우리나라 디지털 증거수사의 효율성 증진방안

Efficiency Improvement about Digital Evidence Investigation in Korea

강맹진, 김정규
남부대학교 경찰행정대학

Maeng-Jin Kang(maengpol@nambu.ac.kr), Joung-Gyu Kim(kjg@nambu.ac.kr)

요약

최근 각종사건 수사에 디지털 증거의 효용성이 증대되고 있다. 디지털 저장매체가 실생활에 폭넓게 사용됨에 따라 유죄입증이 가능한 결정적 증거가 디지털 형태로 남겨져 있는 경우가 빈번하게 발생하고 있기 때문이다. 현재 세계 각국의 수사기관들은 디지털 증거의 효용성을 극대화하기 위한 노력에 많은 관심을 기울이고 있다. 우리나라에서는 디지털 증거의 신뢰성 보증 모델 등에 관한 연구가 컴퓨터 공학, 형사법학 분야 등을 중심으로 꾸준하게 진행되어 왔다. 그러나 수사기관의 수사기법이 신종 범죄를 쫓아가는 상황에서 수사기관의 입법상, 기법상 공백은 발생할 수 밖에 없는 한계를 겪을 수 밖에 없다. 우리나라는 현재 디지털 증거에 관한 명확한 법규가 마련되어 있지 않고 전문 수사 인력이 부족한 실정으로 디지털 수사의 입법적 흠결 보완과 수사기관의 조직개편 등이 요구되고 있다. 본문에서는 날로 전문화되고 다양화되는 각종 사이버 범죄의 효율적 대응을 위한 핵심적 단서인 디지털 증거를 효율적으로 수사하기 위한 방안에 대해 논의하였다.

■ 중심어 : | 디지털증거 | 수사 | 컴퓨터 포렌식 |

Abstract

Recently investigation institutions have found the clue leading to solution of the problem by digital evidence. Digital medium is used extensively in real life. Accordingly, offender is leaving from traces of crime to digital form. But, Korea's digital evidence investigation is low level yet. Definite legislation about digital evidence is not readied in present our country. And professional investigation manpower about digital evidence is insufficient. These problem may have to be supplemented urgently. Systematic, technological supporting is required. Specialize and discussed digital evidence investigation's controversial point and capacity reinforcement way for efficient confrontation in cyber crime who is diversified gradually in text.

■ keyword : | Gambling Crime | Police Investigation | Computer Forensic |

Ⅰ. 서 론

세계적으로 인터넷 사용 인구는 약 6억5천7백만명정도로 추산된다. 2009년에는 7억9천4백만명에 이르리라는 예측이 있다[1]. 초고속 정보통신망의 구축은 사이버 공간에서 활동하는 인구를 빠르고 가파르게 증가시켰

* 본 연구는 남부대학교 학술연구비 지원사업에 의한 교비지원으로 수행되었습니다.

접수번호 : #070117-002
접수일자 : 2007년 01월 17일
심사완료일 : 2007년 01월 31일
교신저자 : 강맹진, e-mail : maengpol@nambu.ac.kr

다.

비교적 짧은 시간에 폭발적으로 증가한 사이버 활동 영역의 확장은 결과적으로 양면적 특성을 나타내고 있다. 거시적 관점으로 접근하면 19세기 후반 석유를 이용한 중화학공업의 발달이 인류에게 미친 순기능 및 역기능과 같은 맥락이다. 사이버공간을 합법적으로 이용하는 자들에게는 더할 수 없는 편리성을 가져다주었지만 범죄적 의도를 가진 자들에게는 새로운 범행 장소로 악용되고 있다. 이러한 현상은 정보화 진전에 큰 걸림돌이 되고 있다.

정보화 환경의 급속한 조성은 국가 수사기관에게도 동일한 결과를 초래했다. 정보화 환경을 통해 업무적 편리성이 증대되었지만 사이버 범죄의 대응이라는 새롭고 무거운 짐을 떠안게 된 것이다. 또한 사이버 범죄의 양상이 공학적인 전문소양을 토대로 모의 및 실행된다는 특성을 가지고 있어 수사기관은 적절한 대응에 어려움을 겪을 수밖에 없다.

2005년 우리나라에서는 88,731건의 컴퓨터 범죄가 발생하였다. 2004년도에 비해 15.1%가 늘었고, 2001년에 비하면 무려 167%가 증가한 수치이다[2]. 발생건수와 증가속도 면에서 모두 위협적인 수준이다.

컴퓨터 포렌식은 이러한 문제를 해결하기 위해 등장한 새로운 연구영역이다. 컴퓨터 포렌식의 목적은 사이버범죄에 있어 디지털화된 흔적이나 증거를 확보하고 이를 보존 및 분석하여 유죄입증 자료로 활용하는 것에 있다.

우리나라의 디지털 증거수사는 미국 등 관련 분야 선진국에 비해 기술적, 법적, 제도적 역량이 부족하다고 생각한다. 본문에서는 수사기관에서 날로 전문화되고 다양화되는 각종 사이버 범죄에 효율적으로 대응하기 위해 디지털 증거 수사의 효율성 증진 방안에 대해 논의하고자 한다.

II. 컴퓨터 포렌식과 디지털 증거에 대한 논의

1. 컴퓨터 포렌식의 개념

현대 과학수사에서 가장 중요한 역할은 법과학(Forensic Science)을 통해 수행되고 있다. 포렌식은 고대 로마시대의 Forum이라는 라틴어에서 유래한 것으로 많은 사람이 모여 상거래를 하거나 논쟁을 하는 장소였다가 근래 공개토론회의나 법정, 재판소의 의미로 통용하고 있다. 포렌식은 사전적 의미로 '법정변론을 위한', '토론의' 등의 의미를 갖는 형용사이며 일반적으로 법정변론을 위하여 이용되는 과학, 즉 법정과학이란 개념으로 이해된다[3].

컴퓨터 포렌식스(Computer Forensics)는 컴퓨터를 이용한 범죄나 컴퓨터를 대상으로 행해진 범죄 등에 있어 디지털화된 흔적이나 증거를 확보하고 이를 보존 및 분석하는 연구분야 라 할 수 있다. 요약하면 컴퓨터와 범죄가 어떻게 연관되어 있는가를 탐구하는 학문인 것이다[4].

