분석과 신뢰성 확보되어야 할 것이다.

그러므로 본 논문에서는 형사소송에서의 증거능력과 증명력에 대해서 살펴본다.

3.2 증거의 신뢰성(자연적 관련성)

증거가 증명하려는 사실에 대하여 필요한 최소한의 증명력을 가져야 하는 것을 자연적 관련성이라 한다. 즉, 최소한의 가치가 있어야 한다는 것으로 당해 사건과 관련 없는 증거, 최소한의 신뢰성조차 없는 증거는 증거능력을 인정할 수 없다는 것이다. 사실인정에 최소한의 관련성도 없는 증거를 조사하는 것은 시간 낭비이고 신뢰할 수도 없으므로 증거조사 할 필요도 없이 배척하여야 한다. 거짓말 탐지기의 검사결과가 그 예이다. 즉 기계와 기술에 대한 일반적 신뢰성과 검사자에 대한 개별적 신뢰성이 인정될 수 없어 증거로 인정할 수 없다[11].

따라서 디지털 포렌식 절차에 의한 증거도 자연적 관련성, 즉 최소한의 신뢰성은 갖추어야 한다.

3.3 위법수집증거배제법칙

위법한 절차에 의해 수집한 증거는 증거능력을 부정하는 법칙을 말한다. 종래 대법원은 압수절차가 위법하더라도 물건 자체의 성질 형상에는 변경을 가져오는 것이 아니므로 증거가치에 변함이 없다고 판단하고 해당 증거의 증거능력이 있다고 판시하였다[12].

그러나 많은 비판을 받고 있었고, 이에 따라 2008년 1월 1일부로 시행되는 개정 형사소송법에서는 위법수집증거배제법칙을 명문으로 규정하였다. 즉, 형사소송법 제308조의2에서 위법수집증거의 배제라는 제목으로 적법한 절차에 따르지 아니하고 수집한 증거는 증거로 할 수 없다고 규정하였다.

따라서 디지털 포렌식 절차에서 증거획득이 위법한 절차에 의해 수집된다면 형사소송법 제308조의2에 의해 증거능력이 인정되지 않을 것이므로, 적법한 절차에 의한 수집이 요구된다.

3.4 전문법칙의 예외

사실인정의 기초가 되는 경험적 사실을 체험자가 법원에 직접 진술하지 않고 다른 형태로 간접적으로 보고하는 것을 전문증거라 하고, 전문증거는 증거능력이 없다는 원칙을 전문법칙이라 한다[12]. 예를 들어, 범행을 목격한 목격자가 법원에 직접 나와 목격한 사실을 증언한다면 그것은 전문증거가 아닌 직접증거이지만, 검사나 사법경찰관이 목격자를 참고인으로 소환하여 참고인진술조서를 작성하고 그 조서를 법원에 제출한다면 전문 증거가 되는 것이다. 이 경우 전문증거인 참고인진술조서는 법원에 목격자가 직접 나왔다면 피고인은 반대신문을 행사하여 자신의 방어를 할 수 있지만 조서만 제출된다면 목격자에게 반대신문을 할 수 없고, 조서의 신용성도 결여되기 때문에 원칙적으로 증거능력을 인정할 수 없다는 것이 전문법칙이다.

그러나 전문법칙을 지나치게 엄격하게 적용할 때에는 재판의 지연을 초래하고, 실체진실발견에 저해를 가져올 수 있기에 형사소송법에서는 엄격한 요건(형사소송법 제312조의 2 이하)을 명시하여 예외적으로 증거능력을 인정하고 있다[12].

앞에서 살펴본 참고인진술조서의 경우에서 피고인이 증거로 함에 동의하거나, 적법한 절차와 방식에 따라 작성된 것으로서, 그 조서가 검사 또는 사법경찰관 앞에서 진술한 내용과 동일하게 기재되었음이 원진술자의 공판준비 또는 공판기일에서의 진술이나 영상녹화물 또는 그 밖의 객관적 방법에 의하여 증명되고, 피고인 또는 변호인이 공판준비 또는 공판기일에 그 기재 내용에 관하여 원진술자를 신문할 수 있었던 때에는 증거로 할 수 있는 것이다. 다시 말해서, 참고인진술조서가 성립하기 위해서는 적법한 절차와 방식으로 작성되어야 하며, 원진술자 진술 또는 영상녹화물 등 객관적 방법으로 성립을 인정하며, 반대신문권을 행사하여야 한다는 것이다.

