연구보고서 2007-07

디지털 증거분석 표준 가이드라인에 대한 연구

≪硏 究 陣≫

연 구 위 원 : 이 성 진 (백석대학교 정보통신학부 교수)

목 차

표 차 례

그 림 차 례

요 약 문

1. 제 목

디지털 증거분석 표준 가이드라인에 관한 연구

2. 연구의 목적 및 중요성

디지털 정보기기를 매개체로 하여 범죄가 발생하는 경우, 컴퓨터내에 있는 자료(디지털 전자자료)를 근거로 하여 증거를 확보하여야 한다. 그러나 컴퓨터의 주메모리 또는 보조메모리 등에 기록되어 있는 자료는 생성/복사/변경/삭제/전송 등이 매우 용이하므로 법정증거로 활용되기 위해서는 특별한 절차와 방법들이 요구된다. 본 연구에서는 컴퓨터, 즉 정보처리기기가 범죄에 직간접적으로 연관되어 있는 경우에 이들로부터 필요한 단서를 확보하는 방법과 획득한 디지털 자료를 분석하는 방법 등을 포함하여, 최종적으로 그 분석한 결과가 법적인 증거로 되기 위한 제반 절차와 방법에 대해서 고찰하여 디지털 증거분석 표준절차에 입각한 증거분석 장비 개발 및 표준지침 마련하기 위한 연구를 수행한다.

3. 연구의 내용 및 범위

디지털 정보기기 등에서 입수되는 디지털 증거의 수집・분석・보관・운반・복구 등의 절차에 대해서 연구하는 것으로 다양한 정보기기들로부터 증거를 획득하기 위한 방법 및 절차 등, 디지털 증거분석 절차 및 제반 법률 등을 연구하며, 최종적으로 디지털 증거의 압수수색・감청 절차 및 지침(안)을 작성한다.

4. 연구결과

연구결과로서, 제 1장에서는 연구의 개요에 대해서 설명한다. 제 2장에서는 디지털 포렌식스 유형에 대해서 설명하고, 제 3장에서는 증거로써 디지털 자료의 특징에 대해서 살펴본다. 제 4장에서는 디지털 포렌식스에 관련 기술들을 설명하고, 제 5장과 6장에서는 디지털 자료의 획득방법 및 분석 방법 및 이에 따르는 이슈들을 살펴본다. 제 7장에서는 디지털 증거자료의 법률적 검토 및 증거능력 향상 방안을 설명하고, 끝으로 제 8장에서는 결론을 말하고, 향후 연구발전방향 등을 제시한다.

5. 기대효과

본 연구로 범죄수사에 공여된 디지털증거의 과학적 분석으로 법정에서 유죄의 증거능력을 확보하고, 범죄수사에서 증거발견과 이의 과학적 입증 등으로 범죄수사역량을 획기적 개선할 수 있으며, 제정될 표준절차를 디지털 증거분석 도구(장비, S/W) 개발에 접목하여 좀더 선진화된 디지털 증거 분석 방법론을 제시할 수 있을 것으로 기대된다.

Ⅰ. 서 론

이제 우리사회에서 컴퓨터가 없는 생활은 상상하기도 어렵게 되어가고 있다. 복잡한 업무에서부터 오락에 이르기까지 컴퓨터가 사용되지 않는 분야를 찾아보기가 힘들어 지고 있으며, 하루 일과 중 많은 시간을 인터넷을 이용하는 사람들이 급격히 증가하고 있는 것으로 나타나고 있다. 또한 버클리 대학의 한 보고서에 의하면 전 세계적으로 생성되는 정보의 약 92%이상이 디지털 형태인 것으로 나타나고 있다[22]. 따라서 범죄수사에 있어서도 컴퓨터는 매우 중요한 수사의 수단이 될 뿐만 아니라 수사의 대상이 되기도 한다[4]. 그러나 컴퓨터에 저장되어 있는 디지털 자료는 생성, 처리, 삭제, 변경, 복사, 전송 등이 매우 용이한 특징을 갖고 있어서, 이들 자료가 법적인 증거가 될 수 있는가?의 의문이 생기게 된다.

본 연구에서는 컴퓨터가 범죄에 직간접적으로 연관되어 있는 경우에 이들로부터 필요한 단서를 확보하는 방법과 획득한 디지털 자료를 분석하는 방법 등을 포함하여, 최종적으로 그 분석한 결과가 법적인 증거로 채택되도록 하기 위한 제반 절차와 방법에 대해서 설명한다.

컴퓨터 포렌식스는 컴퓨터 등과 같은 정보처리기기에서 수집할 수 있는 디지털 자료가 법적증거능력을 갖게 하기위한 제반 절차와 방법을 통칭하는 것이다. 포렌식스(Forensics)의 사전적 의미는 “법정의”, “변론의“ 의미가 되며, 예로서 “forensics medicine”은 “법의학”이라는 뜻이 된다. 따라서 디지털 자료가 증거능력을 갖게 하기위한 절차로써의 의미는 “Digital forensics”가 좀더 광범위하고 정확한 의미가 될 수 있으나 “Computer Forensics”가 초기에서 사용되어 왔고, 그 의미 또한 크게 벗어나지 않으므로 아직까지 통용되고 있는 실정이다. 또한 최근 “Cyber Crime”, “Cyber Forensics”등이 인터넷 범죄영역에서 사용되고 있다.

본 보고서의 제 2장에서는 디지털 포렌식스 유형에 대해서 설명하고, 제 3장에서는 증거로써 디지털 자료의 특징에 대해서 살펴본다. 제 4장에서는 디지털 포렌식스에 관련

기술들을 설명하고, 제 5장에서는 디지털 자료의 획득방법에 대해서 설명한다. 제 6장에서는 디지털 증거자료의 분석 방법 및 여기에 따르는 이슈들을 살펴본다. 제 7장에서는 디지털 증거자료의 증거능력 향상 방안을 설명하고, 제 8장에서는 결론을 말하고, 향후 연구방향 등을 살펴본다.

Ⅱ. 디지털 포렌식스 유형

디지털 자료의 출처 또는 대상에 따라서 기술 및 법률적 관심사항이 약간씩 다르므로 편의상 디지털 포렌식스는 다음과 같은 영역으로 나뉘어 질수 있다.

1. 디스크 포렌식스 (Disk Forensics) [1,5]

대용량의 비휘발성 저장매체로부터 디지털 자료를 획득, 분석하는 영역이다. 자료의 획득 및 분석과정에서 대상 매체의 내용이 우발적으로 변경되지 않게 하고, 만일 변경되었으면 그 위치를 쉽게 찾을 수 있게 하는 도구 등이 필요하게 된다. 대용량 디스크에서 원하는 자료를 빠르고 정확하게 검색하는 기능, 삭제된 파일을 복구하는 기능 등이 주로 활용된다. 최근 다양한 정보기기에서 많이 사용되는 플래시 메모리도 이 영역에 속한다.

2. 네트워크 포렌식스 (Network Forensics) [2,5,6,7]

통신중에 있는 데이터를 감청하여 증거자료로 활용하고자하는 분야이다. 감청의 속성상 은밀하게 취득된 자료는 증거자료가 되기 어려움으로 이에 대한 고려가 필요하고, 더욱이 불법적으로 획득된 자료는 증거능력이 없는 것으로 취급됨으로 이러한 업무를 수행할 경우에는 법률적 검토와 취급상의 많은 주의를 필요로 한다.

3. 전자메일 포렌식스 (E-mail Forensics)

전자메일, 메신저 등에서 증거자료를 확보하고 분석하는 영역이다. 메일발신자 추적기술, 메일검색, 삭제된 메일복구 등의 기술이 주로 활용된다. 압수·수색시 수신자가 읽어본 메일인가, 아닌가에 따라 법적해석이 달리될 수도 있다.

4. 웹 포렌식스 (Web Forensics) [1]

WWW(World Wide Web)과 관련된 제반사항 즉, Web 내용의 지적 재산권, Web click의 법적 효력, 게시판에 게재된 글의 법률적 효력 등이 주요 이슈가 되고, 기술적으로는 웹 방문자, 방문시간, 방문자의 주소 및 경유지 분석 등이 주요 관심사가 된다.

5. 모바일 포렌식스 (Mobile Forensics) [4]

PDA, 휴대폰 등과 같은 휴대용 기기로부터 증거자료를 획득하고 분석하는 영역이다. 이 분야에서의 한 특징은 배터리에 의해 주 메모리 내용이 유지되고 있으므로 이들의 관리가 중요하게 된다. 휘발성 자료를 획득하기 위해서는 별도의 탐침도구(하드웨어 또는 소프트웨어)을 사용하게 되는데, 이 도구를 사용한다는 한편으로 증거물이 일부 훼손된다는 의미도 내포함으로, 이들 도구를 본격적으로 사용하기 위해서는 인증과 검증과정이 필요하게 된다. 만일 무선 기기를 사용하는 휴대폰 또는 PDA 등을 조사하는 경우에는 조사중에 외부로부터 전화 또는 패킷이 들어오거나 나갈 수 있으므로 전자파 차폐장치(실)에서 작업을 해야 한다.

6. 소스코드 포렌식스 (Source Code Forensics) [12]

필적감정과 유사하게 프로그램의 원시코드 유형을 보고 최초 작성자를 구분하는 영역이다. 만일 어떤 컴퓨터에서 프로그램을 개발했었다면 남겨진 흔적들을 조사하여 그 원시코드와 실행프로그램과의 상관관계를 분석할 수도 있게 된다.

7. 멀티미디어 포렌식스 (Multimedia Forensics)

디지털 형태의 그림, 음악, 비디오 파일에 관련된 저작권, 이들 자료의 위변조 여부 분석 및 데이터 은닉 기술 (Steganography) 등이 여기에 해당된다.

8. 데이터베이스 포렌식스 (Database Forensics)

이 영역에서는 압수·수색이 현실적으로 어려운 대형 시스템에서 디지털 증거물 획득 및 분석 방법 등의 이슈를 다룬다. 증거물 획득과정에 관계자를 입회시키고 작업과정과 결과파일에 대해서 해시값을 계산, 문서화 한 후 서명하는 절차 등이 필요하게 된다.

Ⅲ. 증거로서 디지털 자료의 특징

수사 및 법적인 관점에서 디지털 자료는 표 1과 같이 잠재성, 디지털, 취약성, 대량성, 다양성, 휘발성 및 네트워크성 같은 특징이 복합적으로 작용하여 증거자료의 처리에 있어서 특별한 방법과 철차를 요구하게 된다.

<표 1> 증거로서 디지털 자료의 특징

특 징	내 용	대응 방법
1. 잠재성(Latent)	육안으로 식별불가	- 판독장치 필요, 판독장치에 대한 인증 및 검증
2. 취약성 (Fragile)	생성, 삭제, 변경(위.변조) 용이	- 디스크 복제 장치, 쓰기방지 장치
3. 디지털(Discrete)	0과 1들로 구성, 원본과 복사본 구분 어려움	- 무결성 검증도구 MD5,SHA1
4. 대량성(Massive)	기본적으로 방대한 자료	- 강력한 검색 및 분석 도구
5. 다양성(Various)	다양한 소프트웨어 존재인과관계 규명 어려움	- 다양한 분석도구, 분석관 교육 훈련 문제
6. 휘발성(Volatile)	주기억 장치의 내용은 쉽게 소멸됨	- 자료 획득 및 인증 방법
7. 네트워크성 (Networked)	네트워크로 연결되어 있으므로 해킹위험 및 사법한계	- 해킹 / 바이러스 검사 / 분석, 국제공조

1. 잠재성

컴퓨터에서 처리하는 자료는 대부분은 전자기(電磁氣) 또는 광학매체(光學媒體)에 기록되어 있어서 육안으로 읽을 수 없을 뿐만 아니라 코드화 되어 있어서 그 내용을 파악하기 어렵게 되어 있다. 또한 이러한 판독장치는 대부분 하드웨어뿐만 아니라 소프트웨

어로 구성되어 있어서, 만일 판독시스템에 악의적인 소프트웨어가 탑재되어 동작하는 경우에는 그 판독결과를 왜곡시킬 수 있는 위험성이 있다. 따라서 디지털 증거물의 처리에 사용되는 판독시스템은 그 시스템이 정확하게 동작하는지를 검증할 수 있게 하는 수단이 확보되거나 또는 필요시 적절한 기관에 의한 인증이 요구 된다.

2. 디지털

디지털 자료의 근본적인 특징이다. 연속적인 물리량의 변화를 그대로 저장, 처리하는 아날로그 시스템과 다르게 디지털 시스템은 데이터를 0과 1로만 구성되는 이진수로 변환하여 처리함으로 저장장치에 실제로 저장되는 것은 두 가지의 상태만을 구별할 수 있으면 된다. 따라서 저장할 때에는 그 두 상태에 따른 물리적량을 새로 설정하여 기록함으로 원본의 신호형태가 복사본으로 전달되지 않게 된다. 즉 근본적으로 원본과 복사본의 구분이 불가능하게 되는 것이다.

컴퓨터의 특징은 대량의 자료를 신속하고 정확하게 처리할 수 있고, 또한 이들 자료를 빠르게 저장 및 전송할 수 있는 점이다. 컴퓨터가 다루는 자료는 디지털 형태로 기본적으로 0과 1(신호가 있고, 없고)의 이진 데이터로 구성되고, 문자 또는 숫자를 표현하기 위해서는 별도의 코드 값을 부여하여 사용하게 된다.

일반적으로 아날로그 형태의 신호를 복사하는 경우에는 복사본의 신호가 원본의 신호보다 S/N(신호/잡음)비가 감소함으로 이론적으로 원본과 복사본의 구별이 가능하다. 그러나 디지털 신호의 경우에는 신호의 유무만을 검출하면 소기의 목적을 달성할 수 있으므로, 원본의 신호형태를 복사하는 것이 아니라 신호의 유무만을 검출한 후 디지털 형태의 신호를 다시 만들어서 기록하게 된다. 그러므로 기록매체의 신호형태를 근거로 원본과 복사본을 구분하는 것은 무의미하게 하게 되며, 다만 주변의 부가정보 (예, 기록된 시간 등)등을 이용하여 추정할 수 있기는 하나, 이러한 부가정보 또한 변경될 수 있으므로 주의해야 한다.

3. 취약성

취약성은 컴퓨터가 갖는 빠른 자료처리능력과 복잡한 소프트웨어에서 기인된다. 일반적인 개인용 컴퓨터로도 수백만자의 자료를 단 몇 초 이내에 처리하여 저장할 수 있을 뿐만 아니라 한 컴퓨터에 설치되어 있는 소프트웨어의 종류 및 수가 너무 많아서 어떤 작업을 할 때 내부적으로 어떻게 처리되는지를 정확히 알기 어렵게 된다. 한 예로 윈도우즈 운영체제에서 폴더만 열어보아도 해당 디스크에는 쓰기 동작이 일어나게 된다. 이러한 우발적인 문제를 방지하기 위해서는 증거 디스크를 복제하여 사용하거나, 디스크 쓰기방지 장치를 이용할 수 있다. 또한 디스크 전체 또는 부분에 대해서 MD5 또는 SHA1 해쉬값을 계산하여 변경여부를 확인할 수도 있다.

4. 다양성

다양성 문제는 다양한 소프트웨어를 종합적으로 사용하면서 발생한다. 각 소프트웨어의 종류에 따라서 사용하는 자료의 형식이 다를 뿐만 아니라 저장되는 위치 또한 다르기 때문이다. 한 예로 처리하는 자료가 문서인가? 또는 음성 또는 동영상 같은 멀티미디어 자료인가? 에 따라서 그 자료형식이 크게 다르게 되고, 또한 같은 문서 파일이라도 압축이 되었거나 암호화 되어 있는 경우도 서로 다르게 저장되게 된다. 간단한 예로, 메모리 상에서 4116 또는 010000012의 값을 읽어 들였을 때 이를 문자로 보면 영문자 'A′ 로 볼 수 있지만 숫자 정수로 보면 65가 된다. 이러한 상황에서 다른 형식으로 저장되어 있는 자료를 근거로 해당 컴퓨터에서 언제 어떤 일이 발생했는지를 추적하는 작업은 사용되었던 소프트웨어의 종류가 많을수록 복잡해지게 마련이다. 윈도우즈 XP 운영체제에 기본적으로 사용하는 오피스관련 프로그램들을 설치해도 시스템에는 약 10만개 이상의 파일이 존재하게 된다. 이러한 상황에 잘 대처하기 위해서는 운영소프트웨어에 대한 해박한 지식뿐만 아니라 다양한 응용 소프트웨어에 대한 많은 경험을 필요로 하게 된다.

5. 대량성

최근 주로 사용되는 소형의 노트북에도 약 40GB 용량의 하드디스크가 장착되고 있으며, 데스크탑 컴퓨터의 경우에는 120GB 이상의 용량의 디스크가 많이 사용되고 있다. 40GB는 400억 바이트가 저장될 수 있는 용량으로 이중에서 어떤 단서를 수작업으로 찾는 다는 것은 육안으로 해변에서 바늘을 찾는 것에 비유될 수 있다. 따라서 전문적인 검색도구의 사용은 필수적이며, 이러한 자료를 효과적 처리하기 위하여 고도로 전문화된 분석 및 저장장치 등이 요구되고 있다.

6. 휘발성

해당 정보기기에 전원이 공급되지 않으면 저장하고 있던 자료가 모두 소멸되는 행태이며, 컴퓨터의 주메모리의 내용, PDA, 휴대폰 등의 자료가 여기에 해당된다. 이러한 휘발성자료를 획득하기 위해서는 LAN 또는 USB와 같은 통신장치와 서브렛(servlet) 또는 액티브싱크(ActiveSync) 같은 소프트웨어가 사용되는데, 이들 소프트웨어가 일단 설치된다는 것은 증거가 훼손되는 것을 의미하므로 이들 하드웨어 및 소프트웨어에 대한 인증 및 검증이 필수적이 되며, 이들의 사용방법도 매우 철저하게 통제될 필요가 있다.

7. 네트워크성

대부분의 정보기기는 통신기능을 갖고 있으므로 언제든지 해킹의 위험에 노출되어 있고, 또한 인터넷 등에 연결되어 있는 경우에는 국경을 넘어서 행위가 일어남으로 사법처리에 한계를 보이게 된다. 이들 문제를 해결하기 위해서는 증거자료를 분석할 때 해킹을 당했는지의 여부를 검토해 보아야 하며, 국제적인 사법공조를 원활히 할 필요가 있다.

Ⅳ. 디지털 포렌식스 기술 및 해외 동향

1. 디지털 포렌식스 기술 개요

일반 범죄에 컴퓨터가 관련되어 있는 경우 해당 컴퓨터에서 혐의에 대한 단서 또는 직접적인 증거를 확보하거나, 정황을 좀더 구체화하기 위한 보조자료 등을 얻을 수도 있다. 컴퓨터 등에서 보편적으로 얻을 수 있는 정보는 대략 언제, 어떤 프로그램이 수행되었는지의 정보와 문서를 작성한 경우에는 그 파일내용을 찾을 수 있다. 또한 인터넷을 통하여 방문한 경우에는 방문한 사이트 주소, 시간 등과 같이 의외로 많은 정보를 얻을 수도 있다. 그러나 시스템 상태에 따라 특정 자료의 수집을 실패할 수도 있으므로 이를 고려하여야 한다.

공갈, 사기(위조), 협박, 횡령, 명예훼손 등 같은 종류의 범죄에서 컴퓨터가 이용된 경우 이러한 범죄에 대한 수사는 비교적 간단하게 이루어 질수 있다. 인터넷을 이용하여 게시판에 글을 올리거나 또는 전자우편을 이용하여 협박편지를 보낸 경우에는 경유된 관련 서버에서 로그 자료를 확보하고 피의자가 최종적으로 사용했을 것으로 추정되는 컴퓨터에서 인터넷 접속 및 사용 로그 또는 메일 발송 로그 또는 원본 파일 등을 찾는다. 물론 이러한 과정에서 압수수색에 필요한 제반 절차는 지켜져야 하며 그렇지 아니한 경우에는 획득한 증거물이 증거능력을 상실할 수 도 있게 된다.

주의해야할 사항은 아무리 단순한 보조 자료를 획득하는 경우라 하더라도 가능하면 디지털 포렌식스 방법 및 절차를 따라야 한다는 것이다. 왜냐하면, 컴퓨터상의 간단한 조작만으로도 단서 또는 증거를 훼손할 수 있기 때문이다[14,15,16].

좀더 기술적인 범죄에 대해서는 컴퓨터 해킹 및 바이러스 등과 같은 컴퓨터 범죄에 대한 증거를 획득 및 분석하는 것이다[6,11]. 이론적으로 해킹 피해시스템에서 획득된 자료는 해킹의 의해 조작되어 있을 수 있으므로 증거물로 채택되기 어려운 측면이 있지만

디지털 포렌식스 방법과 절차를 따르면 최소한 해킹 및 바이러스에 의한 피해 상황을 정확하게 보존할 수 있으며, 경우에 따라서는 해킹 방법 및 경로 등을 추적할 수 있는 단서 등도 발견할 수 있다[28,32]. 또한 사이버테러 등과 같은 고도의 지능범죄도 디지털 포렌식스 분야에서 다룰 수 있지만 정보은닉 (steganography) 등과 같이 복잡한 기술 문제들이 다루어지므로 본고에서는 더 이상 언급하지 않는다.

<그림 1> 쓰기방지장치의 예

디지털 포렌식스는 기본적으로 컴퓨터라는 기술적인 장치를 주 대상으로 조사 및 분석하는 절차 및 방법이므로 다양한 기술들이 종합적으로 사용되게 된다. 중요하고 많이 사용되는 하드웨어 장치 및 소프트웨어들로는 표 2와 같은 도구들이 있다.