컴퓨터 포렌식스에서 가장 높은 관심의 대상은 디지털 증거를 어떻게 유죄입증이 되도록 자료화 하는가에 집중된다. 디지털 증거의 대상은 디지털 저장매체에 저장되어 있는 모든 자료이다. 그것이 사진이든 음성이든 혹은 네트워크 기록이든 디지털 자료이면서 증거가치가 있는 정보라면 모두 다 포함된다. 오늘날은 과거에 비해 훨씬 많은 자료가 디지털로 생성되고 있으므로 컴퓨터 포렌식의 중요성 앞으로 더욱 증대될 수밖에 없다.

기존의 포렌식과 컴퓨터 포렌식은 연구방법의 접근에 차이가 있다. 일반적인 포렌식의 경우 수사관은 범죄현장에 위치하여 물리적 증거를 찾고 발견된 증거들을 분석하여 범죄자를 밝혀내게 된다. 하지만 컴퓨터 포렌식스에서는 일반적인 경우 수사관이나 전문가들(specialists)은 발견한 데이터를 평가하거나 해석을 시도하지 않으며 심지어 과학적으로 판단하지도 않는다. 다만, 컴퓨터에서 자료를 추출하거나 생성하며 사건과 관련된 적합한 정보를 찾는다. 결국 찾아낸 증거를 법정에 보내는 일은 기존의 포렌식과 동일하지만 과학적 방법을 동원하여 자료를 해설하지 않는다는 점에서 차이가 있다[5].

또한 기존의 포렌식스가 대부분의 경우 유형의 증거물을 대상으로 그 형상과 성질을 과학적으로 분석하거나 가시적인 범죄현장에 남겨진 범죄흔적을 연구대상으로 하는데 반하여 컴퓨터 포렌식스는 눈으로 직접 볼

수 없는 디지털 형태로 존재하는 정보를 연구대상으로 하며, 범죄가 이루어지는 현장도 눈에 보이지 않는 컴퓨터시스템 내부이거나 인터넷과 같은 사이버공간이다. 따라서 기존의 법과학에서 사용하는 연구방법론을 그대로 적용하기에 어려움이 따른다[6].

컴퓨터 포렌식은 1980년대 중반부터 디지털 증거의 보존, 신원확인, 문서를 다루는 것에서 시작되었는데, 법 집행기관들과 군사기관에서 수사와 정보수집의 주요기술로 인정 받아왔다. 컴퓨터 포렌식이라는 용어가 최초로 사용된 것은 1991년 미국 오레곤주, 포틀랜드의 국제 컴퓨터전문가학회(International Association of Computer Specialists ; IACIS)에서 였다[7].

현재 우리나라에서는 2004년 12월부터 경찰청 사이버테러 대응센터에 디지털증거분석센터가 설치되어 포렌식 기술이 활용되고 있으며, 검찰청에서는 디지털증거분석시스템이 운용되고 있다.

2. 디지털 증거의 속성

디지털 증거는 일반적으로 범죄현장에서 남겨진 증거와는 근본적으로 많은 차이가 있다. 이러한 차이를 디지털 증거의 속성이라 하며 잠재성, 이진성, 방대성, 휘발성 등으로 대표된다. 사이버 수사시에는 디지털 증거의 속성을 이해하는 일이 무엇보다 중요하며 사이버 범죄현장에서는 특히 높은 주의를 기울여야 한다. 디지털 증거의 속성을 좀 더 세부적으로 살펴보면 다음과 같다.

첫 번째 속성인 잠재성이란 증거가 육안으로 식별되지 않는 특징을 의미한다. 디지털 증거의 대부분은 전자기 또는 광학매체에 기록되어 있으며 입력형태가 코드화 되어 그 내용을 알 수 없다. 이를 확인하기 위해서는 하드웨어와 소프트웨어 등의 판독장치가 필요한데 이때 어떠한 프로그램을 활용하였는지에 따라 유죄입증여부가 결정될 수 있다.

두 번째 속성으로 이진성은 디지털 자체의 특성에 기인한다. 일반적 형태의 물리적 증거는 원본과 진본의 차이가 분명하다. 설사 흡사할지라도 동일할 수는 없다는 것이다. 그러나 디지털 증거는 그렇지가 않다. 우선 디지털은 기본적으로 '0'과 '1'의 숫자 조합으로 이루어져 있다. 복제를 하여도 숫자조합을 넘어서지 못한다. 결국 진본과 사본에 차이가 불분명하다. 나아가 이러한 속성은 사용자의 의지에 반하여 컴퓨터 스스로 데이터를 생성해 내는 결과를 초래하기도 한다[8].

세 번째 디지털 증거의 속성은 방대성이다[9]. 일상생활에서 컴퓨터나 디지털 기기의 활용이 확대됨에 따라 디지털 자료를 저장하는 매체의 용량이 크게 늘어나고 있는 추세이다. 디지털 기기 전반에 걸친 저장매체 용량의 증가는 디지털 증거를 확보하는데 절대적인 시간과 에너지를 소진시키는 결과를 초래하게 되었다.

마지막으로 디지털 증거는 휘발적이라는 속성이 있다. 휘발성을 용이하게 설명하자면 전원이 끊어지면 데이터가 손실되는 성질이라 할 수 있다. 휘발성은 사이버 수사에도 많은 영향을 미친다. 현재 진행되고 있는 실시간 사이버 범죄정보나 데이터에 대한 관리가 중요하기 때문이다. 그러므로 디지털 증거를 확보 단계에서 현재 실행되고 있는 프로세스 정보는 무엇인지, 현재 시스템에 접속하고 있는 자가 누구인지, 현재 열려있는 포트는 몇 번인지, 실행되고 있는 프로그램들은 무엇인지, 최초 접속기록은 무엇인지 등에 관심을 가져야 한다[10].