디지털 증거는 기존에 형사소송법에서 예상했던 증거가 아니다. 즉 형사소송법에서는 문서, 진술, 압수물 등에 대한 증거능력과 증거조사 방법을 규정하고 있다. 그중에서 진술과 진술을 기재한 문서만이 전문법칙의 적용을 받는다. 판례는 컴퓨터 디스켓에 들어있는 문건이 증거로 사용되는 경우 그 디스켓은 매체만 다를 뿐, 실질에 있어서는 진술을 기재한 서류와 크게 다를 바 없고, 압수 후의 보관 및 출력과정에서 조작 가능성이 있으며, 기본적으로 반대신문의 기회가 보장되지 않는 점 등에 비추어 기재내용의 진실성에 관하여는 전문법칙이 적용되어 형사소송법 제313조 제1항에 의해 작성자 또는 진술자의 진술에 의해 성립의 진정이 인정되어야 증거로 사용할 수 있다고 하였다[13]. 판례에 의하면 디지털 증거 역시 전문법칙의 적용을 받으므로, 포렌식 절차에 의해 수집, 분석된 증거가 진술 등을 내용으로 하는 것이라면 전문법칙의 적용을 받을 것이다.

3.5 증명력

증명력이란 증거의 실질적 가치를 의미한다. 형사소송법은 증거의 증명력 판단은 법관의 자유판단에 따른다고 규정하는 자유심증주의를 채택하고 있다. 이는 법정증거주의와는 대립되는 개념으로 증거능력은 형식적으로 법으로 정의되어있지만, 증거력은 법관의 자유로운 판단에 맡기는 것이다.

증명력에는 신용력과 협의의 증명력이 포함되는데 신용력이란 증거 그 자체가 진실일 것을 의미하고 협의의 증명력은 증거의 진정성을 전제로 그 요증사실을 추인하는 힘을 말한다[12]. 증명력은 자유심증에 의하므로 디지털 포렌식 절차와는 엄격히는 관련이 없다. 그러나 증거의 진정성을 확보하는데 있어서는 디지털 포렌식 절차 중 증거의 정확한 분석과, 원본데이터 훼손 방지 등이 논의될 수 있다.

3.6 디지털 포렌식에서의 증거의 범죄사실 인정

앞에서 살펴본 것과 같이, 증거로 법죄사실을 인정하기 위해서는 증거가 될 수 있는 자격으로서 증거능력과 사실에 대한 가치의 의미로서 증명력이 있어야 한다.

증거능력에 관해서 첫째, 증거가 최소한의 신뢰성(자연적관련성)이 있어야 한다. 이 과정에서는 디지털 포렌식 툴이 최소한의 신뢰성이 있어야 한다. 둘째, 수사절차에서 위법이 행해지면 증거능력을 가질 수 없으므로 위법절차에 의해 수집되면 안 된다. 즉, 영장주의와 적법절차에 의한 수집이어야 한다. 셋째, 전문법칙이 적용되는데 이 과정에서는 디지털 포렌식에서 사용되는 툴과 기술과는 무관하게 형사소송법상의 예외에 해당하여야 한다.

증명력에 관해서는 증거능력이 인정되었을 때 법관의 심증 형성 시에 증거의 진정성 확보와 정확한 분석으로 범죄사실 인정에 보다 높은 가치를 가지게 하는 것이 디지털 포렌식 절차에서 필요하다.

Ⅳ. 현행 증거법에 따른 디지털 포렌식 절차 제안

[표 1]에서는 앞에서 살펴본 디지털 증거처리 표준 7단계 절차에 따라서 각 단계의 증거의 신뢰성, 위법증거배제법칙, 전문법칙의 예외, 증명력에 대해 정리하였다.

4.1 증거의 신뢰성의 확보

증거의 신뢰성은 포렌식 절차 중 증거분석 단계와 관련된다. 앞에서 살펴 본 것과 같이 증거는 최소한의 증명력을 가져야 하는 자연적 관련성을 필요로 한다. 디지털 포렌식 절차의 경우에는 포렌식 도구를 사용하여 획득한 증거의 최소한의 신뢰성을 인정할 수 있는가가 문제가 된다. 현대 사회에서 디지털 증거는 그 중요성, 컴퓨터 등 정보기기의 광범위한 사용, 정보기술의 발전 등으로 어느 정도의 신뢰성을 가지고 있다.