이들 중에서 “MD5” 또는 “SHA1”으로 불리는 해싱 소프트웨어들은 디지털 자료를 읽어서 128비트 또는 160비트의 유일한 숫자를 생성해내는 기능을 수행한다. 따라서 임의의 길이의 데이터에 대해서 같은 해싱 값이 나오면 그 데이터는 변경되지 않았다고 검증할 수 있게 된다.[1)]

1) 최근에 자료의 일부를 조작하여 같은 해시값이 나오도록 한 연구결과가 발표된바 있다. (http://www.jabo.co.kr/sub_read.html?uid=10076&section=section4&wdate=1112251408) 그러나 같은 해시값을 나오도록 조작하여 유의미한 자료를 만들기는 어려움으로 증거자료의 조작여부를 증명하는데에는 큰 문제가 발생되지 않고 있지만 장기적으로 보다 큰 수의 해시값을 사용하는 알고리즘들이 사용될 것으로 보임

<표 2> 컴퓨터 포렌식스 기술

구 분	명 칭	용 도	비 고
하드웨어	디스크 복제 장치	디스크를 비트단위로 복제	Logicube www.logicube.com
	디스크 쓰기방지 장치	우발적으로 디스크에 쓰기가 일어나지 않도록 방지 IDE -> IDE, SCSI -> IDE USB2 -> IDE, IEEE1394 -> IDE	www.encase.com www.logicube.com www.digitalintel.com
개별 소프트웨어	MD5 또는 SHA1 Hashing	디스크 전체 또는 특정 블록, 또는 파일단위로 해시를 계산하여 봄으로 데이터가 변경되지 않았음을 검증	dd (Linux) [38,39]
	삭제된 파일 복구	삭제된 파일을 복구, 삭제된 데이터베이스 복구	FinalData [36,37] www.finaldata.com
	고급검색도구	다양한 형식의 파일들에 대해서 검색 - 워드, 엑셀, 파워포인트, 압축파일, 슬랙영역[2], 삭제된 파일	www.hurricanesoft.com www.winhex.com
	암호 및 패스워드 해제	Zip 또는 Windows 시스템의 암호를 크랙	www.hackersnews.org/pds/sniffer.htm
종합 소프트웨어	디지털 포렌식스 종합	증거자료 획득, 검색, 분석, 보고서 작성 등 일련의 작업을 한 소프트웨어에 수행할 수 있게함	www.encase.com www.finaldata.com www.ftk.com

2. 디지털 포렌식스 관련 해외 동향

디지털 포렌식스는 컴퓨터 관련 기술, 요원, 법률 및 제도 등이 종합적으로 발전되어야 하는 분야이다. 절차법이 잘 발달되어 있는 영·미의 경우, 다양한 디지털 포렌식스 관련 하드웨어 및 소프트웨어 들이 개발되어 사용되고 있으며, 다양한 교육기관에서 다양한 교육 프로그램이 개설되고 있다. 특히 잘 정리된 디지털 증거 압수·수색 매뉴얼인 Searching and Seizing Computers and Obtaining Electronic Evidence in

2) 파일을 디스크에 저장할 때 블록단위로 저장하는데 마지막 블록의 사용되지 않은 영역을 슬랙이라 한다. 이 영역은 일반 문서 편집기 등으로는 볼 수 없고, 섹터내용을 직접 편집할 수 있는 도구들을 이용하여 자료를 저장 하거나 열람할 수 있다.

Criminal Investigations[3] 작성하여 게제하고 있으므로 디지털 포렌식스에 대한 이슈를 대부분의 관계자들이 빠르게 공감하고 있다. 매우 중요한 기능 중에 하나는 그림 2와 같이 NIST내에 포렌식스 도구 검증 기능을 두어 많이 사용되고 있는 도구들을 시험하고 그 결과를 홈페이지에 게시하고 하고 있다는 점인데, 이는 인증과 검증이 매우 중요한 포렌식스 분야에 매우 중요한 기능으로 여겨진다.

<그림 2> 컴퓨터 포렌식스 도구 시험 프로젝트 홈피 예

그림 3에와 같이 교육 훈련과정은 서로 분리되어 운영되고 있으며 교육과정에서는 이론적이고 관련 제품, 제도, 법률 등의 제정 및 개발 등에 중점을 두고 있고, 훈련과정에서는 포렌식스 제도 및 기술등의 활용쪽에 많은 비중을 두고 있다. 훈련과정에서는 대부분 인증제도를 두고 있으며 최소한의 교육과정 및 관련 분야 실무경력, 주어진 시험에서 통과를 해야 자격증을 발급하고 있다.

ROLE	EDUCATION	TRAINING
CNF technician	Introduction to forensic science Introduction to computer science Introduction to computer hardware Introduction to operating systems Introduction to criminal and civil law	A+ training Net+ training Basic computer seizure Basic data recovery and duplication
CNF policy maker	Information management Forensic science Information assurance Knowledge management Enterprise architecture	Survey or seminar courses in information assurance, legal issues, and CNF techniques
CNF professional	All of CNF technician items Upper-level BS/MS courses in information systems,network systems, architecture, and criminal, civil, and procedural law	All of CNF technician training plus advanced data recovery and moot court training
CNF researcher	Doctorate-level education or a masters degree with extensive experience in computer forensics	Specific research areas are difficult to project, but researchers should receive hands-on training in the research areas

<그림 3> 디지털 포렌식스 관련 교육 및 훈련 과정 예[44]

3) http://www.usdoj.gov/criminal/cybercrime/tecpa.html

Ⅴ. 디지털 증거자료의 획득 방법

1. 디지털 증거의 처리 원칙

본 장에서는 법적증거로 사용할 목적으로 디지털 정보기기로부터 자료를 획득하는 방법에 대해서 살펴본다. 증거를 획득하는 과정에는 수사관, 획득 및 분석시스템, 수사 대상시스템, 관련 지침 등이 관여된다. 획득된 증거자료가 얼마나 신빙성이 있느냐 하는 것은 이들 구성요소들에의해 많은 영향을 받게 된다. 수사관은 수사의 주체로서 증거의 획득에서부터 분석, 보관이송 및 보고의 전과정을 관리 감독하는 역할을 담당하므로 만일 피의자 또는 해당 사건과 특별한 관계가 있다면 그에 의해 처리된 증거의 신빙성은 잃게 될 것이다. 증거 획득 및 분석 시스템은 대부분 증거처리과정에서 원본 훼손을 최소화하도록 설계되어 있으므로 전문화된 포렌식 도구를 사용하는 것은 매우 중요하며, 경우에 따라서는 이들 포렌식 도구도 악의적으로 조작되어 있을 수 있으므로 이들을 미리 방지할 수 있도록 제품에 대해 인증 및 검증절차 등이 마련되어야 한다.

정보기기 기반의 디지털 증거를 처리하는 지침 등은 해당 기관의 업무의 성격에 따라 조금씩 다르지만 공통적으로 무결성, 당위성, 증적보존 및 합치성 원칙들이 준수되어야 하는 것으로 주장되고 있다[9, 23, 33].

무결성 원칙: 증거를 처리할 때 행해진 조작에 의해 원본 자료가 변경되지 않아야 한다.

당위성 원칙: 원본 자료에 대해 직접 조작을 하는 경우 이에 대한 당위성이 있어야 한다.

증적보존 원칙: 증거를 처리할 때 사용되는 방법과 절차는 기록되어 보관되어야 하며, 이는 제 3자에 의해 검토될 수 있어야 한다.

합치성 원칙: 수사관(수사관서)는 앞서 언급된 절차와 방법이 상위법 또는 규칙에 저촉되지 않으며, 이 절차가 잘 지켜지게 할 책임이 있다.

증거 획득과정에서의 주된 관심사는 획득을 하는 과정에서 자료가 조작 또는 변경되는가의 여부와, 향후 분석과정에서 필요한 정보를 어떻게 확보할 것인가의 문제이다. 또한 대상 시스템이 획득시점에서 운영중인가 또는 대형컴퓨터 시스템 같이 전체 시스템 또는 저장매체를 압수·수색할 수 없는 경우 등이 이슈가 되고 있다.

디지털 증거를 획득하는 과정에서 원본자료 접근에 대해서 무결성 원칙을 지킬 수 없는 경우에는 이에 대한 당위성을 확보한 후에 객관적 소명자료를 확보하기위해 제 3자를 입회시키고 증거획득에 대한 모든 조작과정을 문서화 한 후에 이에 대한 서명날인을 받는 방법(이하, 3자입회) 또는 전작업 과정을 캠코더로 촬영하여 작업기록를 보존하는 방법 등이 사용될 수 있다.

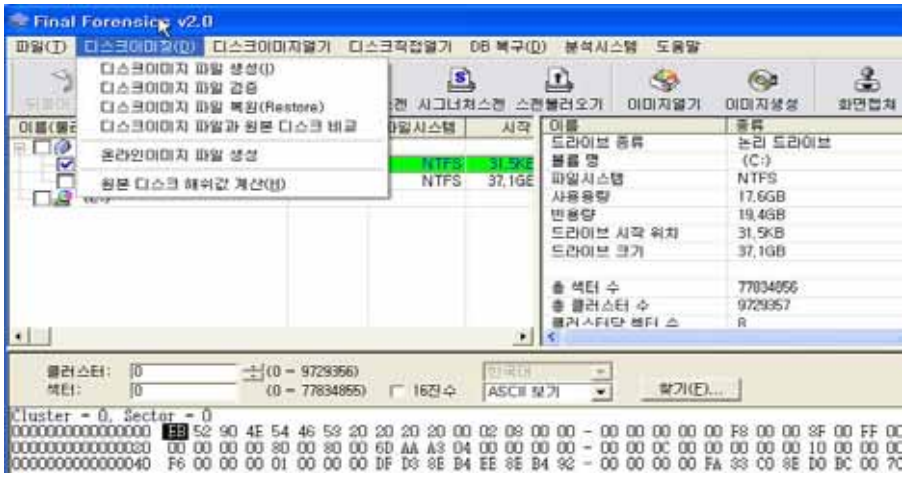
또한 획득하려는 대상 시스템의 종류에 관계없이 해당 시스템이 위치해 있는 장소 주변 환경에 대한 정황, 시스템의 결선상태, 시스템의 모델번호를 포함하는 제원 등의 정보를 카메라 또는 캠코더 등을 이용하여 확보하고, 주 사용자, 주변에 있는 각종 외장 저장매체(외장 디스크, 백업 디스켓, CD-R, 각종 프린트 결과 물, 등)의 확보가 매우 중요하다. 시스템이 켜져 있는 경우에는 현재 설정되어 있는 시스템의 시간 및 수행되고 있는 프로그램들을 사진으로 확보하는 것은 나중에 그 증거물을 분석할 때 매우 유용한 정보가 될 수 있다.

현재 압수·수색을 하고 있는 컴퓨터가 피의자의 소유 또는 주사용로 보는데 어려움이 있는 경우에는 키보드 등에 남아 있는 지문 등도 함께 확보할 필요가 있다.

2. 운용중이 아닌 시스템에서 증거획득

운용중이 아닌 시스템에서 증거자료의 획득은 비교적 간단하다. 대부분의 디지털 증거는 시스템에 장착된 디스크 등에 저장되어 있으므로, 이 디스크를 시스템에서 탈착하여

같은 종류의 하드디스크에 복제하거나 또는 디스크 이미지 획득 등의 증거획득 방법을 사용한다. 디스크 이미지 획득 방법은 대상 저장매체의 모든 내용을 섹터단위로 읽어서 분석 시스템에 파일로 저장하여 놓고, 이 파일을 마치 디스크처럼 사용하도록 하는 것이다. 일단 디스크를 이미지로 획득하면 더 이상 원본 디스크 또는 복제 디스크를 사용하지 않아도 삭제된 파일 복구 등 원본 디스크에서 하던 모든 분석업무를 수행 할 수 있게 된다[36, 37]. 또한 이미지를 획득하는 단계에서 MD5 또는 SHA1 해쉬를 계산하여 두면 분석 과정에서 디스크의 내용이 변경된 것을 검증할 수 있으며, 이 획득된 이미지를 이용하여 다른 매체에 원본과 같은 상태의 디스크를 만들 수도 있다. 이러한 디스크 이미징 기술은 디스크 뿐만 아니라 이동식 저장매체에서도 사용할 수 있다. 대부분의 디지털 증거분석 소프트웨어에서는 이러한 디스크 이미지 획득 방법을 제공하고 있고, 이 방법을 사용할 것을 권고하고 있다. 그림 4는 파이널포렌식스의 이미징관련 기능의 예이다[8].



<그림 4> 디스크 이미지 생성 및 검증

가. 디스크를 탈착하여 쓰기방지장치 사용:

이 방식은 대상 시스템이 비교적 소규모인 개인용 컴퓨터 또는 소규모 서버시스템 등

인 경우에 적합하다. 대상 시스템의 디스크를 탈착하여 그림 5와 같은 쓰기방지장치를 경유하여 분석시스템에 연결한 후 디스크의 내용을 복제하거나 또는 분석하는 방식이다. 이러한 쓰기방지장치를 사용하는 방식의 장점은 분석시스템에서 우발적으로 대상 디스크에 쓰기동작을 하여도 쓰기방지장치까지만 쓰기가 되고 최종적으로 분석 디스크에는 쓰기가 되지 않으므로 비교적 안전하게 분석업무를 빠르게 수행할 수 있다는 점이다.

<그림 5> 디스크쓰기방지 장치의 예

나. 대상 시스템을 별도의 운영체제로 구동:

수사 또는 조사의 대상 시스템에 이미 적재되어 있던 운영체제로 시스템을 부팅하면 시스템의 마지막 상태 정보들을 모두 잃어버릴 수 있을 뿐만 아니라 본의 아니게 압수시점에서 디스크에 쓰기동작이 발생하여 오해의 소지가 발생할 수 있다. 이를 해결하기 위한 방법은 시스템에 설치되어 있는 운영체제를 사용하지 않고 별도의 CD 또는 디스켓에 있는 분석용 운영체제로 시스템을 기동하여, 원래 탑재되어 있던 하드디스크에 어떤 변경도 일어나지 않도록 하는 방법이다. 이러한 부팅 CD 또는 디스켓에는 대부분의 LAN 카드 드라이버도 같이 준비되어 있으므로 이를 이용하여 원래 디스크에 있던 내용을 네트워크를 통하여 분석시스템에 보내서 분석 할 수 있도록 되어 있다. 이러한 분석 소프

트웨어로는 FIRE 또는 Helix 등이 있다. 이들 소프트웨어는 한 장의 CD-ROM에 Linux 부팅을 포함하는 운영체제 및 포렌식 소프트웨어가 함께 탑재되어 있어서, 이 CD-ROM을 이용하여 부팅한 후 간단한 디지털 증거자료 획득 및 분석작업을 수행 할 수 있다[42,43]. 그림 6은 Helix로 소프트웨어를 이용하여 개인용 PC를 부팅한 경우의 예이다.

<그림 6> Helix로 부팅한 화면의 예

다. 이동식 저장매체 분석:

이 방식은 floppy, tape, CD-ROM/R/RW, DVD-R/RW, flash memory 및 외장형 하드디스크 등과 같이 비휘발성 디지털 자료 저장매체로부터 디지털 증거자료를 획득하는 경우이다. 이러한 이동식 저장매체로부터 증거자료를 획득하는 경우에도 사소한 실수로도 그 내용이 변경될 소지가 있으므로 최소한의 안전조치를 취할 필요가 있다. 만일 취급되는 매체가 그림 7과 같이 쓰기 잠금 기능이 준비되어 있으면, 반드시 'Lock' 스위치를 쓰기방지 모드로 전환한 후 분석시스템에 삽입한다. 이러한 외장형 저장장치에서 자료를 획득하는 경우에도 가능하면 디스크 이미지를 만든 후 이 이미지 파일을 기반으로 분석하는 것을 권장하고 있다.

<그림 7> 이동식 저장매체의 쓰기잠금 기능 예

3. 운용중인 시스템에서 증거 획득

운용중인 시스템에서 디지털증거를 획득해야 하는 경우는 디스크를 착탈하기 어려운 상황, 또는 대규모 시스템에서 파일의 일부를 획득해야하는 상황 등이 있다.

이러한 경우에는 시스템의 자료가 계속 변하고 있는 상태에서 증거를 획득하는 경우이므로 이렇게 확보한 자료의 신뢰성을 확보가 어렵게 된다. 따라서 가능하면 제 3 자를 입회 시키고 증거자료의 획득 과정 및 획득된 자료를 해시하여 그 결과값을 기재한 문서에 서명날인을 받아 놓을 필요가 있다. 특히 운용중인 시스템의 경우 증거를 획득하는 방법과 시점이 매우 중요함으로 이에 대한 대비책을 세워놓아야 한다. 만일 압수·수색 당시 시스템이 운용중에 있더라도 운용중인 상태의 현재 정보에 대한 필요성이 그렇게 크지 않으면 최소한의 정보만을 획득하고 시스템을 정지한 후에 5.2절의 방법을 사용하여 디지털 증거를 획득할 수 있다.

가. 탐침(probe) 하드웨어 또는 소프트웨어 사용:

이 방식은 대상시스템을 끄지 않고 여기에 간단한 하드웨어(주로 USB 케이블)와 드라이버 소프트웨어를 설치한 후에 이를 통하여 필요한 자료를 획득하도록 하는 것이다. PDA 또는 휴대폰에서의 증거자료 획득 또는 EnCase Enterprise Edition에서 SAFE 서버를 경유한 원격지 시스템 분석방법 등이 이 경우에 해당된다. 이러한 방식에서 증거자료를 획득하기 위해서는 필연적으로 대상시스템의 내용이 일부 변경되는 문제가 발생

되므로 이들 하드웨어 및 소프트웨어의 기능에 대한 검증 및 인증은 반드시 이루어져야 한다. 그림 8은 paraben사의 PDA 분석도구, 그림 9는 Guidance Soft사의 SAFE 서버 사용의 예이다. Paraben사의 PDA Data Acquisition 소프트웨어는 분석시스템과 통신 모듈로 ActiveSync 통신 모듈을 사용하여 PDA의 자료를 분석시스템으로 가져오도록 하고 있다.

<그림 8> PDA에서 증거자료 획득의 예

<그림 9> EnCase SAFE 서버를 경유한 증거획득

EnCase SAFE서버를 경유하는 경우에는 수사 대상 시스템에 Java 기반의 servlet 프로그램을 설치하고 이를 통하여 필요한 증거자료를 획득하도록 하고 있다.

나. 별도의 분석 소프트웨어 사용:

이 방식은 주로 대상시스템이 웜·바이러스에 감염되었거나, 또는 해킹당하여 시스템에 있는 실행파일들이 더 이상 정상적이지 못하다고 판단될 때 사용된다. 일반적으로 크래커들은 시스템을 해킹한 후에 해킹한 사실을 은폐하거나 또는 후에 재침입을 용이하기 위해 필요한 소프트웨어를 설치하여 놓는데, 이를 통칭 루트킷(rootkit) 이라고 한다. 이러한 루트킷이 일단 설치되면 시스템에서 기존에 사용하던 주요 명령어들 즉, 프로세스 상태를 보는 명령(ps), 디렉토리의 파일리스트를 보여주는 명령어(ls)등이 정상적으로 동작을 하지 못하게 된다. 따라서 이러한 경우에는 표 3과 같이 별도로 준비해놓은 명령어 프로그램들을 이용해야 한다. 리눅스 운영체제의 경우에는 Helix 또는 FIRE 같이 포렌식 분석용으로 제작된 패키지를 사용할 수 도 있다[42, 43].

<표 3> 증거물 분석을 위한 기본 도구

명 령 어	용 도
ls	디렉토리의 내용을 표시
dd	디스크를 이미지로 복사
df	디스크 사용량을 표시
des	파일을 암호화
file	파일의 유형을 표시
pkginfo	패키지 정보를 표시
find	조건에 부합되는 파일을 재귀적으로 검색
grep	파일에서 조건에 부합되는 라인을 출력
icat	디바이스를 개방하고 지정된 i-node 와 함께 파일을 복사
lsof	현재 개방되어 있은 파일들을 출력
md5sum	주어진 파일에 대한 md5 해시를 계산
netcat or cryptcat	TCP, UDP 연결을 통한 파일 출력
netstat	네트워크 연결, 라우팅테이블, 등을 출력
pcat	프로세스 메모리를 복사
perl	Practical Extraction and Report Language
ps	프로세스 상태를 출력
stace, truss	프로그램이 수행되면서 사용하는 시스템 호출 및 시그날들을 출력
strings	프로그램에 있는 스트링을 출력
vi	파일 편집기
cat	파일 출력기
more or less	페이지 단위 파일 출력기
gzip	파일 압축 및 복원
last	마지막으로 로그인한 기록목록을 출력
rm	파일 삭제
script	터미널에서 발생하는 모든 세션을 파일에 기록
bash	명령언어 해석기 (Bourne-Again Shell)
modinfo	커널 모듈에 대한 정보를 출력
lsmod	적재된 커널 모듈들을 표시
ifconfig	네트워크 인터페이스를 설정

다. 대상 시스템에 내장되어 있는 소프트웨어 사용:

이 방식은 대상 시스템이 해킹 등을 당하지 않고 비교적 정상적으로 운용되고 있는 시스템에서 증거물을 획득하거나 분석할 때 사용한다. SAN(Storage Area Network)등을 사용하는 대규모 데이터베이스관리 시스템 등에서 사용되는 방식이다. 이 방식에서는 해당 시스템 관리자의 협조가 매우 중요하며, 조사단계에서 행해진 모든 조작은 기록되어야 하며, 도출된 결과 파일에 대해서 해시를 계산하고 서명날인을 받아 놓을 필요가 있다.