이러한 디지털 증거의 속성이 수사 실무 면에서 오히려 장점으로 작용할 수도 있다. 예컨대, 지문이 눈에 쉽게 발견되지 않기 때문에 수사관들도 어려움을 겪지만, 범인도 자신의 지문이 범죄현장에 남겨진다는 사실을 잊게 되는 실수를 범하게 된다. 또, 디지털 증거가 기술과 장비가 동원되어야만 현출 할 수 있다는 점이 수사를 어렵게 하지만 범인에게도 증거를 인멸하기 어려운 점으로 작용한다는 것을 주목할 필요가 있다. 그리고 변경이 쉽고 디지털 형태로 되어 있다는 점도 그것이 변형되지 않았다는 사실만 과학적으로 입증할 수 있다면, 오히려 수사에 큰 도움을 줄 수 있다. 방대성의 문제도 수사관에게 어려운 문제지만 범죄자도 증거인멸에 있어서 동일한 문제에 봉착시킬 것이다[11].

3. 컴퓨터포렌식의 절차

컴퓨터 포렌식은 사실에 대해 법적으로 증명하거나 반증하기 위해서 전자기적 데이터를 인지, 획득, 보관,

분석 및 레포팅하는 행위이다. 그러므로 컴퓨터 포렌식을 수행하기 위해 수사준비단계, 증거물획득단계, 증거물 보관 및 이송단계, 증거물 분석단계, 보고서 작성 단계를 신중하게 거쳐야 한다.

이와 같은 절차를 수행하면서 주의할 사항은 데이터가 변경되서는 안 되고, 모든 증거는 동일한 방법으로 다루어져야 한다는 점이다. 또한 매 사건 마다 중요도와 관계없이 동일한 수준의 최대한 안전한 방법으로 관리되어야 한다[12].

표 1. 포렌식 절차

증거물 획득 ↓	대상 컴퓨터 압수, 백업 데이터 찾기, 물리적 안정성 제공, 데이터 무결성 제공, 휘발성 메모리 덤프, 프로세스 확인 등
증거물 분석 ↓	로그 분서, 은닉 파일 찾기, 암호화파일 복구, 프로세스 실생시간 확인
증거물 보관 ↓	이동 시에 안전한 물리적 장치, 무결성 유지, 바이러스 삭제 하드 이미징 작업
보고서	증거들에 꼬리표 달리, 일련의 과정 표현, 검증 기능

증거물 획득 단계는 피해 사고 발생장소 또는 용의자의 컴퓨터를 압수하는 현장에서 각종 저장 매체와 시스템에 남아 있는 디지털 증거를 획득하는 과정이다. 하드 디스크와 같은 저장 매체의 내부 정보를 전부 수집하는 과정을 디스크 이미징(Disk Imaging)이라고 하는데, 컴퓨터 포렌식 과정에서 매우 중요한 영역을 차지한다. 디스크 이미징은 디스크와 정확히 같은 사본을 만드는 과정으로써, 입수된 하드 디스크를 그대로 조사·분석하게되면 증거물이 손상될 우려가 있으므로, 디스크와 똑같은 사본을 통해 조사·분석을 진행하게 된다. 또한 원본과 복사본에 대한 해쉬 값을 보관함으로써 하드디스크 변조 의혹을 불식시킬 수 있다[13].

증거획득시 주의사항으로는 획득할 증거범위의 수립여부, 컴퓨터의 전원상태, 용의자의 현장유무, 주변 장치의 점검, 사용자 정보(id/password), 정전기 주의 등이다[14].

증거물 보관 및 이송단계는 수집된 증거물을 안전한 방법으로 보관하는 과정이다. 전술한 바와 같이 디지털 증거는 훼손 등의 위험성이 크기 때문에 높은 주의가 요구된다. 특히, 디지털 증거가 약한 전자기파라 하여도 노출되면 내용이 변경되거나 삭제 될 수 있다. 따라서 디지털 증거는 반드시 이중적으로 확보해야 하고 전자기파와 물리적 충격으로부터 보호되는 정전기 방지용 팩, 하드 케이스 등의 보관 도구를 사용해야 한다.

증거물 분석단계에서는 다양한 기법들이 사용되고 있다. 일반적으로 포렌식에 사용되는 프로그램들은 증거물 획득 및 분석을 제공하고 있다. 분석을 위해 우선 획득 과정에서 복사한 이미징을 이용하여 파일을 확인한다. 확인 과정에서는 범죄 증거를 발견하면 파일의 확인 과정이 어떻게 되었는지 문서화하고 원본의 데이터는 직접 건드리지 않았으므로 원본 데이터의 무결성을 제공할 수 있다. 즉 사본 데이터의 파일은 실행 시간이 변경되었지만 원본의 파일은 실행 시간이 변경되지 않았으며 이전부터 범죄자의 컴퓨터에 파일이 존재하고 있다는 것을 보여 줄 수 있다. 이러한 분석에는 범죄자의 삭제 파일 복구, 은닉 및 암호화되어 있는 데이터 찾기 등이 포함되어 있다[15].

컴퓨터 포렌식 절차 중 마지막 단계인 보고서 작성단계에서는 디지털 증거 수집, 운송 및 보관, 조사·분석 단계의 모든 내용을 문서화하여 법정에 제출하는 단계이다. 보고서를 읽게 되는 법관은 컴퓨터에 대한 지식이 부족한 경우가 많기 때문에 이에 대한 해박한 지식이 없는 사람이라 할지라도 이해할 수 있는 쉬운 형태로 작성되어야 한다. 따라서 증거물 획득, 보관, 분석 등의 과정을 6하 원칙에 따라 명백하고 객관성 있게 설명해야 하며, 예상하지 못한 사고로 데이터가 유실되어 변경이 생겼을 경우 이를 명확히 기재하고, 범죄 혐의 입증에 무리가 없음을 논리적으로 설득 할 수 있어야 한다. 또한 수사 기관에서 조사 분석할 수 없어 외부에 이를 의뢰하였거나, 컴퓨터 포렌식 서비스 또는 전문가에게 상담을 의뢰하였다면, 그 결과를 전문가 소견서 형태로 제출하고, 전문가를 법정에 참고인으로 출석할 수 있게 해야 하는 과정도 포함된다[16].