그러므로 최소한의 신뢰성을 위해서는 첫째, 포렌식 도구가 일반적으로 사용되는 검증된 도구 이어야 하며, 둘째, 전문가에 의해 포렌식 절차가 행하여져야 한다. 서울고등법원이 소위 일심회판결에서 증거능력을 배척한 이유 중 한 가지는 전문가가 별로 없는 점을 감안 할 때 그 자체로 신뢰성이 없다는 것이었다[14]. 따라서 Encase와 같이 일반적으로 사용되는 도구를 사용하여 전문가가 증거분석을 한다면 증거의 신뢰성을 인정할 수 있을 것이다.

그러므로 증거의 신뢰성을 확보하기 위해서는 사전준비 단계에서 검증된 포렌식 도구를 준비하고 전문증거수집팀을 구성하면서 증거수집 절차 및 계획을 수립해야한다. 그리고 증거수집 단계에서 정의된 포렌식 절차에 따라 휘발성 증거를 우선 수집하고, 비휘발성 증거는 전원은 끊은 후에 증거수집을 해야 한다. 그리고 증거품을 포장하고 상세정보를 기재하며 증거물의 목록을 작성하며 입회인의 서명을 받아야 한다. 또한 증거물 이송단계에서 수사관이 수행한 조치사항에 대해 기술해야하며, 증거분석 단계에서는 검증된 디지털 포렌식 소프트웨어를 이용하여 전문가가 증거를 분석해야하고 분석과정을 기록해야한다. 마지막으로 증거물의 입출력 내역을 관리해야하며, 증거수집 과정의 기록을 보관해야 한다.

4.2 위법수집증거배제법칙의 준수

형사절차에서 확보된 증거는 어떠한 경우라도 위법하게 수집 되어서는 증거로 사용될 수 없다. 이 점은 디지털 포렌식 절차에 의해 획득된 증거의 경우도 마찬가지이다. 따라서 디지털 포렌식 절차 역시 적법절차, 영장주의 등이 적용된다. 위법수집증거배제법칙의 준수와 관련된 과정은 앞에서 살펴 본 절차 중에서 증거수집 전 준비 단계와 증거 수집단계가 해당된다.

증거수집 전 단계에서는 중대 범죄가 아님에도 수사기관이 증거수집을 위해 피의자, 피고인에게 기망을 한다든지 위법한 함정수사를 하게 되면 위법하게 수집된 증거로 증거 능력이 부정 될 수 있다. 따라서 증거 수집 전 준비 단계에서는 이러한 위법 절차 없이 디지털 포렌식 절차를 진행하기 위해 포렌식 도구를 준비하고 점검하는 것이 요구된다. 수사관은 수사 이전에 포렌식 도구가 신뢰성이 있는지를 점검 하여야 한다. 국내에서는 경찰청, 국가사이버안전센터, 인터넷 침해사고 대응센터 등에서 Encase 도구를 사용하고 있다.

증거 수집단계에서는 디지털 기기의 확보가 임의제출물이 아닌 압수, 수색 등의 강제처분인 경우에 영장주의가 적용된다. 따라서 영장주의의 예외가 적용되지 않는 한 검사의 청구에 의해 판사가 발부한 영장이 있어야 한다. 이를 위반하고 압수 수색하여 획득한 경우 법정 제출 시 증거능력과 관련해 위법수집증거로서 증거

