리뷰논문 정보화정책 제13권 제4호, 2006년 겨울, pp.3~19

디지털 포렌식의 기술 동향과 전망

전상덕*, 홍동숙**, 한기준***

요 약 디지털 포렌식(Digital Forensics)은 법정 제출용 디지털 증거를 수집하여 분석하는 기술을 말하며 인권을 강조하는 요즘 IT 관련 기관과 기업을 중심으로 많은 관심이 집중되고 있다. 디지털 증거 수집 및 분석 과정은 기술적으로 복잡하고 난해하여 분석가의 전문성에 의해 증거의 무결성과 신뢰성이 결정된다. 디지털 증거 수집 및 분석 과정의 수준향상을 위해 IT 분야에서 많은 전문가의 참여와 디지털 포렌식의 고급기술에 대한 연구가 필요하다.

본 논문에서는 디지털 포렌식의 개요, 디지털 포렌식 도구의 소개, 디지털 포렌식 절차를 설명하고, 마지막으로 결론에서 디지털 포렌식 산업 육성 방안, 디지털 포렌식 전문 인력 양성 방안, 디지털 포렌식의 전망에 대하여 제시한다. 현재 국내외에서 활발히 수행되고 있는 디지털 포렌식 기술은 향후 유비쿼터스 컴퓨팅 환경을 지향하는 IT 분야에서 핵심 기술로서 인식되고 있으며, 또한 새로운 포렌식 기술에 대한 연구 개발이 더욱 체계적이고 활발히 수행됨으로써 새로운 비즈니스 영역도 창출될 수 있을 것이다. 그리고 첨단 과학기술을 이용하는 디지털 포렌식은 사법기관의 인권 보호와 사법 정의 구현에도 크게 기여할 수 있을 것이다.

키워드 : 디지털 포렌식, 디지털 증거, 포렌식 도구, 포렌식 절차, 증거 수집 및 분석, 컴퓨터 범죄

Ⅰ. 서론

정보통신 전문가들은 향후 5년간 세상을 바꿀 10대 신기술로서 유비쿼터스 컴퓨팅, 초고속 인터넷, 차세대 디스플레이 등 IT 관련 기술을 주목하고 있다. 가정의 디지털 TV, 인텔리전트 냉장고 등 가전기기도 네트워크를 통해 유·무선으로 연결돼 외부에서 언제든지 조작이 가능하고, PDA, 이동전화, 차량에 설치된 노트북, 회사에서 사용하는 컴퓨터 등 언제 어디서나 인터넷과 컴퓨터가 연결되는 유비쿼터스 세상이 도래할 것이다. 그러나 이러한 장점에도 불구하고 인터넷은 해킹, 정보 유출, 서비스 거부 공격 등 보안 사고에 대한 많은 취약점을 갖고 있다(Russell, 1991).

2003년 초에 발생한 '1.25 인터넷 대란'에서 외부 해커나 웜 등의 공격으로 인해 인터넷 기간망이 마비되는 경험을 하였다. 이러한 침해 사고는 우리 사회에 큰 파장을 불러왔다. PC방, 게임 업체, 인터넷 쇼핑몰 등 온라인을 이용하여 업무를 수행하는 회사에서는 큰 손실을 보았고, 전자상거래나 인터넷 뱅킹 등에 대한 불신도 가중되었다. 또한 해커 수준의 전문지식이 없어도 약간의 노력만으로 개인 정보 유출이 가능하며 이로 인한 피해는 심히 우려되는 상황에 이르렀다. 더욱 다양한 형태로 확산되고 있는 침해 사고는 특정 개인이나 기업만의 문제에 그치지 않

* 건국대학교 정보통신대학원 감리전공 겸임교수
** 건국대학교 일반대학원 컴퓨터공학과 박사과정
*** 건국대학교 컴퓨터공학부 교수

고 사회의 질서를 파괴하는 범죄로서 인식되고 있다(Gordon, et al., 2004; Stephenson, 2004).

포렌식은 "법정의", "공개토론이나 변론에 사용되는", "수사와 법정에서의 증거 또는 사실관계를 확정하기 위하여 사용하는 과학이나 기술에 관한(Houghton Mifflin Company, 2000)", "범죄와 관련된 증거물을 과학적으로 조사하여 정보를 찾아내기 위한(Cambridge University Press, 2006)"이라는 의미를 갖는다. 포렌식은 범죄와 관련된 분야에서 Forensic Examination, Forensic Laboratory, Forensic Medicine, Forensic Science 등의 용어로 사용되어 왔으며, 최근에는 범죄수사 및 민·형사 소송 등 법정에 사용되는 증거의 수집, 보존, 분석을 위한 응용과학 분야를 통칭하는 용어(최득신, 2006; Herath, et al., 2005: 135-141)로 사용되고 있다.

전통적으로 포렌식은 법의학 분야에서 지문, 모발, DNA 감식, 변사체 검시 등이 주류를 이루었다. 얼마 전 사회적 이슈가 되었던 줄기세포 조작사건의 경우에도 DNA 감식이 수사에 중요한 역할을 담당하였다. 그러나 최근 다양한 정보기기들의 활용과 정보생산 및 유통에 있어서 95% 이상이 디지털 형태로 이용되고 있기 때문에 물리적 형태의 증거뿐만 아니라 전자적 증거(Electronic evidence)를 다루는 디지털 포렌식(Digital forensics) 분야가 점차 확대되고 있다.

하드웨어, 소프트웨어, 또는 컴퓨터 내의 데이터를 불법적으로 사용하거나 변경, 파괴하는 행위를 컴퓨터 범죄라고 한다. 이러한 컴퓨터 범죄에 대한 수사는 전자적 신호로 전송되거나 저장매체에 기록되는 전자적 증거를 수집하고 분석하기 위한 지식과 기술을 요구한다. 수사의 근본적인 특성에 따라 법적으로 유효한 전자적 증거의 확보를 목표로 과학적 지식과 기술을 활용하여 전자적 증거를 수집하고 분석하는 제반 행위를 디지털 포렌식이라고 한다(박윤해, 2005).

미국에서는 90년대 이후 아동 포르노, 해킹, 개인정보 유출, 기술 유출 등 컴퓨터 범죄의 위협이 증가하면서 디지털 포렌식의 연구·개발을 위한 연구실과 민관 교육기관이 설립되고 관련 교육과정이 개설되기 시작하였다. 디지털 포렌식이라는 용어도 1991년에 포렌식 교육을 목적으로 한 법집행기관의 전문가들이 결성한 비영리단체인 국제컴퓨터수사전문가협회(IACIS)가 미국 포틀랜드에서 개설한 교육과정에서 처음으로 사용되었다(이임영, 2006).

디지털 증거에 대한 과학적인 조사를 주요 내용으로 하는 디지털 포렌식은 탐정 제도 등이 발달되어 있고 적법 절차를 중시하는 영·미 등 선진국에서 많이 발전되어 왔으며, 민·형사 소송의 증거에 매우 중요한 역할을 해왔다. 디지털 포렌식은 컴퓨터를 이용한 수사 혹은 컴퓨터와 관련된 수사과정에서 과학적이고 체계적인 증거확보 절차에 따라 합법적인 증거를 산출해냄으로써 정확한 범죄자 색출 및 범죄사실의 증명을 통한 실체적 진실의 발견에 크게 기여할 수 있다(Wilsdon, et al., 2005: 48-55).

유비쿼터스 컴퓨팅 등 새로운 패러다임을 선도하는 정보사회에서 범죄 증거는 다양한 형태로 존재하게 되고 디지털 포렌식 기술은 더욱 중요하게 될 것이다. 그러나 국내에서는 수사기관이나 일부 보안업체를 중심으로 최근 디지털 포렌식에 대한 관심이 급증하였다. 향후 디지털 포렌식에 대한 관심과 연구를 활성화하여 압수수색 및 분석분야에 우선 적용하면서 표준 절차를 개발하고, 이러한 절차를 통해 얻어낸 증거가 형사사법의 이념인 실체적 진실의 발견과 적법 절차 원칙 실현에 중요한 역할을 하여야 하며, 또한 피의자의 인권보호에도 기여하여야 할 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 분석 목적과 분석 대상에 따른 디지털 포렌식의 유형별 분류에 대해서 설명한다. 3장에서는 디지털 포렌식에서 사용되는 다양한 디지털 포렌식 도구를 소개하고, 객관적이고 신뢰성있는 증거 수집 및 분석을 위한 디지털 포렌식의 절차에 대해서 기술한다. 4장에서는 본 논문의 결론으로써 디지털 포렌식 산업 육성 방안,

디지털 포렌식 전문 인력 양성 방안, 디지털 포렌식의 전망에 대해서 제시한다.