[그림 1]은 디지털 증거물 압수시 행동요령이다[17].

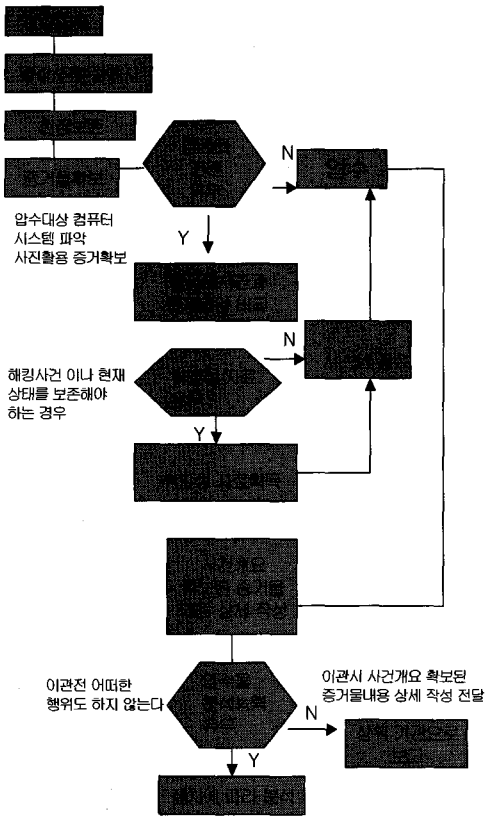


그림 1. 디지털 증거물 압수시 행동요령

4. 디지털포렌식의 기술

디지털 포렌식을 위해서는 프로그램에 대한 전문적 지식을 필요로 한다. 보안 툴이나 분석 방안의 기술들을 활용할 수 있어야 하며 관련범죄의 양상에 대한 지속적인 연구도 필요하다. 디지털 포렌식의 기술은 증거물 획득 기술과 증거물 분석기술로 구분할 수 있다.

디지털 증거물 획득 기술은 우발적으로 디스크의 내용이 변경되는 것을 방지하는 디스크 쓰지 방지기술, 디스크 이미지 파일을 비트스팀으로 복제하는 기술, 증거물에 대해서 해쉬를 계산한 후 원래의 계산 값과 비교하여 내용이 변경되지 않았음을 보장하는 메시지 다이제스트 기술, 일회용 쓰기 시스템 또는 저장 매체 기술이 있다. 증거물 분석 기술은 획득기술에 비해 더욱 많은 방법이 동원된다. 우선 흔적과 내용을 파악하는 디렉토리·파일목록 열람, 로그분석, 프로세스분석, 열람 프로그램호출,파일이 생성된 시간, 변경된 시간, 사용된 시간 및 삭제된 시간 등을 일목요연하게 나타내어 분석하는 시계열 분석 기술이 있다. 그리고 손상된 자료를 복구하여 분석하는 기술로는 삭제되거나 손상된 파일을 복원하는 삭제된 파일복구 기술, 삭제메일함까지 비운 경우 삭제된 메시지를 복원하는 삭제된 전자우편 복구기술, 삭제된 데이터베이스 복구, 패스워드를 알아내는 암호화된 파일 복호화 및 패스워드 크랙 기술 등이 활용되고 있다. 그리고 네트워크의 디지털 증거수집을 위해서는 이벤트 모니터링(event monitoring), 트랩 앤 트레이스 모니터링(trap-and-trace monitoring), 모든 네트워크 통신정보를 수집하는 풀 컨텍스트 모니터링(full-context monitoring) 기법이 사용 중이다.

III. 디지털증거에 대한 증거법적 논의

1. 형사증거법과 디지털증거

우리 형사소송법 제307조는 "사실의 인정은 증거에 의하여 한다"라고 규정하여 법관의 자의에 의한 사실인정이 허용 될 수 없고, 반드시 증거에 의하여야 한다는 증거재판주의를 증거법의 기본원칙으로 선언하고 있다[19]. 이때 증거란 재판의 객관성과 합리성을 보장하기 위하여 사실인정의 근거가 되는 자료를 의미한다.

형사소송법상 증거는 증거방법과 증거자료의 의미로 사용되고 있다. 증거방법은 사실인정의 자료가 되는 물건이나 사람자체를 말한다. 따라서 증거방법은 증거조사의 객체가 된다. 증거자료는 증거방법을 조사함으로써 알게 된 내용을 의미한다[20].

법정에서 증거로 채택되기 위해서는 증거능력과 증명력을 갖춰야 된다. 증거능력이란 증거가 엄격한 증명의 자료로 사용 될 수 있는 법률상의 자격으로 법률에 의해 형식적으로 결정되어 있다. 증명력이란 증거의 실질적 가치를 의미한다. 또 형사증거에 있어 전문증거란 사실인정의 기초가 되는 경험적 사실을 경험자 자신이 직접 법원에 진술하지 않고 다른 형태에 의하여 간접적으로 보고하는 것을 말한다. 예컨대, 피고인 갑이 을을 살해한 혐의로 기소된 사건에서, A가 증인으로서 법정

에 출석하여 "나는 갑이 을을 살해하고 있는 현장을 보았다"라고 증언하면 이는 원본증거이다. 그러나 A가 목격한 바를 B에게 말하고 B가 증인으로서 법정에 출석하여 "나는 A로부터 갑이 을을 살해하는 것을 보았다는 말을 들었다."라고 증언하면 이 B의 증언이 바로 전문증거이다. 전문증거에는 경험한 사실을 들은 타인이 전문한 사실을 법원에서 진술하는 경우, 경험자 자신의 경험사실을 서면에 기재하는 경우, 경험사실을 들은 타인이 서면에 기재하는 경우가 포함 될 수 있다. 이와 관련하여 전문법칙이란 전문증거는 증거가 아니며 증거능력이 인정 될 수 없다는 원칙이다[21].

디지털 증거는 본래 속성상 기존의 증거에 비해 대상이 유체물이 아니라는 점, 가시성과 가독성이 없다는 점, 위조·변조가 용이하다는 점 등의 특성이 있다. 그러므로 기존의 증거법에서 규정하고 있는 내용만으로는 디지털 증거를 다루는 것은 한계가 따를 수 밖에 없다. 이에 대해 구체적으로 논의되고 있는 사항들은 다음과 같다.

