제21회 한국정보처리학회 춘계학술발표대회 논문집 제11권 제1호 (2004. 5)

법적 증거능력 및 증명력을 위한 컴퓨터포렌식에 관한 연구

이도영*, 김일곤**
고려대학교 컴퓨터과학기술대학원 컴퓨터공학과 *
고려대학교 컴퓨터학과 **
e-mail : leesheen@korea.ac.kr, igkim@formal.korea.ac.kr

A Study on Computer Forensics for the Legal Evidence Effect and the Proof

Do-Yeong Lee *, Il-Gon Kim **
*Dept. of Computer Science ,Graduate Schools of Computer Science & Technology, Korea Univ. *
*Dept of Computer Science & Engineering, Korea Univ. **

요 약

컴퓨터가 현대 생활의 필수 도구로 자리잡으면서 컴퓨터를 매개로 이루어지는 범죄행위에 대하여 법적인 처벌 문제가 중요하게 대두되고 있다. 컴퓨터범죄를 형사적으로 처벌하기 위하여는 디지털증거의 증거능력과 증명력이 인정되어야만 한다. 하지만 디지털증거는 그 특성상 조작, 손상, 멸실의 우려가 높다. 디지털증거가 형사소송법상 유효한 증거로서의 증거능력을 인정 받기 위하여는 데이터의 변형 없이 수집하고 때로는 손상된 디지털 증거를 복구하여 원본과 동일하게 복사하여 정확히 분석한 후 제출되어야 한다. 이와 관련된 학문 전반을 컴퓨터포렌식이라고 하는데 국내법 혹은 국제법적으로 유효한 절차 및 수단에 따라 관련 증거들을 수집하여 함은 물론이고 과학적인 논거들로 입증하는 것이 또한 매우 중요하다. 현재 국내법상 디지털증거에 관한 입법이 없으므로 일반적인 증거증력에 관한 규정과 일부 판례를 차용하여 증거능력과 증명력을 갖춘 컴퓨터포렌식 절차를 제안 한다.

1. 서론

컴퓨터와 초고속 인터넷 망의 보급 확대는 우리의 생활을 편리하게 하고 국경을 초월하여 정보교환을 할 수 있게 하는 순기능이 있다. 반면에 컴퓨터를 이용한 범죄의 급격한 증가라는 역기능을 가져왔다. 또한 몇몇 범죄들은 사회 이슈화 되어 큰 파장을 불러왔다. 컴퓨터 범죄는 이제 생활 깊숙이 자리 잡은 현실의 문제가 되었다. 컴퓨터범죄자는 배경지식의 전문성과 고도의 기술로 법망을 기민하게 회피할 뿐 아니라 새로운 범죄유형의 등장으로 인한 처벌법규의 미비라는 한계를 최대한 이용하기도 한다.

컴퓨터를 범죄로부터 보호하기 위하여는 지속적인 범죄 추적과 형사처벌이 중요하다. 이러한 필요에 따라 우리 나라에서도 1995 년 형법개정을 통하여 전자기록 위작, 변작죄 등과 같이 컴퓨터범죄를 처벌할 수 있는 규정을 삽입하였으며, 「정보통신이용촉진및정보보호에관한법률」을 제정, 개정하여 명문으로 컴퓨터 범죄를 처벌할 수 있는 근거를 마련하였다.

하지만 현행 형사소송법에는 컴퓨터범죄의 증거조사와 증거능력에 대한 명문의 규정이 없다. 따라서 어렵게 수집한 디지털증거가 법적인 증거능력을 인정받을 수 있도록 하기 위하여 증거수집과 보존, 복원을 위한 과학적인 연구 뿐만 아니라 법적 절차에 관한 연구 및 제안도 시급하다.

본 연구의 구성은 다음과 같다. 2 장 관련 연구에서는 현대사회의 컴퓨터범죄에 대한 고찰과 컴퓨터포렌식에 대한 연구 및 문제점을 도출하였고, 3 장에서는 형사소송법상 유효한 증거 및 판례에 대하여 연구

하였다. 4 장에서는 이에 따른 포렌식 절차 및 제반환경을 제언하였으며, 5 장에서는 결론 및 향후 연구방안을 서술하였다.