Ⅱ. 디지털 포렌식 유형

1. 분석 목적에 따른 분류

디지털 포렌식은 증거의 수집, 보존, 분석, 문서화, 그리고 재판 과정에 증거로 제출하기까지의 모든 과정을 포함한다. 지금까지는 디지털 포렌식이라고 하면 컴퓨터의 하드디스크에서 개인이 작성한 데이터를 증거로 확보하는 분야가 주류를 이루었고 디스크의 검시 정도에 불과하였다. 그러나 디지털 기술의 발달로 증거는 네트워크, 인터넷, 데이터베이스, 모바일 기기, 휘발성 메모리 등 다양한 곳에서 존재하기 때문에 전문성이 더욱 심화되고 대형 시스템의 하드웨어 종류나 운영체제 종류에 따라 다양한 방법론에 대한 연구가 필요하다. 일반적으로 디지털 포렌식은 분석 목적에 따라 다음과 같이 크게 두가지로 분류할 수 있다.

사고 대응 포렌식(Incident response forensics)은 해킹 등 침해 시스템의 로그, 백도어, 루트킷 등을 조사하여 침입자의 신원, 피해내용, 침입경로 등을 파악하기 위한 분야로서 네트워크 기술과 서버의 로그 분석기술, 유닉스, 리눅스, 윈도우즈 서버 등 운영체제 기술 등이 필요하며 주로 운영체제 및 서버에서 이루어진다(서희명, 2005; Northcutt, et al., 2001; Prosise, et al., 2001).

정보 추출 포렌식(Information extraction forensics)은 범행 입증에 필요한 증거를 얻기 위하여 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 검색하여 증거를 찾아내는 것을 목적으로 한다(Kruse, et al., 2001).

2. 분석 대상에 따른 분류

디지털 포렌식은 분석 대상에 따라 다음과 같이 몇 가지 포렌식 유형으로 분류된다.

1) 디스크 포렌식

디스크 포렌식은 물리적인 저장장치인 하드디스크, 플로피디스크, CD ROM, DVD 등 각종 보조 기억장치에서 증거를 수집하고 분석하는 포렌식 분야이다. 1980년대 말부터 디스크에 데이터를 보존하고 분석하기 위한 기법이 개발되기 시작하여 현재는 포렌식 분야에서 가장 발전된 분야이다.

디스크를 검색하여 삭제된 파일을 복구하고, 여러 가지 종류의 파일을 파일명, 확장자, 작성자, 작성일시 등을 기준으로 분류하고, 키워드 검색을 통하여 수사의 단서를 추출하는 작업을 한다. 디렉토리 구조, 파일 열람, MAC(Modification, Access, Creation) Time 및 시계열 분석 등의 기법도 사용한다(Garfinkel, et al., 2003: 17-27). 파일 확장자를 바꾸어 데이터를 은닉하게 되면 이를 찾기 위해 파일 포맷과 파일 서명에 대한 분석 과정으로 증거를 찾을 수 있다.

디스크 포렌식 과정에서는 증거의 손상이나 훼손을 방지하기 위해서 2개의 복제본을 만들어 하나는 증거로 보존하고 나머지 복제본을 대상으로 분석이 이루어져야 한다. 〈그림 1〉은 디스크의 변경을 방지하기 위한 미국 Guidance사의 쓰기방지 장치(Write-block device) 도구인 FastBloc™이다(Guidance Software, 2006).

〈그림 1〉 FastBl●c™

2) 시스템 포렌식

시스템 포렌식은 컴퓨터의 운영체제, 응용 프로그램 및 프로세스를 분석하여 증거를 확보하는 포렌식 분야이다. 컴퓨터 시스템은 윈도우즈, 리눅스, 유닉스, 멕킨토시, ZENIX 등 여러 가지 운영체제를 사용한다.

윈도우즈 운영체제에서 사용되는 파일 시스템으로 FAT16, FAT32, NTFS가 있고 특히, 윈도우즈 2000 이후부터 사용되는 NTFS는 보안성이 뛰어나다. 리눅스는 업그레이드가 쉬운 EXT(Extended File System)2 파일 시스템과 EXT2의 약점인 디스크 복구기능을 보완하여 만든 EXT3 파일 시스템을 주로 사용한다.

유닉스의 경우 과거에는 전문가들만 사용하는 시스템으로 한정되었으나 최근에는 교육 기회의 확대로 많은 기업의 정보 시스템에서 가장 많이 사용되는 운영체제가 되었다. 유닉스의 파일 시스템은 대부분 비슷한 구조를 가지고 있으며 기본구조는 파일 시스템의 크기와 전반적인 정보를 담는 슈퍼 블록(Super block), 해당 파일의 모든 정보(파일 이름은 제외)를 가지고 있는 인덱스 노드(Index node 혹은 Inode), 데이터를 저장하기 위해 사용되는 데이터 블록(Data block), 파일 이름과 인덱스 노드를 저장하기 위해 사용되는 디렉토리 블록(Directory block), 많은 양의 데이터 블록이 필요할 경우 인덱스 노드 외부에 생성되어 있는 데이터 블록을 알려주는 간접 블록(Indirect block) 등으로 구성된다.

3) 네트워크 포렌식

네트워크 포렌식은 네트워크를 통하여 전송되는 데이터나 암호 등을 특정 도구를 이용하여 가로채거나 서버에 로그 형태로 저장된 것을 접근하여 분석하거나 에러 로그, 네트워크 형태 등을 조사하여 단서를 찾아내는 포렌식 분야이다. 대부분의 네트워크는 사용자의 행태를 감시하기 위하여 추적을 위한 기능을 지원한다. IP 헤더는 발신지 IP, 목적지 IP 정보를 포함하고 있으며, 데이터 링크 헤더는 하드웨어 주소(MAC address)를 포함하고 있다. 네트워크의 관문 역할을 하는 라우터(Router)에는 라우팅 테이블, ARP 캐쉬 테이블, 로그인 사용자, TCP 연결 관련 정보, NAT(Network Address Translation) 관련 정보가 존재하기 때문에 침해 시스템을 조사할 때 라우터의 분석도 필요하다. 또한, 라우터의 로그정보 분석을 위해 특별한 네트워크 전문가가 필요하다(Ford, 1993).

4) 인터넷 포렌식

인터넷 포렌식은 인터넷으로 서비스되는 월드와이드웹(WWW), FTP, USENET 등 인터넷 응용 프로토콜을 사용하는 분야에서 증거를 수집하는 포렌식 분야이다. 인터넷은 기술의 편리성을 넘어서 부도덕한 익명의 사용자 폭주 및 그들의 무분별한 인터넷 남용으로 인해 수많은 역기능을 낳게 되었다. 그러므로, 인터넷 포렌식은 이러한 역기능 중 불법행위를 한 용의자를 추적하기 위해 사용되는 웹 히스토리 분석, 전자우편 헤더 분석, IP 추적 등의 기술을 이용하여 증거 수집을 수행한다.

게시판에 불법 정보를 업로드하거나 명예훼손과 관련된 글을 올린 용의자 추적, 전자메일 발신자 추적, 인터넷 서핑 내역 추적 등을 위하여 웹 서버나 메일 서버, WAS(Web Application Server) 등의 서버를 분석하는 작업이 필요하며, 이러한 분석 작업을 통하여 유용한 증거로 얻을 수 있다(Manzano, et al., 2001: 289-295).

5) 모바일 포렌식

모바일 포렌식은 휴대폰, PDA, 전자수첩, 디지털 카메라, MP3 Player, 캠코더, 휴대용 메모리카드, USB 저장장치 등 휴대용 기기에서 필요한 정보를 입수하여 분석하는 포렌식 분야이다. 유비쿼터스 컴퓨팅 시대의 도래와 이동성 기기의 확대 보급으로 다양한 종류의 멀티미디어 기기가 개발되어 보급되고

있는 시점에서 소형의 휴대용 기기의 데이터에 대한 범죄 증거의 확보는 매우 중요하다. 특히 휴대용 기기는 작고 휴대가 간편하여 은닉이 편리하다는 장점이 있다. 따라서 증거 확보가 필요한 경우 은닉 여부를 세심히 확인할 필요가 있다. 예를 들어, 휴대용 저장장치를 이용하여 개인 PC에 데이터를 복사하거나 읽는 경우 최근에 열어본 파일의 드라이브 위치를 확인하거나 링크 여부를 확인함으로써 휴대용 저장장치의 사용여부를 확인해 볼 수 있다.

6) 데이터베이스 포렌식

데이터베이스 포렌식은 데이터베이스로부터 데이터를 추출·분석하여 증거를 획득하는 포렌식 분야이다. 기업의 모든 데이터는 개인 PC와 정보 시스템 부서의 대형 시스템내에 저장되어있으므로 기업의 분식회계, 횡령, 탈세 등 각종 범죄를 수사할 때 대상 기업의 정보 시스템에 저장되어 있는 데이터베이스를 분석하는 것은 필수적인 과정이 되었다(이종상, 2000). 예를 들어, 건설업체의 경우 건설공사의 수주 및 발주를 관리하는 공사 관리 시스템, 자재의 입고와 출고를 관리하는 자재 관리 시스템, 기업의 모든 회계 관리를 위한 회계 관리 시스템 등이 있다. 제조업체의 경우는 제품을 공정별로 관리하는 제품 관리 시스템이 있고, 유통업체는 상품의 입고와 출고를 관리하는 유통 관리 시스템이 있다. 이러한 모든 경우에 데이터는 정보 시스템의 데이터베이스에 일정 규칙에 따라 저장되어 있다.