4. 제3자 시스템에서 증거 획득

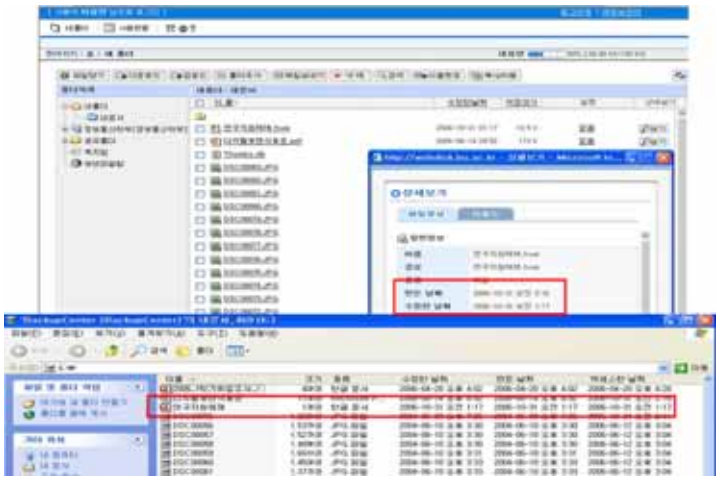
이해 당사자의 소유물이 아니고, 단지 이용자로서 사용하고 있는 웹디스크, 메일서버 및 웹 콘텐츠(홈페이지, 또는 게시판 내용)의 내용을 수색하는 경우에는 이용자 수준에서 데이터에 접근하는 방법과 서버관리자 수준에서 데이터에 접근하는 방법이 있다. 이용자 수준에서의 데이터 접근 방법은 마치 일반 사용자가 정상적으로 서비스를 받은 것처럼 데이터에 접근해서 증거자료를 획득하는 방식이므로 획득과정에서 엑세스에 따른 변경이 일어나게 된다. 즉, 무결성 원칙이 지켜지지 않게 되는 문제가 있다.

한편 서버 관리자 수준에서의 데이터접근 방식은 시스템이 해당 서비스를 제공하는 시스템에 관리자 모드로 로그인 하여 시스템에 접근하거나 또는 5.2절의 증거획득 방법들을 사용할 수 있다. 그러나 이 방식에서는 여러 사용자가 그 서비스를 이용하고 있는 경우에 해당 서비스에 많은 무리를 줄 수 있으므로 꼭 필요한 경우가 아니면 적용하기 어렵게 된다. 또한 이러한 서버 관리자 수준에서의 데이터접근에 대해서는 필요한 영장을 발부 받아야 한다.

가. 웹디스크의 내용:

웹디스크는 인터넷을 통하여 원격지 서버 파일시스템의 일부를 자신의 디스크처럼 사

용하게 하는 서비스이다. 이 서비스에서 제공하는 디스크도 일반 디스크와 같이 파일 및 폴더접근에 대해서 MAC(Modified, Accessed, Created) time 변경이 일어남으로 이를 고려하여야 한다. 따라서 일반 사용자 수준에서 디지털 증거를 획득하는 경우, 만일 웹디스크에 있는 자료가 중요한 증거로 사용될 것으로 예상되면 5.1절에서 언급된 것처럼 제 3자 입회 및 필요한 파일에 대한 해시계산 및 서명날인이 필요하게 된다. 웹디스크 서비스는 그림 10과 같이 기본적으로 원격지에 있는 저장소를 마치 자신의 한 디스크인것 처럼 사용할 수 있게할 뿐만아니라 웹화면을 통해서도 원격 저장소의 파일을 접근할 수 있게하고 있다. 이런 경우 사용자에게 사용자에 의해 변경된 시간은 서로 다를 수 있으므로 이점을 유의해야 한다.



<그림 10> 웹디스크의 사용의 예

나. 메일서버의 내용:

메일서버의 구성은 그림 11과 같이 기능적으로 크게 중계 역할을 담당하는 중계서버(SMTP)와 사용자와의 인터페이스를 담당하는 웹메일 서버 또는 POP3메일서버로 구성된다.

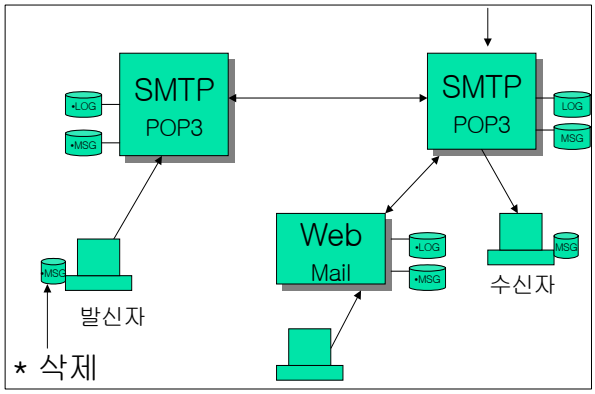
중계서버는 전자메일(e-mail)이 송수신되는 메일에 대한 메시지 ID, 송수신 시간 등의 메타정보가 로그로 남게되므로 이들에 대한 자료를 획득할 수도 있다. 웹메일 서비스

를 제공하는 시스템의 경우 서버에 사용자의 메일이 저장되는 형태를 취하므로 사용자가 삭제하지 않은 메시지는 확보할 수 있다. POP3메일서비스를 제공하는 시스템의 경우, 사용자가 Outlook, Outlook express 등과 같은 메일 클라이언트 소프트웨어를 사용하여 메일을 가져가면, 서버의 메시지는 삭제되도록 하고 있다[4]. 따라서 피의자가 주로 사용하는 컴퓨터를 먼저 조사하여 각 메일계정에 대해서 어떤 방식의 메일서비스를 사용하는지 파악한 후에 해당 서버 관리자에게 필요한 자료를 요청할 필요가 있다. 이러한 요청에 대해서도 영장을 필요로 한다.

다. 웹 콘텐츠 (홈페이지, 게시판 내용 등)

웹에 게시되어 있는 내용은 모든 이용자에게 공개된 내용과 특정 회원들에게만 공개되는 제한공개 내용으로 구분된다. 사용자 수준에서의 증거 획득은 시간 간격을 두고 해당 사이트를 방문하여 컴퓨터 모니터에 나타난 화면을 출력하여 두거나 또는 제 3 자로 하여금 같은 절차와 방법으로 수행하도록 하여 자료를 남겨놓게 할 수도 있다.

서버 관리자 수준에서의 증거획득에서는 해당 콘텐츠의 내용뿐만 아니라, 콘텐츠가 게시된 일자, 게시한 사람의 ID 및 IP(Internet Protocol) 주소 또는 그 게시물을 삭제한 일자 등의 자세한 내용을 확보할 수 도 있다.



<그림 11> 전자메일 시스템 구성도

4) 사용자 설정에 의해 서버에 메시지를 남겨 놓을 수 도 있음

정보기기에서 디지털자료를 획득하는 목적은 기본적으로 법정의 증거로서 사용될 수 있도록 하거나 또는 단순히 수사의 참고자료로 사용될 수도 있으므로 디지털 증거를 획득하는 방법은 사건의 종류 또는 해당 증거자료가 적재되어 있는 시스템 및 주변 상황에 따라 매우 다르게 된다. 또한 그 자료가 어떻게 사용될 것인가에 따라 획득하는 방법도 달라 질 수 있다. 따라서 책임 수사관은 디지털 포렌식스 이슈를 충분히 이해하고 해당 사건의 속성 및 상황에 따라 적절한 대처 방법을 강구할 필요가 있다.

Ⅵ. 디지털 증거물 분석

디지털 증거의 처리는 일반적으로 디지털 증거물 획득, 분석, 보관, 보고 등의 과정을 거치게 된다. 본 장에서는 디지털 증거물의 분석과정에 대해서 설명한다.

증거물을 분석하기 위해서는 다양한 분석기술들이 활용되며, 주로 관심 있는 증거를 담고 있는 파일들을 찾거나, 이들 증거자료의 생성, 변조, 전송, 삭제 등과 같은 행위에 대한 부수적인 정보를 파악하는 과정이다. 분석은 컴퓨터상에서 이루어진 어떤 행위에 대한 사실관계를 확증하는 과정이므로 기본적으로 누가, 무었을 언제, 어떻게, 어디서, 왜 했느냐의 물음에 답하는 것이므로, 주로 사용자 실명 또는 ID, 프로그램, 특정 파일의 이용시간(Modified, Accessed, Created Time, Deleted Time[5]), 관련 IP(Internet Address)를 분석하게 된다.

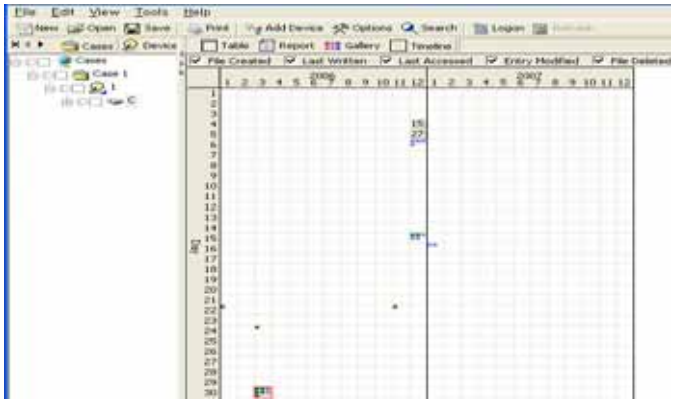
분석을 효과적으로 하기 위해서 시계열 분석, 폴더브라우징, 포렌식검색, 로그분석, 해시분석, 시그니처분석, 파일복구, 암호분석, 프로세스분석 등과 같은 다양한 기법들이 개발되어 사용되고 있다. 디지털 증거물 획득에서와 같이 증거물 분석과정에서도 가능하면 전문 포렌식 도구를 사용할 것을 권장하고 있는데 이는 사소한 부주만으로도 증거물이 훼손될 위험을 갖고 있기 때문이다.

1. 시계열 분석 (Timeline Analysis) [8,24,27]

이 분석에서는 파일 시스템에 있는 파일들이 변경, 생성, 사용 및 삭제된 시간별로 분류하여 어느 시간에 어떤 파일들이 이용되었지를 확인하는 작업이다. 이 분석에서 주의해야 점은 첫째로 시스템의 CMOS 시간 설정이 잘못되어 있으면 파일들의 이용 시간도 이에 따라 달라질 수 있는 점이고, 둘째로 외부에서 USB 저장장치등을 이용하여 복사하

5) 여기에서 삭제된 시간은 파일이 실질적으로 삭제된 시간이 아니고 휴지통(Recycle Bin)으로 옮겨진 시간을 의미한다.

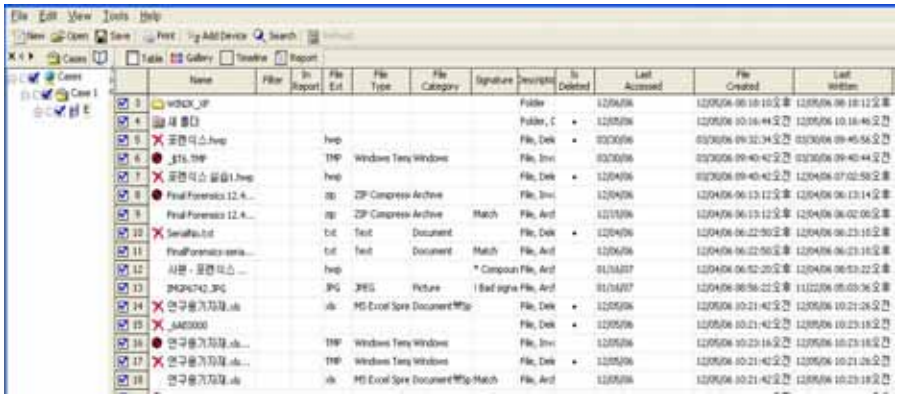
여 가져온 파일의 경우 그 시간값을 신뢰할 수 없게 된다. 셋째로 간단한 프로그램의 조작만으로도 파일에 관련된 시간 속성 값을 변경할 수 있다는 점이다. 따라서 시계열 분석을 통하여 어떤 사실을 확증하고자 할 경우에는 매우 주의를 요하게 된다. 그림 12는 EnCase를 사용한 시계열 분석의 한 예로 주어진 디스크의 전체 파일에 대해 사용된 시간대 별로 파일들을 숫자 또는 심볼로 나타내어, 사용자가 화면에서 해당 날자와 시간대를 마우스로 클릭하면 자세한 파일 목록을 볼 수 있도록 하고 있다.



<그림 12> EnCase를 사용한 시계열 분석의 예

2. 폴더 브라우징 (Folder Browsing) [24]

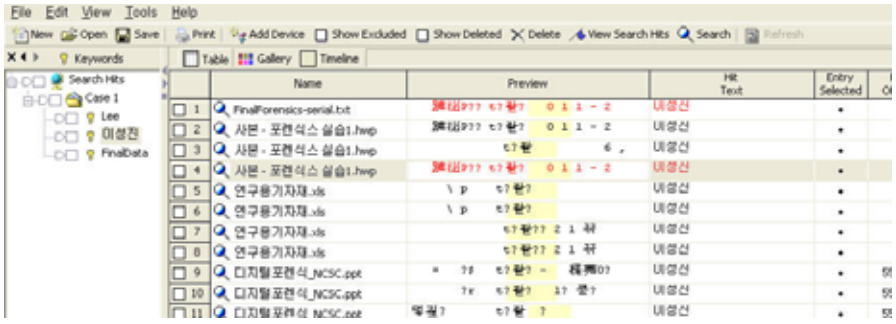
파일 및 디렉토리의 엑세스 시간을 변경하지 않으면서 효과적으로 파일목록을 열람하고 필요한 경우 해당 파일의 내용을 볼 수 있게 한다. 파일의 이름, 확장자, 확장자 변경 유무, 사용된 시간, 삭제 유무, 물리적 위치, 파일의 해시값 등을 필요에 따라 시간별 또는 이름 순으로 정렬하여 볼 수 있도록 하여 찾고자 하는 파일을 쉽게 발견할 수 있도록 하고 있다. 그림 파일의 경우 조그만 그림(Thumb nail) 을 볼 수 있도록 하는 소프트웨어들도 있다. 그림 13은 EnCase를 사용하여 폴더 열람을 하는 경우의 예이며, 정상적인 파일과 삭제된 파일을 쉽게 구분 할 수 있고, 각 파일의 확장자, 사용된 시간 등을 일목요연하게 확인 할 수 있도록 하고 있다.



<그림 13> EnCase를 사용한 폴더 블라우져의 예

3. 고급 검색 (Forensic Search) [24,38]

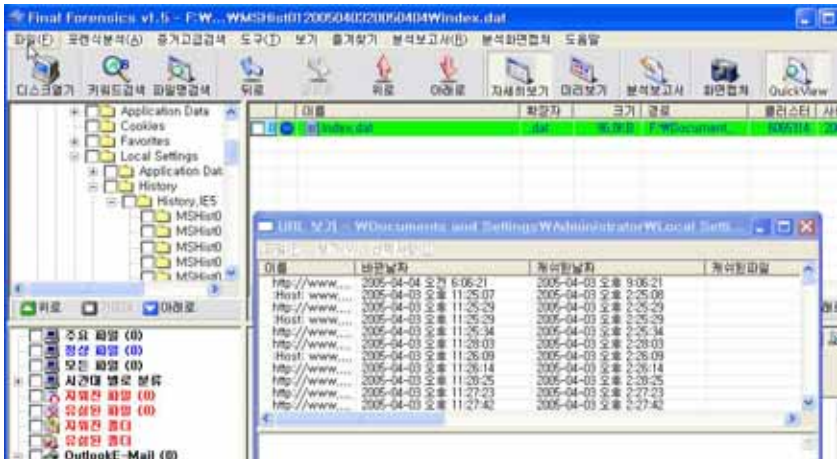
일반검색과 다르게 고급검색 (Forensic Search)은 대상 파일시스템에 있는 정상적인 파일뿐만 아니라 파일슬랙영역, 삭제된 파일 또는 압축된 파일에 있는 내용에 대해서도 검색할 수 있도록 한다. 파일시스템의 용량이 수십기가 바이트만 되더라도 고급검색에 소요되는 시간은 수시간 이상으로 소요되어 분석 작업에 많은 영향을 미치게 된다. 이 검색시간은 표면적인 파일시스템의 용량 뿐만 아니라 그 안에 있는 자료의 형식, 삭제된 파일의 량 등에 의해서도 좌우됨으로 검색을 하기전에 이에 대한 고려를 할 필요가 있다. 그림 14는 EnCase 도구를 이용하여 '이성진' 이라는 키워드로 검색한 결과를 보여주는 예이다.



<그림 14> 포렌식 검색의 예

4. 로그 분석 (Log Analysis)

로그 분석은 디지털 증거분석에 있어서 매우 광범위한 작업에 속하는 것으로서 웹브라우져, 메신져, FTP 등 다양한 응용 프로그램의 사용 흔적을 조사하는 작업이다. 응용 프로그램들이 수행하면서 남기는 로그(Log)의 내용은 매우 다르게 된다. 따라서 주로 보편적으로 사용되는 응용 프로그램들에 대한 로그의 종류와 포맷 등을 미리 분석하여 원하는 분석을 조직적으로 할 수 있도록 준비하여 놓는 것이 매우 중요하게 된다. 그림 15는 파이널 포렌식스를 이용하여 웹방문기록 로그를 분석하는 화면의 예이다.

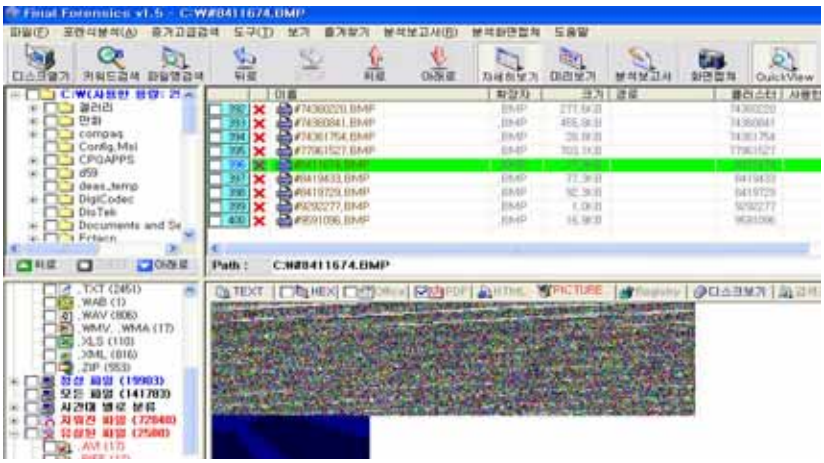


<그림 15> 로그 분석의 예

5. 파일 복구 (Deleted file Recovery) [36,37]

삭제된 파일을 복구하는 것은 디스크 포렌식 영역에서 매우 중요한 분석 방법 중에 하나이다. 현재 Windows XP 운영체제상에서 파일을 정상적으로 삭제하면 일단 디렉토리(폴더)에서 그 목록을 삭제한 후 휴지통(Recycled Bin)으로 옮겨 놓는다. 만일 휴지통에 쌓여 있는 삭제된 파일의 총 크기가 일정량 이상이 되거나 사용자가 휴지통비우기 명령을 실행하면 휴지통내에 있던 파일들을 삭제하게 된다. 여기에서 파일이 삭제된다 함

은 그 파일의 내용을 담고 있던 클러스터(몇몇 섹터)를 더 이상 사용하는 클러스터로 등록하여 다른 파일에서 사용할 수 있도록 하는 것이다.



<그림 16> 삭제된 파일 복구의 예

파일 복구 기능은 삭제된 것으로 마크된 디렉토리 목록을 조사하여 시작 클러스터를 찾아 사용중인가의 여부를 점검하여 조건에 맞는 내용을 조합하여 파일로서 복원하는 것이다. 따라서 복구된 파일 명과 그 내용이 정확히 일치한다고 보기 어려움으로 잘못된 결론으로 이끌 수 있으므로 사용상에 주의가 필요하다. 그림 16은 파이널 포렌식스를 이용하여 삭제된 파일을 복원하고 있는 예이다. 이 예에서 그림 파일의 일부가 깨져서 나오고 있는데 이는 해당 클러스터의 내용이 덥혀 쓰여졌기 때문이다. 또한 이름이 숫자로 나오는 이유는 디렉토리 목록에서 관련 정보를 얻을 수 없는 경우이기 때문이며, 이러한 경우를 유실된 파일을 복구한다고 한다.

6. 해시 분석 (Hash Analysis) [24]

파일의 내용을 직접 비교하지 않고 해시값을 이용하여 동일한 파일이 있는지를 찾아내는 일종의 검색방법이다. 해킹 프로그램 등과 같이 그 외형만을 보고는 그 내용을 파악하기

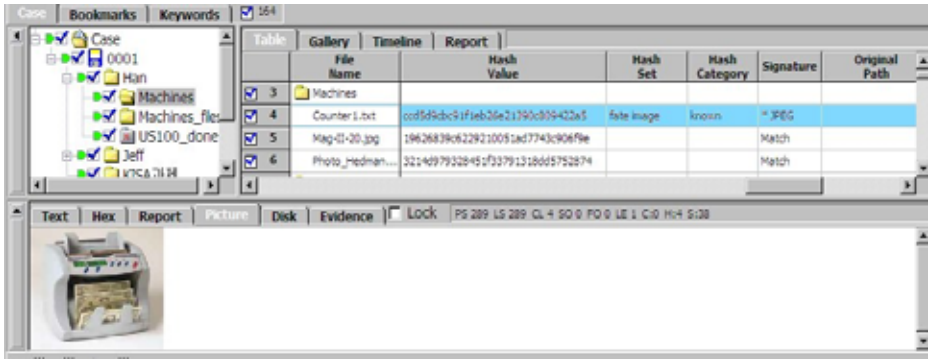
어려운 파일들의 해시값을 미리 계산하여 목록을 만들어 놓고, 대상이 되는 시스템에서 모든 파일에 대해 해시를 계산한 후에 이들 해시값을 미리 계산해둔 해시값과 비교하여 동일한 파일이 존재하는지를 알아내는 방법이다. 미국의 경우 http://www.nsrl.nist.gov 사이트 등을 통하여 각종 파일들의 해시값을 제공하고 있다. 그림 17은 word.exe 실행파일에 대한 해시값의 예이다.

```
"SHA-1","FileName","FileSize","ProductCode","OpSystemCode","MD4","MD5","CRC32","Spec
ialCode" <13><10>
"AC91EF00F33F12DD491CC91EF00F33F12DD491CA",WORD.EXE",1217654,103, "T4WKS",
"CC12130FF145DE78DCC12130FF145DE79", "DC2311FFDC0015FCCC12130FF145DE78",
"14CCE9061FFDC001","""<13><10>
```

<그림 17> NSRL에서 제공하는 해시셀의 예

7. 시그니처 분석 (Signature Analysis)

시그니처 분석은 고의 또는 조작오류로 파일의 확장자가 변경되었을 때 이를 효과적으로 발견하기 분석이다. 파일의 이름, 확장자, 길이, 사용시간 등과 같은 정보는 파일의 내용에 기록되지 않고 그 파일이 속한 디렉토리(폴더)에 저장됨으로 파일의 확장자를 변경해도 그 내용에는 전혀 변화가 일어나지 않는다. 그러나 폴더 브라우져등과 같은 많은 프로그램들은 단순하게 파일의 확장자를 기준으로 프로그램을 실행시키도록 되어 있고, 사용자 또한 이에 쉽게 착각하게된다. 그림 18에서 같이 Counter1.jpg라는 파일을 Counter.txt라고 확장을 변경한 경우 시그니처 분석을 통하여 그 파일은 원래 이미지 파일이었다고 표시를 하고 있다. 이러한 분석의 원리는 자주 사용되는 파일의 내용에 그 파일의 속성을 나타내는 숫자 또는 문자열을 포함하고 있으므로 이들 숫자 또는 문자열과 확장자를 분석하여 확장자의 변경여부를 판단하게 된다.