〔표 1〕 디지털 포렌식의 각 절차와 관련된 증거법칙 정리

	프로세스 모델		단계별 절차 및 주의사항	관련 증거법칙
증거수집	사전준비		검증된 포렌식 도구 준비	1.증거의 신뢰성 2.위법수집증거배제법칙 3.전문법칙의 예외
			전문지식을 가진 증거수집팀 구성	1.증거의 신뢰성 2.위법수집증거배제법칙 3.전문법칙의 예외
			적법한 증거수집 절차 및 계획 수립	1.증거의 신뢰성 2.위법수집증거배제법칙
	증거수집		휘발성 증거 우선 수집	1.증거의 신뢰성 2.위법수집증거배제법칙
			비휘발성 증거는 전원 OFF 후 증거 수집	1.증거의 신뢰성 2.위법수집증거배제법칙
			증거품 포장, 상세정보 기재	1.증거의 신뢰성 2.위법수집증거배제법칙
			증거물 목록작성, 입회인 서명	1.증거의 신뢰성 2.위법수집증거배제법칙
			디스크 이미징을 이용한 사본 생성	2.위법수집증거배제법칙 3.전문법칙의 예외
			쓰기방지 기술을 적용한 사본 생성	2.위법수집증거배제법칙 3.전문법칙의 예외
			원본과 사본의 해쉬값 생성	2.위법수집증거배제법칙 3.전문법칙의 예외
증거 분석의뢰	분석의뢰・접수・운반		증거물 이송 시 봉인하여 내용물의 변경 방지	4.증명력
			이송과정에서 수사관이 행한 조치내용을 기술	1.증거의 신뢰성 4.증명력
			전자파나 물리적 충격을 막아주는 보관도구 사용	4.증명력
증거분석	조사		사본을 이용한 분석	3.전문법칙의 예외 4.증명력
			해쉬값을 이용한 사본과 원본의 동일성 여부	3.전문법칙의 예외 4.증명력
			증거분석 과정의 기록	1.증거의 신뢰성 4.증명력
			제3의 분석관이 증거를 분석하더라도 동일한 분석결과가 도출되는지 확인	3.전문법칙의 예외 4.증명력
	증거분석		다른 증거분석 소프트웨어나 장비를 사용해도 동일한 분석결과가 도출되는지 확인	3.전문법칙의 예외 4.증명력
			증거분석 의뢰서 작성을 통한 수사관과 전문 증거분석과의 명확한 역할 정의	4.증명력
			전문가에 의한 분석	1.증거의 신뢰성 3.전문법칙의 예외 4.증명력
			검증된 디지털 소프트웨어를 이용한 분석	1.증거의 신뢰성 3.전문법칙의 예외 4.증명력
결과 보고서 작성	결과보고서 작성		증거분석의 공정한 결과만을 수록	4.증명력
			증거분석에 사용된 프로그램의 기록	4.증명력
			분석결과를 이해하기 쉬운 형태도 작성	4.증명력
			데이터 유실 및 변경 사항도 정확히 기재	4.증명력
	보존 및 증거관리		증거물의 입출력 내역 관리	1.증거의 신뢰성 4.증명력
			증거분석 과정의 기록	1.증거의 신뢰성 4.증명력
			증거보관실과 증거물에 대한 접근통제	4.증명력
			증거물 데이터베이스 구축 및 관리 운영	4.증명력

능력이 인정되지 않을 것이다. 또한 적법절차 원칙도 준수 되어야 하는데 영장이 있다 하여도 사생활 침해가 심하다든지, 집행과정에 당사자의 참여를 배제한다든가, 긴급을 요하지 않음에도 집행의 일시와 장소를 알리지 않는 경우에는 마찬가지로 위법수집증거로서 증거능력이 배제 될 수 있다. 가능하면 증거를 획득하는 과정과 획득 자료를 기재한 서류에 당사자의 서명 날인을 받는 것이 당사자가 참여하였다는 점에 대한 신뢰 확보에 도움을 줄 수 있다. 또한, 암호화된 데이터의 경우 피의자, 피고인에게 진술거부권을 고지하지 않은 채 강압에 의해 임의성 없는 진술로 암호를 획득한다면 이로 인해 출력한 문서는 증거능력을 인정할 수 없다.

그래서 증거수집 단계에서는 검증된 포렌식 툴을 준비해야하며, 전문지식을 가진 증거수집팀을 구성하고 적법한 증거수집 절차 및 계획을 수립해야한다. 그리고 절차와 계획에 따라서 증거를 수집해야한다.

4.3 전문법칙의 예외사항 준수

전문법칙과 관련해서는 디지털 증거가 진술, 진술을 기재한 서류가 아님에도 전문법칙을 적용할 것인가가 문제이다. 앞에서 살펴본 것과 같이 대법원의 경우에는 디지털 증거의 조작가능성, 반대신문권의 결여 등을 이유로 하여 전문법칙을 적용하고 있다.