2. 관련연구

컴퓨터를 이용한 범죄가 증가하는 것 만큼, 범죄를 구체적으로 규정하고 증거를 찾아서 범죄를 입증하기 위한 다양한 노력들이 진행중이다. 아래에서는 증거보전을 위한 방법론인 컴퓨터포렌식에 대하여 자세히 살펴보도록 한다.

2.1 컴퓨터범죄의 개념

컴퓨터범죄는 컴퓨터 자체가 범죄의 대상이 되는 경우와 컴퓨터가 범죄 행위의 도구로 이용이 되는 경우가 있다. 컴퓨터범죄의 기술에는 위장 기법(Spoofing method), 스니핑 기법(Sniffing method), 도청기법(Wiretapping method), 트랩도어(Trapdoor), 백도어(Backdoor), 트로이 목마(Trojan horse), 서비스 거부(Denial of Service), 사이버 사기(Cyber fraud) 등이 있다.

컴퓨터범죄는 피해자가 피해를 인식하지 못하는 경우도 있고, 피해를 인식한 경우라 할지라도 거래의 신용도나 명예의 실추를 우려하여 외부에 피해 사실을 알리지 않는 경우도 많아 수사기관의 범죄사실 인지와 범죄발생 초기의 증거 수집에 어려움이 많다.

2.2 컴퓨터포렌식 연구

컴퓨터포렌식이란 컴퓨터를 매개로 이루어지는 범죄행위에 대한 법적 증거 자료 확보를 위하여 컴퓨터 저장 매체 등의 컴퓨터 시스템과 네트워크로부터 자료(정보)를 수집, 보존, 복구 및 분석하여 법적 증거물로서 제출할 수 있도록 하는 일련의 행위를 의미한다. 범죄자체는 컴퓨터와 관련 없으나 범죄의 증거가 될만한 사실이 컴퓨터에 저장되어 있는 경우도 그 대상이 될 것이다.

컴퓨터포렌식 연구의 목적은 컴퓨터범죄를 행하는 범죄자를 신속, 정확히 찾아내고 범죄행위에 이용된 증거 확보를 통한 법적 대응을 가능하게 하여 궁극적으로는 컴퓨터 범죄를 지속적으로 감소 시키는데 있다.

2.2.1 디지털증거의 수집 및 보존

디지털증거 수집 및 보존시 가장 우선적으로 고려되어야 할 사항은 어떤 형태로든 조작 또는 훼손되지 않도록 보호하는 것이다. 데이터 수집의 순서는 휘발성이 큰 데이터부터 비휘발성 데이터 순인데 레지스터와 캐시 등 휘발성 강한 정보, 라우팅 테이블 등 네트워크 정보, ARP 캐시, 프로세스 테이블, 커널 통계, 시스템 메모리의 내용, 임시 파일 시스템, 디스크의 데이터에 담긴 전자 메일, 웹, 프로그램의 원시코드 등, 데이터베이스 및 파일시스템, 기타 PDA, 전자수첩, 휴대폰 등 모바일 기기 및 각종 백업장치 순서이다. 그 외에 일명 잊혀진 데이터로 불리는 웹캐시와 URL 히스토리, 각종 임시파일, 스왑 파일과 페이지 파일 등을 수집한다.

수집된 데이터를 보호하기 위해서는 디스크 이미징 등을 통한 정확한 사본을 만드는 것이 중요한데 디스크의 구조와 상대 위치 등이 정확한 비트스트림 사본의 형태로 원본과 동일하게 작성되어야 한다. 데이터의 분석 및 복구는 사본에서 수행함으로써 원본의 조작 및 훼손 가능성 없이 정밀 조사가 가능하다. 디스크 이미징을 위한 소프트웨어는 국내외에서 여러 종류의 제품으로 개발된 것이 있으므로 제품의 특성에 주의하여 선택, 사용하면 된다.

