물리적 복구 방법을 활용한 디지털 포렌식 기술[1)]

*최재민 *신대민 *이상진 *임종인

*고려대학교 정보경영공학전문대학원

*koreamath@korea.ac.kr

Digital Forensic Techniques using physical recovery method

*Choi, Jaemin *Shin, Dae-Min *Lee, Sangjin *Lim, Jongin

*Graduate School of Information Management and Security, Korea University, Korea

요약

2000년대에 접어들어 컴퓨터가 보급화 되면서, 컴퓨터를 도구로 하는 범죄가 폭발적으로 증가하기 시작하였다. 컴퓨터 시스템에 접근하여 중요 정보를 빼돌리거나, 범죄의 목적이 되는 해킹과 같은 정보보호 침해사고가 크게 증가하였으며, 컴퓨터를 이용한 정상적인 서비스를 방해하는 형태의 디지털 범죄들이 다수 발생하기 시작하였다. 따라서 범죄 수사 과정에서 전자 매체에 대한 분석이 필수 불가결한 요소로 등장하고 있으며, 이를 분석하려는 디지털 포렌식 연구가 활발히 진행되고 있다. 특히 전자 매체에 기록되는 디지털 정보는 보관이 편리하지만 삭제와 복제가 용이하므로 디지털 증거는 매우 세심하게 다루어야 하며, 수사관에 의한 의도적인 훼손이 없었음을 증명할 수 있는 절차와 제도가 필요하다. 국내에서는 적법한 수사 절차와 무결성을 보장하기 위하여 '절차 연속성(chain-of-custody)'을 제공하는 수사 가이드라인을 제작하였으며, 체계적인 수사를 수행하고 있다.[4] 이와 더불어 포렌식 수사 과정에서 물리적인 접근을 통해 디지털 저장 매체에 대한 복구할 수 있는 방법이 존재하며, 이에 대한 구체적인 방안을 논한다.[1]

1. 서론

디지털 포렌식의 기원은 1980년대 중반부터 시작된 기술 기반의 범죄수사 영역이지만, 군 또는 정보기관의 전자정보 수집기술이 디지털 범죄 수사의 시초라 할 수 있다. 자필 문서, 필름 현상된 사진, 비디오·테이프 영상 등과 같은 아날로그 데이터들이 디지털시대에 접어들면서 고도화된 신기술을 통해 데이터의 영역이 넓어지고 있으며,수사관이 수집하는 데이터의 종류가 다양해지고 있다.

'디지털 포렌식(Digital Forensic)'은 1991년 미국 Portland에서 열린 'International Association of Computer Investigative Specialists (IACIS)'에서 처음으로 사용되었다.[2] 하지만 그 당시에는 널리 알려지지 않았고 필요에 의해 기술이 발전되어 가는 시기였으며, 정형화 되지 않은 형태를 띠고 있었다. 이후에 컴퓨터가 보급화되고 사용율이 점차 증가하면서 컴퓨터가 관련된 범죄들과 디지털 정보에 근거한 각종 민·형사상 소송 사례들이 증가하게 되었고, 법정에 제출된 디지털 증거의 신빙성을 지원하기 위한 각종 전문 기술들이 필요하게 되어, 컴퓨터 포렌식을 통한 과학 수사 분야 연구가 가속화되기 시작했다. 1990년대 중반까지의 초기 디지털 포렌식은 컴퓨터 관련 범죄자를 기소하고 처벌함으로써, 유사 범죄의 증가를 막고자 하는 취지가 강했다. 따라서 컴퓨터 관련 사건에 대한 수사를 지원하며, 각종 디지털 자료가 법적 효력을 갖도록 과학적이고 논리적인 수사 절차와 방법을 연구하는 학문으로 정의되었다.