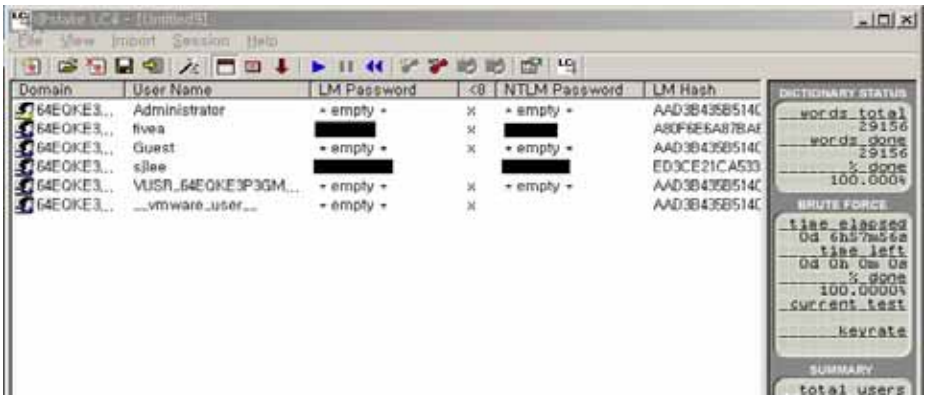
<그림 18> 해위 분석의 예

시그니처 분석은 특정한 파일을 매우 단순하게 숨기는 형태이며 보다 적극적인 은닉을 한 경우에는 전문적인 스테가노그라피(steganography) 분석을 필요로 하게 된다. 어떤 정보를 은닉하기 위해서 사용될 수 있는 방법은 크게

1) 확장자 변경 - 파일확장자 변경 (예, aaa.jpg ==> aaa.txt)
2) 파일명 변경 - 특수문자사용 (예, aaa.jpg ==> .aa.jpg)
3) 특정 디렉토리 - /dev 또는 \windows\system32\ 디렉토리에 원하는 파일을 보관
4) 파일 슬랙 영역 - 크기가 고정되어 있는 파일의 끝 이후에 필요한 정보 저장
5) 인위적 베드섹터 - 특정 섹터를 인위적으로 오류가 있는 것처럼 처리하고 그곳에 정보 저장
6) 임베딩(imbedding) - 주로 대용량 멀미미디어 파일에 소량의 필요한 정보를 넣음 (손실압축을 사용하는 파일에서 효과적임)로 나누어 볼 수 있다. 특히 6) 임베딩 방법은 다양한 기술적 도구들이 개발 되면서 많은 관심을 받고 있다.

8. 암호 분석 (Crypto Analysis)

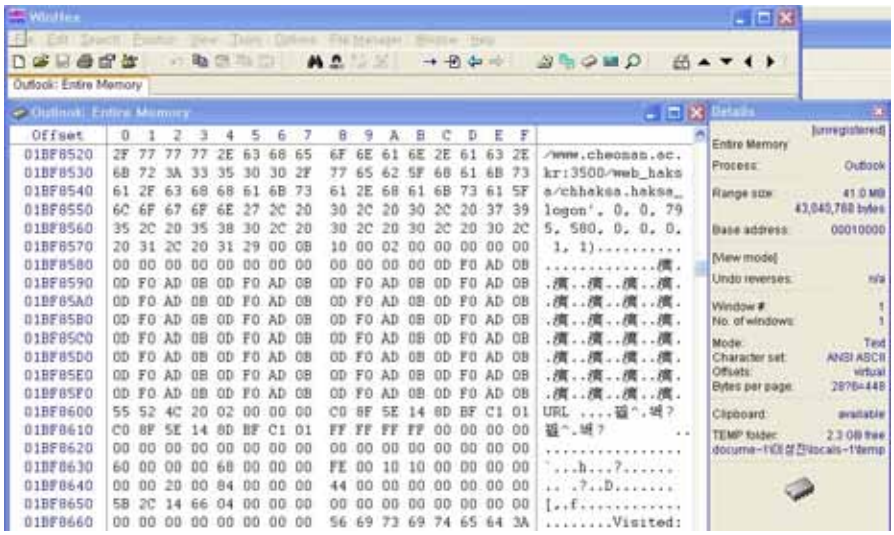
패스워드로 보안 조치되어 있는 시스템에 접근하거나 또는 암호화된 파일 (예, Zip 또는 엑셀 파일 등)등의 내용에 접근하기 위해서는 암호를 알아내는 방법이 중요하게 된다. 물론 수사기법을 활용하여 피의자로부터 필요한 암호를 넘겨받으면 쉽게 해결되지만 그렇지 못한 경우에는 기술적으로 해결해야만 하게 된다. 이런 경우에 사용할 수 있는 방법은 피의자의 신상정보로부터 유추된 문자열과 적당한 숫자를 조합하여 패스워드로 입력하여 보는 방법과, 피의자 시스템에 가능한 모든 문자열을 추출하여 이를 시스템적으로 대입해 보는 방법, 마지막으로 모든 가능한 문자조합을 만들어서 대입하는 방법 (brute force 대입)들이 있다. 그림 19는 마지막 방법을 사용하는 프로그램을 이용하여 8자리로 구성된 패스워드를 찾아내는 예를 나타낸 것으로 약 6시간 57분이 소요되었음을 알 수 있다. 대부분의 일반 사용자는 유사한 패스워드 체제를 사용하고 있는 경우가 많으므로, 일단 간단한 시스템을 분석하여 피의자가 사용하는 패스워드 체제를 알게 되면 이를 응용하여 웹 또는 시스템 로그인 등 다른 시스템에도 비교적 손쉽게 접근할 수 있게 된다.



<그림 19> 암호분석의 예

9. 프로세스 분석 (Process Analysis)

프로세스 분석은 현재 수행되고 있는 프로세스의 메모리 내용을 분석하는 방법과 프로그램의 동작상태를 분석하는 방법으로 크게 나누어 진다. 프로세스의 메모리 내용을 분석하기 위해서는 그림 20과 같이 프로세스의 내용을 볼 수 있는 도구를 이용한 간단한 검색명령을 수행하여 원하는 결과를 얻을 수 있다. 프로세스의 동작 현상을 분석하기 위해서는 디버거 또는 프로세스 모니터 같은 도구를 이용하여 프로그램을 수행되는 과정과 이 수행되면서 남기는 흔적을 조사해 나가게 된다. 이러한 작업과정은 많은 시간과 집중력이 필요하므로 사전에 철저한 준비를 할 필요가 있다. 만일 분석대상이 악성코드인 경우에 한번의 실수로도 치명적인 결과를 초래할 수 도 있으므로 VMWare 같은 소프트웨어를 이용하거나 격리된 네트워크 환경에서 분석작업을 할 필요가 있다.



<그림 20> 프로세스 분석의 예

◎ 보관 및 이송 과정

디지털 증거물은 대부분 미세신호를 이용하여 저장매체에 전자기 또는 광학적으로 자료를 기록하게 된다. 따라서 이들 매체는 전자기적 간섭 또는 매체의 물리적 변질에 의

해 그 내용이 변경될 수 있으므로, 이에 대한 대비책을 강구하여야 한다. 또한 전자매체의 특성상 간단한 조작만으로도 그 내용이 위변조 될 수 있으므로 보관 및 이송절차가 엄격해야 한다. 저장매체의 종류에 따라 다르지만 자료의 보존연한은 약 수년에서 30년 내외가 됨으로 중요한 자료를 장기간 보관할 경우에는 주기적으로 백업을 해야 한다.

분석결과를 일반인이 이해할 수 있도록 쉽게 보편적으로 기술해야 하며, 가능하면 증거물의 획득, 분석, 보관 과정 등에서 무결성이 유지되었음을 보여야 한다. 발견된 주요 증거자료에 대해서는 그 논리 및 물리적 위치, 크기, 시간 등을 기술하여, 제 3 자도 그 내용을 확인 할 수 있도록 해야 한다.

Ⅶ. 디지털자료의 법률적 검토

1. 디지털 자료의 증거능력

컴퓨터 등 정보처리기기에서 발견되는 자료는 일반적으로 전문증거(傳聞證據)로 보고 있다. 컴퓨터에 발견되는 자료는 크게 두 종류로 나누어 볼 수 있는데 그중 하나는 사람에 의해 작성되고 컴퓨터에는 단순히 기록만되어 있는 일반 문서파일이다. 엑셀, 파워포인트 발표자료 등이 이에 속한다. 이와 반대로 컴퓨터에서 어떤 동작의 정상 유무를 확인하기 위해서 만들어진 - 즉 컴퓨터에 의해서 생성된 - 로그 자료로 웹 방문기록, 파일 사용시간, 자료전송 로그 등이 있다. 이러한 파일 들이 증거능력과 증명력을 갖고 있는가는 좀더 많은 연구가 필요하겠지만 현행 법률 조문에 대입하여 볼 필요가 있다.

형사소송법 제 310조의2 에서는 전문증거와 증거능력의 제한을 규정하고 있다. 따라서 디지털 자료가 증거능력을 갖기 위해서는 동법 311조에서부터 316조에 정의된 전문증거 예외 규정을 적용해야 한다. 우선 일반 문서파일의 경우 이는 단순한 진술서에 해당됨으로 동법 313조에 언급된 것처럼 진정성을 확보해야한다. 그러나 컴퓨터에 있는 파일에 서명날인 또는 입회자 서명 등 형식적 진정성[6]을 확보하기 어려움으로 그 파일이 실제적으로 그 컴퓨터에 사용되었다는 사실들을 확보하여 실질적 진정성을 확보할 필요가 있다. 이와 반대로 컴퓨터에 내장된 로그파일의 내용은 제315조(당연히 증거능력이 있는 서류)로 쉽게 적용할 수 있지만, 만일 그 컴퓨터의 실질적 관리 주체가 피의자 이거나 또는 제 3자에 의 해 해킹을 당한 흔적이 발견된다면 이 또한 그 신뢰성을 확보하기 어렵게 된다.

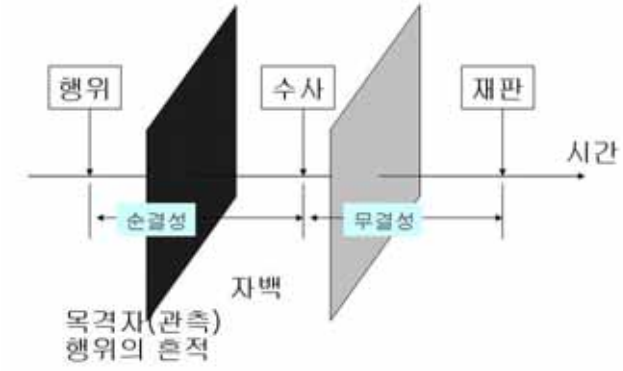
따라서 정보처리기기에 존재하는 자료는 두개로 명확하게 구분하기 어려운 경우가 많고, 각각의 경우에서 명확하게 필요한 정보를 확보 하지 못하는 경우도 많으므로 실제 디지털 증거 분석에 있어서는 모든 상황을 종합적으로 고려하여 실체적 진실을 발견하고

6) 전자거래에서 사용되는 비대칭 암호화 알고리즘의 개인키를 이용하고 CA(Certificate Authority)을 경유하여 처리된 서명은 형식적 진정성을 확보하고 있다고 볼 수 있다.

자 하는 노력이 매우 요구되는 어려운 작업이라고 할 수 있다.

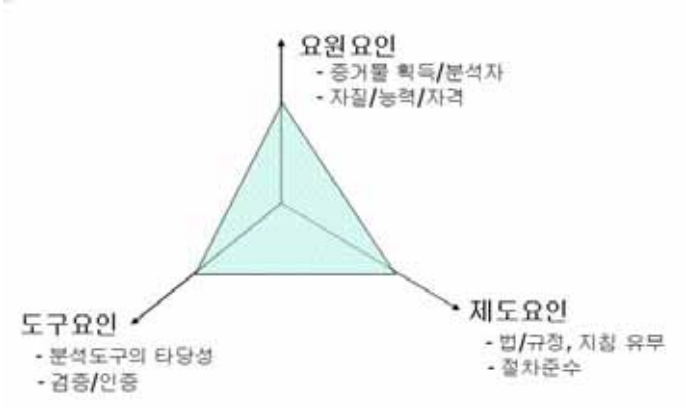
2. 디지털 자료의 증거능력 향상 방안

일반적으로 어떤 행위의 사실관계를 확증하기 위해서는 1) 그 행위의 과정을 목격 또는 관측한 정보, 2) 행위의 결과 또는 결과로 남겨진 흔적, 3) 행위 당사자의 진술 등이 모두 있으면 매우 확실하게 사실관계를 확증할 수 있게 된다. 이러한 맥락에서 디지털 자료가 증거능력을 갖게 하기 위해서는 앞절에서 언급된 각종 절차를 준수하여야함은 물론이고, 수사 시점의 전후관계도 살펴볼 필요가 있다.



<그림 21> 디지털 증거물 획득 및 분석 단계

사실관계의 확인은 그림 21에서 자료의 압수시점 이전에 일어난 행위에서 대해 관련된 근거를 이용하여 추정하는 과정이므로, 만일 행위가 일어난 시점 이후에 제 3자에 의해 그 시스템이 조작되었다면 - 즉, 순결성을 잃었다면- 그 자료의 진정성은 매우 낮은 것으로 보아야 할 것이다. 또한 수사과정에서 압수된 자료가 조작될 위험성이 있으므로 전체 증거자료에 대해 해시 계산을 하여 저장·보관하여 놓으면, 향후 자료의 조작여부를 검증할 수 있으므로 수사과정을 투명화 할 필요가 있다.



<그림 22> 디지털 자료의 증거능력 영향 요소

결론적으로 디지털 자료가 증거능력을 갖게하기 위해서는 증거물의 획득, 분석, 보고, 보관 등의 과정이 합리적으로 수행되어야 할 뿐만 아니라, 그 증거물이 획득되기 이전의 과정에 대해서도 분석이 이루어 져야 한다. 또한 그림 22와 같이 증거물의 획득 및 분석에 관련된 요원, 도구 및 관련 제도·규정등도 영향을 미치므로 이들에 관한 연구도 심도있게 진행되어야 할 것이다.

Ⅷ. 디지털 포렌식스 발전 방안 및 결론

일반 범죄에서 지문, 혈흔, 흉기 등과 같은 증거물을 처리하는 절차와 방법에 대해서는 잘 정리되어 지켜지고 있으나, 디지털 증거는 최근에 부각되기 시작하여 아직 잘 정립되지 않은 측면이 있다.

자료의 생성, 변경, 삭제 등이 매우 손쉽게 일어날 수 있는 디지털 자료가 증거자료가 될 수 있도록 하기 위해서는 특별한 절차와 방법을 따라야 된다. 증거물을 수거할 때부터 문제가 될 만한 자료는 해시 값을 계산하여 보관하거나 또는 디스크를 복제하여 별도로 보관할 필요가 있게 된다.

컴퓨터 기술은 급속도로 발전하고 있으므로 이를 다루는 수사관은 컴퓨터 증거물에 대해 적절한 교육 훈련이 되어 있어서 증거물이 훼손되지 않도록 하여야 할 것이다. 필요한 경우에는 면허·자격증 제도를 시행할 필요도 있을 것으로 판단된다.

증거물 처리과정에 대해서 분쟁이 발생할 경우가 많아 질 수 있으므로 이를 대비하기 위한 지침 등도 마련되어야 할 것이다. 최근 디지털 포렌식스 도구의 발전과 더불어 컴퓨터에서 삭제된 자료가 복구되지 않도록 하는 영구삭제 프로그램이 보급되어 사용되고 있으므로 이에 대한 고려도 함께 이루어져야 한다[19].

본 연구에서는 디지털 자료가 법적인 증거자료로 활용되기 위해서 필요한 절차와 방법, 즉 디지털 포렌식스에 대해서 고찰하여 보았다. 디지털 자료가 법적 증거로서 사용되게 될 때는 자료의 잠재성, 디지털, 취약성, 다양성, 대량성의 특징에 대해서 음미해볼 필요가 있다. 특히 취약성 특징으로 인해 디지털 포렌식스에서는 다른 증거물의 처리 방법과 다르게 자료의 해싱 또는 복제 후 별도의 보관 등과 같은 절차가 필요하게 된다. 물론 사건의 종류에 따라 모든 디지털 증거물에 대해 이러한 절차를 따를 필요는 없겠지만 이는 매우 특이한 절차이고 또한 번거로울 수 있게 된다. 따라서 이들 절차를 편리하고 합리적으로 수행할 수 있는 제도가 만들어질 필요가 있게 된다. 또한 다양성과 대량성의 특성을 극복하기 위해서는 한국 환경에 적합한 포렌식스 전문도구가 시급히 개발되어 보급되어야 할 것이다.

참 고 문 헌

Eoghan Casey, Digital Evidence and Computer Crime, Academic press, 2000.

Eoghan Casey, Handbook of Computer Crime Investigation, Academic press, 2002.

Albert J. Marcella etc., Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Auerbach, 2002.

Micheal A. Caloyannides, Computer Forensics and privacy, Artech House, 2001.

Warren G. Kruse Ⅱ, etc., “Incident Response Essentials”, Computer Forensics, Addison-Wesley, 2002.

Kevin Mandia & Chris Prosise, “Investigating Computer Crime”, Incident Response, Osborne/McGraw-Hill, 2001.

Orin Kerr, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, U.S. Department of Justice, Jan. 2001.

파이널데이터, 파이널포렌식스 V2.0 사용자매뉴얼, 2006.

Guidelines on PDA Forensics, NIST Special Pub. 800-72, NIST, 2004.

이성진, 컴퓨터 포렌식스 기술, NETSEC-KR2003 Workshop Proc., 정보보호진흥원.

SANS, System Forensics, Investigation and Response, SANS FIRE 2003 Proc., 2003.

Robert M. Slade, Software Forensics - Collecting evidence from of a digital crime, McGraw-Hill, 2004.

한국정보보호센타, 2001 정보시스템 해킹.바이러스 현황 및 대응, 한국정보보호센터.

김종섭, 컴퓨터 포렌식스와 전자공증을 응용한 [전자증거 관리 시스템] 설계 및 운영방향, 동국대학교 국제정보대학원 석사학위 논문, 1999.

최득신, Computer Forensics에 관한 연구, 서울대학교 행정대학원 정보통신방송정책과정 논문, 2002.

김종섭, 김귀남, 국내 Computer Forensics의 연구동향과 발전방향, 정보보증논문지, Vol. 3, No. 1, March 2003.

D. Brezinski and T. Killaea, Guidelines for Evidence Collection and Archiving, RFC 3227.

Peter Gutmann, Secure Deletion of Data from Magnetic and Solid-State Memory, 6th USENIX Security Symposium, 1996.

Stephen Northcutt, Judy Novak, 네트워크 침입탐지와 해킹분석 핸드북, 인포북, 2001.

Stephen Northcutt, Mark Cooper, Matt Fearnow, Karen Frederick, Intrusion Signatures and Analysis, New riders pub., 2001.

www.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm#report.

양근원, 형사절차상 디지털 증거의 수집과 증거능력에 관한 연구, 박사학위논문, 경희대학교, 2006.

EnCase V4.0 User Manual, Guidance Software, 2003.

John Patzakis, EnCase Legal Journal, Second Edition, 2002, www.guidancesoftware.com.

J. Bryan Davis, Computer Intrusion Investigation Guidelines, FBI Law Enforcement Bulletin, Jan, 2001.

Craig W. Meyer, etc., Investigative Uses of Computers - Analytical Time Lines, FBI Law Enforcement Bulletin, Aug. 2000.

John Ashcroft, Electronic Crime Scene Investigation - A Guide for First Responders, NIJ, U.S. Department of Justice. www.ojp.usdoj.gov/nij.

IOCE, G8 Guidelines for Best Practice in the Forensic Examination of Digital

Evidence, 2002, www.ioce.org/2002/ioce_bp_exam_digit_tech.html.

Samuel Chanson, Comments on the Government's Report on Computer Related Crime, presentation material, www.isfs.org.hk.

NIST, Hard Disk Write Block Tool Specification, Ver 2.0 Draft, NIST.

Dave Dittrich, Basic Steps in Forensics Analysis of Unix Systems, http://staff.washington.edu/dittrich/misc/forensics/.

SWGDE, IOCE, Digital Evidence: Standards and Principles, Forensic Science Comm., Apr 2000, Vol. 2, No. 2.

Michael R. Anderson, Computer Evidence Processing, white-paper on www.forencis-intl.com.

임종인, 컴퓨터 범죄의 법적증거 수집방안 - 컴퓨터 포렌식스, 정보보호21c (www.secuinfo.com).