기업의 대형 전산 시스템으로부터 증거 데이터를 확보하기 위하여 적절한 기법들이 연구되어야 한다. 이러한 연구는 데이터베이스를 압수 수색하는 분야와 압수된 데이터베이스를 복구하여 SQL을 이용해 분석하는 분야에서 모두 요구된다. 예를 들어, 방대한 양의 데이터로부터 증거 수집 및 분석을 위한 기술, ERP 기반에서 개발된 회계 시스템 등의 대형 시스템을 위한 하드웨어 및 소프트웨어 기술, 다양한 데이터베이스 관리 시스템에 대한 제어 기술 등이 필요하다.

7) 암호 포렌식

암호 포렌식은 문서나 시스템에서 암호를 찾아내는 포렌식 분야이다. 증거 수집에서 비인가자의 접근을 막기 위해 문서나 각종 시스템에 암호를 설정해 놓은 경우가 흔히 있다. 이러한 문서나 시스템을 열어보는 것이 쉽지는 않다. 그러나 이런 문서나 시스템은 아주 중요한 내용을 담고 있는 경우가 많기 때문에 절대로 소홀히 지나칠 수 없는 것이다.

1995년 암호학자들이 100만 달러짜리 컴퓨터를 가지고 암호를 해독하였는데, 40비트 키의 경우 약 0.2초, 56비트의 경우 3.6시간, 128비트의 경우 1,018년의 시간이 걸렸다고 한다. 근래에는 256비트, 1,024비트 암호키가 존재하며 이는 소프트웨어적인 기법이나 하드웨어의 성능을 높이는 것으로 한계가 있다는 것을 의미한다.

문서나 네트워크, 컴퓨터 시스템에 설정되어 있는 암호를 풀어내기 위해 가능한 암호를 추측하기에는 한계가 있다. 따라서, 암호가 될 수 있는 숫자나 문자를 고속으로 대입하여 비교하는 크랙 프로그램을 개발하여 사용하기도 한다. 패스워드 크랙 프로그램은 암호를 찾아내기 위해 무차별 대입 공격(Brute-force attack) 기법이나 사전대입 공격(Dictionary attack) 기법을 빠른 속도로 실행하여 암호를 찾아낼 수 있다. 무차별 대입 공격 기법은 모든 경우의 수를 무작위로 대입하여 암호를 찾아내는 방법이고, 사전대입 공격 기법은 일반적으로 사용하는 단어들을 미리 사전에 등록하고 이것을 하나씩 대입하여 암호를 찾아내는 방법이다.

8) 회계 포렌식

회계 포렌식은 저장된 회계 데이터를 추출하고 회계사 등 회계 전문가가 분석할 수 있도록 데이터를 정제하는 포렌식 분야이다. 기업의 부정과 관련된 수사를 할 때, 필수적으로 회계 시스템을 압수하고 분

석해야 할 것이다. 회계 시스템은 기업의 자금 조달 방법과 운용에 대한 모든 것을 정리하기 위한 것이고, 최근에는 거의 전산 시스템을 이용하여 저장 및 관리하고 있다. 이 분야에서는 회계 시스템에 대한 프로그램을 개발한 경험이 있거나 회계 시스템을 운영해 본 경험이 있는 전문가가 필요하다.

회계 시스템은 크게 세 가지로 나누어 볼 수 있다. 첫번째, 중소기업에서 주로 사용되며 PC나 워크스테이션에서 운영되는 회계 프로그램으로 값이 저렴하고 유지비용이 적게 드는 패키지 형태의 더존, SAWIN, 얼마에요 등의 상용 소프트웨어가 있다. 두번째, 상용 데이터베이스 관리 시스템을 활용하여 기업에서 자체 개발하거나 개발 전문기업에 아웃소싱하여 개발된 회계 시스템이 있다. 세번째, 글로벌 표준으로 활용되고 있는 회계 시스템으로 ERP가 있다. 이러한 ERP에는 SAP/R3 ERP나 Oracle ERP가 있으며 미국, 독일 등 각 선진국에서 회계 부정에 대한 불신을 줄이기 위해 ERP 시스템 구축에 박차를 가하고 있다.

Ⅲ. 디지털 포렌식 기술

1. 디지털 증거의 특성

지금까지는 컴퓨터 증거(Computer evidence)라는 용어가 많이 사용되어 왔지만, 최근에는 물리적 증거와 구분하기 위해 디지털 증거(Digital evidence) 또는 전자적 증거(Electronic evidence)라는 용어가 많이 사용되고 있다(Casey, 2000).

전자적으로 처리되는 디지털 증거는 다음과 같은 특성을 가지고 있다.

• 디지털(Digital)

2진법의 디지털 신호로 되어 있어 원본과 동일한 복제를 무제한으로 할 수 있으며 원본과 복제본의 구분이 어렵다.

• 불가시성(Latent)

디지털 형태로 저장되므로 눈으로 바로 확인되지 않고 적발 및 증명이 어렵다.

• 취약성(Fragile)

변조나 손상이 쉽고 변조 사실을 찾아내기 어렵기 때문에 법정에서 조작 여부, 증거 획득 절차의 적법성 등이 문제가 될 소지가 있다.

• 대용량성(Massive)

기업의 대용량 데이터베이스, 파일 등의 데이터는 수십 테라바이트에 이를 만큼 양이 방대하여 특별한 분석 도구나 IT 분야의 전문 인력이 없는 상태에서는 범죄의 단서나 증거를 찾는 것이 거의 불가능하다.

2. 디지털 포렌식의 도구

원본과 복제본의 구분이 어렵고 증명이 어려우며, 변조나 손상에 취약한 대용량의 디지털 증거의 수집 및 분석을 위하여 다양한 디지털 포렌식 도구가 사용된다. 디지털 증거의 신뢰성과 무결성을 보장하기 위하여 증거물의 수집과 분석에 사용되는 디지털 포렌식 도구는 검증된 것을 사용하여야 하며, 동일한 조건에서 제 3자가 분석하더라도 동일한 결과가 산출되어야 한다(Casey, 2001; Stroz, 2003: 344-352).

1) 디스크 이미징과 디스크 복제 도구

원본 디스크에서 증거를 추출하기 위해 바로 분석할 경우 디스크 상의 데이터의 손상이나 변경의 위험에 노출된다. 디스크 이미징과 디스크 복제 도구는 원본 디스크에 손상이나 변경이 가해지는 것을 방지하기 위해 원본 디스크를 물리적으로 동일한 형태의 다른 디스크로 복제하거나 미러(Mirror) 이미지 파일을 생성하는 도구이다. 디스크 이미징은 섹터 대 섹터 복사 또는 비트 스트림 복사 방식으로 분류된다.

디스크 이미징 도구는 다음과 같은 조건을 갖추고 있어야 한다. 첫번째, 복제 과정에서 원본을 훼손시켜서는 안된다. 두번째, 디스크 이미징 과정에서 어떤 변경이 있었는지 체크하기 위하여 그 절차를 검증하여야 한다. 대부분의 이미징 도구는 원본과 동일하게 복제가 되었다는 것을 입증하기 위해 MD5, CRC 체크섬(Checksum)과 같은 메커니즘을 사용한다.

관련 소프트웨어로는 SafeBack, SnapBack, DataArrest 등이 있으며 비트 스트림 이미지를 지원하는 EnCase(Guidance Software, 2006)도 있다. 하드디스크의 고속 복제용으로 개발된 하드웨어로는 〈그림 2〉의 MagicJumbo DD-121과 MASSter 500 (Upgrade Solutions, 2006) 등이 있다.

2) 데이터 무결성 도구

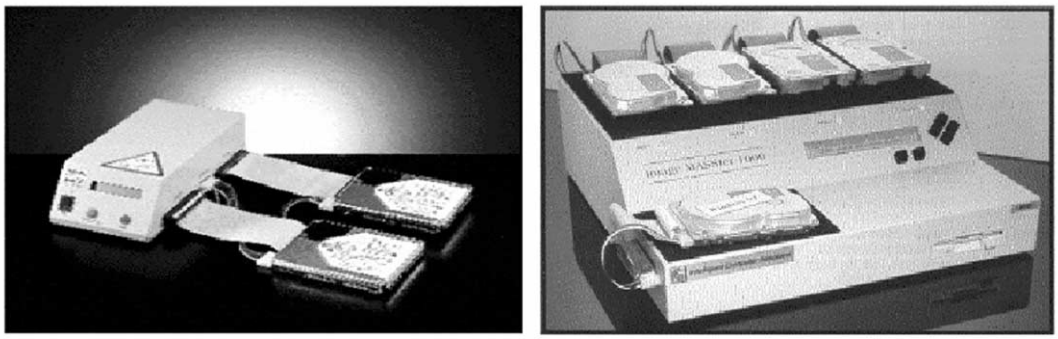
데이터 무결성 도구는 증거물이 훼손되지 않았음을 검증해 주는 도구이다. 디지털 포렌식에서는 증거 확보나 분석 과정에서의 증거가 변경되지 않았음을 입증하기 위해 해쉬 함수(Hash function)나 메시지 다이제스트(Message digest) 기법이 사용된다(Stephenson, 2004).