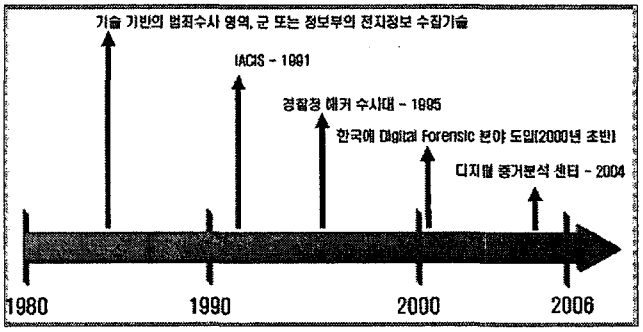

그림 1 디지털 포렌식의 기원

그러나 2000년을 넘어서면서 컴퓨터를 도구로 하는 범죄 뿐만 아니라 컴퓨터 시스템에 불법적으로 접근하여 중요 정보 탈취하는 해킹과 같은 정보보호 침해사고가 크게 증가하게 하였다. 특히 과거의 정보보호 침해사고는 초보 해커에 의한 자기과시 또는 호기심을 충족시키기 위한 것이었으나, 최근에는 전문적 해커 집단에 의해 경제적 이익이나 정치적 시위를 위하여 민간 부분뿐만이 아니라 국가 기관에 대해서도 조직적이고 체계적인 형태로 공격하는 범죄가 급증하고 있다.

이러한 정보보호 침해사고를 조사하고 후속조치를 취하는 과정에 디지털 포렌식 기술을 도입하고자 하는 움직임이 활발해지고 있으며, 국내에서도 수사 기관 이외에 기업에서 자체적인 조사 부서를 설치하여 정보보호 침해사고 수사 및 예방에 힘쓰고 있다. 최근의 디지털 포렌식은 컴퓨터를 이용한 범죄뿐만 아니라 컴퓨터와 네트워크 등을 목표로 하는 범죄를 예방하는 등 영역이 확대되고 있으며, 범죄가 발생하면 적절한 절차에 의해 디지털 증거를 수집하여 법적 효력이 있는 증거로 가공함으로서 민·형사상 책임을 지울 수 있도록 재판에 제출하

1) 본 연구는 과학재단 디지털 정보 획득 기반기술 연구(M10640010005-06N4001-00500)의 지원으로 수행되었습니다.

게 되는 일련의 과정을 포괄하고 있다.

2. 국내 디지털 포렌식 수사의 연구 동향

국내에서는 1995년 경찰청 해커 수사대가 창설된 이래로 2000년대부터 사이버 테러대응 센터로 확대되는 등 디지털 포렌식 연구가 활발히 진행되고 있으며, 해마다 증가하는 사이버 범죄에 적극적으로 대응하기 위해 2004년에는 디지털 포렌식 수사 시 증거물 분석을 전담하는 디지털 증거분석 센터를 설립함으로써 수사의 정밀성을 더하였다.[6] 이외에도 대검찰청에서는 컴퓨터 수사를 전담하는 '컴퓨터 수사과' 기구를 두어 자체 기관의 효율적 수사를 제공하고 있으며, 경찰청 등 타 기관과의 공조를 통해 검거율을 높이고 있다.[7]

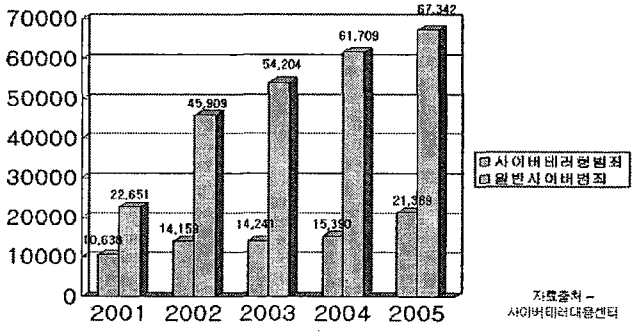

그림 2 국내 사이버 범죄 발생현황

그림 2와 같이 해마다 급격히 증가하는 사이버 범죄에 대응하기 위하여 디지털 포렌식의 수사 기법 연구가 적극적으로 진행 중이며, 이로 인해 사이버 범죄의 검거율이 매년 상승하고 있다. 국내에서는 정부기관 및 학계에서 활동하는 전문가들이 빠르게 증가하는 사이버 범죄에 대한 수사 기법 및 정책적 연구의 필요성을 인식하여 2005년 10월 '한국 디지털 포렌식 학회'를 창립하였으며, 디지털 증거에 대한 수집·보관·분석에 관한 정보통신 기술 및 법률적 방안에 대한 학술연구를 활발히 진행하고 있다.[5]