첫째, 디지털 증거에 대한 서면성 문제이다. 형사소송법에 서면의 정의는 내려져 있지 않으나 기본적으로 형법상의 문서와 유사한 것이라고 볼 수 있는데 디지털 증거가 이에 해당하는 것인가에 대해 의문이 제기될 수 있다. 이 문제에 대한 대법원의 태도는 "컴퓨터 디스켓에 들어 있는 문건은 진술을 기재한 서류와 다를 바 없다"는 판시를 통해 전문법칙의 예외규정을 적용함으로써 컴퓨터기록에 대한 서면성을 인정하고 있는 것으로 풀이된다. 한편, 디지털 증거를 출력한 서면의 성질에 대해서도 명확히 할 필요가 있다. 디지털 증거의 서면성이 인정된다 하더라도 서면으로 출력하여 증거로 제출하여야 하는데 이것을 증거서류로 볼 것인지 아니면 증거물인 서면으로 판단할 것인지에 따라서 증거능력의 인정에 차이가 발생하기 때문이다.

둘째, 디지털 증거의 증거능력에 관한 문제이다. 대법원에서는 진술내용이 담긴 컴퓨터 디스켓의 경우 성질에 있어 피고인 또는 피고인 아닌 자의 진술을 기재한 서류와 다를 바 없고, 압수 후의 보관 및 출력과정에 조작의 가능성이 있으며, 기본적으로 반대신문의 기회가 보장되지 않는 점 등에 비추어 그 기재내용의 진실성에 관하여는 전문법칙이 적용된다는 입장을 취하고 있다[22].

그러나 디지털 증거가 사용되는 방법은 단순하지 않다. 어떤 증거는 수사관의 요청에 의해 시스템 관리자 등이 시스템에 저장된 디지털 증거를 분석한 뒤 그 결과를 문서화하여 증거로 제출하기도 하고 어떤 증거는 디지털 데이터 자체가 증거로 사용되고 나아가 가시성·가독성을 부여하기 위해 데이터 원문이 변형 없이 그대로 출력되어 사용되기도 한다. 또한 디지털 증거 자체가 진술내용을 토대로 하는 경우에도 그것이 전문을 기록한 것인 경우가 있는가 하면 사람의 관념이나 마음의 상태 등이 특정 범죄의 구성요건에 해당하는 요소로서 기능을 하는 경우도 있다. 따라서 디지털 증거에 대한 전문법칙의 적용여부는 개별적 사안에 따라 검토되어야 성질의 것이라 할 수 있다[23].

셋째, 증거조사 방법이다. 서면형태의 증거로 제출되지 않고 디지털 증거로 제출된 경우 그 내용을 출력해야 할 필요가 발생한다. 이 경우에 증거조사방법으로 출력되는 절차에 관하여 견해의 대립이 있는 바, 전자기록은 "부호"에 포함되므로 번역규정을 준용하여 전자적 기록의 내용을 출력해서 "서류"로서 증거조사하면 된다는 견해와 전자적 기록 자체로서 시각적 인식이 불가능하고 전문적 조작을 거쳐야 한다는 점에서 감정을 준용해야 한다는 견해로 나누어지고 있는 실정이다.

2. 디지털증거의 압수수색 문제

수사상 압수란 수사기관이 증거방법으로 의미가 있는 물건이나 몰수가 예상되는 물건의 점유를 취득하는 강제수사를 말하고 수색이란 압수할 물건이나 피의자를 발견하기 위한 목적으로 수사기관이 사람의 물건 또는 주거 기타의 장소에 대하여 행하는 강제수사를 말한다. 수색은 주로 압수와 함께 이루어지고 실무상으로도 압수·수색영장이라는 단일영장이 발부되고 있다[24].

형사소송법 제216조와 제217조 제1항에서는 압수와 수색은 강제처분으로서 개인의 재산권과 주거권을 침해하기 때문에 영장이 요구되지만 압수, 수색의 긴급성에 대처하기 위한 예외적 사정이 있는 경우에는 영장없는 압수, 수색이 허용된다.

이러한 영장주의의 원칙은 디지털 증거를 압수, 수색함에 있어서도 지켜져야 하는 원칙이다. 다만 컴퓨터 데이터와 같은 전자적 기록들은 일반적인 유체물의 압수, 수색의 경우에 비하여 개변과 소거가 용이하기 때문에 긴급성의 예외에 해당한다고 판단될 수 있다. 따라서 영장에 의하지 않는 압수·수색이 허용되는 경우 유체물에 대한 압수, 수색에 비해 더 많을 수 있다. 즉 유체물에 비하여 무체물인 전자적 기록의 압수, 수색에 대한 영장원칙의 예외를 판단함에 있어서는 좀 더 신중하게 판단하여 개인의 인권이 불법부당하게 침해되는 일이 없도록 해야 한다는 것을 의미하는 것이라고 보아야 할 것이다[25].

또, 형사소송법 제106조는 "증거물 또는 몰수할 것으로 사료되는 물건"만을 압수의 객체로 하고 있다. 이를 따르면 압수할 수 있는 디지털 증거의 범위에 문제가 발생할 수 있다. 압수영장에 디지털 데이터의 저장 장치만을 기재하였을 경우에 저장장치에 기록된 전자적 기록이 압수 영장의 범위에 포함되는지, 압수한 저장장치에 전자적 기록을 입력한 사람이나 저장장치 소유자의 동의 없이 전자적 기록을 출력하거나 프로그램을 실행할 수 있는지에 대한 의문이 일게 된다. 그러나 우리 형사소송법 제120조는 "압수, 수색영장의 집행에 있어서는 잠금장치를 열거나 개봉 기타 필요한 처분을 할 수 있다"라고 규정하고 있으므로 압수한 저장장치에 기록된 전자적 기록을 재생, 출력하거나 저장된 프로그램을 실행할 수 있다고 보아야 할 것이다. 또 다른 문제는 범죄수사를 위한 압수, 수색은 행위자의 범행을 추적하거나 행위자가 범죄행위에 사용된 부분, 범죄행위를 생성된 부분만이 수사에 필요할 뿐인데 반하여, 압수대상인 컴퓨터에는 위와 같은 부분 이외에 단순히 컴퓨터의 소유자에 불과한 사람이나 범죄행위와 아무런 관련이 없는 제3자의 소유의 전자적 기록이 포함된 경우가 대부분이다. 그러므로 이러한 경우 고의로 동 부분을 열람, 삭제, 변경하거나 동인들의 프로그램을 실행하는 것은 압수, 수색의 범위를 초과하는 직무상 불법행위가 될 것이므로 유의하여야 한다[26].