해쉬 함수를 이용하는 MD5 알고리즘은 입력 데이터로부터 특정 비트 길이(주로 128비트)의 메시지 다이제스트를 생성함으로써 복제본과 원본이 동일함을 입증하고 데이터의 무결성을 검증하는데 사용하는 알고리즘이다. 원본 파일에 대한 MD5 해쉬값을 생성하여 보관하고 있으면, 복제본의 해쉬값을 계산하여 원본의 해쉬값과 비교하면 변경이 되었는지 여부를 알 수 있다. MD5 알고리즘을 구현하고 있는 데이터 무결성 도구로는 상용 소프트웨어인 HashMD5가 있다.

타임스탬프(Timestamp)를 이용하는 방법인 Time Stamping Service(TSS)는 신뢰할 수 있는 제 3의 기관에 의하여 특정 시점에 해당하는 데이터가 존재하였음을 증명해 주는 서비스이다. TSS는 디지털 공증(Digital notary)의 한 종류로 컴퓨터 데이터를 입수한 시점에 컴퓨터 데이터의 해쉬값을 계산하고, 그 해쉬값과 시간을 제3의 공증기관에서 확인을 받아 두는 방법으로 증거 시점을 확정하고 최소한 특정 시점에 특정 문서가 존재했다는 것을 입증하는 것이다.

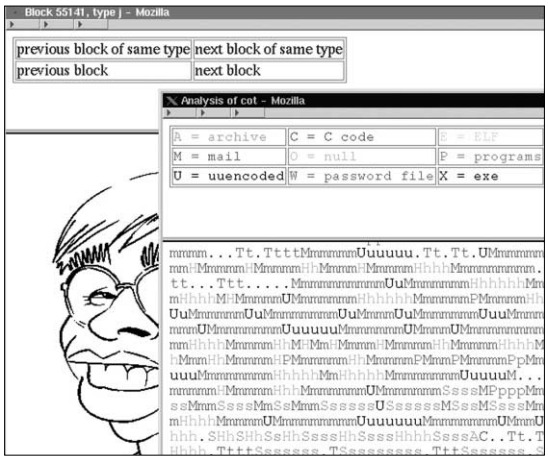
3) 데이터 복구 및 분석 도구

데이터 복구 및 분석 도구는 디스크에서 삭제되거나 손상된 데이터를 분석하고 복구하는 도구이다. 이러한 도구는 하드디스크의 파티션 테이블이 손상된 경우나 파일의 MAC Time을 분석할 때 사용하는 도구이며 현재 포렌식 도구로는 가장 많이 사용되고 있다. 국산 소프트웨어로는 FinalData, DataMedic, LiveData 등이 있으며 외국산 소프트웨어로는 EnCase, FTK(Forensic ToolKit), TCT(The Coronor's

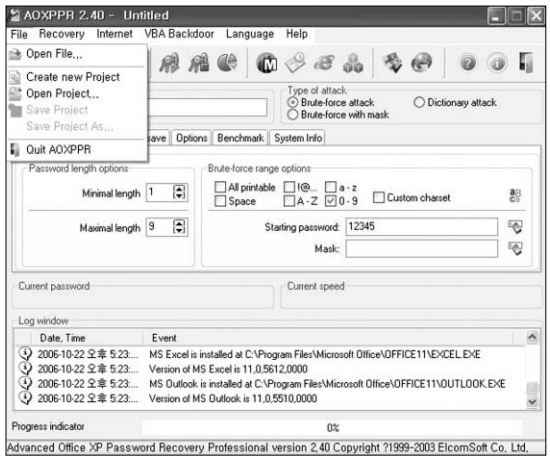


MagicJumbo DD-121　　MASSter 500

〈그림 2〉 디스크 복제 도구의 예



〈그림 3〉 삭제된 파일을 분석하는 Lazarus 실행 화면



〈그림 4〉 암호 복구를 위한 AOXPPR 실행 화면

Toolkit) 등이 있다. 〈그림 3〉은 삭제된 파일을 복구하기 위해 사용되는 TCT에 포함된 Lazarus 도구의 실행 화면이다(Venema, et al., 2004).

4) 암호 복구 도구

암호 복구 도구는 다양한 서버용 시스템이나 문서 파일에 암호가 설정된 경우 암호를 알아내기 위한 포렌식 도구이다. 증거로 확보한 데이터에 암호가 설정된 경우를 종종 볼 수 있다. 문서 파일 뿐만 아니라 윈도우즈 서버, 리눅스, 유닉스 등 서버용 시스템에 접근하기 위해서도 관리자나 사용자 계정이 필요하다. 일반적으로 사용자들은 암호를 잃어버리지 않기 위해 일정한 규칙에 따라 암호를 설정하거나 다른 암호와 동일하게 암호를 설정하는 경우가 많다. 따라서 사용자의 다른 암호를 알아냈다면 다른 문서 파일의 ID, 암호를 복구하는데 사용할 수 있다. 암호 복구용 도구로는 Password Recovery, Passware Kit, Advanced Office XP Password Recovery (AOXPPR) 등이 있다. 〈그림 4〉는 AOXPPR 도구의 실행 화면이다(ElcomSoft, 2006).

5) 데이터 조사 도구

데이터 복구나 암호 복구가 끝나면 데이터 조사 도구를 통해 많은 문서들이 증거와 관련이 있는지 확인을 해볼 필요가 있다. 많은 문서들은 각 응용프로그램에 종속되어 실행되기 때문에 대응되는 응용프로그램이 있어야만 데이터를 볼 수 있다. 예를 들면 hwp, doc, xss, txt, xls, ppt 등의 파일들은 각 파일의 속성에 맞는 해당 응용프로그램이 있어야 볼 수 있다. 이러한 문제를 해결하기 위해 Quick View Plus와 같은 뷰어를 사용하여 문서의 내용을 빠르게 확인하거나 Simmani, Google 등의 검색 도구를 이용하여 키워드 검색으로 관련 문서들을 용이하게 추출할 수 있다.

6) 증거 수집 도구

증거 수집 도구는 컴퓨터나 인터넷에서 증거를 수집할 때 사용하는 도구이다. 증거 수집을 위해 특수 목적으로 개발된 소프트웨어도 있지만 일반 범용 프로그램을 사용할 수 있다. 현재 화면 캡쳐, 웹사이트 저장, 파일의 MAC Time 추출 등 증거 수집을 위한 많은 도구들이 존재하며, 자주 사용되는 증거 수집 도구로는 Adobe acrobat, Webzip 등이 있다.

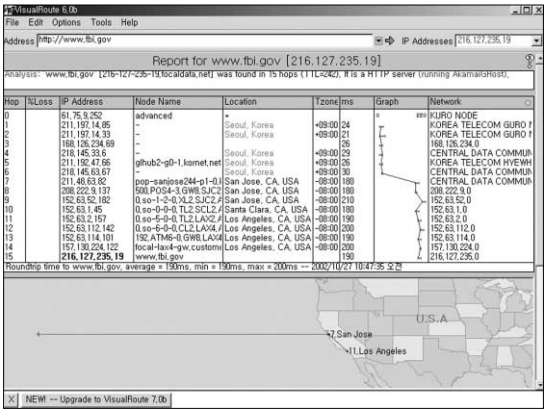
특히, 화면 캡쳐는 현재 보이는 화면을 증거로 수집하는 방법이며 화면 캡쳐 소프트웨어를 사용하거나 키보드의 PrintScreen 키를 이용하여 모니터 상

〈그림 5〉 화면 캡쳐를 위한 SnagIt 실행 화면

에 보이는 화면을 이미지 파일로 저장할 수 있다. 인터넷 게시판이나 음란 사이트의 화면을 저장할 때와 같이 컴퓨터 화면을 캡쳐하기 위하여 HyperSnap, SnagIt 등의 프로그램을 사용하면 편리하다. 〈그림 5〉는 미국 TechSmith사의 SnagIt을 실행한 화면이다(TechSmith, 2006). 증거로 확보하기 위해서는 화면 캡쳐와 동시에 해쉬값도 생성해야 한다.

7) 네트워크 및 인터넷 분석 도구

네트워크 및 인터넷 분석 도구는 네트워크 트래픽을 모니터링하거나 인터넷 기반 서비스를 이용하여 증거를 수집하는 도구이다. 네트워크 스캐닝이나 스니핑 프로그램, 웹 히스토리 분석 도구, 메일 추적



〈그림 6〉 네트워크 분석 도구의 활용 예

프로그램 등을 이용할 수 있다. 대표적인 네트워크 및 인터넷 분석 도구로는 VisualRoute, Spider, BlackIce, Sniffer, Ethereal 등이 있다.

〈그림 6〉은 네트워크 분석 도구인 VisualRoute를 활용하여 특정 주소('http://www.fbi.gov')에 Trace Route를 실행한 화면이다(Visualware, 2006).