이채홍, 손상된 데이터를 갖는 손상된 디렉토리 정보로부터 데이터 복원 방법 및 이를 저장한 컴퓨터가 판독 가능한 기록 매체, 특허청 특허번호308873.

이채홍, 하드 디스크의 조각난 데이터 복원 방법 및 이를 저장한 컴퓨터가 판독 가능한 기록 매체, 특허청, 특허번호 308874.

Forensic TOOLKIT User Guide, AccessData Corp, 2000.

John Ashcroft, etc., Test Results for Disk Imaging Tools: dd GNU fileutils 4.0.36, NIJ Special Report. Aug. 2002.

VMWare, http://www.vmware.com/.

Honeynet, http://project.honeynet.org/.

http://www.e-fense.com/helix/.

http://biatchux.dmzs.com/.

Alec Yasinac, etc., Computer Forensics Education, IEEE Security & Privacy, July 2003.

〈부 록〉

디지털 증거분석 표준 가이드라인(안)

제1장 일반사항

1. 목 적

이 표준절차는 조사관, 수사관(이하 '수사관 등'이라한다) 및 디지털증거 분석관이 디지털증거를 수집, 분석, 보관함에 있어 필요한 절차와 준수사항을 정하는데 목적이 있다.

2. 적용범위

이 표준절차는 디지털증거를 적법절차에 따라 수집·분석·보관하는 등(이하 '디지털증거처리'라 한다) 디지털 증거 취급과 관련된 각종 조사 및 수사행위에 적용된다.

3. 용어의 정의

(1) "디지털증거"라 함은 컴퓨터 또는 기타 디지털저장매체에 저장되거나 네트워크를 통해 전송중인 자료로서 조사 및 수사 업무에 필요한 증거자료를 말한다.

(2) "디지털증거 분석"이라 함은 컴퓨터 또는 기타 디지털 저장매체(네트워크를 통해 전송중인 자료를 포함한다)에 남아있는 자료에 대한 원본 보존과 사건 관련 증거를 과학적인 절차를 통하여 추출, 검증, 판단하는 조사 및 수사과정을 말한다.

(3) "휘발성 증거"라 함은 컴퓨터 실행시 일시적으로 메모리 또는 임시파일에 저장되는 증거로 네트워크 접속상태·프로세스 구동상태·사용중인 파일 내역 등 컴퓨터 종

료와 함께 삭제되는 디지털 증거를 말한다.

(4) “비휘발성 증거”라 함은 컴퓨터 종료 시에도 컴퓨터 또는 기타 디지털 저장매체에 삭제되지 않고 남아있는 디지털 증거를 말한다.

(5) “기타 디지털 저장매체”라 함은 플로피 디스크, 휴대폰, USB, 플래쉬 메모리 등 컴퓨터 하드디스크 외의 디지털 저장매체를 말한다.

제2장 디지털 증거수집

1. 기본 원칙

1.1. 적법절차의 준수

(1) 수사 등에 필요한 한도 내에서 적법절차를 준수한 최소한의 증거 수집을 원칙으로 한다.

(2) 형사소송법, 경찰관직무집행법 등의 법규 및 지침에 규정된 일반적인 원칙과 절차를 준수한다.

1.2. 증거 원본의 안전한 보존

(1) 증거수집 시에는 반드시 쓰기방지장치를 이용하여 증거 원본에 대한 무결성을 유지한다.

(2) 증거 원본은 이송 및 보관에 주의하여 손상을 방지한다.

1.3. 증거의 무결성 확보

(1) 증거 수집 시점에 수집된 디스크 또는 각각의 파일에 대해서 단방향 암호화 알고리즘으로 계산값(이하 해쉬값)을 확보한다.

(2) 생성된 해쉬값을 출력 후 입회인의 서명 날인을 받는다.

(3) 증거 원본에 대한 사본을 생성하고 이에 대한 해쉬값을 생성 후 이미 생성된 원본 해쉬값과 비교하여 무결성을 검증한다.

(4) 증거분석은 원본 해쉬값과 동일한 해쉬값을 가진 사본을 이용하여 수행한다.

(5) 무결성 확보가 어려운 상황에서는 제 3자 입회 또는 캠코더 촬영 등을 이용하여 객관적으로 소명을 할 수 있도록 한다.

2. 준비사항

2.1. 증거수집계획의 수립

수사관 등은 신속하고 효과적인 증거수집을 위하여 다음과 같은 사항에 유의하여 증거수집계획을 수립한다.

(1) 수사관등은 증거수집과 관련하여 아래와 같은 사항을 사전에 파악하여 둔다.

- 컴퓨터 하드웨어, OS, 소프트웨어, 저장매체, D/B
- 네트워크 관련 정보
- 시스템 또는 네트워크 책임자나 관리자
- 수집해야 할 매체의 개수나 데이터의 분량

(2) 수집 및 이송에 필요한 인원, 장비를 준비한다.

(3) 필요에 따라 압수 수색 영장을 신청한다.

2.2. 증거수집팀 구성

(1) 기업 등 대규모 압수수색이나, 해킹사범 수사 등 증거수집에 디지털 포렌식 관련 전문지식이 필요한 경우는 증거수집팀을 별도로 구성한다.

(2) 증거수집팀은 OS, DB, 네트워크, 프로그래밍, 해킹, 악성코드 등 분야별 전문가로 구성한다.

(3) 증거수집팀 구성이 완료되면 증거수집 방법, 범위, 역할 분담, 주의사항에 대한 사전 교양을 실시한다.

2.3. 수집장비

(1) 하드웨어

① 증거수집 및 분석용 컴퓨터

증거수집 및 현장 초동 분석업무 수행을 위한 휴대용 컴퓨터 및 아래와 같은 추가장비

※ 증거 수집 및 분석용 컴퓨터는 이동시 충격을 완화하기 위해 보호용 케이스에 보관할 것

용 도	필 요 장 비
인터넷접속	100Mbps 또는 Gigabit 이더넷 카드, 무선랜(IEEE 802.11bga) 카드 등 장착
주변기기 및 외부장치 연결	USB 2.0 포트, IEEE 1394b 포트, RS-232 시리얼 포트 등
증거보관	대용량 storage, HDD, CD 등

② 쓰기방지 장치

현장 초동분석 업무 필요시 사용할 하드디스크 등 원본증거의 위·변조 방지를 위한

쓰기방지 장치

- USB, IEEE1394 등과 같은 외부 포트에 연결되어 저장매체에 대한 쓰기방지 기능 필요
- IDE, SATA, SCSI 등 다양한 저장매체에 대한 쓰기방지 지원 가능

③ 증거사본 보관용 대용량 저장 장치

- 증거 원본에 대한 압수가 어려울 경우 사본을 생성하여 저장하기 위한 대용량 디스크
- 사본 보관용 디스크는 안전하게 이동 가능한 보호용 케이스 사용
- 보관용 디스크는 기존에 보관되어 있던 자료와 혼동되지 않도록 데이터를 완전 삭제 후 사용

④ USB 메모리, CD-R, DVD-R 등 외장형 저장 매체

- 휘발성 증거 또는 파일 증거 수집을 위해 USB 메모리 등과 같은 외장형 저장 매체
- 보관용 메모리는 기존에 보관되어 있던 자료와 혼동되지 않도록 내용을 완전 삭제 후 사용
- 수집된 증거 파일의 보관을 위한 공 CD-R, DVD-R

⑤ 증거 운반용 박스

- 하드디스크 등 외부충격에 약한 증거물을 위한 스티로폼, 스펀지 등이 내장된 충격 완화용 보호박스
- 디스켓 또는 CD 등을 분류·보관을 위한 지퍼백과 같은 형태의 투명한 비닐 봉투
- 기타 케이블 등 부가적인 증거보관을 위한 압수물품용 박스 준비

⑥ 다양한 규격의 연결 케이블 및 어댑터

현장 증거분석에 필요한 케이블 및 어댑터는 다음과 같다.

구 분	필 요 장 비
전원 케이블과 어댑터	멀티플러그 종류별 전원케이블 110V to 220V 전원 어댑터
네트워크 케이블	이더넷 다이렉트 케이블 이더넷 크로스 케이블 등
데이터 전송케이블	USB 케이블 IEEE 1394 케이블 시리얼 케이블 패러럴 케이블(프린트 케이블) IDE 80핀 케이블, IDE 40핀 케이블 SATA 케이블 SCSI 케이블 등

⑦ 분해와 해체를 위한 공구

- 컴퓨터 등 분해를 위해 사이즈 별로 +/- 드라이버 준비
- 케이블 등의 절단을 위하여 니퍼, 플라이어 등의 공구 준비

⑧ 서류 작성을 위한 각종 서식, 휴대용 프린터

⑨ 현장 촬영을 위한 카메라, 캠코더

(2) 소프트웨어

① 증거 원본에 대한 사본을 생성하기 위한 이미지 복제용 소프트웨어

② 디지털증거 현장 초동분석에 필요한 분석 소프트웨어

③ 휘발성 증거 수집을 위한 휘발성증거 수집 소프트웨어

3. 디지털 증거수집 절차

(1) 사진촬영 및 현장 스케치를 수행한다.

① 컴퓨터등 대상물의 앞·뒷면 사진, 주변장치를 포함한 사진, 전원이 켜져 있는 경우는 모니터 화면 촬영

② 현장에 있는 수집 대상물의 위치를 상세히 스케치

(2) 네트워크 정보등 휘발성 증거를 수집한다.[1)]

(3) 수집 대상물의 전원을 확인한다.

① 컴퓨터 등 대상물의 전원이 꺼져 있는 경우 그대로 수집

② 전원이 켜져 있는 경우, 정상적인 시스템 종료 절차를 수행하면 임시 데이터가 삭제되므로 이를 방지하기 위해서 컴퓨터의 경우 종료 절차 없이 전원플러그를 강제 분리(단, 서버는 정상 종료 절차 수행)

<표 3> 운영체계별 전원분리방법

운 영 체 계	전 원 분 리 방 법
DOS	전원 플러그 분리
Windows 3.1	전원 플러그 분리
Windows 9x/ME	전원 플러그 분리
Windows NT	전원 플러그 분리
Windows NT Server	정상 종료
Windows XP/2000 pro	전원 플러그 분리
Windows 2000 Server	정상 종료
Linux	정상 종료
Unix	정상 종료
Macintosh	전원 플러그 분리

1) 휘발성 증거수집이 필요한 경우 경찰청에서 제작, 배포한 포도미CD를 활용한다

(4) 본체 수집을 원칙으로 하되, 부득이한 경우 하드디스크만 분리하여 수집한다.

① BIOS의 메인 메뉴에서 시스템 시간과 날짜정보 확인 2)

② BIOS 시간과 표준 시간 간의 오차를 확인 후 기록

③ 컴퓨터 본체에서 하드디스크를 안전하게 분리

(5) 외장형 디스크, USB 메모리 등 기타 디지털 저장매체와 각종 소프트웨어, 주변장치, 케이블 등을 수집한다.

(6) 증거물을 포장하고 상세정보를 기재하여 증거물에 부착한다.

① 하드디스크는 보호박스를 사용하여 개별 포장함이 원칙

② 컴퓨터 및 주변 장치 등에 대한 상세 정보를 기재하여 증거물에 부착

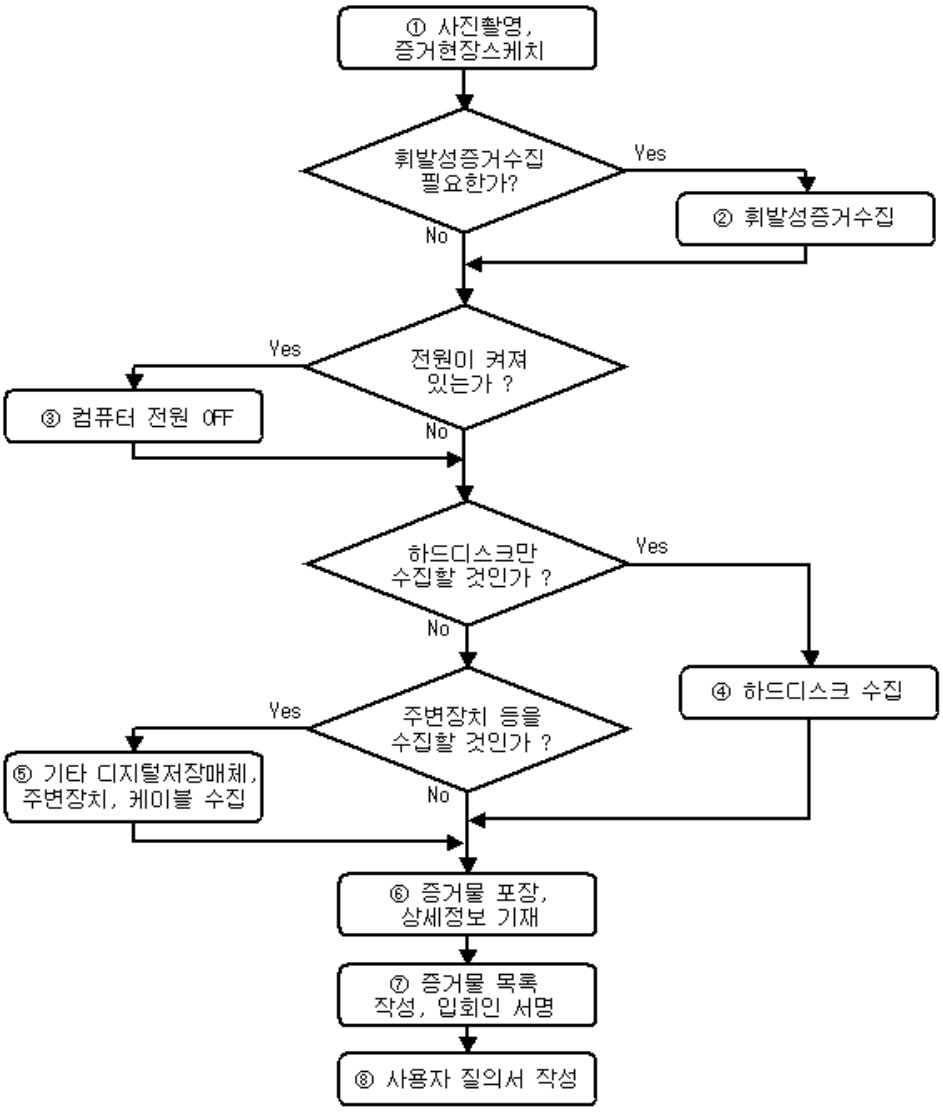
③ 상세정보의 내용은 사건번호, 수집자, 입회인, 수집일시, 장소, 물품, 제조번호 등이고, 하드디스크만 분리하여 수집하는 경우에는 추가로 BIOS 시간 오차를 기재

(7) 압수증명서를 작성하여 입회인에게 교부하고, 입회인으로부터 압수확인서 및 압수증거물 목록에 서명 날인을 받는다.

(8) 사용자 질의서를 작성한다.

※ 컴퓨터 사용자를 상대로 컴퓨터의 용도, 설치된 운영체계, 주로 사용하는 응용 프로그램 명, 패스워드가 설정된 프로그램 명, 패스워드 정보 등을 질의 후 기재

2) 컴퓨터 본체를 부팅하는 즉시 Delete 키를 누르면 BIOS 화면에 들어갈 수 있으며, 예외적으로 F2, Alt-F2, Alt-S 등의 키를 사용하는 경우도 있다.



<그림 1> 디지털 증거 수집 절차도

4. 준수사항

4.1. 현장도착시 준수사항

(1) 압수할 시스템이 확인되었으면 각 시스템별 현재 시각과 컴퓨터 시간이 일치하는지 반드시 확인한다.

(2) 시스템에 어떤 종류의 소프트웨어가 있는지 파악한다.

※ 회계관리 프로그램, 기타 범용소프트웨어가 아닌 것을 체크하여 확인한 후 분석관에게 이관

(3) 시스템 하드웨어나 네트워크를 파악하고 원본의 손상을 방지한다.

① 장비의 종류를 확인하고, 기능이나 용도를 알 수 없는 장비가 있는 경우 사진 촬영 등 자료확보하고 전문가와 상의

② 시스템 전원을 차단여부를 먼저 파악하고, 수집해야할 휘발성 자료가 있거나 운영 중인 시스템이라면 피해가 가지 않는 최소한의 범위 내에서 작업 수행

※ 휘발성 자료가 없을 경우 그 자리에서 전원을 차단한 후 압수하여 담당자에게 인계

(4) 어떤 시스템을 압수할 것인지를 목록에서 확인하여 신속 정확하게 압수한다.

① 하드디스크만 압수할 경우 충격 등으로 인해 증거물에 손상이 가지 않도록 주의

② 수사관 등은 전문성이 부족하다고 판단되는 경우 증거물을 조작하지 말고 전문가에게 인계

※ 취급 미숙으로 인해 컴퓨터 부팅 만으로도 윈도우 자체에서 날짜가 변경되는 파일이 있으므로 각별한 주의요망

4.2. 유형별 증거물 수집시 준수사항

(1) 컴퓨터 전원이 꺼져 있는 경우

스크린 세이버 작동여부, 하드디스크 및 모니터 작동여부 등 컴퓨터 전원을 재확인 후, 다음 사항을 준수하여 수집한다.

① 네트워크 및 전원케이블 분리

- 컴퓨터 및 기타 장비들과의 연결 상태 등을 스케치하거나 사진촬영
- 네트워크 케이블 분리시 네트워크를 통해서 컴퓨터의 데이터 삭제 및 변경되는 경우를 미연에 방지해야 하며 케이블을 분리하기 전에 케이블의 물리적인 연결 상태 기록

② 컴퓨터 등 장비 분리

- 연결 포트와 케이블은 차후 장치에 재연결할 수 있도록 동일 숫자의 라벨을 부착
- 장치들을 분리시 신중을 기하고, 쉽게 식별 가능하도록 넘버링 작업
  ※ 압수번호가 있더라도 각 장치 별로 구성이 쉽도록 또 다른 방식으로 넘버링
- 노트북은 전원 어댑터를 분리하기 전에 전원상태 및 대기 모드 등을 확인하고 AC 어댑터 압수

③ 이동식 메모리 및 패스워드 관련 자료

- CD, 디스켓, USB 메모리 등 이동식 보조기억장치의 존재여부를 확인하여 관련 드라이브와 함께 압수
- 컴퓨터, 책상주변에 위치한 다이어리나 노트, 메모 등에서 사용자 ID와 패스워드 등 인증정보 수집

④ 컴퓨터 전원을 다시 켜야 할 경우

- 압수대상자 또는 참관인의 입회하에 수행하되 미리 플로피 디스크, 부팅 CD 등을 준비

하여 만약의 경우에 대비

⑤ 증거물 이송시 준수사항

- 전원을 켜지 않은 상태 그대로 압수하여 하드디스크 등이 충격을 받지 않도록 디스크 보관함 이용 등 안전조치
- 제조일자, 고유번호, 모델 등의 정보 기록 후, 모든 드라이브와 본체, 전원코드까지 함께 이송
- 압수한 컴퓨터에 외상이 있는 경우, 압수대상자 및 참관인이 입회한 상태에서 해당 사실을 인지시키고 기록
- 압수한 컴퓨터 장비(특히 디스크)에 남아있는 지문 채취가 필요한 경우 과학수사요원에게 통보

※ 단, 지문 채취에 사용되는 시약, 분말가루, 테이프 등은 컴퓨터 및 저장매체드라이브 등의 인식에 영향을 미칠 수 있으므로 주의할 것

(2) 컴퓨터 전원이 켜져 있는 경우

컴퓨터의 전원을 종료함으로서 소실되는 휘발성 증거에는 해킹, 웜·바이러스 등의 사건 수사에 중요한 단서가 되는 경우가 많으므로 다음 사항을 준수한다.

① 증거의 손상을 막기 위해 사건관련자 및 제3자들을 컴퓨터나 전원공급기에서 분리 조치

② 시스템의 현재 시각을 정확하게 기록

③ 네트워크에 연결되어 있지 않은 경우 컴퓨터 시각정보와 UTC 표준시각 정보를 비교해서 정확하게 기록

※ UTC 표준시각의 경우 국내표준시각보다 9시간 느림

④ 컴퓨터가 네트워크에 연결되어 있는 경우 원격접속을 통한 증거인멸 등을 사전에 차단하기 위하여 다음과 같은 사항을 확인 후 즉시 네트워크 케이블을 분리

- 컴퓨터 시스템의 네트워크 연결 상황 확인
- 네크워크 장치(허브 등), RAID와 컴퓨터 장치 사이의 연결 상황 확인
- 정보제공자와 각 개인이 제공하는 정보 확인 등

⑤ 컴퓨터의 전원이 꺼지면 사라지는 현재 실행중인 프로그램이나 프로세스, 로그인 정보 등 휘발성자료 확보를 위하여 다음과 같은 사항을 수행

- 모니터의 상태를 확인하고 현재 화면 등을 촬영
- 시간 정보 기록
- 현재 네트워크 연결 상태 기록
- 현재 오픈된 TCP, UDP 포트 정보 기록
- TCP, UDP 포트를 오픈하고 있는 실행파일 기록
- NetBIOS 캐시 정보 기록
- 현재 접속 사용자 정보 기록
- 인터넷 라우팅 테이블 기록
- 실행 중인 프로세스 내역 기록
- 실행 중인 서비스 내역 기록
- 예약된 작업 내역 기록
- 현재 사용 중인 파일 내역 기록
- 실행 중인 프로세스의 메모리 내용을 파일에 저장
- 휘발성 정보가 저장된 파일에 대한 해시값을 생성하여 증거물 목록에 기재

⑥ 휘발성증거 확보 후 다음의 절차에 따라 컴퓨터의 전원 차단

- 정상적인 시스템 종료 절차를 수행하면 임시 데이터가 삭제되므로 이를 방지하기 위해 컴퓨터의 경우 종료 절차없이 전원플러그를 강제 분리(단, 서버는 정상 종료 절차 수행)
- 컴퓨터의 전원을 정상 종료함에 따라 소실되는 정보를 최소화하기 위하여 사용하는 운영체계에 따라 전원종료 방법을 선택

⑦ 시스템 혹은 운영체계에서 공통으로 제공되는 명령어만 사용

⑧ 키보드나 마우스는 가급적 작동시키지 않도록 하고, 모니터 화면이 보이지 않거나 스크린 세이버가 작동중인 경우는 수사관 등(혹은 증거수집전문가)이 직접 모니터 확인하고 마우스를 움직인 후 나타난 다음화면을 사진 촬영하고 기록을 남김

※ 스크린 세이버에 암호설정이 되어 있는 경우 수사관이 사용자 및 관리자에게 비밀번호 질의

⑨ 파일 혹은 바탕화면의 아이콘을 더블클릭해서 프로그램을 실행시키지 않도록 주의

⑩ 컴퓨터의 구성을 확인하여 원격 저장장치 유무 확인

(3) 컴퓨터 등 RAID 시스템으로 구성된 경우

RAID 기능을 지원하는 운영체계의 수가 지속적으로 증가하고 있으며, RAID 시스템으로 구성된 컴퓨터 압수시에는 다음 사항을 준수한다.