최근 하급심판결(소위 일심회 판결)에서 디지털 증거의 증거능력에 관하여 판시하고 그 요건을 설시하였는데 그 내용을 요약하면 다음과 같다. “컴퓨터 기록은 그 자체로 가시성과 가독성이 없으므로 법원에서의 검증절차를 통해 컴퓨터 기록내용과 출력 문건 기재 내용이 동일하다는 것이 입증 되어야 한다. 컴퓨터 기록의 증거능력이 인정되기 위해서는 컴퓨터 기록이 입력된 후 법원의 검증 절차에 이르기 까지 변경되지 않았음이 인정되어야 하고 이를 위해 보관상황의 신뢰성이 담보 되어야 할 것이며 원본과 ‘하드카피’ 또는 ‘이미징’ 한 매체 사이에 데이터의 동일성이 증명되어야 한다. 이 사건에서 각 원본 디지털 저장매체는 압수수색영장을 통해 압수되고 그 자리에서 봉인되었고 피고인은 압수물의 이미징 작업을 하기 위해 봉인을 해제하는 과정과 작업 후 봉인하는 과정에 참여하였고 수사기관은 피고들로부터 확인서를 받았고 이미징 작업을 하는 경우를 제외하고 계속 봉인 되어 신뢰성이 인정된다. 또한 데이터의 동일성과 관련 일반적으로 이용되는 해시 값 이 동일하므로 동일성이 인정되고 법원의 검증절차에 피고인, 검사, 변호인들이 모두 참여한 가운데 전자 법정시설 및 인케이스를 이용하여 적절한 방법으로 행하여져 증거능력이 부여되었다” 판시하여 엄격한 요건 하에 증거능력을 인정하였다[15].

그러나 이 판결은 항소심 법원에서 다음과 같은 이유로 파기 되었다. 국가정보원과 검찰의 증거 분석과정에 대한 신뢰성을 인정할 수 없고, 피고인들에게 진술거부권을 고지하지 않은 상태에서 강압에 의해 디지털 매체의 암호를 획득하였으며 출력된 문건의 경우 전문 증거의 경우에는 형사소송법 제313조 제1항에 따라 성립의 진정이 증명 되어야 하는 데 그렇지 않다는 것이다[16]. 즉 첫째이유는 원본매체의 변경가능성이 있으므로 신뢰할 수 없고 둘째이유는 위법하게 수집된 증거이고 셋째 이유는 전문법칙의 적용으로 예외 요건을 갖추어야 한다는 것이다.

디지털 증거는 그 동안 형사소송법이 예견하지 않았던 증거이므로 규정이 없다. 그래서 전문법칙이 적용되어야 하는가에 논란이 되는 것이다. 즉 진술, 진술을 기재한 서류와 같이 볼 것 인가의 문제이다. 디지털 증거의 경우에는 쉽게 조작이 가능함으로 전문법칙을 적용하는 것이 타당하다. 즉, 디지털 포렌식에서 분석의 대상이 되는 하드디스크, 메일, 네트워크 역시 체험자의 직접진술이 아닌 다른 형태의 간접 보고이므로 전문법칙의 예외에 해당하여야 증거능력을 인정받을 수 있다. 또한 전문법칙의 존재이유가 전문증거의 경우 신용성의 보장이 없고 피고인의 반대신문권이 보장되지 않을 때 디지털 증거의 경우 위조 변조의 가능성으로 신용성이 결여되고 피고인이 반대신문권을 행사할 수 없으므로 전문증거로서 전문 법칙을 적용하는 것이 타당하다. 그러나 다른 한편으로는 현대사회는 디지털 기기가 광범위하게 사용되고 있으므로 너무 엄격하게 적용하는 것은 형사소송의 다른 이념인 신속한 재판의 이념과 충돌될 수 있다.

따라서 전문법칙을 적용하되 예외 요건을 어느 정도 완화하여 규정하거나, 해석하는 것이 바람직할 것이다. 즉 입법론으로 형사소송법의 증거편에 디지털 증거를 규정하여 어느 요건 하에 증거능력을 인정할 것인가 규정하는 것이 바람직하고, 그렇지 않을 경우 완화 해석을 해야 한다는 것이다. 예를 들어 진술서의 경우 형사소송법 제 313조 제1항에 의해 진술자의 진술에 의해 성립의 진정함이 증명되어야 하나, 디지털 증거의 경우에는

진술자의 의미를 원진술자가 아닌 포렌식 전문가의 성립의 진정의 인정으로 증거능력을 인정 할 수 있다는 것으로 해석하는 것도 고려할 수 있다.

그러므로 디지털 증거분석의 전문가가 검증된 포렌식을 이용해서 증거를 분석해야하며, 사본을 이용한 분석하거나 해쉬값을 이용한 비교 등을 이용해서 증거의 동일성을 인정받아야 한다.