〈그림 6〉에서는 실리콘밸리의 'www.fbi.gov' 서버까지 접속하기 위해서 15개의 경로를 지나가는 것을 알 수 있으며, 6번째 홉(218.145.63.82)과 8번째 홉(208.222.9.137) 사이의 RTT(Round Trip Time) 시간이 크게 차이 나는 것으로 보아 한국과 미국을 연결하는 관문국과 같은 역할을 하는 게이트웨이라고 유추할 수 있다. 이렇게 IP 데이터그램이 어떠한 경로를 경유하여 목적지까지 라우팅 되는가를 시각적으로 보여 줌으로써 네트워크에 대한 용이한 이해와 관리를 가능하게 한다.

8) 데이터베이스 분석 도구

데이터베이스에 저장된 대용량 데이터를 분석하여 필요한 정보를 추출하기 위해 사용되는 데이터베이스 분석 도구는 데이터베이스 관리 시스템에 따라 별도의 분석 도구가 있으며 그 종류도 다양하다. 오라클을 기반으로 제작된 Toad는 분석용 소프트웨어로서 오라클 기반에서 가장 안정적이고 빠른 속도를 자랑하며 전세계적으로 가장 많이 사용되고 있다.

국산 소프트웨어로는 SQL Gate나 Orange 등의 소프트웨어 도구가 있다. 특히, SQL Gate는 오라클용, MS SQL용, My SQL용의 3가지 소프트웨어가 시판되고 있다. 이러한 소프트웨어는 데이터베이스에서 필요한 정보를 추출하는데 중요한 역할을 수행한다.

3. 디지털 포렌식의 절차

일반 범죄 수사에서 증거 수집 절차는 매우 중요하다. 특히 미국에서 전처를 살해한 혐의로 기소된 미

국의 유명한 풋볼 스타인 O.J. Simson 재판에서 증거 수집 중 증거훼손이 문제가 되어 무죄 평결을 받은 이후 증거 수집 절차의 중요성에 대한 인식이 더욱 강화되었다. 이 사건을 계기로 미국은 증거훼손을 방지하기 위한 증거 수집 절차 및 방법을 개발하기 위해 노력하고 있다.

컴퓨터 범죄 수사에서 디지털 데이터를 수집하여 범행의 증거로 사용하는 것은 필수적인 절차이다. 디지털 포렌식은 전자적인 형태로 존재하는 비휘발성이고 잠재적인 증거를 다루기 때문에 증거로서 가치를 획득하기 위해서는 증거를 다루는 절차에 있어 객관성이 매우 중요하다. 따라서, 공판 과정에서 신뢰성있는 증거로 인정받으려면 증거 수집에 대한 절차의 체계화된 기준이 필요하다(김종섭, 2003; Vacca, 2002).

컴퓨터와 관련 증거 수집에서 디지털 증거의 수집이 필수적인 절차가 되었다. 그러나 컴퓨터와 정보통신 기술의 발전은 너무 빠르고 관련 범죄의 유형도 다양화되고 또한 고도화되고 있기 때문에 증거 수집의 상황이나 조사자의 전문지식 여하에 따라 큰 차이가 발생한다. 이러한 다양한 상황에서의 증거 수집을 성공적으로 수행하기 위해서는 디지털 포렌식 조사에 대한 원칙, 절차, 지침 등이 명시적으로 정의되어야 한다.

절차와 기법은 증거를 효율적으로 찾을 수 있도록 도와주지만 법적으로 원본 증거가 변형되지 않았음을 입증하는 것이 가장 중요하다. 또한, 증거 수집을 위한 절차에서 당사자의 프라이버시나 인권을 우선 존중하여야 하며 그 다음 절차에 따른 체계적인 증거 수집이 이루어져야 한다. 디지털 증거 수집은 어떠한 데이터를 수집하여야 하는지 순서를 정해야 하고, 컴퓨터 전문가나 분야별 기술 전문가의 도움을 받고 최소한의 범위 내에서 증거 수집을 수행하여야 한다(Caloyannides, 2001).

디지털 포렌식의 수행 절차는 크게 현장에서 수행되는 증거 수집 단계와 다양한 전문 기관에서 수행되는 증거 분석 단계로 나뉜다. 또한, 이러한 증거 수집과 분석이 체계적이고 객관적으로 진행되기 위하여 증거 수집 이전에 증거 수집 및 분석을 위한 명확한 계획이 디지털 포렌식의 원칙과 지침을 기반으로 수립되어야 한다.

1) 증거 수집 전 단계

(1) 전문 인력과 포렌식 도구의 활용방안 수립

다양한 운영체제 및 파일 시스템, 네트워크, 데이터베이스, 회계 시스템 등 다양한 기술을 가진 전문가들이 디지털 포렌식에 대한 최소한의 교육을 받고 조사관으로 참여하여 각종 전문적인 도구를 이용하여 신속 정확하게 증거를 수집하여야 한다. 또한, 이러한 전문 인력뿐만 아니라 유용한 포렌식 도구의 활용방안도 수립하여야 한다. 포렌식 도구로서는 일반 IT 분야에서 사용하는 소프트웨어를 포함하여 EnCase, FinalData 등과 같은 포렌식 전용 소프트웨어가 될 수 있다.

(2) 보관의 연속성 방안 수립

보관의 연속성이란 증거가 어떻게 수집되어 누구에 의하여 분석, 보존되었는가를 증명할 수 있도록 문서로 기록하는 것을 말한다. 증거를 소유한 사람 또는 가져간 시간, 돌려준 시간, 소지한 이유 등을 정확히 기록함으로써 증거가 훼손되지 않았음을 보여주고 무결성을 입증하기 위한 구체적인 방안을 수립한다. 이러한 방안은 공판과정에서도 수사기관이 증거를 다루는 동안 조작되지 않았음을 제 3자나 정보기술 분야의 전문가가 객관적으로 확인하거나 입증할 수 있도록 도구의 활용을 고려해야 한다. 보관의 연속성 방안이 수립되면, 이러한 방안에 따라 증거 수집 및 분석의 전 과정에서 모든 작업에 대해 적합한 방식으로 기록을 수행해야 한다.

(3) 데이터의 무결성 유지방안 수립

증거 수집 및 분석 수행 중 원본의 훼손을 최대한

방지하여야 한다. 이를 위해서는 자격이 없는 사람이나 관계자들이 증거를 함부로 다루지 않도록 할 필요가 있다. 확보된 데이터의 증거능력을 확보하고 공판과정에서 공소사실을 입증하는 증거로서 가치를 부여하기 위해 무결성을 입증할 수 있는 여러 가지 방법을 결정해야 한다. 컴퓨터 기록의 증거 능력과 관련한 전문 법칙의 적용이 중요하다. 사람의 진술을 포함하여 컴퓨터 저장기록이 증거가 되기 위해서는 컴퓨터에서 출력된 문서 또는 사진도 법정에서 진술에 대신하여 제출되는 서면에 해당되는 형사소송법상 '전문증거'로 보아야 하기 때문에 증거로 사용되기 위해서는 전문 법칙의 예외를 충족하여야 한다. 현재 자동 전화기록이나 컴퓨터 생성기록의 경우에는 전문 법칙이 적용되지 않는다.

최근에는 증명력 확보를 위해 별도의 소프트웨어를 사용하거나 포렌식 도구, MD5 해쉬값 등을 사용하여 증거를 보존함으로써 사전에 부인을 방지할 수 있다. 사후에 증거의 조작, 변형, 파괴에 대비하여 증거물에 대한 이미지 백업, 복제, 디스크 이미징 등을 수행하고 원본은 소유주의 입회하에 봉인하고 복제본을 가지고 분석을 하여야 한다.

2) 증거 수집 단계

(1) 휘발성 증거 우선 수집

컴퓨터 시스템이 가동되고 있는 경우 네트워크 접속 정보, 메모리에 저장된 데이터 등은 쉽게 소멸될 수 있는 데이터이다. 증거 수집 시 이와 같은 메모리나 프로세스, 화면에 있는 정보 등 소멸 가능성이 많은 증거부터 우선 확보해야 한다.

일반적으로 레지스트리와 캐쉬, 라우팅 테이블, ARP 캐쉬, 프로세스 테이블, 커널 정보와 모듈, 메인 메모리, 임시 파일, 보조 메모리, 라우터 설정 정보, 네트워크 위상(Topology)과 같은 순으로 소멸된다.

(2) 전원 차단 여부 결정

전원을 차단하는 것은 증거 수집 현장에 따라 유동적으로 결정되지만 일반적으로 서버의 경우는 전원을 차단하기 전에 프로세스 정보가 유실되지 않도록 Shutdown 시켜야 한다.

문서의 작성, 수정 등의 정보가 문제가 될 때에는 가급적이면 전원을 차단하고 전문가에게 분석을 의뢰하여야 하며, 네트워크에 연결되어 있는 경우에는 수시로 원격으로 접속하여 데이터의 삭제가 가능하므로 이에 대비하여 사전에 네트워크 단자를 제거하여야 한다.