① RAID 하드드라이브 복제본이 있을지라도 RAID 환경을 구성하는 RAID 카드와 프로그램 없이 RAID 환경을 재현하기는 어렵고, 또한 원본과 동일한 업체, 모델, 펌웨어버전, 용량을 가지고 있지 않을 경우 복사 그자체도 어려우므로, RAID 환경으로 구성된 컴퓨터 압수시 세트 전체를 압수

② RAID 카드를 사용할 경우, 카드·케이블·하드드라이브 연결 상태를 기록하고, RAID카드는 커넥터와 하드드라이브 사이의 연결정보를 저장하므로, 재설치시 주의

③ RAID 관련 프로그램, 케이블, 매뉴얼 등 함께 압수

(4) 휴대폰

① 휴대폰 전원이 꺼져 있는 경우

- 증거 훼손 방지를 위해 대상자로부터 휴대폰을 신속하게 압수한 후 배터리 즉시 분리
- 휴대폰 전원을 켜게 되면 새로운 문자 메시지 및 전화호출이 수신되어 기존에 저장된 자료를 덮어쓸 수 있으므로 유의
- 휴대폰 배터리, 충전기 및 컴퓨터 연결용 케이블 등도 함께 압수하고, PC링크 기능을 사용한 경우 휴대폰 데이터가 저장된 컴퓨터도 압수

② 휴대폰 전원이 켜져 있는 경우

- 휴대폰의 통화 수신을 차단해할 경우 전자파 차폐장치에 봉인
- 증거수집 현장에서 휴대폰 정보를 조회할 필요가 있을 경우 압수대상자 및 입회인 참여하에 사용
- 압수된 휴대폰은 즉시 전원 종료 후 배터리 분리
- 휴대폰이 잠금 모드로 설정되어 있을 경우 대상자에게 비밀번호 확인 후 기록

(5) PDA

PDA는 다양한 운영체계, 소프트웨어 및 저장매체로 구성되어 있고 동작방법도 다양하므로 다음 사항을 준수한다.

① 증거 훼손을 막기 위해서 대상자로부터 PDA를 즉시 압수

② PDA가 작동중일 경우 암호 설정여부, 네트워크 연결 여부 등을 파악한 후 정상적인 종료절차를 거쳐 전원을 차단하거나, 대기 모드가 지원될 경우 대기모드로 압수

③ 암호가 설정되어 있는 경우 대상자로부터 관련 정보 확인 후 기록

④ PDA 압수시 플래시 카드, 메모리 스틱, 스마트 카드 등 저장매체와 함께 컴퓨

터 연결 케이블, AC 어댑터, 충전기 등 각종 부속품도 압수

(6) 기타 디지털저장매체

휴대용 저장매체는 소형화, 첨단화 및 대용량화 되고 있으므로 다음 사항을 준수한다.

① 대상자의 의복을 점검해서 USB 메모리스틱 등 저장매체 소지 여부 확인

② CD-ROM 드라이브 등 구동장치 주변에 또 다른 저장매체가 있는지 조사

③ 부득이 저장매체에 저장된 내용 조회 및 검색이 필요한 경우 데이터 변조에 주의

제3장 증거분석 의뢰 및 접수

1. 증거분석 의뢰

수사관 등은 분석관에게 디지털증거분석에 필요한 모든 정보를 제공하고, 분석의뢰자 및 증거분석관은 증거물의 무결성과 연계보관성을 위하여 다음 절차를 준수한다.

(1) 증거물 이송시는 봉인하여 내용물이 변경 내지 멸실되지 않았음을 증명할 수 있도록 조치한다.

(2) 증거 수집, 이송 과정에서 수사관등이 행한 조치에 대해서는 상세한 내용을 문서화하여 향후 발생할 수 있는 법정 증언에 대비한다.

(3) 분석의뢰 시에는 정해진 양식에 따라 증거분석 의뢰서를 작성 제출한다

① 증거분석의뢰서에 기재해야할 사항은 다음과 같다.

- 사건개요
- 증거물 수집 일시 및 장소
- 제조일자, 고유번호, 모델명 이외 기타 정보
- 분석의뢰 내용
- 사건담당자 소속과 계급, 이름 및 연락처
- 기타 참고사항

② 분석의뢰 내용은 다음과 같이 명확하고 상세히 기재한다.

분 야	기 재 내 용
키워드	분석에 참고할 수 있는 사건 관련 주요 단어
파일	작성일자, 확장자, 파일크기 등 찾고자 하는 파일과 관련된 상세정보
인터넷	인터넷 사용내역 분석이 필요한 시간대 특정 및 접속 사이트 등
전자우편	분석이 필요한 시간대 특정 및 사용자 나 상대방 이메일 주소 등
메신저	분석이 필요한 시간대 특정 및 사용자나 상대방의 메신저 아이디 등
인쇄내역	분석대상 컴퓨터에서 최근 수행한 인쇄작업 관련, 추정되는 인쇄물의 내용 등
프로그램	특정 프로그램의 설치 여부 확인 관련, 프로그램이름등 참고 자료
기타	분석시 필요한 참고사항

(4) 분석의뢰 시에는 분석에 참고할 수 있는 수사기록등 관련 기록 사본 1부를 함께 송부한다. 현장에서 초동분석이 이루어진 경우 그 결과 보고서도 반드시 첨부한다.

(5) 분석결과보고서를 받은 후 추가분석이 필요한 부분에 대해서는 새로운 분석의뢰서를 작성, 접수한다.

2. 증거분석의뢰서 접수

(1) 접수자는 접수·관리대장에 의뢰 내용을 기입하고 분석관을 배정한다.

(2) 접수자는 배정된 분석관과 함께 증거물을 인수하고, 다음의 조치사항을 준수하여 증거물을 증거보관실에 예치한다.

① 증거물목록과 증거물이 일치하는지 여부 확인

② 증거물을 인수 인계할 때에는 증거물보관함 또는 운반함의 꼬리표에 인수인·인계인이 함께 서명함으로써 증거물의 무결성과 연계보관성을 보증할 수 있도록 조치

3. 증거물 운반 및 이동시 주의사항

컴퓨터 및 기타 저장매체는 외부환경에 민감하고 파손되기 쉬우므로 운반 및 이동시 다음 사항에 주의한다.

(1) 컴퓨터 본체

물리적인 충격으로부터 보호되도록 완충용 보호 박스를 사용하고, 차량 이동시는 스피커나 전자파가 나오는 장비근처에 보관하지 않는다.

(2) 모니터

완충재를 이용하여 포장한 후, 모니터의 앞면이 차량 뒷좌석의 시트 쪽으로 가도록 위치시키고 벨트로 고정한다. 특히 LCD 모니터위에는 물건을 올려놓지 않는다.

(3) 하드디스크

물리적인 충격이나 전자파의 영향을 받지 않도록 하고, 보호박스를 사용한 개별포장을 원칙으로 한다.

(4) 저장매체

① 물리적인 충격 및 전자파의 영향을 받지 않도록 하고, 플로피디스크, CD 등은 구부리거나 휘지 않도록 주의한다.

② 증거물에 대한 설명을 기재한 인식용 라벨은 저장매체가 들어 있는 가방이나 케이스에 부착하고, 저장매체 표면에 직접 붙이지 않는다.

※ CD-R의 표면에 라벨을 붙이면 반사 층에 영향을 주어 오작동을 유발할 수 음

(5) 휴대폰

전원 확인 후 완충재를 이용해서 개별 포장하고, 액정화면에 손상에 가지 않도록 주의한다.

제4장 증거분석 절차

1. 기본원칙

디지털 증거물의 분석 시에는 다음의 기본 원칙을 준수한다.

1.1. 증거 원본의 안전한 보존 및 무결성 확보

(1) 증거분석은 원본에 대한 사본 이미지를 생성하여 수행하는 것을 원칙으로 한다. 단, 신속한 분석을 요하거나 이미지 생성이 현저히 곤란한 경우는 예외로 한다.
(2) 분석전 증거 원본과 사본 이미지의 해시값 동일성 여부를 확인한다.
(3) 분석으로 인해 증거가 변경되어서는 안 된다.
(4) 분석대상에 실행 파일이 포함되어 있는 경우는 별도의 OS 또는 VMware에서 실행 및 분석하도록 하여 증거의 변경을 방지한다.
(5) 증거물 접수 및 반환시 책임자, 관리자, 일시, 장소, 사유 등을 관리대장에 기재한다.

1.2. 증거기법과 도구의 신뢰성 확보

(1) 경찰청은 연 1회씩 증거분석 소프트웨어 및 도구에 대한 신뢰성 검증을 실시하고, 통과된 소프트웨어 및 도구리스트를 공개한다.
(2) 국제사회에서 널리 사용되는 전문 증거분석 장비 및 프로그램을 사용한다.

1.3. 증거분석 과정의 기록

(1) 분석과정 및 분석자의 성명, 분석일자, 분석방법에 대한 상세히 기록한다.
(2) 분석시 주요 장면은 가급적 사진 또는 비디오로 촬영하여 보관한다.

1.4. 증거분석결과의 신뢰성 확보

(1) 증거물이 동일할 경우, 제3의 분석관이 다시 분석해도 원래의 분석과 일치하는 결과가 도출되어야 한다.

(2) 증거물이 동일할 경우, 다른 증거분석 소프트웨어 및 장비를 사용하여도 원래의 분석과 일치하는 결과가 도출되어야 한다.

2. 준비사항

2.1. 분석장비

분석 실행 전 장비 및 필요한 자재를 미리 준비하고, 사용법 등을 숙지한다. 장비준비 시 다음 사항에 주의한다.

(1) 컴퓨터

① 증거분석 전용 컴퓨터를 사용하고, 데이터 무결성 유지를 위하여 인터넷 접속은 금지한다.

② 증거분석 전용 컴퓨터의 구체적인 권장사양은 아래와 같다.

구 분	권 장 사 양
운영체제	Windows2000, Windows XP 또는 2003 Server 이상
중앙처리장치	Intel/AMD, 3 GHz 이상의 싱글/듀얼 프로세서, 듀얼코어 프로세서
주기억장치	1 GB 이상
포 트	2개 이상의 USB 2.0 포트, 1개 이상의 IEEE1394 B 포트
하드디스크	300GB 이상
기 타	CD/DVD 쓰기 기능

(2) 쓰기방지장치[3)]

(3) 소프트웨어

① 증거물 이미지 생성을 위한 프로그램을 준비한다.

② 증거물의 종류별로 필요한 분석 프로그램 및 기타 응용 프로그램을 준비한다.

③ 사용에 익숙하지 않은 프로그램이나 불법소프트웨어 등을 사용하는 경우 증거분석 결과의 신뢰성이 저해되거나, 분석대상에 악영향을 줄 수 있으므로, 사용에 익숙한 정품만을 사용한다.

(4) 저장 장치

사본 이미지, 분석과정에서 산출되는 특정 데이터 및 분석결과물을 저장할 저장매체를 준비한다.

2.2. 분석담당자 지정

(1) 증거분석관은 전산·정보통신 분야 전공자로 디지털 증거분석전문교육을 이수하고 매년 소정의 보수교육을 수료한 자 중에서 지정한다.

(2) 증거분석관은 OS, DB, 네트워크, 소스코드, 데이터복구, 유무선 통신 등 전문 분야에 대한 분석활동이 필요할 경우에는 전문 영역별로 구분하여 분석을 수행한다.

2.3. 복제본 생성

증거물 복제시 원본과의 동일성 및 무결성 입증을 위하여 다음 사항을 준수한다.

---

3) 쓰기방지장치에 대한 상세한 설명은 '제 3장 2.2. 증거수집 하드웨어' 편 참조.

(1) 물리적인 복제를 수행할 경우 동일한 용량의 하드디스크를 준비하고, 동일한 하드디스크가 없을 경우 원본 디스크보다 대용량의 하드디스크를 준비하여 쓰기방지장치 연결 후 복제본을 생성한다.
(2) 이미지 파일을 생성할 경우는 원본에 대한 쓰기방지장치를 부착하여 원본의 변경을 방지한다.
(3) 복제 후에는 원본과의 동일성 및 무결성 입증을 위해 원본 및 사본의 각 해쉬값을 추출, 비교한다

2.4. 분석 대상 및 범위 결정

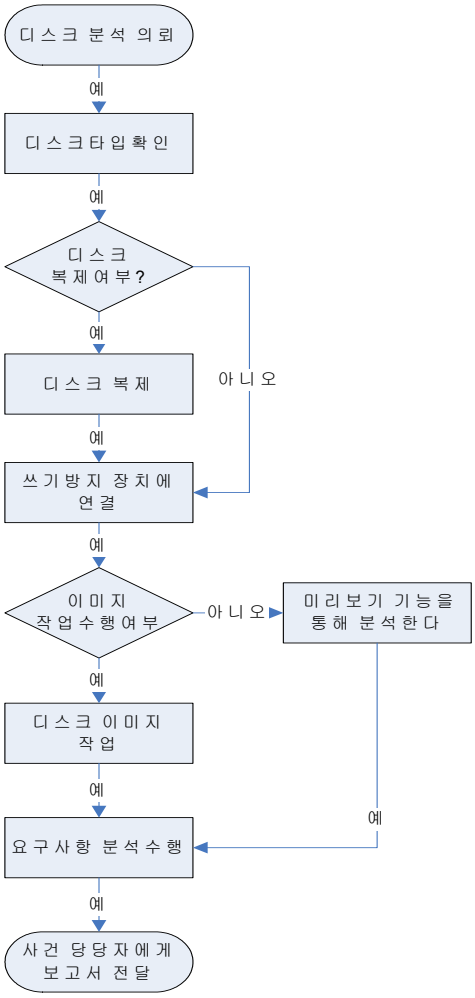
(1) 분석관은 수사관등과 사전 면담을 실시하여 사건개요, 증거물 수집 과정, 분석의 목적 등을 파악하고 분석 대상 및 범위를 결정한다.
(2) 분석관은 증거물의 종류 및 특징에 따라 분석에 필요한 정보 및 기법을 사전에 숙지한다.

3. 유형별 증거분석 표준절차

3.1. 디스크

(1) 분석절차

① 증거 디스크의 형태(IDE, SATA, SCSI, 플래쉬메모리)를 확인
② 증거 디스크의 복제 여부 결정
③ 증거 디스크를 쓰기방지 장치에 연결
④ 증거 디스크의 이미지 작업 수행
⑤ 증거 디스크의 복구가 필요할 경우 파일 시스템 복구 또는 하드웨어 복구
⑥ 의뢰서에 작성되어 있는 요구사항을 분석하고 보고서 작성
⑦ 분석이 끝나면 사건 담당자에게 연락하여 상세설명 후 증거물과 함께 보고서 전달



<그림 2> 디스크 분석 절차

4.2. 네트워크

(1) 증거자료의 추출

① 네트워크 증거를 추출하기 위한 호스트 및 서버 등과 가까운 곳에 탭 장비 설치

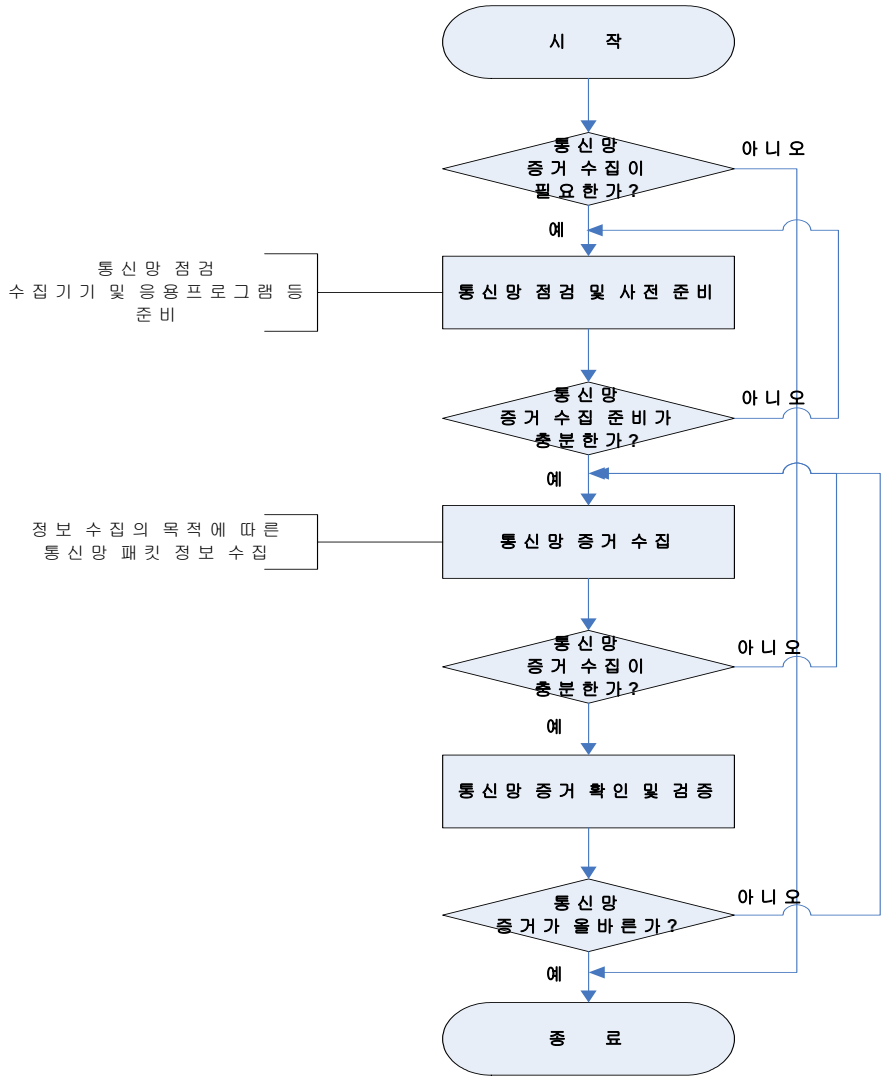
② 네트워크 장비의 탭 장비에 노트북 및 증거추출 기기 연결

③ 노트북 및 증거추출 기기에 추출 목적에 맞는 입력 값을 설정하고 실행

④ 추출 프로그램의 출력이 있을 경우 지속적으로 추출 상태 확인

⑤ 목표하는 네트워크 정보가 추출되었거나 목표하는 시간 또는 용량에 도달하였을 경우 추출 종료

⑥ 추출된 네트워크 증거 파일의 해쉬값을 계산, 기록, 확인 후 보관



<그림 3> 네트워크 증거 추출 절차도

(2) 분석절차

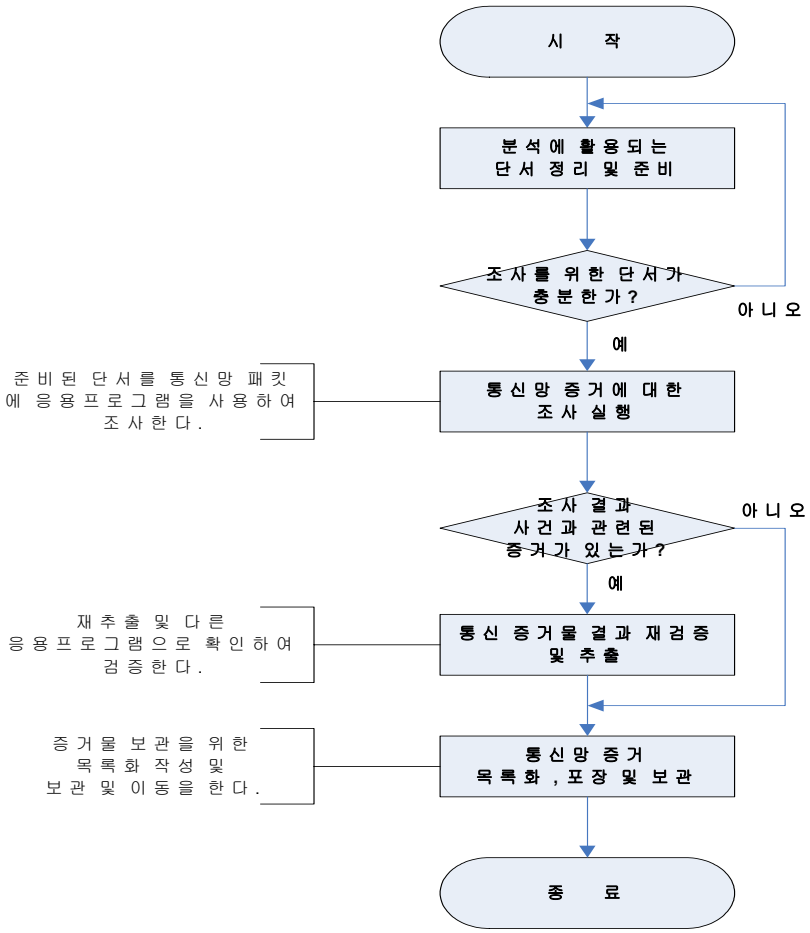
① 추출된 통신망 증거 파일의 해쉬 값을 생성하고 추출 시 작성된 문서에 기재된 값과 비교