4.4 증명력의 확보

증명력의 판단은 결국 법관의 자유심증에 의하는 것이지만, 디지털 포렌식 절차가 일반화되고 신뢰할 수 있고 정확한 분석이 이루어진다면 법관의 심증형성에 기여 할 수 있으므로 디지털 포렌식 기술에 관하여 알아본다.

증명력 확보는 앞서 살핀 포렌식 절차 가운데, 증거물 보관·이송단계, 증거물 분석단계, 보고서 작성 단계가 해당된다.

증거물 보관 이송단계에서는 원본증거가 훼손되지 않아야 하고 보관 상황에 신뢰성이 담보 되어야 한다. 디지털 증거의 경우 대부분 자기의 형태로 저장된다. 따라서 전자기파에 노출되면 훼손될 가능성이 크다. 따라서 전자기파 방지할 수 있는 도구를 사용하여야 한다[17].

동작중인 시스템의 경우에는 탐침 하드웨어 또는 소프트웨어를 사용하는 방법, 별도의 분석 소프트웨어를 사용하는 방법, 대상시스템에 내장되어있는 소프트웨어를 사용하는 방법이 있는데 어느 경우에도 원본자료가 훼손될 우려가 있으므로 주의 하여야 한다, 정지중인 시스템의 경우에는 큰 어려움 없이 분리하여 증거를 획득할 수 있다. 다만, 원본데이터의 변조 위조를 막기 위하여 쓰기방지장치를 사용 하는 것이 바람직하다, 그 밖의 저장장치의 경우 잠금 장치가 있으면 잠금장치를 작동시키는 것이 안전하게 증거를 보관할 수 있는 방법이다[17].

증거물 분석단계에서는 디스크 포렌식의 경우에는 원본이 변경되지 않게 하기 위하여 원본을 사용하지 않고 디스크 이미징을 통하여 증거를 수집하고 분석한다. 원본데이터를 사용할 경우는 쓰기방지장치를 사용하며, 무결성 확보를 위해 해시 함수를 사용하여야 한다. 해쉬함수를 이용하여 원본데이터와 증거분석의 대상이 된 이미지에 대하여 해시값을 비교함으로서 무결성을 확보할 수 있을 것이다.

마지막으로 보고서 작성 단계에서는 법정에 제출하기 위한 것이므로 최대한 전문용어는 피하고 누구나 보아도 알아 볼 수 있을 정도의 쉽게 작성되어야 할 것이다. 또한 앞에서의 보았듯, 최소한의 신뢰성을 위해 검증된 도구를 사용하였고 전문가에 의해 행하여졌으며 적법절차에 따라 행하여지고, 해시에 대한 자세한 설명 이후 해시값이 동일하여 무결성이 확보된다는 것 등을 강조 하여야 할 것이다.

그렇다면 증거능력이 인정되었을 때에 증거의 가치는 더욱 높아질 수 있고, 판사의 자유심증과정에서 증거의 정확성 및 신뢰성을 확보할 수 있어 최종적으로 범죄사실을 인정하는 증거로 사용될 수 있다.

4.5 증거법에 적합한 디지털 포렌식 절차 정리

증거의 신뢰성확보를 위해서 증거 분석 단계에서 사용되는 포렌식 도구가 일반적으로 검증된 도구여야 할 것이며 전문가에 의해 행하여 져야 한다. 위법수집증거배제법칙에 관해서는 증거수집 전 단계에서 압수, 수색의 경우 영장을 발부 받아야 할 것이고, 증거 수집단계에서 적법한 절차에 의해 행하여 져야 한다. 전문법칙과 관련해서는 디지털 증거의 증거능력에 관한 입법이 이루어 져야 할 것이고, 그렇지 않으면 현행 전문법칙을 완화 하여 적용할 필요가 있다.

증거능력이 인정되어 증거로 사용할 수 있을 때 증거의 가치인 증명력을 높이기 위해서는 증거물 보관·이송단계, 증거물 분석단계, 보고서작성 단계에서 정확성과 신뢰성이 담보되어야 한다. 증거물 보관·이송단계에서는 원본데이터의 손실이 되지 않게 하는 것이 중요하다. 그리고 증거물 분석 단계에서는 원본데이터와의 동일성, 무결성 확보 방안이 중요하다. 보고서 작성 단계에서는 법관과 소송 당사자들이 이해하기 쉽게 작성되고, 동일성, 무결성 등이 확보되었다는 것을 강조해야 한다.