(3) 증거 수집 대상에 따른 대응

다양한 증거의 종류에 따라 증거 수집을 위해 적합한 대응 방법을 결정해야 한다. 예를 들어, 개인용 컴퓨터인 경우 증거 수집을 위해 본체를 그대로 증거로 채택하거나 하드디스크를 분리하여 복제해야 한다. 그리고, 데이터가 대기업의 회계 관련 데이터베이스 또는 ERP 등 대형 컴퓨터에 저장되어 있는 경우에는 대용량성, 다중 사용자 접속, 컴퓨터 운영체제의 다양성 등으로 전문가의 도움을 받아 상황에 따른 적절한 증거 수집이 이루어져야 한다.

ISP(Internet Service Provider) 혹은 일반 기업에서 사용되는 서버의 경우는 전원을 차단할 때 서비스가 중단되므로 적절한 증거 수집 및 보존 수단을 고려하여야 한다. 특히, 다수의 사용자가 접속하는 대형 시스템의 경우 전산 시스템 자체를 압수하게 되면 선의의 피해자가 생길 수 있기 때문에 필요한 데이터를 현장에서 추출하고 별도의 저장장치에 복사하거나 양이 적은 경우는 프린터로 출력한다.

(4) 증거 수집

일단 증거의 위치나 수집 순서가 결정되면 증거 수집 프로그램 및 도구를 사용하여 사건과 관련성이 있는 데이터를 중심으로 증거를 수집하여야 한다. 증거 수집 과정에서 중요한 것은 수집한 매체의 종류에 따라 PC, 서버, 이동형 저장매체 등의 출처, 사용자, 관련부서, 연락처 등을 정확히 기재하여 나중에 혼동

되는 일이 없도록 해야 하며 라벨을 부착하는 것이 좋다. 이때 증거 데이터의 타임스탬프나 서명한 문서 등을 반드시 포함시켜야 한다. 증거 수집 과정에서 사용한 도구의 이름, 버전, 분석과정, 시간, 산출 결과 등 전 과정도 기록하여야 한다(Middleton, 2001).

3) 증거 분석 단계

(1) 데이터 복구 및 증거 분석

디지털 증거를 추출하기 위해 암호 복구, 데이터 복구, 키워드 검색 및 정보 추출, MAC Time 분석 등 다양한 포렌식 도구를 사용하여 증거물을 과학적이고 기술적으로 분석하여야 한다. 숨겨진 파일, 삭제된 파일, 확장자가 변경된 파일, 암호화된 파일, 일반적으로 데이터를 저장하지 않는 공간에 감춰진 파일 등 은닉된 파일을 조사하고, 복구된 파일은 별도로 보관한다(Marcella, et al., 2002).

(2) 결과에 대한 보고서 작성

증거는 재판의 모든 것이라고 할 수 있다. 따라서 분석된 증거를 법정에 정확하고 충분하게 전달하는 것도 매우 중요한 일이다. 분석 결과를 비전문가가 보아도 이해할 수 있을 정도로 간단하고 쉽고 명료한 상태로 보고서가 작성되어야 한다. 즉, 보고서는 신뢰성이 있어야 하며 기술적으로 비전문가인 법관이나 관계자가 보아도 쉽게 이해가 되어야 한다.

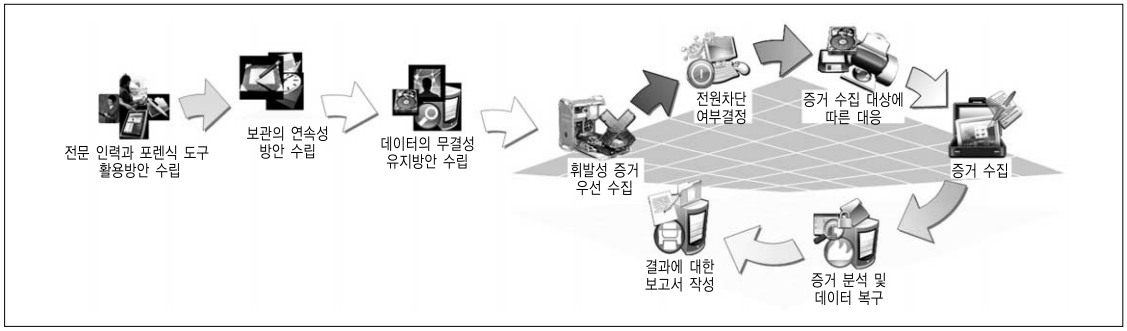
〈그림 7〉은 앞서 설명한 디지털 포렌식의 절차를 그림으로 설명한 것이다.

Ⅳ. 결론

우리나라는 정보 인프라의 구축을 위해 과감한 투자를 해왔고 이제는 그러한 발전에 힘입어 전세계 IT 분야를 선도하며 도약하고 있다. 이러한 정보기술의 발전과 하드웨어의 첨단화에 따라 법정에서 가장 중요한 증거도 대부분 디지털화 되고 있다. 미국 FBI에서 "현대 사회의 기업에서 생산되는 정보의 93%가 디지털 형태로 생산된다."고 발표한 바 있다. 수사기관이 수집하고 법정에서 활용되는 거의 모든 증거가 디지털 증거라고 할 수 있을 정도이며, 또한 수많은 컴퓨터와 네트워크가 디지털 증거를 저장하는데 사용되고 있다. 따라서 이를 입증하는 방법으로 법정 제출용 디지털 증거를 수집하는 기술인 디지털 포렌식이 필요하게 되었다.

1. 디지털 포렌식 산업 육성 방안

디지털 포렌식 기술이 활용되는 산업 분야는 크게 포렌식 소프트웨어 산업과 하드웨어 산업으로 분류될 수 있다. 포렌식 하드웨어 산업 분야는 법정 제출용 디지털 증거의 훼손을 방지하는 장치를 개발하는 분야이다. 예를 들면, 전자매체에 기록된 데이터를



〈그림 7〉 디지털 포렌식의 절차

파괴할 수 있는 자기장으로부터 분리가 가능한 장치, 하드디스크를 빠른 속도로 복제할 수 있는 장치, 디지털 증거의 훼손 없이 오랜기간 저장할 수 있는 장치, 개인 분석용 포렌식 관련 기능이 내장된 서버, 이동성을 가지고 현장으로 휴대하고 가서 분석가능하고 다양한 기능을 제공하는 포렌식 가방 등 새로운 형태의 장치 개발이 절실히 요구된다.

포렌식 소프트웨어 산업 분야는 법정 제출용 디지털 증거의 수집 및 분석을 위한 여러 가지 소프트웨어를 개발하는 분야이다. 주로 현장에서 증거의 수집, 증거의 분석, 증거의 무결성 입증, 증거의 분석과정의 연속성 기록, 디지털 포렌식 전과정에 대한 보고서 작성 등을 위한 소프트웨어의 개발이 요구된다.

현장에서 확보된 데이터로부터 정제를 통해 유용한 증거를 추출하기 위하여 저장매체에서 삭제된 파일 복구, 키워드 혹은 자연어 기반의 검색, 다양한 단어를 분류하고 정렬하는 인덱싱, 원본의 수정 또는 변경 없는 복제, 로그 기록 및 분석 기술 등이 디지털 포렌식에서 요구되는 주요 소프트웨어 기술이라 할 수 있다. 이와 같이 저장매체, 운영체제, 데이터베이스, 네트워크 기술 등 기존의 IT 기술이 포렌식과 연관성을 갖고 디지털 포렌식 영역내에서 포렌식 기관의 수요에 맞는 형태로 적응하여 발전되어야 한다.

국내의 디지털 포렌식 산업은 아직 시작단계에 있으며 아직 해결해야 할 과제가 많다. 첫번째, 법정에서 객관성이 인정되고 또한 주로 사용되고 있는 디지털 포렌식 도구들은 대부분 미국 등 국외에서 개발된 것들이다. 국내에서도 관련 기술 개발이 시작되었으나 실제 디지털 포렌식 산업 분야에서 활용될 수 있는 신뢰성 높은 도구의 개발을 위해서는 정부 차원의 국산화 지원 정책이 요구된다.

두번째, 검찰청, 경찰청 등의 수사기관의 폐쇄적 성향으로 인해 기관 간의 협조 체제가 미비하다. 각 기관마다 디지털 포렌식 기술 개발을 위한 독자적인 정책을 수립하여 추진 중이나 법원, 검찰청, 경찰청, 국정원, 감사원 등의 관련 기관들이 중복 투자를 줄이고 디지털 포렌식 산업의 활성화를 앞당기기 위해서는 서로간의 대화와 협의를 통해 국가적 차원의 관련 표준 개발 및 법제도 강화에 힘을 모아야 한다. 포렌식 증거력에 대한 최종 판단을 하는 법원의 의견뿐만 아니라 소추 제기를 전담하는 검찰청, 수사를 담당하는 검찰, 경찰, 국정원, 기무사 등 각 기관의 의견이 모두 반영된 표준화 모델이 만들어져야 할 것이다.