2.2.2 디지털증거의 복구 및 분석

수집된 증거 자료는 내용의 정밀 분석이 필요하며 이미 삭제되거나 암호화 된 형태로 숨겨진 경우도 많다. 이런 경우 좀더 본격적인 컴퓨터포렌식 도구들이 필요한데 국내에서는 Final Data, TechKorea 하우리 등의 업체가 소프트웨어 또는 물리적 방법을 통해 데이터 복구를 가능하게 하는 정도이다. 해외에서는 이미징 소프트웨어, “undelete” 프로그램, 파일 텍스트 검색 프로그램, 비트스트림 사본의 정확성을 검증하는 프로그램, 데이터에서 이전 문자를 제거하여 쉽게 데이터 분석을 할 수 있게 해주는 프로그램, 캐시를 재구성하는 프로그램, 압축 해제 프로그램, 시스템검사 유틸리티, 스테가노그라피 탐지 소프트웨어, 비밀번호 복구 프로그램 등의 다양한 컴퓨터포렌식 도구들이 개발되어있다.

컴퓨터포렌식의 소요 기술로는 첫째, 백업(Backup) 기술이 있다. 파일이나 대용량 저장 장치에 저장된 자료를 물리적으로 복사하고 해쉬 함수 및 CRC 값을 이용하여 무결성 보장한다. 둘째, 데이터 검색 기술이다. 파일과 및 연관된 논리적인 정보의 내용을 분석하여 파일 특성 등의 정보를 추출한다. 셋째, 데이터 복원기술 이다. 손실된 데이터로부터 침입자의 흔적 확인을 위해 데이터 복원한다. 넷째, 로그분석 기술 이다. 웹 브라우저 로그, 메일 로그, FTP 로그, 시스템 부팅 로그 등을 분석하고 침입 방법, 침입 시스템의 IP 등 확인한다. 다섯째, 암호분석 기술 이다. 접근 제어된 데이터의 패스워드를 크래킹하고 암호 알고리즘을 통해 암호문의 의사 난수성을 이용하여 판별 가능 하도록 한다. 여섯째, 증거물 검증 기술 이다. 조사가 완료된 증거물의 변경 여부 검증하고 원본과 복사본 데이터의 해쉬값 및 CRC 값을 지정하여 각각의 값을 비교 한다. 일곱째, IP 추적 기술 이다. 로그파일 분석을 통해 침입 컴퓨터 및 인터넷 IP 추적 한다.

2.2.3 디지털증거의 제출

법정에서 증거로서 채택되기 위해서는 일정한 형식을 갖추어서 제출되어야 한다. 증거물품은 6 하 원칙에 따라 수집된 경위와 제출까지의 관리단계가 정확히 기록되어야 한다. 제출시 꼬리표 등 식별 가능한 표식이 필요하며, 디지털증거의 특성상 전자인증 등의 방법이 사용될 수도 있다.

또한 제출되는 증거의 내용을 분석한 문서와 분석

된 내용이 의미하는 것, 어떤 절차를 거쳐서 분석되었는지에 등의 설명도 있어야 한다. 법관은 제출된 증거 문서를 기반으로, 증거능력을 인정할지 여부와 어느 정도의 증명력을 부여할지를 결정한다. 따라서 증거의 확실성을 증언할 과학적 증빙 문서를 명확히 작성하여 첨부 하는 것이 중요하다. 극단적으로는 단 한 사람의 전문가 증언에 의해서 모든 내용이 증거로 인정되거나 거부될 수 도 있다.

3. 형사소송법상의 증거능력

우리나라 형사소송법상에는 디지털증거에 대한 별도의 내용은 없다. 그러므로 디지털기록의 컴퓨터범죄 관련 증거가 어떻게 취급해야 하는가에 대한 문제는 기타 다른 증거에 대한 규정과 과학적 증거들에 대한 유사한 판례를 통해 유추할 수 밖에 없다.