V. 결 론

현대 사회에서 디지털 기기의 사용이 광범위 한 만큼 범죄에도 디지털 기기의 사용이 확산되고 있어 그 동안 디지털 포렌식 절차에 대한 많은 연구가 있어왔다. 경찰청에서는 디지털 증거처리 표준가이드라인을 발표 하였고, 학회에서도 이와 관련된 많은 논문들이 발간되었다. 이러한 연구들은 대부분 디지털 포렌식 절차를 시간적

으로 분석하고 해당 단계에서 기술적인 연구(예를 들어 디스크복원 방법)에 치중되어 있다.

그러나 디지털 포렌식 절차의 궁극적 목적인 디지털 증거의 사용을 위해서는 증거능력이 확보되어야 하고 보다 높은 증명력이 있을 것을 요구하므로 현행 증거법상의 증거능력과 증명력을 기준으로 포렌식 절차를 분석하게 된 것이다.

증거능력과 관련해서는 증거의 신뢰성(자연적 관련성), 위법수집증거배제법칙, 전문법칙이 문제된다. 증거의 최소한의 가치를 의미하는 증거의 신뢰성과 관련해서는 일반적으로 검증된 포렌식 도구의 사용과 전문가에 의해 디지털 포렌식 절차가 행하여 질것을 요구한다. 위법수집증거배제법칙과 관련해서는 영장주의, 적법절차의 원칙이 적용되어야 하고, 전문법칙과 관련해서는 현행 형사소송법상 디지털 증거의 증거능력에 관한 규정이 없으므로 입법론적으로 디지털 증거의 증거능력 인정요건을 규정할 필요가 있다. 마지막으로 증명력 확보와 관련해서는 원본데이터가 보관·이송 중에 훼손되지 않을 것과, 원본데이터와의 동일성 확보, 무결성 확보 할 것을 요구한다. 이러한 요구사항을 만족하기 위해서는 디지털 증거를 보관·이송 할 때에는 전자기파를 방지하는 도구를 사용하고, 증거분석을 할 때에는 쓰기방지장치를 이용하여 원본데이터와 동일성을 확보하고, 해시 함수를 사용하여 무결성을 담보한다면 디지털 증거는 보다 높은 증거가치를 가지게 되어, 디지털 포렌식 절차의 궁극적 목적인 증거로의 사용이 보다 용이해 질 것이다.

참고문헌

[1] 전상덕, 홍동숙, 한기준 디지털 포렌식의 기술 동향과 전망, 정보화정책 제13권 제4호, 2006

[2] 임의열, 박태규, 최용락 컴퓨터 포렌식스 절차에 기반한 사용도구 분석

[3] 이규안, 박대우, 신용태 포렌식 자료의 무결성 확보를 위한 수사현장의 연계관리 방법연구, 한국 컴퓨터정보학회 논문집 제 11권 제6호, 2006