세번째, 기술적으로 복잡하고 난해하여 디지털 포렌식을 위한 분석가의 전문성이 매우 중요함에도 불구하고 국내 디지털 포렌식 전문 인력은 상당히 부족한 실정이다. 법원, 수사기관, 조사기관, 그리고 일반 기업을 포함하여 다양한 포렌식 관련 기관은 외부의 전문가를 채용하고 외부 자문위원을 위촉하며 내부의 포렌식 전문가를 다양한 외부 교육과정에 적극 참여시켜 디지털 포렌식을 위한 IT 기술에 대한 전문성을 더욱 높일 수 있도록 해야 한다.

2. 디지털 포렌식 전문 인력 양성 방안

국내 디지털 포렌식 전문 인력의 체계적이고 효과적인 양성을 위해서 크게 두가지의 방안을 소개한다. 본 논문을 빌어 필자가 제안하는 디지털 포렌식 전문 인력 양성 방안은 IT 전문 인력을 중심으로 양성하는 방안과 수사 전문가를 중심으로 양성하는 방안이다.

첫번째, IT 분야별로 기술 능력이 인증된 전문 인력을 중심으로 형법 및 형사소송법, 수사학 등 기초적인 포렌식 분야의 기술에 관하여 일정 기간 교육하여 인력을 양성하고, 국가기관이나 민간기관에서 필요시 인력 아웃소싱을 통하여 활용하는 방안이다. 이러한 방안은 수사기관이 아닌 제 3자에 의하여 증거를 수집함으로써 증거 수집에 대한 객관성을 높이고 증거의 변경 및 조작에 대한 시비를 좀 더 안전하게 방지할 수 있다는 장점이 있다.

두번째, 수사기관에서 증거 수집 활동을 한 경험자를 중심으로 디지털 포렌식 인력을 양성하는 방안이

다. 이들은 포렌식의 기본 개념을 잘 알고 있는 반면, IT 전반적인 기술과 전문영역에 대한 이해가 부족하므로 운영체제론, 데이터베이스론, 데이터구조론 등 IT 전문분야별 기술에 관하여 일정 기간 교육하여 디지털 포렌식 전문가로 활동하도록 한다. 이러한 방안은 정예 인력으로 포렌식 분야의 증거능력을 높일 수 있는 전문가의 양성이 가능하다는 장점이 있다.

활발한 국내 IT 분야에서 전문 인력이 풍부하고 고부가가치 창출을 위한 새로운 솔루션에 대한 기대치가 높다는 관점에서 첫번째 인력 양성 방안은 우수한 다수 인력의 활용이 가능하다는 점과 짧은 시간에 인력 양성이 가능하다는 장점을 갖는다. 또한, 국내에서 수사기관의 증거에 대한 객관성이나 무결성에 대한 문제는 큰 약점일 수밖에 없었다. 이러한 문제를 제 3자가 참여함으로써 좀 더 신뢰성과 객관성 있는 증거의 수집이 가능하고, 해당 분야의 전문가의 활용을 통해 디지털 포렌식의 전문성을 한층 높을 수 있을 것이다. 그러나 포렌식 교육을 이수한 IT 전문 인력이라고 하더라도 수사기관의 특성을 이해하는데 어려움이 있을 수 있으므로 가능하면 수사기관의 직원과 함께 작업하는 것이 바람직할 것이다.

두번째 인력 양성 방법은 IT 분야의 기초이론과 전문분야의 이론을 갖추기 위해서 최소한 3년에서 5년의 긴 시간이 필요하다는 단점을 갖는다. 또한, 지금까지 국내의 수사기관 종사자가 많지 않다는 점도 근본적인 취약점이라고 할 수 있다. 그러나, 기존의 수사 경험을 기반으로 디지털 포렌식 수행 시 총체적 요구사항을 이해하고 있는 전문가가 다양한 IT 기술과 요소 기술에 대한 전문 지식을 배양함으로써 디지털 포렌식을 위한 수행 인력이 늘어나게 되고, 실제 관련 작업의 규모가 커질수록 이를 체계적으로 관리하여 효율성을 더욱 높일 수 있을 것이다.

3. 디지털 포렌식 분야의 전망

2004년 CSI/FBI 컴퓨터 범죄 및 보안 조사에서 컴퓨터 범죄가 널리 퍼지면서 증명할 수 있는 손실액이 백만 달러에 이른다고 발표되었고(Gordon, et al., 2004), 2006년 USA Today 기사에서는 1년 동안의 컴퓨터 범죄에 의한 손실액이 670억 달러를 넘는다고 발표하고 있다(Acohido, 2006). 컴퓨터를 이용한 범죄가 늘어나고 그에 따른 재정적 손실이 커지면서 디지털 포렌식의 숙련된 기술자와 전문적인 도구들에 대한 요구사항은 점점 커지고 있다(Carrier, 2003; Vanston, et al., 2004).

세계적인 시장 조사 회사인 IDC(International Data Corporation)가 컴퓨터 포렌식을 포함하는 사고 대응 서비스 시장을 2001년에 133백만 달러에서 2004년 284백만 달러로 성장할 것이라고 전망하였듯이 디지털 포렌식 분야의 시장은 계속해서 확대되고 있다(LeClaire, 2003). 최근 미국을 중심으로 디지털 포렌식과 관련된 다양한 영역들이 연구되고 있으며 디지털 포렌식을 위한 하드웨어 및 소프트웨어를 개발하는 관련 기업들도 폭발적으로 늘어나고 있는 추세이다(Moore, 2006; Richardson, 2006; Ryan, et al., 2003).

디지털 포렌식 분야의 표준화를 위해 국제적으로 활발한 연구가 진행되고 있다. 1995년에 설립된 IOCE (International Organization on Computer Evidence)를 시작으로 많은 국가들이 디지털 증거의 정의, 디지털 증거를 과학적으로 다루기 위한 원칙(Principle) 및 절차(Procedure) 등에 대한 표준 문서를 개발하고자 노력하고 있다. 대표적으로, 미국을 중심으로 1998년에 설립된 SWGDE(Scientific Working Group on Digital Evidence)는 1999년에 발표된 "Proposed Standards for the Exchange of Digital Evidence", 2006년에 발표된 "Data Integrity Within Computer Forensics", "Best Practices for Computer Forensics" 등 디지털 증거의 복구(Recovery), 보존(Preservation), 조사(Examination)에 대한 지침(Guideline)과 표준을 위한 많은 문서를 개발하여 공개하고 있다(SWGDE,

2006).

FIT-WG(Forensic Information Technology Working Group)는 유럽 ENFSI(European Network of Forensic Science Institutes)의 후원으로 1998년에 설립되었으며 2004년에 발표된 "Performance based Standards for Forensic Science Practitioners", 2005년에 발표된 "Guidance on Best Practice for Management of Case Handing System in Forensic Laboratory" 등 디지털 포렌식 수행을 위한 절차와 데이터 보호 및 보고에 관한 지침을 위한 문서를 개발하여 공개하고 있다(ENFSI, 2006).

국내에서도 IT 관련 기업뿐만 아니라 일반 사용자들 사이에 컴퓨터 보안과 지적 재산권에 대한 관심이 매우 높아졌고, 네트워크 보안, 시스템 보안 등 보안과 관련된 기술 개발이 활발하게 진행 중이며, 특히 디지털 포렌식의 표준 개발을 목표로 하는 협회도 등장하여 활동 중에 있다. 또한, 디지털 관련 시장 확대에 대한 기대와 고급 기술을 소지한 전문가에 대한 요구사항의 증대를 고려할 때, 향후 3년~4년 내에 디지털 포렌식 수행의 표준 절차에 대한 모델을 수립하고 효과적인 전문 인력 양성을 통해 디지털 포렌식 수행을 위한 기술적 인프라뿐만 아니라 사회적 인프라를 구축할 수 있으리라 예상된다.

디지털 포렌식 기술은 범죄수사 뿐만 아니라 첨단 기술 유출 방지, 지적재산권보호 등을 위하여 적극 활용될 수 있다. 다가올 미래에는 디지털 포렌식의 활용 범위가 더욱 넓어지고 전문화되어 IT 영역의 큰 줄기 중 하나가 될 것이다. 디지털 포렌식 기술이 활용될 수 있는 기관은 법원, 수사기관, 조사기관, 그리고 일반기업으로 분류된다. 법원은 재판과정에서 최종기관으로 증거력의 유무를 판단하고 죄의 유무를 결정하는 기관이다. 수사기관이란 검찰청이나 경찰청, 기무사, 국정원과 같은 기관으로 과거부터 현재까지 증거 수집과 관련된 업무를 지속적으로 수행하여 온 기관을 말하며 최근에는 디지털 포렌식 기술을 도입하여 많은 발전을 거듭하고 있다. 조사기관은 국세청, 감사원, 공정거래위원회 등이 해당되며 포렌식의 개념을 도입하지는 않았지만 유사한 개념을 도입하여 활용하고 있고 지속적인 약진을 거듭하고 있다.