3.1 증거능력과 증명력

증거능력이란 증거가 엄격한 증명의 자료로 사용될 수 있는 법률상의 자격을 말하며 증거의 실질적 가치를 의미하는 증명력과 구별된다. 증거능력은 미리 법률에 의하여 결정되어 있는 것이고, 증명력은 법관의 자유심증에 맡겨져 있다. 증거능력 없는 증거는 사실인정의 자료가 될 수 없을 뿐만 아니라, 공판정에 증거로 제출하여 증거조사를 하는 것도 허용되지 않는다. 하지만 앞서 언급한대로 디지털증거에 대한 명문규정이 없는 탓에 실무적으로 법관에게 많은 부분이 위임되어 있고 디지털증거의 지위가 불안해지는 근본원인이 되고 있다.

현행 소송법상 증거수집은 수사기관에 의한 임의수사(피의자심문, 감정·통역·번역의 위탁, 임의영치 등)가 원칙이나, 영장에 의한 강제수사(법관이 발부한 구속영장·압수수색영장 등)도 가능하다. 영장 없는 강제수사는 증거능력이 배제되며 전문증거(傳聞證據) 또한 증거능력이 없다. 즉, 수사기관에 의해 적법하게 수집된 범죄와 관련된 증거는 증거능력을 가지게 된다. 이후 채택된 증거가 범죄에 대한 증명력을 가지는지 여부는, 다른 모든 형사소송과 마찬가지로, 자유심증주의 원칙에 의거해서 법관 자신의 논리와 경험칙에 따라 판정하게 된다.

3.2 과학적증거에 대한 판례의 입장

디지털증거와 같이 새로운 과학적 원리에 입각한 증거가 법정에 제출되면, 법원으로서는 이 증거의 타당성에 대하여 쉽게 사법적 확인을 할 수 없고, 당연히 전문가증인의 증언에 의해서 그 타당성을 확인한다. 이때 법관은 어떤 원칙에 의해서 과학적 증거를 수용하는지에 대한 논란이 있다. 디지털증거와 마찬가지로 과학적증거로 분류되는 유전자감정결과에 대한 판례를 통해 우리나라 법원의 태도를 대략 알 수 있다.

광주고등법원 제주부 1997.12.5. 선고 97 노 58 판결에서는 유전자감정결과의 증거능력을 인정하기 위해 감정인이 충분한 전문적인 지식경험과 기술수준을 가지고 있어야 하고, 감정자료는 적절히 관리되어 보전되어야 하고, 감정에 사용될 정도로 양적으로 충분하여야 하며, 검사기법은 그 당시 일반적으로 확립된 표준적인 검사기법을 사용하여야 하고, 객관적인 방법에 의하여 조작과 검사결과에 대한 분석이 이루어질 것 등의 요건을 갖추어야 할 것을 제시하였다. 디지털증거를 판정함에 있어서도 위의 원칙에서 크게 벗어나지 않는다고 유추해 볼 수 있다.

하지만 법관은 이전 판례를 단지 참고만 할 뿐이지 이에 구속되어 판결할 의무가 없다. 따라서 비록 과학적 진실이라 하더라도, 공판정에서 법관을 충분히 설득하지 못한다면 증거에서 배제될 수 도 있으며, 비슷한 증거에 대하여 서로 다른 판결이 내려질 수도 있다. 해당 결정은 재심의 사유도 되지 않으므로 심대한 불확실성에 노출되었다고 할 수 있다.

4. 증거능력인정을 위한 포렌식 절차 제안

앞서 우리는 범죄증거를 수집하기 위한 과학적 방법들과 형사소송법상의 증거능력과 증명력에 관하여 살펴보았다. 유감스럽게도 과학적으로 유의미한 것이 항상 법적으로도 동일한 의미를 가지는 것은 아니다. 법적으로는 증거의 내용보다 형식이 훨씬 더 중요할 수 있다. 따라서 애써 수집,보존,복원한 자료들이 범죄를 증명하는 도구에서 배제되는 문제를 사전에 방지하기 위하여 법적 절차에 따른 과학적 연구가 중요하다. 따라서 아래에서는 사고대응팀 또는 수사기관이 취해야 할 절차를 단계별로 제안하기로 한다.