3. 디지털 증거에 대한 외국의 태도

아직 많은 국가들이 디지털 증거분석에 대해 구체적 대안을 마련하고 있지 않은 실정이다. 이에 비해 미국은 디지털 증거분석에 있어 선구적인 지위를 점하고 있으므로 미국의 관련법규를 검토하도록 한다. 미국의 디지털 증거분석 관련 규정인 미국증거규칙 제1001조 3호는 컴퓨터에서 출력된 기록도 원본으로 명시하고 있고 동 규칙 제1003조는 사본의 내용이 정확하다는 보장이 있으면 사본을 원본과 같이 취급하고 있다. 이를 근거로 미국에서는 이메일 등이 법정에서 중요한 증거로 인정받고 있다.

미국도 처음에는 연방법원에서는 컴퓨터 관련 증거를 허용할 것인가의 문제에 대해서 컴퓨터 증거를 잠정적인 전문증거로 취급하고 있고 컴퓨터 관련 기록들을 전문법칙 중 연방증거규칙 제803조 제6호에 규정된 업무상기록의 예외 규정으로 판단하여왔다. 그러나 연방법원도 컴퓨터기록에 익숙해지면서 이러한 일원론적 취급방법에서 벗어나 컴퓨터 기록이 어떠한 종류인가에 따라 어떻게 증거를 허용할 것인가 하는 증거법적인 문제가 자주 발생하게 되었는데, 예컨대 법원에서는 문서적 성격을 지닌 컴퓨터 기록이라 할지라도 컴퓨터로 생산된 문서와 단순히 컴퓨터에 저장된 문서로 구분하여 취급하였다. 여기에서 컴퓨터에 저장된 문서는 사람이 단순히 컴퓨터를 이용하여 자신의 사상이나 관념을 기재한 것으로서 전문증거로 취급되었으며, 반대로 인터넷 로그 등과 같이 컴퓨터 프로그램 등이 생산한 문서는 컴퓨터의 산출물에 불과하기 때문에 전문증거로 취급되지 않는 것이다. 디지털 증거의 압수·수색에 관해 미국의 형사소송규칙 제41조(h)항에 압수, 수색의 대상이 되는 물건을 '문서, 장부, 서류, 기타 유체물'을 포함한다고 정의하고 있다. 여기서 유체물이라고 명시적으로 규정하고 있는 이 규정의 문언을 엄격하게 해석하게 되면 컴퓨터 데이터와 같은 전자적 기록과 같은 무체물은 압수, 수색의 대상에 포함되지 않는다고 볼 수밖에 없다. 그러나 판례는 형사소속규칙 제41조9(h)항에서 물건이라 함은 문서, 장부, 서류 기타 유체물을 포함한다고 정의하고 있으나 이는 한정적 열거가 아니며 대상으로 될 수 있는 물건을 모두 열거코자 한 취지도 아니다. 동 규칙 제41조는 유체물에 한하지 않는다.

라고 판시하였다. 즉, 동판결은 미국 형사소송규칙 제41조가 유체물과 마찬가지로 컴퓨터 데이터 등의 전자적 기록과 같은 무체물에 대해서도 압수대상물로서 포함된다고 봄으로서, 동 규칙의 물건의 정의는 적법한 압수, 수색의 대상에 대하여 한정을 가하고자 한 것이 아니라 단순한 예시에 불과한 것이라고 한 점에 의미가 있다고 할 것이다. 미국의 경우 연방증거규칙 제901조 a항에 따라 디지털 형태의 증거가 문서방식으로 제출되었을 경우에 관련자의 직접 진술 등에 의해 문서의 진정성을 인정하고 있다.

Ⅳ. 효율적인 디지털 증거수사를 위한 제언

1. 사이버수사 체계도 구축

일반적 범죄수사와 마찬가지로 사이버 범죄수사의 진행과정은 기술적 측면과 절차적 측면으로 구분할 수 있다. 성공적인 수사를 위해서는 두 가지 요소가 고르게 갖춰져야 한다. 그러나 사이버 범죄수사의 경우 공학적인 기술에 대해서는 활발한 연구가 진행되고 있는 반면 절차적 측면에 대해서는 다소 소홀하게 다루어지는 경향이 있다. 디지털 증거수사의 핵심이 컴퓨터 공학적 기술이 바탕이 되는 신뢰성 보증에 있기 때문으로 이해된다. 그러나 사이버범죄가 고도로 지능화되고 복잡해지고 있다. 절차적 측면에 대해서도 심도 깊은 논의가 요구된다.

현재 경찰청 사이버테러대응센터 내에 설치·운영중인 디지털증거분석센터에서는 의뢰받는 사건마다 디지털 증거 현장체크리스트를 작성하고 있다. 디지털증거에 대해 체계적 관리를 하기 위한 조치이다. 사이버수사의 초기단계에서도 수사절차를 구조화하는 체계도를 구축한다면 복잡한 절차를 명확히 하는데 유용하리라 생각된다. 사이버수사 체계도는 수사진행 단계에 따라 구성하는 것이 바람직할 것 같다. 수사의 진행방향이 변경되었을 경우 즉각적인 대응이 가능하기 때문이다. [그림 2]는 금융사기 사건 수사 절차 체계도의 예이다[27].