② 네트워크 증거 파일을 복사 및 복제하고 분석 프로그램 실행

③ 목적에 맞게 용의 IP 주소, 용의 MAC 주소, 피해 IP 주소, 피해 MAC 주소, 포트 번호 등의 초점을 맞춰 프로그램을 설정하고 분석을 실행

④ 분석을 통해 IP 주소, MAC 주소, 서비스, 기능, 원리 및 내용 등을 목적에 맞게 획득

⑤ 네트워크 증거분석의 분석자, 분석 과정, 분석 결과 등 세부 사항을 빠짐없이 기록



<그림 4> 네트워크 증거분석 절차도

4.3. 월드와이드웹 (www)

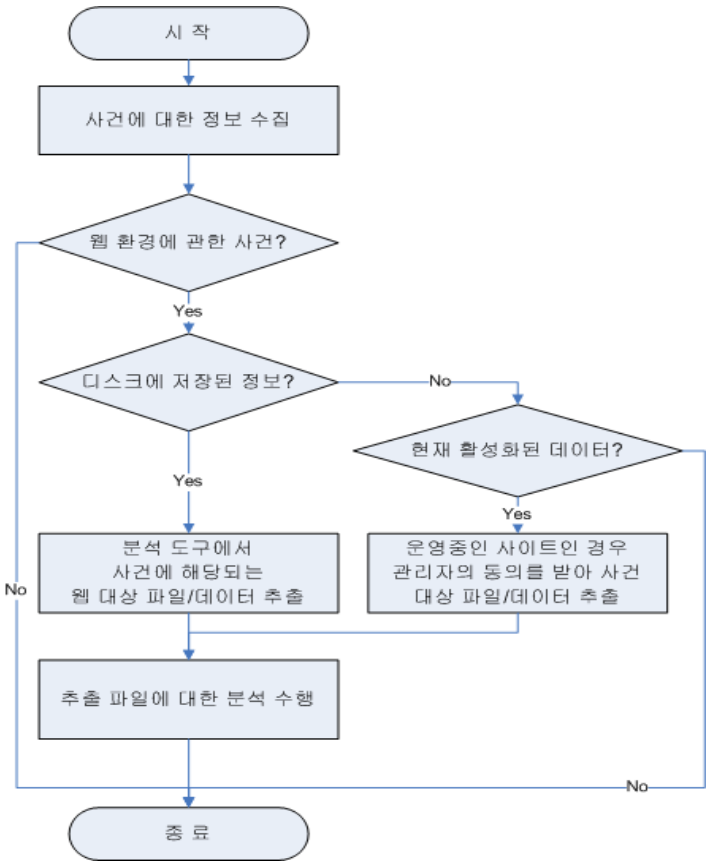
(1) 증거자료의 추출

① 사용된 운영체계 및 웹 브라우저 또는 웹 서버의 종류 및 설정 정보 확인

② 운영 중인 웹 서버에서 추출해야만 할 경우 웹 설정 파일 및 웹 서비스를 하는 프로세스 정보 추출

③ 웹 서버 또는 웹 브라우저의 기록 파일과 사용 파일을 확인 및 추출

④ 운영 중인 웹 서버에서 추출하였을 경우 추출된 웹 사용 파일 및 기록 파일의 해쉬값을 계산, 기록, 확인 후 보관



<그림 5> 웹 증거추출 절차도

(2) 분석절차

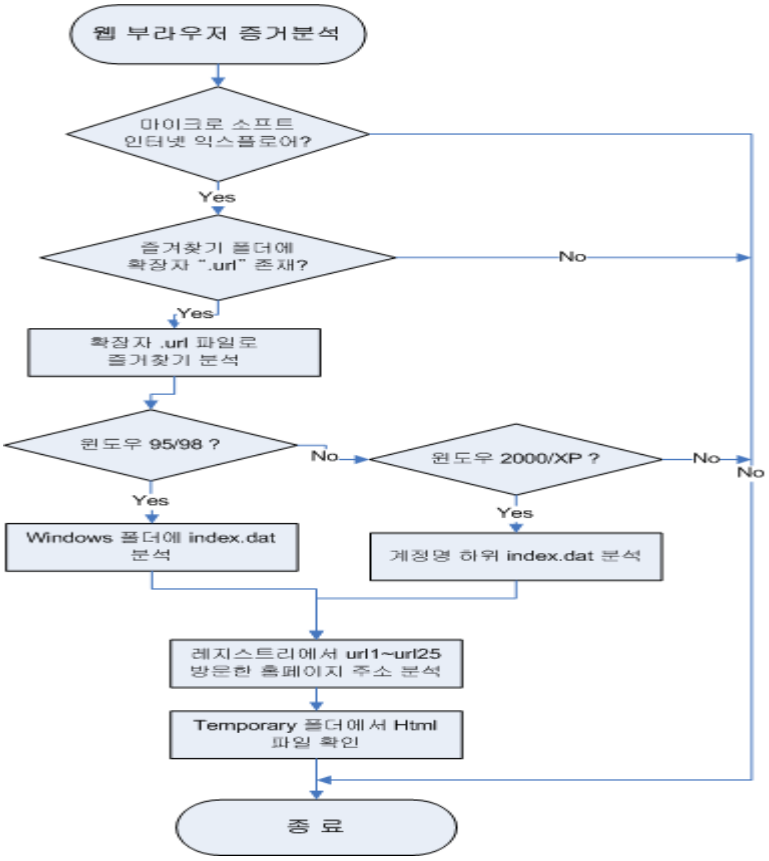
① 추출된 웹 증거 복사본 및 증거 파일의 해쉬값을 생성하고 추출 시 작성된 문서에 기재된 값과 비교

② 웹 증거의 종류에 따른 분석 프로그램을 구축하고 증거 파일을 복사 및 복제

③ 웹 분석 프로그램 및 응용 프로그램을 사용하여 사용 파일 및 기록 파일을 분석

④ 설정 정보, 웹 사용 기록 파일, 웹 소스 파일, 임시 인터넷 파일, 인터넷 사용기록, 인터넷 쿠키 등을 분석하여 사용 방법, 접속자 IP, 사용 내역 등을 목적에 맞게 분석하고 증거를 획득

⑤ 웹 분석의 분석자, 분석 과정, 분석 결과 등의 세부 사항을 빠짐없이 기록

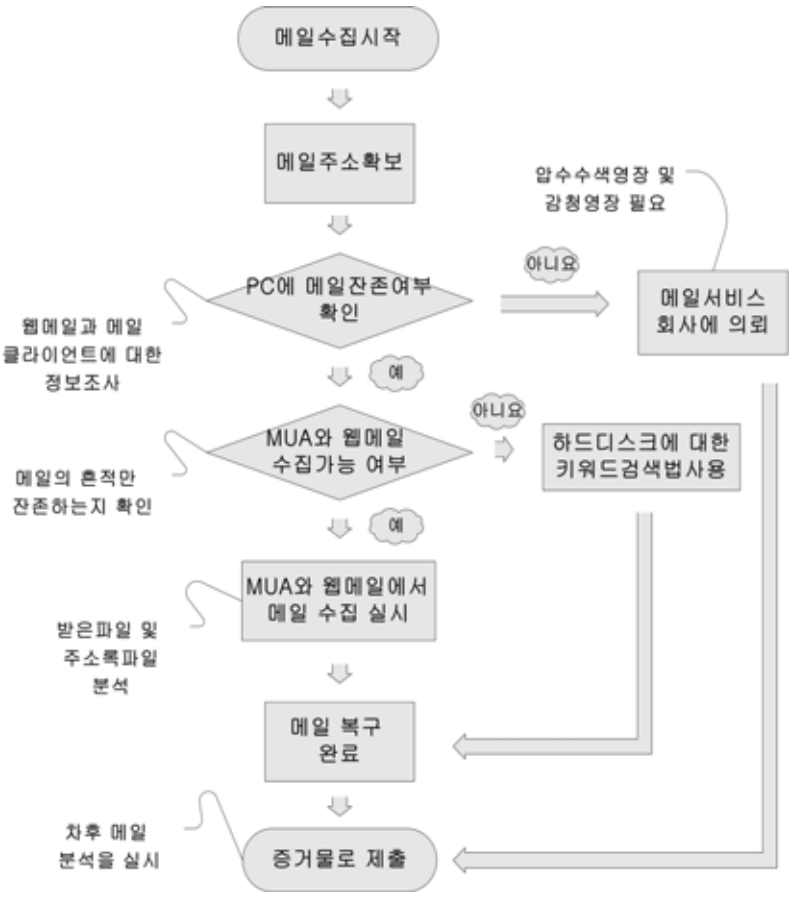


<그림 6> 웹 분석 절차도

4.4. 전자우편

(1) 증거자료의 추출

① 사용된 운영체계 및 전자우편의 종류 및 설정 정보 확인
② 운영 중인 전자우편 서버에서 추출해야할 경우 운영자에게 문의하여 관리자 계정 획득
③ 전자메일의 편지함 파일과 주소록 파일을 확인 및 추출
④ 전자우편 서버에서 전자우편 파일만을 추출하였을 경우 추출된 전자우편의 복사본 또는 저장한 증거 파일의 해쉬값을 계산, 기록, 확인 후 보관



<그림 7> 전자우편 증거추출 절차도

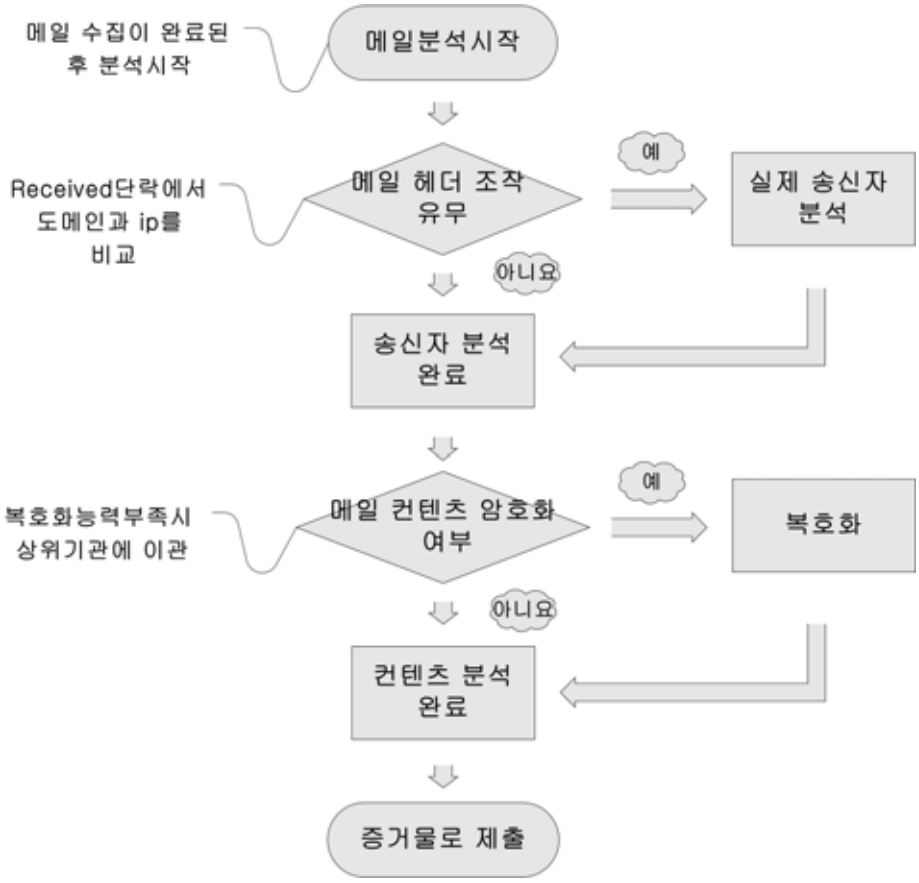
(2) 분석절차

① 추출된 전자우편 복사본 및 증거 파일의 해쉬값을 생성하고 추출 시 작성된 문서에 기재된 값과 비교

② 전자우편 증거의 종류에 따른 전자우편 프로그램을 구축하고 증거 파일을 복사 및 복제

③ 전자우편 분석 프로그램 및 응용 프로그램을 사용하여 설정 정보, 헤더, IP 주소, 송신자, 수신자, 내용, 경로, 첨부 파일 등을 목적에 맞게 분석

④ 전자우편 분석의 분석자, 분석 과정, 분석 결과 등의 세부 사항을 빠짐없이 기록



<그림 8> 전자우편 분석 절차도

4.5. 악성코드

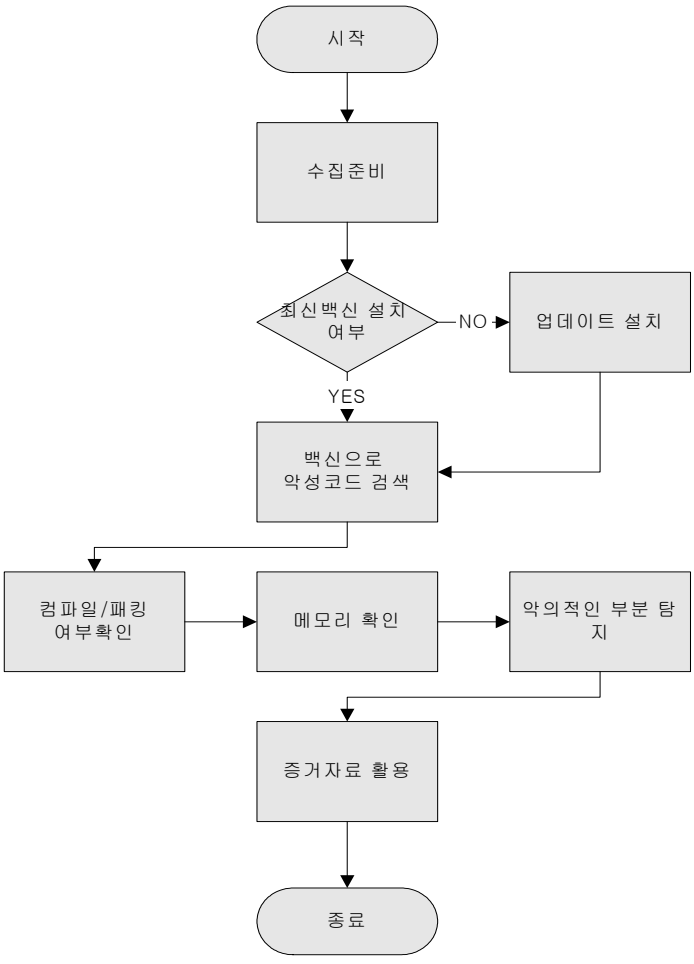
(1) 증거자료의 추출

① 분석 시스템의 최신 백신 설치여부 확인

② 백신으로 악성코드를 검색하여 악성코드가 들어있는 파일 판별

③ 악성 코드가 들어있는 파일의 실행파일구조, 압축된 실행 파일 상태, 메모리 확인

④ 해당 악성 코드 및 관련 파일들을 추출하여 해쉬 값을 계산, 기록, 확인 후 보관



<그림 9> 악성프로그램 증거추출 절차도

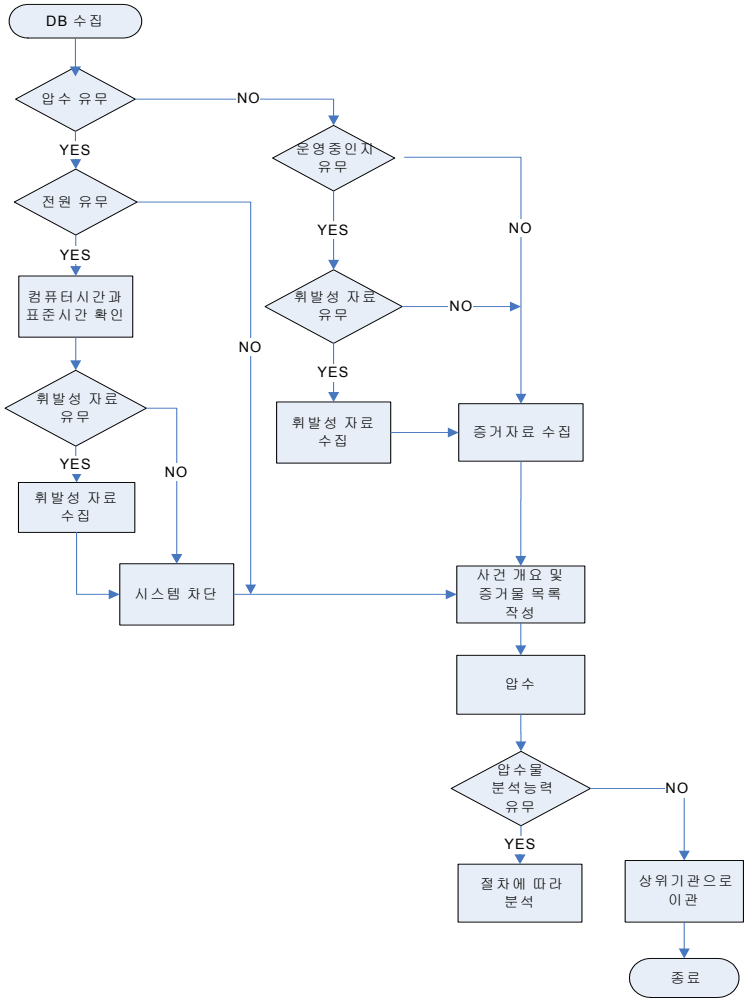
(2) 분석절차

① 추출된 악성코드의 해쉬값을 생성하고 추출 시 작성된 문서에 기재된 값과 비교
② 악성 코드를 복사·복제하고 실행 파일의 구조 획득
③ 압축된 실행 파일일 경우 압축 실행 프로그램 또는 소프트웨어 역공학 기법을 사용하여 분석 가능한 구조로 복원
④ 특정 문자열 및 명령어 검색을 실행하여 근원, 기능, 원리 등을 획득
⑤ 악성 코드의 사용 파일, 메모리 정보 등의 자원 사용 정보를 통해 해당 악성 코드의 세부 기능을 파악
⑥ 이메일, IP, URL 등의 원격지를 추적할 수 있는 정보를 획득
⑦ 악성 코드의 분석자, 분석 과정, 분석 결과 등의 세부 사항을 빠짐없이 기록

4.6. 데이터베이스

(1) 증거자료의 추출

① 운영체계 및 데이터베이스의 종류 및 설정 정보 확인
② 접속 프로그램을 사용하여 데이터베이스에 접속한 후 메모리, 사용자 정보, 자원사용 정보 등의 휘발성 정보 추출
③ 데이터베이스 서버를 압수할 경우 서버 프로그램 종료 후 운영체계 정상 종료
④ 목적하는 자료만을 추출할 경우 데이터베이스 또는 운영체계 명령어를 사용하여 자료를 추출 및 복사
⑤ 데이터베이스 운영자 또는 개발자가 있을 경우 데이터베이스 설계 개념, 사용 목적 및 방법, 추가적인 백업 데이터 여부 조사
⑥ 추출된 데이터베이스의 복사본 또는 저장한 증거 파일의 해쉬값을 계산, 기록, 확인 후 보관



<그림 10> 데이터베이스 증거추출 절차도

(2) 분석절차

① 추출된 데이터베이스 복사본 및 증거 파일의 해쉬값을 생성하고 추출 시 작성된 문서에 기재된 값과 비교

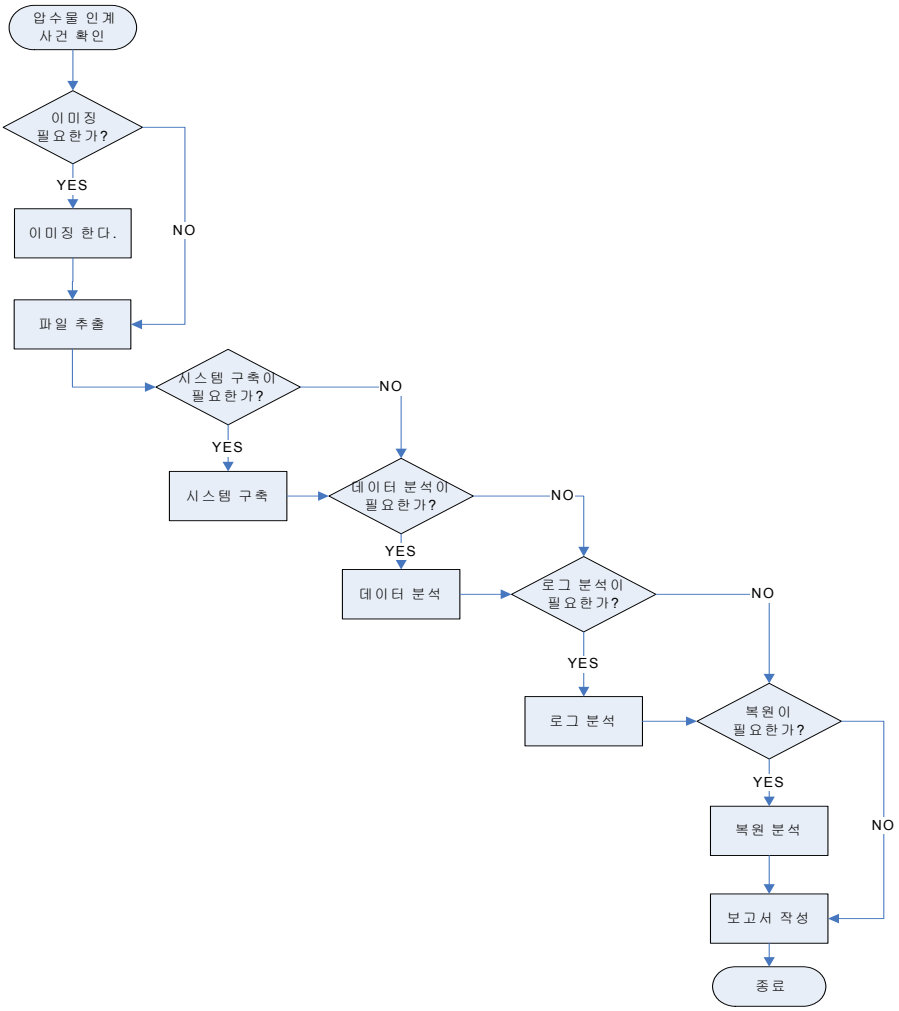
② 데이터베이스의 휘발성 정보를 획득하였을 경우 메모리, 프로세스, 사용 파일 등의