4.1 단계별 대응 및 증거수집 절차

첫째, 사전 대응 단계이다. 컴퓨터범죄를 대비해서 사고대응팀을 두고 사고발생시 처리 절차를 명문화하여 충분히 숙지해둘 필요가 있다. 예를 들어 기업체의 경우 사고 발생시 직원들의 업무용 컴퓨터등에 관한 압수, 수색에 관한 서약을 미리 받아두면 차후 법적 논란을 방지할 수 있다.

둘째, 1 차 대응 단계이다. 1 차 대응자는 범죄현장을 구분하고, 현장을 보호하고 임시증거와 사라지기 쉬운 증거를 보존하는 역할을 한다. 범죄현장에 변화를 주지 않는 것이 중요한데, 부득이한 경우에는 처리한 작업의 내용을 시간대별, 기능별, 처리자별로 소상히 기록해둘 필요가 있다. 또한 변경전의 상황을 카메라로 촬영해 두거나 자세히 메모를 해두어서 법정에서 증언할 수 있도록 한다. 시스템의 스풀, 갭쳐, 덤프기능 등을 이용하여 자신의 작업내용을 기록하는 것도 좋은 방법이다.

컴퓨터 범죄의 특성상 수사기관에 의뢰하기 전에 중요한 범죄증거를 채증 해야 하는 경우가 많으므로 사전 명문화된 절차와 준비된 장비로 신속, 정확히 행동하는 것이 중요하다. 불필요한 행동을 최소화 함으로써 위변조에 대한 의심을 최소화 시키고 불의의 데이터 변경 등을 막을 수 있다.

셋째. 수사기관의 증거수집 단계이다. 증거수집 단계에서 가장 중요한 것이 수사자의 처리내용과 증거

가 수집된 경위를 가능한 상세히 기록하는 일이다. 기록된 내용은 자체로서 법정 증거로 채택될 수도 있고 수집된 증거의 신뢰도를 높여 줄 수 도 있으며 혹시 수사자의 잘못으로 수집과정에서 일부 데이터의 변경이 가해졌을 때 증거전체의 신뢰도가 저하되는 것을 방지할 수 도 있다.

따라서 모든 방법을 동원한 빠짐없는 기록이야 말로 증거로서 가치는 높이는 가장 확실한 방법이다. 작업에 대한 기록은 조작 여부를 보다 쉽게 판단할 수 있는 아날로그 방식이 좋다. 증거수집을 위해서 사용되는 하드웨어 및 소프트웨어는 범죄에 사용된 컴퓨터 이외의 것 중에서 업계 또는 학계에서 널리 인정을 받거나 국가정보원 등에서 검증한 제품을 준비해서 사용하도록 한다.

또한 법정증언의 경우 2 인 이상의 성인이 동일한 내용을 증언할 때 보다 신뢰성 있는 증언으로 채택되는 경우 등이 있는데 이처럼 일반적으로 법관에게 보다 높은 확신을 줄 수 있을만한 최대한의 방법을 동원한다.

4.2 증거분석, 제출, 입증방안

디지털 증거를 분석하기 위한 요구 사항으로는 첫째, 기밀 유지 조치가 취해진 매체를 사용해야 한다. 둘째, 원시 매체(original media)의 무결성이 유지되어야 한다. 따라서 디스크 이미징 작업등을 할 때는 사본을 저장하는 매체가 완전 무결한 원시 매체라는 것이 증명된 것을 사용해야만 한다. 셋째, 검사대상 매체에 대한 기록은 명확한 하드웨어와 소프트웨어의 통제 속에서 이루어져야 하며 일정한 형식에 따라 사용된 도구를 명문화할 필요가 있다. 넷째, 검사결과의 출력정보 및 기타 결과 내용은 적절히 서명, 통제, 전달되어야 한다. 검사결과가 증거로서 인정되기 위하여는 문서 또는 기타의 증거력을 가진 형태로 변환되어야 한다. 물리적인 디지털증거를 제출 할 때는 꼬리표를 달거나 표식을 남긴 뒤, 담당자, 날짜와 시간, 시건 번호를 기록해두어야 하며 증거기록을 첨부한다.