3. 디지털 포렌식의 5단계 절차

전자 매체에 기록되는 디지털 정보는 보관이 편리하지만 삭제와 복제가 용이하므로 수사 시에 압수한 디지털 증거물은 매우 세심하게 다루어야 하며, 수사관에 의한 의도적인 훼손이 없었음을 증명할 수 있는 절차와 제도가 필요하다. 실제로 각 수사 기관 별로 적법한 수사와 무결성을 보장하기 위하여 '절차 연속성(chain-of-custody)'을 제공하는 적절한 수사 방법을 만들어 수행하고 있으며, 국내에서도 수사에 적합한 가이드라인를 제작하여 무료 배포중이다.[4]

현재 디지털 포렌식에서 사용되고 있는 범죄 수사 기본 절차는 그림 3과 같이 수사 준비 단계(Preparation), 증거물 획득 단계(Acquisition), 증거물 보관 및 이송 단계(Preservation), 증거물 분석 단계(Examination & Analysis), 보고서 작성 단계(Reporting)로 이루어진다.

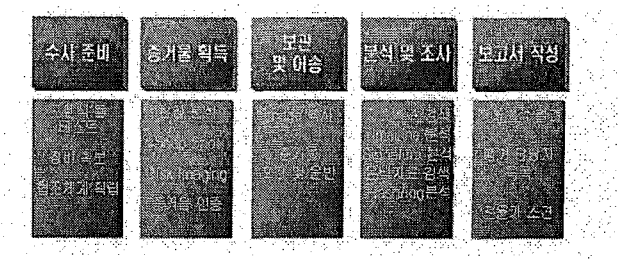

그림 3 디지털 포렌식 프로세스 (Process)

가. 수사 준비 단계

디지털 포렌식 수사를 위해서는 각종 소프트웨어와 하드웨어를 준비하고 점검하는 과정이 가장 우선적으로 필요하다. 특히 수사 시에 증거물들이 훼손되거나 변형되지 않도록 사전에 이와 관련된 수사 도구들을 필히 점검해야 한다. 디지털 포렌식에 사용되는 소프트웨어를 디지털 포렌식 도구(Tool)라고 한다. 디지털 포렌식 도구는 컴퓨터 및 다양한 디지털 범죄 수사에서 수사 절차에 대한 신뢰성을 제공하며, 효율적이고 체계적으로 실시할 수 있는 독립 또는 통합 도구이다. 디지털 포렌식 도구 중에서 가장 널리 알려진 제품은 Guidance 사의 EnCase 이며, 국내에서도 경찰청, 국가사이버안전센터, 인터넷 침해사고 대응센터 등에서 EnCase 도구를 사용하고 있다. 미국의 경우에도 EnCase 도구를 사용하여 획득된 디지털 증거와 조사 분석 결과가 법정에서 받아들여지고 있기 때문에, 수사관이 수사 시에 가장 많이 사용되는 도구들 중에 하나이다.[8]

나. 증거물 획득 단계

사건 발생 현장에서 각종 저장 매체와 시스템이 존재하면 용의자의 범죄 수사를 위해 압수하게 되는데, 이러한 과정은 증거물 획득 단계에서 이뤄지며 획득된 증거물은 디지털 증거물로써 분류된다. '디지털 증거(Digital Evidence)'는 디지털 형태로 저장되는 데이터와 네트워크 상으로 전송되는 데이터들 중에서 증거로서 가치를 가지는 정보를 말한다. 저장 매체에 저장된 파일, 네트워크 패킷, 메모리의 정보, 운영체제(OS) 또는 소프트웨어의 정보 등이 디지털 증거물에 포함된다. 그 중에서 하드디스크와 같은 저장 매체의 내부 정보를 전부 수집하는 과정을 디스크 이미징(Disk Imaging)이라고 하며, 디스크의 모든 정보를 복제하는 작업을 일컫는다. 증거물로써 입수된 하드디스크를 그대로 분석 시스템에 연결하면 증거물이 손상될 우려가 있기 때문에 이러한 작업이 필수적이며, 수사 과정에서 이미징된 디스크를 사용하여 분석을 수행하게 된다. 디스크 이미지 파일은 디스크 이미징 작업으로 생성된 디스크 사본 파일을 말하며, 디스크 이미지 파일을 사용하여 조사와 분석을 진행하게 된다.