자원 사용을 분석하여 사용됐던 기능 및 상황 파악

③ 데이터베이스 증거에 맞는 운영체계 및 데이터베이스 프로그램을 구축하고 증거 파일을 복사 및 복제

④ 데이터베이스 접속 프로그램 및 로그 분석 프로그램을 사용하여 자료 구조, 자료 관계, 접속자, 사용 내역, 자료 복구 등을 목적에 맞게 실행하고 증거 획득

⑤ 데이터베이스 분석의 분석자, 분석 과정, 분석 결과 등의 세부 사항을 빠짐없이 기록



<그림 11> 데이터베이스 분석 절차도

4.7. CC TV

(1) 증거자료의 추출

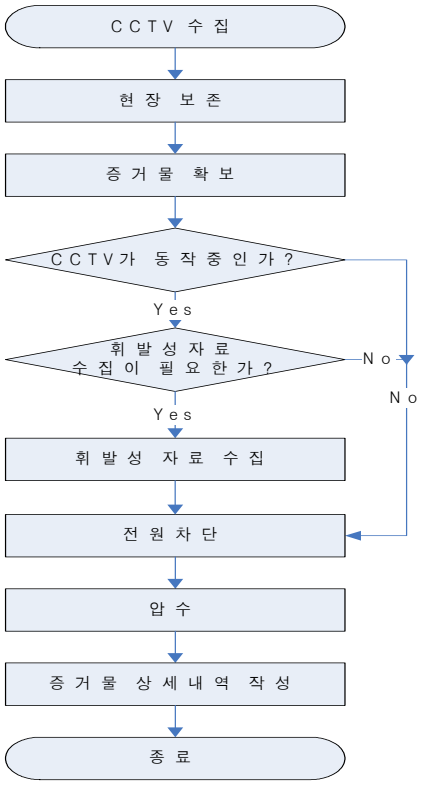
① 사용된 운영체계 및 멀티미디어 증거의 종류, 설정 정보 확인

② CC TV의 회사명 및 제품 정보를 확인하고 자료가 저장되는 컴퓨터의 통신 및 전원을 차단

③ 운영 중인 CC TV에서 증거를 추출해야 할 경우 설정 파일 및 동영상 파일 추출

④ CC TV 제품을 동작할 때 필요한 하드웨어를 추출

⑤ CC TV 자료가 저장되는 저장장치 또는 추출된 파일들의 해쉬 값을 계산, 기록, 확인 후 보관



<그림 12> CCTV 증거 압수 절차도

(2) 분석절차

① 추출된 CCTV 증거의 복사본 및 증거 파일의 해쉬값을 생성하고 추출 시 작성된 문서에 기재된 값과 비교

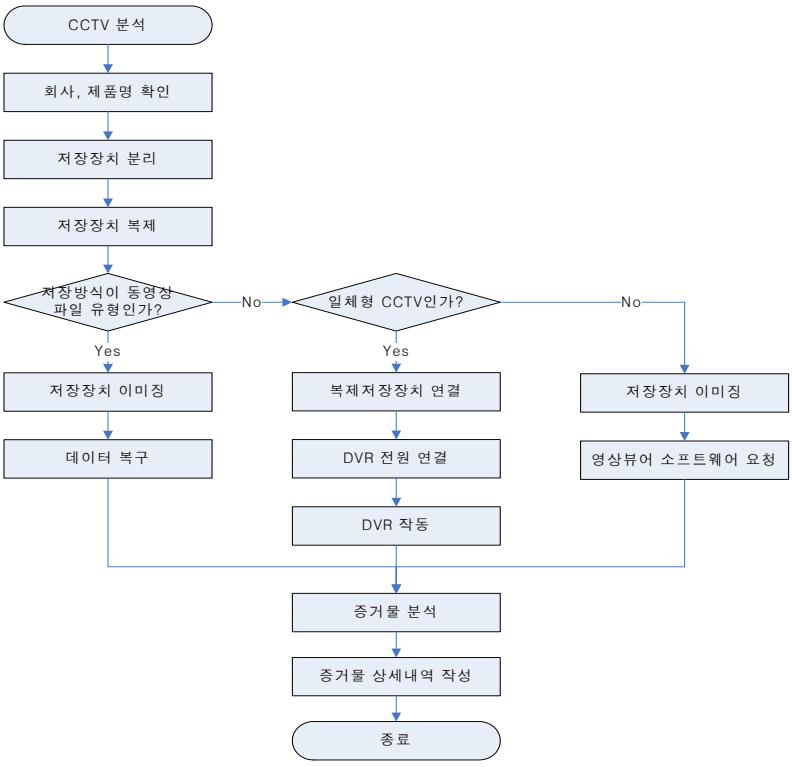
② CCTV 증거의 종류에 따른 분석 프로그램을 구축하고 증거 파일을 복사 및 복제

③ 삭제된 동영상 파일을 복구할 경우 파일 시스템 또는 동영상 저장 방식에 따라 복구

④ CCTV 분석 프로그램 및 응용 프로그램을 사용하여 사용 파일 및 동영상 파일을 분석

⑤ 설정 정보, 동영상 내용 등을 분석하여 사용 시간대, 수사와 관련된 동영상 존재 여부 및 내용 확인 등을 목적에 맞게 분석하고 증거 획득

⑥ CCTV 분석의 분석자, 분석 과정, 분석 결과 등의 세부 사항을 빠짐없이 기록



<그림 13> CCTV 분석절차도

4.8. 휴대폰

(1) 증거자료의 추출

① 휴대폰에서 삭제된 자료를 복구할 필요가 있는지 결정

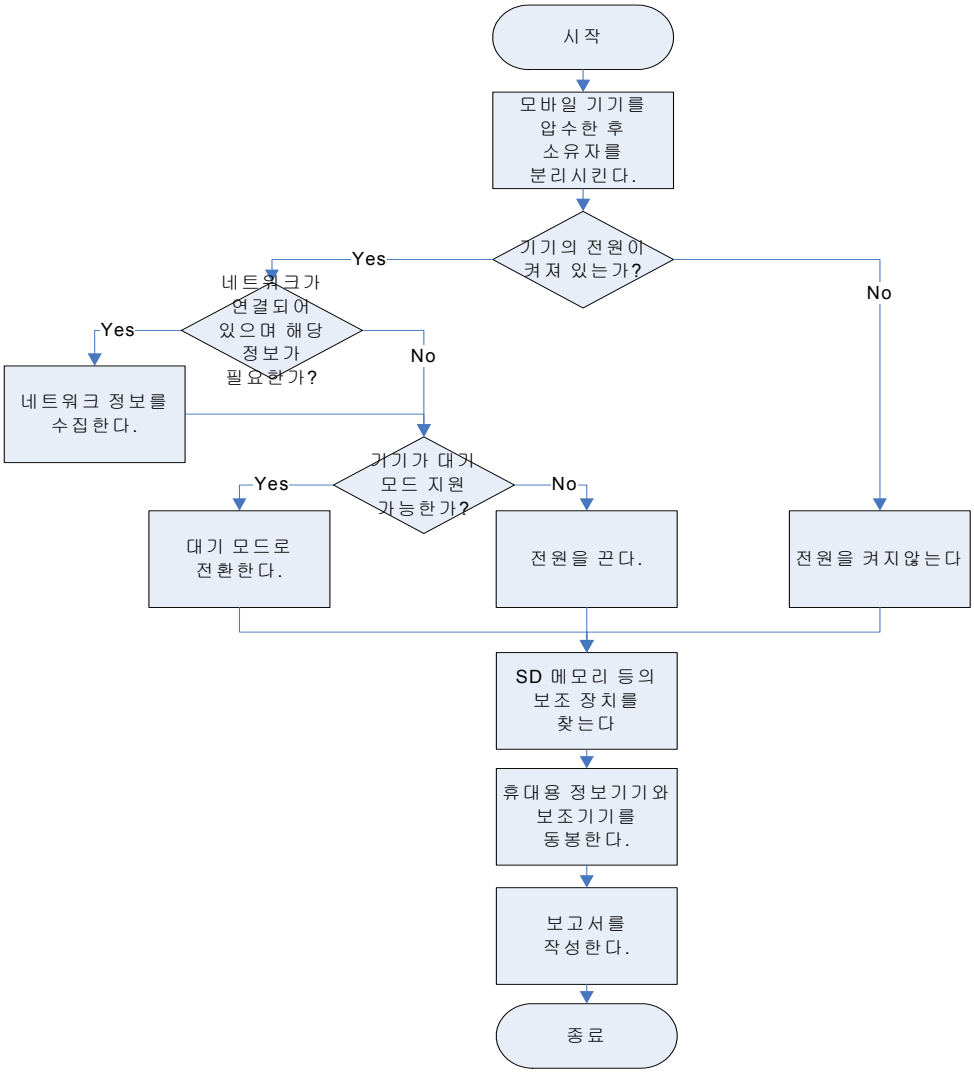
② 삭제된 자료를 복구할 필요가 있을 경우 휴대폰의 내장 메모리를 분리하여 자료를 복제하거나 복사본 생성

③ 삭제된 자료를 복구하기 위해 복제 및 복사본을 생성하였을 경우 복제 및 복사본에 대해 검사 및 복구를 시행

④ 전파차폐장치를 사용하여 통신을 차단하고 쓰기 방지 장치를 사용하여 노트북 및 분석 컴퓨터에 연결

⑤ 노트북 및 분석 컴퓨터에서 휴대폰과 상호작용하는 응용프로그램을 실행시켜 휴대폰에 저장된 정보를 이동

⑥ 추출된 휴대폰 데이터의 복사본 또는 저장한 증거 파일의 해쉬값을 계산, 기록, 확인 후 보관



<그림 14> 휴대폰 증거추출 절차

(2) 분석절차

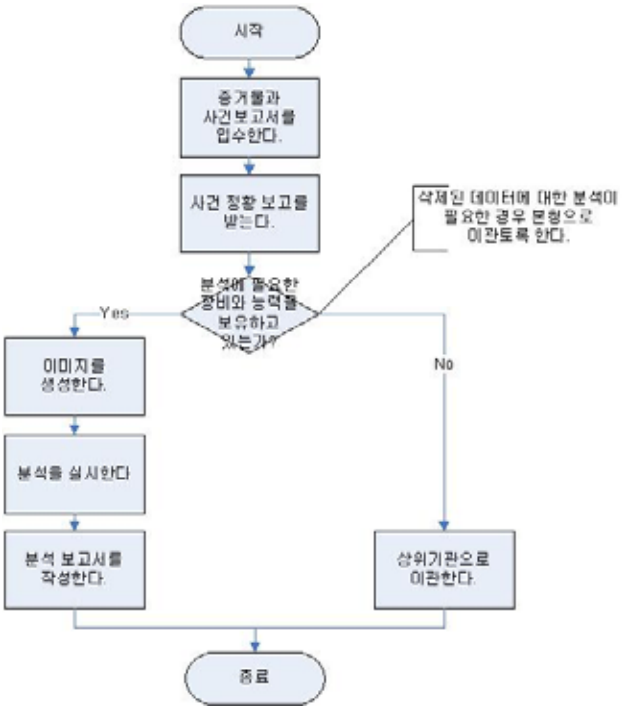
① 추출된 휴대폰 데이터 복사본 및 증거 파일의 해쉬값 비교 확인

② 휘발성 정보를 획득하였을 경우 메모리, 프로세스, 사용 파일 등의 자원 사용을 분석하여 종료 전 사용됐던 기능 및 상황을 인지

③ 휴대폰 증거 파일을 복사 및 복제하고 종류에 따른 분석 프로그램 실행

④ 분석을 통해 전화번호, 주소, 메모, 스케줄 등의 기록 및 삭제된 기록, 시간과 관련된 정보들을 목적에 맞게 획득

⑤ 분석자, 분석 과정, 분석 결과 등의 세부 사항을 빠짐없이 기록



<그림 15> 휴대폰 증거분석 절차

4.9. 암호화 파일

(1) 증거자료의 추출

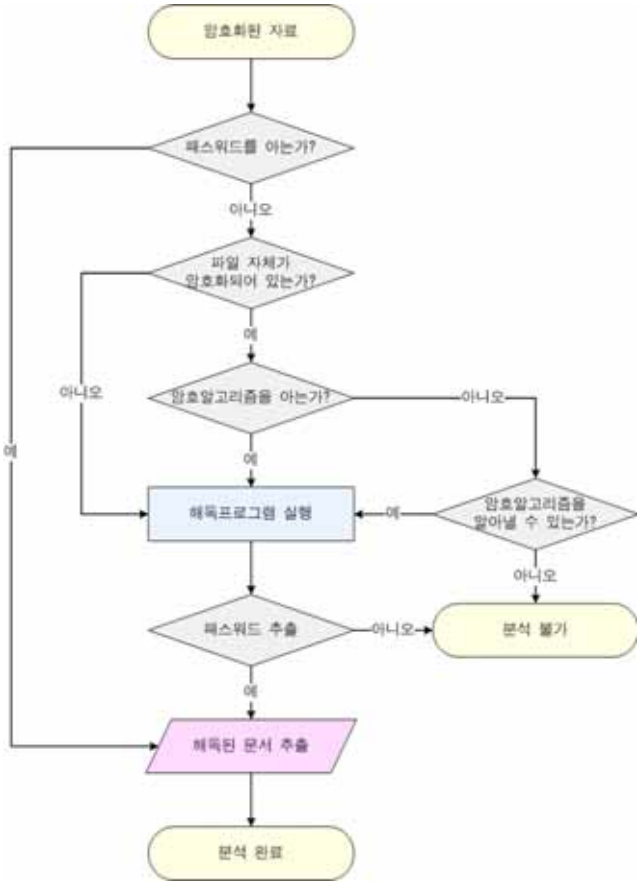
① 암호화 파일이 사용된 운영체계 또는 응용 프로그램의 종류 및 설정 정보 파악

② 암호화 파일이 사용될 때 특정 하드웨어가 필요할 경우 해당 하드웨어 추출

③ 암호화 파일을 해독하는 방법을 알고 있을 경우 해당 위치에서 파일을 추출

④ 암호화 파일을 해독하는 방법을 모르고 있을 경우 저장장치 및 암호화와 관련되어 사용되는 하드웨어 일체를 추출

⑤ 암호화 증거의 파일 또는 저장장치의 해쉬 값을 계산, 기록, 확인 후 보관



<그림 16> 암호화된 자료 해독 절차도

(2) 분석절차

① 추출된 암호화 증거 복사본 및 증거 파일의 해쉬 값을 생성하고 추출 시 작성된 문서에 기재된 값과 비교

② 암호화 증거의 종류에 따른 해독 프로그램을 구축하고 증거 파일을 복사 및 복제

③ 암호화 증거를 해독하는 방법을 알고 있을 경우 추출한 파일을 해독 프로그램에 입력하여 실행

④ 암호화 증거를 해독하는 방법이 알려져 있지 않은 경우 응용 프로그램 및 암호화 증거를 암호화 패턴 검사, 역공학 기법 등의 방법으로 분석

⑤ 비밀 번호를 해독한 후 암호화 증거에 따른 응용 프로그램에 입력하여 확인

⑥ 암호화 증거분석의 분석자, 분석 과정, 분석 결과 등의 세부 사항을 빠짐없이 기록

<그림 17> 암호화 증거분석 절차도

제5장 결과보고서 작성

1. 결과보고서 작성 및 준수사항

결과보고서는 수사관이 쉽게 이해할 수 있는 용어를 사용하여 정확하고 간결하며 논리정연하게 작성한다. 또한 작성자는 결과보고서에 서명하고 작성내용에 대해 책임을 진다.

(1) 결과보고서는 추정을 배제하고 사실관계를 중심으로 작성한다.

(2) 결과보고서는 객관적 사실, 설명내용, 분석관 의견을 구분하여 작성한다.

(3) 증거 발견방법 및 증거물에 대한 작업 내용은 명확하게 문서화한다.

(4) 분석 및 처리과정을 사진 또는 화면캡처 등으로 기록을 유지한다.

(5) 분석에 사용된 하드웨어와 소프트웨어의 정보를 반드시 기록한다.

(6) 결과보고서 작성이 완료되면 분석담당관 서명 후, 원본 증거물과 함께 의뢰인에게 송부한다.

(7) 결과보고서는 수정이 불가능한 문서자료 형태로 부본을 작성하여, 관련 사건의 재판 종결시 또는 공소시효 만료시까지 증거보관실에 보관한다.

2. 증거자료 관리 및 준수사항

(1) 온도와 습도 등 기후의 영향을 받지 않으면서 충격과 자기장, 먼지 등으로부터 보호될 수 있는 증거보관실을 설치・운영한다.

(2) 증거물은 쓰기방지처리가 된 상태로 충격방지용 보관함에 담아 분석이 끝날 때까지 증거보관실에 보관한다.

(3) 증거분석을 위해 생성한 복제본과 분석과정에서 나온 결과물은 반영구적인 저장매체에 저장하여 증거보관실에 보관한다.

(4) 증거물 데이터베이스를 구축하여 관리 및 운영한다.

① 사건종료 후 관련 분석자료 검색 및 열람을 통해 유사사건 분석 또는 처리에 도움을 제공한다.

② 증거물의 연계보관성을 보증할 수 있도록 증거물의 입출내역 등을 기록한다.

(5) 증거분석에 사용되는 도구 및 프로그램은 차후 수사 및 재판과정에서 재검증이 필요할 경우를 대비하여 제조사, 제작연도, 업그레이드 버전별로 구분, 지속적으로 관리 보관한다.

(6) 증거보관실 및 증거물에 대한 접근을 통제한다.

〈 별 첨 〉

디지털 증거분석 의뢰서

1. 사건담당자

관할서	부 서	계 급	성 명	연 락 처
				경비) 일반)

2. 사건 개요

3. 증거 압수 일시 및 장소

사건번호	
일 시	
장 소	

4. 분석의뢰 대상물 정보

압수증거물번호	품 명	제조사	모델명	일련번호	비 고
	컴퓨터				
	CPU				
	RAM				
	☐ 3.5인치				
	☐ 5.25인치				
	☐ CD-R/W				
	☐ DVD-R/W				
	☐ 테이프				
	☐ 기타				
	모니터				
	키보드				
	마우스				
	모뎀				
	프린터				
	하드디스크				

5. 분석의뢰 내용 (대상물 별 작성)

압수증거물 번호	
항 목	분 석 의 뢰 내 용
키 워 드	
파 일	
인 터 넷	
전자우편	
메 신 저	
인쇄내역	
프로그램	
기 타	

〈 별 첨 〉

디지털증거 분석 결과 보고서

1. 사건 개요

발생일시	년 월 일
발생장소	
사건개요	
참고사항	

2. 증거 수집일시 및 장소

사건번호	1. 2006 - 00001
일 시	2006년 05월 02일 15시 30분
장 소	서울 양천구 신정4동 1번지 용의자 변학도 주거지 및 사무실

3. 분석 의뢰자

관할서	부 서	계 급	성 명	연 락 처

4. 분석의뢰 대상물 정보

압수증거물번호	품 명	제조사	모델명	일련번호	비 고
	컴퓨터				
	CPU				
	RAM				
	☐ 3.5인치				
	☐ 5.25인치				
	☐ CD-R/W				
	☐ DVD-R/W				
	☐ 테이프				
	☐ 기타				
	모니터				
	키보드				
	마우스				
	모뎀				
	프린터				
	하드디스크				

5. 분석의뢰 내용

압수증거물 번호	
항 목	분 석 의 뢰 내 용
키 워 드	분석에 필요한 주요 단어들을 기재 예) 피해자, 주변인 이름, 특정 장소, 회사명 등 사건과 연관된 단어
파 일	사건과 관련되어 찾고자 하는 파일의 상세정보 기재 예) 흔글/워드/엑셀 문서, 그림파일 등
인 터 넷	특정 시간대에 인터넷을 사용한 내역을 기재 예) 2006년 4월 30일 21시 30분경 디씨인사드 게시판에 악성 댓글을 게시한 기록
전자우편	특정 시간대에 다른 사람과 주고받은 메일 내역을 상세하게 기재 예) 용의자 변학도와 피해자 성춘향이 주고받은 메일 내역 조사
메 신 저	특정 시간대에 메신저를 사용한 사용자나 대화한 내역을 기재 예) 용의자 변학도가 2005년 4월 30일에 메신저를 사용했는지 조사
인쇄내역	최근 인쇄한 내역에 대한 내용을 기재 예) 용의자 변학도가 최근에 10만원권 자기앞 수표를 인쇄했는지 조사
프로그램	사건과 관련된 프로그램이 설치되었는지에 대한 내역을 기재 예) 차대번호 제작 프로그램 Engrave가 설치되었던 흔적이 있는지 조사
기 타	분석시 필요한 참고사항을 기재 예1) 용의자 변학도는 범죄모의 카페에서 활동한 경력이 있음 예2) 분석대상물은 용의자 변학도의 주거지에서 압수하였으며, 용의자 가족(부모와 동생)이 함께 사용하였음

6. 분석경과

작 업	일 시	장 소	담 당 자	비 고
접 수	년 월 일	디지털증거분석실		
개 봉	년 월 일	디지털증거분석실		
복 제	년 월 일	디지털증거분석실		
분석 완료	년 월 일	디지털증거분석실		

7. 분석결과 요약

8. 분석순서

9. 세부분석결과

압수증거물 번호	
항 목	분 석 결 과 내 용
키 워 드	
파 일	
인 터 넷	
전자우편	
메 신 저	
인쇄내역	
프로그램	
기 타	

10. 기 타

위의 분석 결과는 디지털증거물에 대한 무결성과 연계보관성을 보증하면서 디지털증거 분석 표준절차를 준수하여 도출된 결과임을 증명함

200 년 월 일

소속 증거분석관 (印)