마지막으로 자신이 사용한 방식에 대하여 과학적인 근거가 되는 자료를 꼭 제출해야 하는데 권위 있는 기관 또는 개인의 보증이 필수적이다.

4.3 국가적 대응방안

현재의 형사소송법상 증거능력 규정은 디지털증거 등 과학적 자료들에 적용하기에는 매우 부족하다. 특히나 컴퓨터범죄의 경우 국내법과 국제법의 충돌로 매우 복잡한 양상을 나타낼 수 있기 때문의 법적용의 혼란을 막기 위해서라도 시급히 구체적인 입법이 뒤따라야만 한다. 디지털증거는 복잡한 과학적 지식의 산물이다. 따라서 이에 대한 판단을 법관의 논리와 경험칙에만 일임하는 것은 실체적 진실 발견에 문제일 수 있다. 법관에게 디지털증거에 관한 권위 있는 조언할만한 기관의 설립이 도움이 될 것이라고 본다.

5. 결론 및 향후 연구방안

본 연구는 형사소송법상 유효한 증거능력과 증명력을 얻기 위한 컴퓨터포렌식에 절차 대한 것이다. 날로 고도화되는 컴퓨터범죄에 대항하여 치밀한 디지털 증거의 확보와 더불어 증거의 증거능력과 증명력을 최대한 높일 수 잇는 방법을 알아보았다.

본 연구에서는 컴퓨터범죄 발생시 각 대응단계별로 행해야 할 기술적 행위들과, 해당 행위의 법적 테두리를 살펴보았다. 하지만 법규정의 미비와 사례의 부족으로 구체적인 부분에서는 논란의 여지가 있을 수 있다고 본다. 0 과 1 로서 표현할 수 있는 디지털증거의 명확성에 비하여 법관의 재량권이 넓은 법적용은 대단한 불명확성이다. 하지만 그러기에 증거로서 능력을 인정 받기 위한 보다 과학적인 연구와 기준 제시의 노력이 절실하다고 본다.

앞으로도 법규정의 정비에만 기대지 말고 과학적으로 증명할 수 있는 사실들을 더욱 적극적으로 연구 제시하여 해당분야의 예측가능성을 견인해야 할 것이다.

참고문헌

[1] Debra L. Shinder. “Scene of the Cybercrime Computer Forensice Handbook,” synress, 2002.

[2] Albert J. Marcella, Robert S. Greenfield. “Cyber Forensics a field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes,” Auerbach Publications, 2002.

[3] Stephen Northcutt, Judy Novak, “Network Intrusion Detection Third Edition,” New Riders, 2002.

[4] The Honeynet Project, “Know Your Enemy,” Addison-Wesley, 2001.

[5] Eoghan Casey, “Digital evidence and computer crime,” Academic press, 2003.

[6] 이현우, 심정재, “사례로 배우는 해킹사고 분석 & 대응”, 영진출판사, 2004.

[7] 국정원, 국가정보보호 백서, 2003.

[8] 국정원, 국가정보보호 실무기술 편람, 2002.

[9] IACIS, 포렌식 조사 절차 표준, http://www.cops.org/forensic_examination_procedures.htm

[10] 오기두, “형사절차상 컴퓨터관련증거의 수집 및 이용에 관한 연구,” 서울대학교 박사학위 논문, 1997.

[11] 원혜욱, “인터넷 범죄의 특징과 범죄유형별 처벌조항,” 형사정책연구, 제 11 권 제 2 호.

[12] 하태훈, 강동범, “정보사회에서의 범죄에 대한 수사와 재판,” 정보통신정책연구원 참고자료.

[13] 류인모, “사이버범죄의 유형과 형사법적 문제,” 제 2 회 한국법률가대회 자료집 2, 한국법학교수회, 2000.

[14] 한국 정보보호센터, 정보시스템 해킹, http://www.kisa.or.kr/pds/att/ish.hwp

[15] 심희기, “유전자감정의 증거능력과 증명력,” 고시계, 1999.