다. 증거물 보관 및 이송 단계

사건 현장의 증거물을 획득하게 되면, 수집된 증거물을 안전한 방법으로 분석실 또는 보관소로 옮기는 과정이 필요하다. 디지털 증거물 보관 및 이송 시에는 일반 증거물에 비해 안전하게 다루어져야 한다. 디지털 증거물의 경우 대부분 자기 기록 저장 매체에 저장되므로, 전자기파(EMP)에 노출되면 저장된 내용이 모두 훼손되거나 삭제되기 때문이다. 따라서 디지털 증거는 반드시 이중으로 확보함과 동시에 전자기파와 일반적인 물리적 충격에도 견딜 수 있는 정전기 방지용 팩과 하드 케이스와 같은 보관 도구를 반드시 사용해야 한다.

'E-Boom'이라는 전자기 폭탄의 경우, 강력한 전자기파를 한순간에 발생시키면서도 어떤 소리나 빛을 사람이 인지할 수 없다는 특성을 가지고 있기 때문에 매우 위험한 증거훼손 도구가 될 수 있다. 용의자가 증거물 이송 시에 멀리 떨어진 장소에서 증거물에 전자기 폭탄을 은밀하게 피폭시킨다면, 한순간에 모든 디지털 증거물을 무력화 시킬 수 있는 위험성이 존재하게 된다. 이와 같이 디지털 증거물을 의도적으로 숨기거나 파괴 또는 훼손시키는 행위를 'Anti-Forensic'이라 한다.

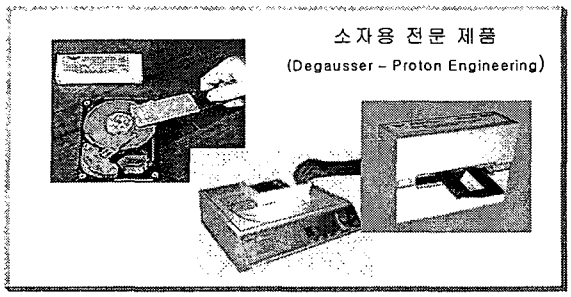

그림 4 소자(Degaussing)

소자(Degaussing)는 강력한 자기장을 형성하여 매체의 자기상태를 중화시켜 데이터를 파괴하는 방법으로서, 그림 4와 같은 도구들이 다양하게 존재한다. 또한 데이터 복구 회피 기법으로서 디스크 덮어쓰기(Overwriting)가 있다. 데이터 덮어 쓰기 방법을 이용하면 증거 후에도 삭제된 파일의 데이터가 남아있을 지 모르는 데이터에 대해 다른 내용으로 덮어쓰고 삭제하는 과정을 반복하여 데이터 복구를 회피하게 된다.

라. 증거물 분석 단계

증거물 분석단계에서는 수집된 디지털 증거물의 내부 조사를 통해 범죄에 관련된 파일 또는 정보를 획득하는 작업을 수행한다. 저장매체 기술이 발전함에 따라 개인용 컴퓨터의 하드디스크는 100GByte대가 넘어가는 등 점차 대용량화 되고 있고, 그러한 디스크 안에는 수만에서 수십만 가지의 다양한 파일이 존재하므로 모든 파일을 수사관이 수동으로 확인하는 작업은 많은 시간이 소요되며 매우 비효율적인 방법이 될 것이다.

위와 같이 수사 시에는 대용량 저장 매체에 대한 수사 어려움이 존재하게 되는데, 조사 및 분석에서 소요되는 시간을 단축시키기 위해서 잘 알려진 파일은 검색 대상에서 제외하고, 집중적으로 검색할 대상을 선정하는 접근 방식을 통해 검색 범위를 축소하여 조사 우선순위를 부여하는 것이 중요하다. 이러한 기능을 제공하는 검색 기술 중 하나가 '해쉬 값 생성을 통한 검색(Hashed Search)'이며, 이 방식은 준비된 참조 데이터 셋(Reference Data Set) 적용을 통해 조사 분석 대상을 구분하는 기술이다. 이미 미국에서는 이러한 해쉬 값 생성을 통한 검색(Hashed Search) 기술을 활성화하고 있으며, 일반 수사관들도 쉽게 사용할 수 있게 하기 위해 잘 알려진 파일들의 표준 해쉬셋을 NIST에서 제작 후 무상으로 배포하는 'National Software Reference Library(NSRL) 프로젝트'를 실시하고 있다.[3]

증거물 분석 시에는 용의자가 사건에 연루된 파일을 삭제하거나 변형하여, 수사관이 확인할 수 없도록 훼손하는 경우가 발생한다. 이러한 경우에는 수사관이 증거물 획득을 위해 파일 복구(Recovery)작업이 필요하며, Encase와 같은 디지털 포렌식 소프트웨어 도구를 이용하여 하드디스크 등과 같은 저장 매체에 존재하는 데이터를 복구할 수 있다. 이러한 복구 작업을 논리적 복구라 하며, 대부분의 수사관은 삭제 및 훼손된 파일, 파일시스템을 복구하는 기술로서 위 방식을 적용하여 수사하게 된다. 복구된 데이터가 증거물로서 효력을 갖기 위해서는 데이터가 변형되지 않도록 유지하는 작업이 필요하며, 대표적으로는 해쉬 값 생성을 통해 데이터 무결성을 보장하는 방법이 있다.