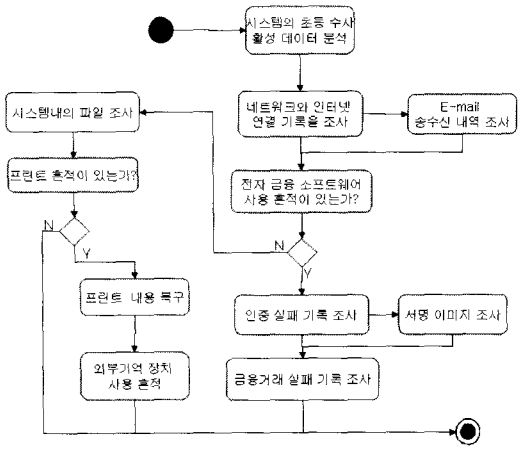


그림 2. 금융사기 사건 수사 절차 체계도

2. 디지털 증거에 대한 외부 관리방안 모색

디지털 증거는 획득과 동시에 객관화 시키는 작업이 필요하다. 디지털 증거의 속성상 가변성이 높기 때문이다. 객관화를 고려해야 하는 요소는 생성시간, 내용, 기록 및 저장방식 등이다. 실제로 허위비방문서를 게시하여 기소된 사건에서 디지털 증거 즉, 허위문서의 생성일자의 변경이 밝혀져 무죄판결이 내려진 경우가 있었다. 이에 대해 검찰은 문서파일을 수집하는 과정에서 비전문가에 의해 저장일자가 변경되는 사고가 발생하였다고 밝힌바 있다[28]. 사실의 진위를 떠나 디지털 증거 획득에 실패한 것임에는 틀림없으며, 디지털 증거를 획득한 후 객관화시키는 작업의 중요성을 일깨워주는 사례이다.

디지털 증거의 객관화 방안은 여러 가지형태가 가능하겠으나 가장 강력한 객관화는 분산관리 방안이 될 것이다. 디지털 증거 생산과정에서 얻어진 디지털 증거의 프로파일을 암호화하여 신뢰할 수 있는 제3의 기관에 전송하여 보관하고 이후 원본의 신뢰성에 대한 의심을 제기하는 경우에 이를 기준으로 디지털 증거의 개체를 식별하는 방식이다[29].

제3기관은 해당사건과 이해관계 있는 자와의 접촉을 철저하게 봉쇄하는 관리 방안을 마련하여야 할 것이다. 제3기관으로는 민간기관 보다 정부기관이 신뢰성 측면에서 보다 바람직할 것이다.

한국정보보호진흥원(Korea Information Security Agency)은 제3기관으로 가능성이 있다고 생각한다. 한국정보보호진흥원의 설립근거는 정보통신망이용촉진및정보보호등에관한법률 제52조로써 "정부는 정보의 안전한 유통을 위한 정보보호에 필요한 시책을 효율적으로 추진하기 위해서 정보보호진흥원을 설립한다."고 명시되어 있고 정관에 규정하고 있는 임무에 정보보호에 관한 기술지원 및 자문(정관 제4조의 7), 정보시스템 침해사고 처리 및 대응체계운영(정관 제4조의 10)을 포함하고 있다. 한국정보보호진흥원 혹은 여타의 제3기관을 이용하기 위해서는 서버구축 등을 위한 예산 지원이 뒷받침 되어야 할 것은 물론이다.

3. 디지털 증거분석 가이드라인의 보완

디지털 증거분석의 중요성은 날로 증대되고 있음에도 불구하고 우리나라에서 이를 뒷받침할 법규는 전술하였듯이 매우 미흡한 실정이다. 디지털 증거분석을 규정하는 법규가 명확하게 마련되어 있지 않은 상황을 극복하기 위해 그간 경찰 등 수사기관은 디지털 증거분석의 가이드라인을 개발하고자 학계와 연계하여 많은 노력을 기울여 왔다. 그 결과 2006년 11월 1일 1일 경찰청과 한국디지털포렌식학회는 공동 연구를 통해 「디지털 증거처리 표준 가이드라인」을 국내 최초로 발표했다. 디지털 증거처리 표준 가이드라인과 디지털 증거분석 표준 절차 두 가지로 구성돼 있다. 이미 미국과 영국 등 디지털 증거분석 분야가 발전한 국가들은 가이드라인을 제정하여 활용하고 있음을 고려하면 때 늦은 감이 없지 않다. 가이드라인의 제정은 사이버 범죄에 대한 투명하고 정확한 수사에 진일보 시켰음은 분명한 사실이다.

그러나 가이드라인은 불완전할 수밖에 없음을 인식해야 한다. 범죄의 양상이 계속해서 진보하기 때문이다. 또한 증거훼손의 범위를 어디까지 할 것인지, 증거물 자료 관리를 어떻게 할 것인지, 증거 분석 환경과 인력 운영 문제 등이 명확하지 하지 않다. 뿐만 아니라 증거분쟁에 관한 도구를 과연 외국산에 의존할 것인지 아닌지, 표준화 논쟁을 국내에서만 국한시킬 것이 아니라 국제적 표준으로 제정해야 되는지 아닌지에 대해서도 그러하다.

그러므로 디지털 증거 분석을 가이드라인은 지속적인 관심을 가지고 보완해 나가야 할 것이다[30].

4. 디지털 증거에 대한 수사기관 상호 공조체계 구축

미국의 경우 국방부, 연방정부, 주정부, 지방 법집행기관 등이 공동으로 디지털증거에 관한 정보를 공유하고 공동 연구를 진행하고 있다. 이를 통해 컴퓨터포렌식실험 2000(The Computer Forensics Experiment 2000)을 구축하였다. 참여한 기관들은 세 개팀으로 편성하여 디지털 증거를 탐색하며 방대한 디지털 증거를 수집하고 사이버 범죄를 찾아내게 된다[31].

우리나라에서 디지털 포렌식을 수행하는 수사기관은 경찰, 검찰, 국정원, 기무사 등이 있다. 이들 상호간에 디지털 포렌식에 대한 정보를 공유하고 실무사례에 대해 토의하는 시스템을 마련한다면 디지털 증거분석을 발전시킬 수 있을 것이다. 이 경우 어느 기관에서 주관을 하느냐가 문제가 될 수 있다. 미국의 CFX-2000은 뉴욕 주 경찰의 포렌식 수사센터(Forensic Investigation Center)에서 주관하고 있다.