[4] 강맹진, 김정규 우리나라 디지털 증거수사의 효율성 증진방안 pp182 2007.1.31

[5] 백승조, 심미나, 임종인, 국가 디지털 포렌식 법률체계와 국내외 디지털 포렌식 법제 현황, 한국정보보호학회 학회지, 2008.2

[6] 탁희성, 법정에서 디지털 증거의 허용가능성, 디지털 포렌식 연구 논문지 창간호, 2007.11

[7] 김정옥, 디지털증거의 증거능력 인정 요건 : 일심회 판결을 중심으로, 디지털 포렌식 연구 논문지 창간호, 2007.11

[8] 길연희, 은성경, 홍도원, 디지털 증거의 신뢰성 확보 방안, 디지털 포렌식 연구 논문지 창간호, 2007. 11

[9] 변정수, 한국형 디지털 증거분석 표준화, pp.8,9 2007.11

[10] 전상덕, 홍동숙, 한기준, 디지털 포렌식의 기술 동향과 전망, 정보화정책 제13권 제4호,

[11] 대법 1999. 5.12, 99다1789

[12] 이재상, 형사소송법 제6판 pp.548 2006. 2.10

[13] 대법 1994. 2.8, 93도3318

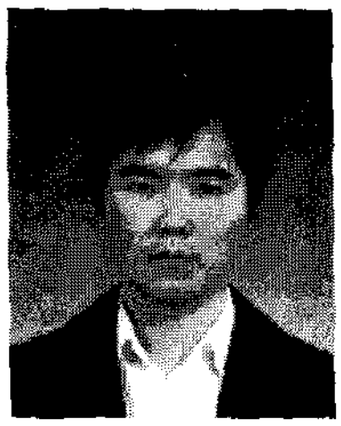
[14] 대법 2001. 3.23, 2000도486

[15] 서울중앙지방법원 2007.4.16 선고 2006 고합1365

[16] 서울고등법원 2007.8.16 선고 2007 노 929

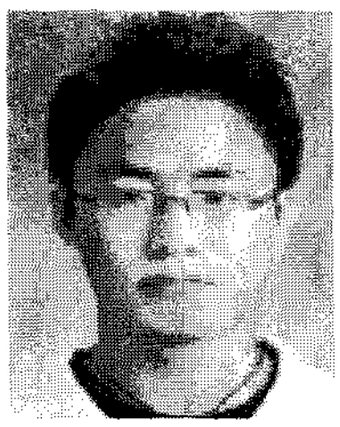
[17] 이상진, 디지털 포렌식스 기술 발전방안, 디지털 포렌식 연구 창간호 2007. 11

〈著者紹介〉



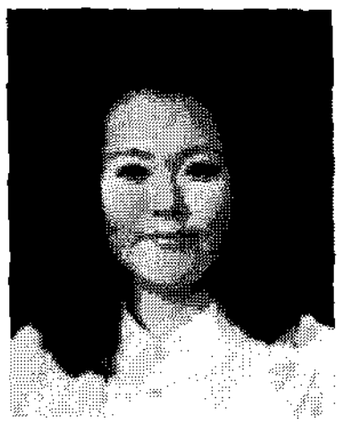
이 광 열 (Kwangyul Lee)
학생회원

2000년 3월~현재 : 성균관대학교 정보통신공학부
2007년 제49회 사법시험 합격
2008년 3월~현재 : 사법연수원 제39기 연수생
<관심분야> 디지털 포렌식, 과학수사, 정보보호



최 윤 성 (Choi Younsung)
학생회원

2006년 2월 : 성균관대학교 정보통신공학부 학사
2007년 8월 : 성균관대학교 전자전기컴퓨터공학과 석사
2007년 9월~현재 : 성균관대학교 일반대학원 전자전기컴퓨터공학과 박사과정
<관심분야> 디지털 포렌식, 정보보호, 취약성 분석

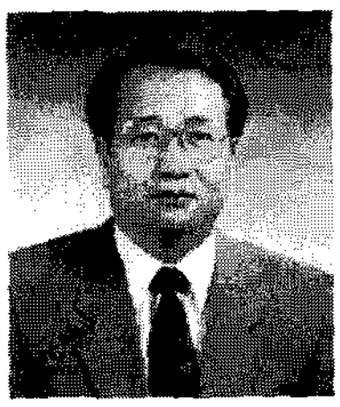


최 해 랑 (Haelahng Choi)
학생회원

2007년 2월 : 성균관대학교 정보통신공학부(공학사)
2007년 3월~현재 : 성균관대학교 일반대학원 전자전기컴퓨터공학과 석사과정
<관심분야> 암호이론, 포렌식, 정보보호 응용, 네트워크보안

김 승 주 (Seungjoo Kim)
종신회원

1994년 2월 : 성균관대학교 정보공학과 (공학사)
1996년 2월 : 성균관대학교 정보공학과 대학원 (공학석사 (정보통신공학 전공))
1999년 2월 : 성균관대학교 정보공학과 대학원 (공학박사 (정보통신공학 전공))
2004년 3월~현재 : 성균관대학교 정보통신공학부 부교수
현재 : 한국정보보호학회 이사, 대검찰청 디지털수사자문위원, 전자정부서비스보안위원회 사이버침해사고대응 실무위원, 기술보증기금 외부자문위원, 수원시 지역 정보화 촉진 협의회 위원, 한국은행 금융정보화추진분과위원회 자문위원, 법무부 법률서비스산업 경쟁력강화 위원회 위원
<관심분야> 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET



원 동 호 (Dongho Won)
종신회원

1976년~1988년 : 성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년 : 한국전자통신연구원 전임연구원
1985년~1986년 : 일본 동경공업대 객원연구원
1988년~2003년 : 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년~1998년 : 국무총리실 정보화추진위원회 자문위원
2002년~2003년 : 한국정보보호학회 회장
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, IT보안성평가연구회 위원장
<관심분야> 암호이론, 정보이론, 정보보호