증거물을 조사 및 분석하다보면 물리적으로 훼손되어 있거나, 증거로서 가치 있는 데이터가 다른 데이터로 물리적인 방법을 통해 덮어쓰는 경우가 발생할 수 있다. 그러한 경우에는 물리학적인 방법을 통해 하드디스크와 같은 저장 매체에 대하여 데이터를 일부 또는 완벽하게 복구할 수 있다.

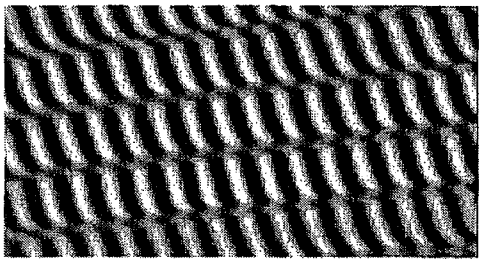

그림 5 하드디스크의 원자현미경 확대 사진

1) 하드디스크의 물리적 복구 I

그림 5와 같은 구조를 갖고 있는 하드디스크는 디스크의 표면을 전자기적으로 변화시켜 대량의 데이터를 저장하고 비교적 빠르게 접근할 수 있는 저장 매체이다. 이와 같이 자성을 이용해 데이터를 저장하게 되는 매체들을 마그네틱 미디어(Magnetic Media)라 말한다.

범죄 발생 현장에서 압수된 하드 디스크에 존재하는 디지털 증거물이 디지털 포렌식 소프트웨어 도구로 논리적 복구가 불가능하거나, 물리적으로 훼손되어있는 경우에는 물리적 복구 방법을 통해 작업을 수행하게 된다. 물리적 복구는 저장매체의 물리·전자적인 복구를 말하며, 물리적 또는 전자적으로 단·합선으로 훼손된 저장매체를 정상상태로 복구하게 된다.

하드디스크를 물리적인 방법을 통해 복구하는 방안은 1996년 Peter Gutmann이 제시하였다.[1] 본 소절에서는 마그네틱 미디어 중에서 대표적으로 하드디스크를 물리적인 복구 방안을 설명한다.

첫 번째로 자기력을 재는 원자 현미경을 이용하여 디스크의 조사하는 방법이 있다. 검사 방식에는 Magnetic Force Microscopy(MFM)와 magnetic force Scanning Tunneling Microscopy(STM)가 존재하며, 위와 같은 현미경 도구를 활용한 관찰 방법으로 하드디스크에 저장된 데이터를 조사하게 된다. 데이터를 디스크에 저장하는 경우, 극 성질을 이용하여 데이터를 0과 1의 2진수 값을 비트단위로 저장하게 된다. 하드디스크의 '헤드(Head)'라는 장치를 통해 데이터를 입력하며, S극과 N극 성질에 각각 0과 1의 2진수 값을 부여하게 된다. 즉 데이터를 디스크 저장 시에 S극의 성질을 먼저 읽게 되면 0, 반대로 N극의 성질을 읽게 되면 1의 비트 값을 갖게 된다. 데이터를 읽는 경우에도 극 성질을 통해 먼저 읽히는 극에 따라 0과 1이 결정된다.

디스크 초기 상태	첫 데이터 입력	기울기	덮어쓴 데이터	기울기
0	0	0	1	0.95
0	1	1	1	1.05

표 1 하드디스크의 데이터 입력 시 기울기 비교

하드디스크는 기본적으로 0으로 설정되어 있고, 자성의 성질에 따라서 데이터를 입력하면 표 1과 같이 기울기가 나타나는데, 0인 경우 S극, 1인 경우 N극으로 정확히 위치해 있다는 것을 의미한다.