V. 결 론

유비쿼터스 컴퓨팅 환경의 조성으로 디지털 증거분석이 수사에서 차지하는 비중이 증가하고 있다. 수사기관은 디지털 증거분석에 관한 역량을 강화시키기 위한 노력을 기울여야 한다. 우리나라의 정보화 환경은 세계적으로도 최고 수준이다. 그러나 디지털증거분석의 기술적, 절차적 수준은 그에 미치지 못하고 있다. 정보강국의 모순된 모습이다. 사이버 분야의 국가 경쟁력을 지속적으로 유지하기 위해서는 정보화 환경을 수호하는 노력이 뒷받침 되어야 한다. 디지털 증거분석의 효율성 증대방안에 대한 많은 논의가 필요한 이유도 여기에 있다.

본문에서는 사이버수사 특히 디지털 증거획득에 있어 체계적 진행절차의 개발과 적용, 디지털 증거의 객

관성 확보방안을 위해 제3기관을 활용하는 문제, 디지털 증거분석의 가이드라인에 대한 지속적 보완 작업, 디지털 증거에 대한 수사기관 상호 공조체계 구축에 관한 도입을 제시하였다.

참 고 문 헌

[1] J. R. Vacca, Computer Forensics computer crime scene investigation, Charles River Media, Hingham, Massachusetts, p.5, 2005.

[2] 경찰청, 2006 경찰백서, pp.209-211, 2006.

[3] 유영찬, 법과학과 수사, 현암사, p.22, 2002.

[4] R. Jones, Internet Forensics, O'reilly, Sebastopol, p.1, 2006.

[5] E. Baucher, Computer Investigation, Mason Crest Publisher, India, p.13, 2006.

[6] 김종섭, *디지털증거의 신뢰성 보증 모델*, 경기대학교 대학원 박사학위청구논문, p.10, 2003.

[7] Alfred C, 해킹과 포렌식 입문, 도서출판 그린, pp.152-153, 2002.

[8] J. R. Vacca, Computer Forensics computer crime scene investigation, Charles River Media, Hingham, Massachusetts, p.39, 2005.

[9] 김용호, 디지털증거분석, 경찰수사보안연수소, p.200, 2006.

[10] 김성혜, 윈도우즈 증거분석(휘발성 증거수집), 경찰수사보안연수소, p.107, 2006.

[11] 김종섭, *디지털증거의 신뢰성 보증 모델*, 경기대학교 대학원 박사학위청구논문, pp.44-45, 2003.

[12] 윤오영, 디지털증거분석의 개용, 경찰수사보안연수소, pp.76-77, 2006.

[13] 임종인, 유비쿼터스시대의 컴퓨터 포렌식의 중요성과 향후 전망, 수사연구, p.14, 2005.

[14] 윤오영, 디지털증거분석의 개용, 경찰수사보안연수소, p.77, 2006.

[15] 이임영, 디지털 증거 분석을 위한 포렌식, 정보통신연구진흥원, 주간기술통향 1232호, p.3, 2006.

[16] 임종인, 유비쿼터스시대의 컴퓨터 포렌식의 중요성과 향후 전망, 수사연구, pp.15-16, 2005.

[17] 김용호, 디지털증거분석, 경찰수사보안연수소, p.210, 2006.

[18] 윤오영, 디지털증거분석의 개용, 경찰수사보안연수소, p.278, 2006.

[19] 신이철, 형사증거법, 유스티아누스, p.10, 2005.

[20] 박동규, 형사소송법, 법문사, p.428, 2004,

[21] 신이철, 형사증거법, 유스티아누스, p.102-103.

[22] 대판 1999. 09. 03. 99도 2317.

[23] 양근원, "디지털 증거의 특징과 증거법상의 문제고찰", 한국경찰학회, 한국경찰학회보 12호, p.151, 2006.

[24] 박동규, 형사소송법, 법문사, pp.213-214, 2004.

[25] 탁희성, 형사절차상 digital evidence에 관한 연구 -압수,수색을 중심으로-, 한국형사정책연구원 연구보고서, Vol.2, No.2, p.98, 2002.

[26] 양근원, "디지털 증거의 특징과 증거법상의 문제고찰", 한국경찰학회, 한국경찰학회보 12호, p.152, 2006.

[27] 이석희 외, "디지털 범죄 수사절차 모델링 기법에 관한 연구", 고려대정보보호기술연구센터 컴퓨터포렌식연구실, p.4, 2006.

[28] http://www.inews.com, 2006(6.18).

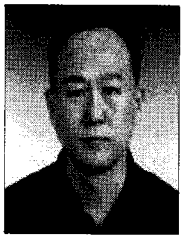
[29] 김종섭, *디지털증거의 신뢰성 보증 모델*, 경기대학교 대학원 박사학위청구논문, p.78, 2003.

[30] http://www.zdnet.co.kr/news/network/security/0,39031117,39152424,00.htm

[31] J. R. Vacca, Computer Forensics computer crime scene investigation, Charles River Media, Hingham, Massachusetts, p.36, 2005.

저 자 소 개

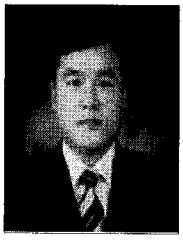
강 맹 진(Maeng-Jin Kang) 종신회원



- 1990년 8월 : 동국대학교 (행정학석사)
- 2000년 8월 : 동국대학교 경찰행정학과 (법학박사)
- 2003년 3월 ~ 현재 : 남부대학교 경찰행정대학 조교수

<관심분야> : 국가보안, 경찰관리

김 정 규(Joung-Gyu Kim) 정회원



- 1999년 2월 : 원광대학교 경찰행정학과(법학사)
- 2002년 8월 : 부산대학교 행정학석사
- 2006년 2월 : 원광대학교 경찰학박사
- 2006년 3월 ~ 현재 : 남부대학교 경찰행정대학 전임강사

<관심분야> : 경찰학, 경찰수사