일반 기업은 IT 보안 관련 기업, 손해보험 및 생명보험회사의 사고조사반, 대기업의 감사실, 법무법인의 증거 분석팀, 변호사 사무소, 회계 법인의 회계 분석팀, 회계사 사무소, 첨단기술을 보유하고 있는 대기업의 법무팀, 첨단기술연구소의 기술 유출방지를 위한 감사팀 등이 해당되며, 뒤늦게 출발하여 현재 많은 준비와 투자를 하고 있으며 가장 성장 잠재력이 큰 분야이기도 하다.

디지털 포렌식 분야의 발전은 국가나 기업의 중요 기술의 유출 방지를 통해 국가와 기업의 재산과 권익을 보호하며, 적법한 절차에 의한 증거력의 확보는 국력 신장과 함께 인권 보호에도 크게 기여할 것이다. 즉, 수사의 전 과정에 디지털 포렌식에 의한 증거 확보 및 분석과 같은 과학적 수사기법이 정착되면, 피의자의 자백이나 진술을 얻는 것으로 무리한 수사를 진행하던 과거와는 달리 포렌식 기술의 활용을 통해 적법한 절차에 의해 명확한 증거를 확보하고 궁극적으로는 피의자 및 피고인의 인권을 보장함으로써 컴퓨터 범죄로 부터 국민의 불안을 해소시킬 수 있게 될 것이다.

결론적으로 최첨단 정보기술에 바탕을 둔 디지털 포렌식의 발전은 사법 환경의 변화와 함께 국민의 인권 보장에도 크게 기여할 것이다. 정보기술 업체와 소프트웨어 개발자, 정보보호 기술 전문가들의 적극적인 참여를 통해 새로운 포렌식 시장을 창출하고 포렌식 시장의 더 큰 발전과 확대를 기대할 수 있다. 또한, 앞으로 국내의 발전된 디지털 포렌식 기술을 해외로 역수출할 수 있는 그날까지 디지털 포렌식 분야의 무궁한 발전도 기대할 수 있다.

■ 참고문헌

김종섭 (2003).「디지털 증거의 신뢰성 보증 모델」. 박사학위논문, 경기대학교 대학원.

박윤해 (2005).「컴퓨터 범죄에 관한 연구」. 박사학위논문, 숭실대학교 대학원.

서희명 (2005).「로그분석과 포렌식 모델 적용을 통한 리눅스 시스템 포렌식 기법에 관한 연구」. 석사학위논문, 연세대학교 대학원.

이임영 (2006). "디지털 증거 분석을 위한 포렌식." http://www.dbguide.net/know /know104001.jsp?mode=view&order=reg_date&by=desc&pg=6&idx=2764 (검색일: 2006. 11. 04).

이종상 (2000).「컴퓨터 데이터 압수 · 수색에 관한 연구」. 석사학위논문, 서울대학교 대학원.

최득신 (2005).「컴퓨터 포렌식에 관한 연구」. 연구논문, 대검찰청.

Acohido, B. (2006). "Cybercrime Robs $67.2 Billion a Year." http://www.crime-research.org/news/10.12.2006/2290/ (검색일: 2006. 11. 03).

Caloyannides, M.A. (2001). *Computer Forensics and Privacy.* Boston: Artech House.

Cambridge University Press (2006). "Forensic Definition." http://dictionary.cambridge.org/define.asp?key=30477&dict=CALD (검색일: 2006. 10. 02).

Carrier, B. (2003). "Open Source Digital Forensics Tools: The Legal Argument." http://www.digital-evidence.org/papers/opensrc_legal.pdf (검색일: 2006. 11. 03).

Casey, E. (2000). *Digital Evidence And Computer Crime.* New York: Academic Press.

Casey, E. (2001). *Handbook Of Computer Investigation Forensic Tools and Technology.* New York: Academic Press.

ElcomSoft (2006). "Password Recovery Software." http://www.elcomsoft.com/prs.html (검색일: 2006. 11. 02).

ENFSI (2006). "Forensic Information Technology Working Group." http://www.enfsi.org/ewg/fitwg/ (검색일: 2005. 11. 01).

Ford, W. (1993). *Computer Communications Security Principle Standard Protocols and Techniques.* New Jersey: Prentice Hall PTR.

Garfinkel, S.L. & Shelat, A. (2003). "Remembrance of Data Passed: A Study of Disk Sanitization Practices." *IEEE Security and Privacy,* 1(1): 17-27.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. & Richardson, R. (2004). "2004 CSI/FBI Computer Crime and Security Survey." http://www.theiia.org/download.cfm?file=9732 (검색일: 2006. 11. 02).

Guidance Software (2006). "EnCase Forensic Manuals." http://www.guidancesoftware.com/support/downloads.asp (검색일: 2006. 10. 01).

Herath, A., Herath, S., Samarasinghe, P., Herath, J. & Herath, S. (2005). "Computer Forensics, Information Security and Law: A Case Study." *Proc. First International Workshop on Systematic Approaches to Digital Forensic Engineering.* Taipei. November: 135-141.

Houghton Mifflin Company (2000). "Forensic Definition." http://www.bartleby.com/61/42/F0254200.html (검색일: 2006. 10. 02).

Kruse, W.G. & Heiser, J.G. (2001). *Computer Forensics Incident Response Essentials.* New York: Addison-Wesley Professional.

LeClaire, J. (2003). "Computer Forensics Sees Growing Business." http://eastbay.bizjournals.com/eastbay/stories/2003/09/15/focus3.html (검색일: 2006. 11. 01).

Manzano, Y. & Yasinsac, A. (2001). "Policies to Enhance Computer and Network Forensics." *Proc. 2nd Ann. IEEE Systems, Man, and Cybernetics Information Assurance Workshop.* New York. June: 289-295.

Marcella, A.J. & Greenfield, R.S. (2002). *Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes.* Boca Raton: CRC Press.

Middleton, B. (2001). *Cyber Crime Investigator's Field Guide.* Boca Raton: CRC Press.

Moore, T. (2006). "The Economics of Digital Forensics." http://citeseer.ist.psu.edu/749301.html (검색일: 2006. 11. 04).

Northcutt, S., Cooper, M., Fearnow, M. & Frederick, K. (2001). *Intrusion Signatures and Analysis*. New York: New Riders Publishing.

Prosise, C. & Mandia, K. (2001). *Incident Response Investingating Computer Crime*. New York: McGRAW-Hill/Osborne.

Richardson, R. (2006). "The CSI/FBI Computer Crime and Security Survey: 2006." http://GoCSI.com/ (검색일: 2006. 11. 02).

Russell, D. & Gangemi, G.T. (1991). *Computer Security Basics*. Sebastopol: O'REILLY Media.

Ryan, D.J. & Shpantzer G. (2003). "Legal Aspects of Digital Forensics." http://www.danjryan.com/Legal%20Issues.doc (검색일: 2006. 11. 01).

Stephenson, P. (2004). *Investigating Computer-related Crime*. Boca Raton: CRC Press.

Stroz, E. (2003). "Handbook of Computer Crime Investigation - Forensic Tools and Technology." *Journal of Forensic Identification*, 53(3): 344-352.

SWGDE (2006). "Scientific Working Group on Digital Evidence." http://www.swgde.org (검색일: 2006. 11. 01).

TechSmith (2006). "SnagIt Screen Capture." http://www.techsmith.com (검색일: 2006. 11. 03).

Upgrade Solutions (2006). "Upgrade Solutions." http://www.upgradesolutions.com/downloads.html (검색일: 2006. 10. 02).

Vacca, J.R. (2002). *Computer Forensics: Computer Crime Scene Investigation*. Rockland: Charles River Media.

Vanston, J., Elliott, H. & Bettersworth, M.A. (2004). "Emerging Technology Programs ADM, Hybrids, Computer Forensics and MEMS." http://www.system.tstc.edu/forecasting/reports/emergingtech.asp (검색일: 2006. 11 .01).

Venema, W. & Farmaer, D. (2004). "Forensic Discovery." http://www.porcupine.org/forensics/forensic-discovery/ (검색일: 2006. 10. 02).

Visualware (2006). "VisualRoute." http://www.visualroute.com/index.html (검색일: 2006. 10. 03)

Wilsdon, T. & Slay, J. (2005). "Digital Forensics: Exploring Validation, Verification and Certification." *Proc. First International Workshop on Systematic Approaches to Digital Forensic Engineering*. Taipei. November: 48-55.

■필자소개

전상덕(Sang-Duk Jeon)
2003, 공학석사, 연세대학교
현재, 건국대학교 정보통신대학원 감리전공 겸임교수,
건국대학교 일반대학원 컴퓨터공학과 박사과정
관심분야 : 데이터베이스, 디지털 포렌식, 정보시스템 감리

홍동숙(Dong-Suk Hong)
2001, 공학석사, 건국대학교
현재, 건국대학교 일반대학원 컴퓨터공학과 박사과정
관심분야 : 데이터베이스, 텔레매틱스, 데이터베이스 포렌식

한기준(Ki-Joon Han)
1985, 공학박사, KAIST
현재, 건국대학교 컴퓨터공학부 교수, 한국정보시스템감리사협회 회장
관심분야 : 데이터베이스, GIS, LBS, 텔레매틱스, 정보시스템 감리