초기 상태에서 첫 데이터를 입력하면 정확히 극 방향으로 위치해 있지만, 데이터를 덮어쓰면 기울기가 각기 다르게 나타나는 것을 표 1을 통해 알 수 있다. 즉 0.95와 1.05인 경우에는 정확히 N극으로 위치하지 않고 비스듬하게 기울어져 있음을 의미한다. 이러한 기울기 성질을 이용하면, 이전 데이터가 0 또는 1인지를 각 비트별로 이전 데이터가 무엇인지 판단이 가능하게 되므로 복구할 수 있다.

2) 하드디스크의 물리적 복구 II

두 번째로는 헤드를 이용하여 디스크에 데이터를 입력 시의 간격 차를 이용하는 방법이며, 이를 이용하는 복구 방법 또한 존재한다.

입력 상태	쓰기 간격 (단위: ㎛)
첫 데이터 입력	0.5
데이터 덮어쓰기	0.49
간격 차	0.01

표 2 하드 디스크의 데이터 입력 시 간격 차

표 2의 결과는 데이터 입력 시 쓰기 간격을 표시한 것이며, 덮어쓰기를 마친 데이터는 이전 데이터에 비해 폭이 좁게 입력된다. 즉 0.01㎛의 간격이 나타나게 되며, 원자 현미경을 이용하여 이전 데이터를 일부 복구할 수 있다.[1]

지금까지의 설명한 두 가지 물리적 복구 방법들은 덮어쓰기 이전의 데이터만을 복구할 수 있지만, 그 이전의 데이터를 복구하는 것은 불가능하다. 따라서 증거물이 삭제되고, 여러 번 덮어쓰기가 수행되어도 복구할 수 있는 기술이 연구되어야 할 것이다.

마. 보고서 작성 단계

디지털 포렌식 절차 중의 마지막 단계에서는 디지털 증거 수집, 운송, 보관, 조사, 분석 단계를 총 망라하는 내용을 문서화하여 증거물과 함께 법정에 제출하게 된다. 보고서를 읽게 되는 판사와 검사, 변호사 등은 컴퓨터에 대한 기본 지식이 부족한 경우가 대부분이기 때문에 비전문가도 알기 쉽고 가독성 있게 작성해야 한다. 따라서 증거물 획득, 보관, 분석 등의 과정을 논리 정연하며 명백하고 객관성 있게 설명해야 한다. 수사 시에 수행했던 기록을 상세하게 기록함으로서, 예상치 못한 사고로 데이터가 유실되어 변경이 생겼을 경우에 범죄 혐의 입증에 무리가 없음을 논리적으로 설득할 수 있어야 한다.

4. 결론

수시 시의 체계적이고 적법한 절차를 사용하는 디지털 포렌식은 신기술을 이용하여 세분화 및 전문화되는 모든 범죄에 대응하여 필수적으로 사용되고 있다. 따라서 절차 연속성을 보장하는 절차와 함께 증거물에 대한 체계적인 관리 및 수사가 이뤄져야 하며, 다양한 환경에서 디지털 증거물을 획득할 수 있도록 기술이 더욱 향상되어야 할 것이다. 이를 통해 컴퓨터나 네트워크 이외에도 임베디드 시스템에 저장되어 있는 모든 정보들을 수집하고 분석할 수 있어야 하며, 그러한 분석을 위해서는 디지털 포렌식에 대한 연구를 통해 수집·분석 도구를 개발해야 할 것이다. 이러한 연구를 바탕으로 모든 전자적 정보를 이용하여 범죄 수사를 진행할 수 있는 디지털 포렌식 기술의 구축이 이뤄져야 할 것이다.

5. 참고문헌

[1] P. Gutmann, Secure Deletion of Data from Magnetic and Solid-State Memory, 6th USENIX Security Symposium Proceedings, July, 1996.

[2] International Association of Computer Investigative Specialists, http://www.iacis.info

[3] NIST, http://www.nsrl.nist.gov/, National Software Reference Library.

[4] 한국디지털포렌식학회, 디지털증거 표준 가이드라인, 경찰청사이버테러대응센터, 2006.

[5] 한국디지털포렌식학회, http://kdfs.or.kr/

[6] 경찰청 사이버테러대응센터, http://www.ctrc.go.kr/

[7] 대검찰청, http://www.sppo.go.kr/ , 대검찰청 중앙수사부 컴퓨터수사과.

[8] Guidance Software, http://www.guidancesoftware.com/, Encase Forensic Tool.