컴퓨터 포렌식스 기술에 관한 연구

홍성욱*, 서영선*, 송정환*

*한양 대학교, 수학과

A Study on Computer Forensics Technology

SungWook Hong*, YoungSun Seo*, JungHwan Song*

*Department of Mathematics Hanyang Univ.

요 약

컴퓨터 포렌식스(Computer Forensics)란 컴퓨터 범죄자료가 법적 증거물로써 제출될 수 있도록 증거의 확인, 복사, 분석 등 일련의 행위를 하는 것을 말한다. 컴퓨터에서 각종 증거자료를 추출하기 위해서는 컴퓨터 특성 이해와 고도의 보안기술을 갖추지 않으면 실제로 증거자료가 존재함에도 불구하고 그냥 간과해 버릴 수도 있다. 본 논문에서는 컴퓨터 범죄를 소개하고 컴퓨터 포렌식스의 소요 기술을 분류하며, 컴퓨터 포렌식스 기술에서 중요한 부분을 차지하고 있는 삭제된 파일 복구기술에 대하여 고찰한다.

I. 서론

정보 통신 기술의 발전으로 인하여 현대 사회에서 컴퓨터와 인터넷의 비중이 날로 커져감에 따라, 이러한 발전의 역기능으로서 컴퓨터 범죄의 증가 및 범죄 기술의 고도화 현상이 갈수록 심화되고 있다. 따라서 컴퓨터 범죄의 대응 기술도 함께 발전되어야 할 필요성이 대두되고 있는데, 이와 관련하여 컴퓨터 범죄 수사의 핵심이라 할 수 있는 컴퓨터 포렌식스에 대한 연구가 중요하게 부각되고 있다. 국내에서는 현재까지 컴퓨터 포렌식스의 개념에 대한 이해조차 미숙한 실정이며, 컴퓨터 포렌식스의 기술 개발 또한 체계적으로 진행되지 않고 있다. 이러한 시점에서 컴퓨터 포렌식스의 개념 확립과 그 절차 및 도구에 대한 연구는 매우 의미 있다 하겠다.

본 논문에서는 컴퓨터 범죄를 소개하고 컴퓨터 포렌식스의 소요 기술을 분류하며, 컴퓨터 포렌식스 기술에서 중요한 부분을 차지하고 있는 삭제된 파일 복구기술에 대하여 고찰하고자 한다.

II. 컴퓨터 범죄

1. 컴퓨터 범죄의 정의

"컴퓨터 범죄(Computer crime)"는 다양한 형사상의 범죄 활동, 논쟁들을 자연스럽게 포함하는 말이다. 이것은 이와 비슷한 의미로 종종 사용되는 "컴퓨터 관련 범죄(Computer-related crime)"라는 말을 통해 보다 넓은 개념으로 표현되기도 한다. 일상 생활에 컴퓨터가 보급됨에 따라 범죄와 컴퓨터 사이에는 언제나 특정한 관계가 존재하게 되었는데, 특히 증거 수집, 수사, 법정 관리와 관련하여 컴퓨터가 폭넓게 사용되는 것에서 그러한 관계를 볼 수 있다.

경제협력개발기구(OECD)에 의하면 컴퓨터 범죄는 데이터의 자동처리와 전송을 수반하는 불법적이고 비윤리적이며 정당하지 않은 방법으로 인한 컴퓨터 자료에 대한 비정상적인 행위로 규정되고 있다. James A. Sweizer는 컴퓨터를 사용하거나 컴퓨터, 단말기, 통신망 등 컴퓨터의 구성요소에 대한 접근을 요소로 하는 범죄로 컴퓨터 범죄

를 정의했다. 또한 Steven L. Mandel은 컴퓨터를 사용함으로써 같은 조건에서 컴퓨터를 사용하지 않는 경우보다 큰 위험을 일으킬 비난 가능성이 있는 행위로 규정했으며, Don Parker는 컴퓨터시스템 내에서 행해진 화이트칼라의 범죄이고, 상업 범죄의 도구로써 컴퓨터를 사용하는 행위로 컴퓨터 범죄를 정의했다[1].

이와 같이 컴퓨터 범죄는 컴퓨터 및 주변기기를 이용하거나, 이를 대상으로 하여 저지르는 불법적이고 비윤리적인 범죄를 총칭하여 일컫는 용어이다. 최근에는 독립된 컴퓨터 자체에 대한 범죄의 범주를 넘어서서 네트워크를 통하여 행해지는 컴퓨터 범죄를 포괄하여 "사이버 범죄(Cyber crime)"라는 용어가 자주 사용되고 있다. 이러한 컴퓨터 범죄가 인터넷을 통하여 이루어지는 경우 "인터넷 범죄(Internet Crime)"라고 하며, "고도 지능 범죄(High-tech Crime)"라고도 한다.

2. 컴퓨터 범죄의 유형

컴퓨터 범죄의 유형을 정확하게 설정하는 것은 쉽지 않은 일이지만, 컴퓨터와 범죄의 상관관계를 통해 그에 대한 개략적인 기준을 설정할 수 있다. 먼저 컴퓨터가 범죄 행위의 대상이 되는 경우가 있는데, 이러한 경우에는 컴퓨터의 기밀성, 무결성, 가용성이 공격을 받아 서비스나 정보를 도난당하거나 공격된 컴퓨터가 손상되기도 한다. 그리고 컴퓨터가 범죄 행위의 도구로 이용되는 경우가 있는데, 예를 들어 음란물 배포, 사이버 사기, 지적 소유권 침해, 불법상품의 온라인 판매, 정보의 은닉/암호화 등이 여기에 해당된다고 할 수 있다. 마지막으로, 컴퓨터가 범죄의 부수적인 수단으로 사용되기는 하나, 법의 집행에 있어서 직접적인 목적이 되지 않는 경우가 있다. 예를 들어 마약 밀매자가 마약 거래라는 범죄와 관련된 자료를 컴퓨터에 저장하는 경우가 여기에 해당된다. 이중 둘째와 셋째의 경우를 하나로 묶는다면 결국 컴퓨터 범죄는 컴퓨터가 범죄행위의 대상이 되는 경우와 범죄행위의 수단이 되는 두 가지의 경우로 구분될 수 있다.

III. 컴퓨터 포렌식스

1. 정의

사전적으로 'forensics'는 "법정의", "변론에 적합한" 등의 뜻을 갖는 단어로서 "forensics medicine" 은 법의학이라는 의미가 된다. 오늘날 컴퓨터가 일상 생활과 불가분의 관계에 놓이게 됨으로써, 컴퓨터에 저장되어 있는 자료 등을 비롯한 여러 가지 컴퓨터 관련 증거물이 법정에서 다루어지는 경우가 많이 발생하고 있으며, 이와 관련된 컴퓨터 범죄의 수사 분야가 바로 컴퓨터 포렌식스(Computer Forensics)이다[8].

컴퓨터 포렌식스는 컴퓨터 범죄에 대한 증거 자료가 법적 증거물로써 제출될 수 있도록 증거물을 수집, 복사, 분석, 제출하는 일련의 행위로 정의된다. 컴퓨터 포렌식스는 모든 컴퓨터 범죄를 행하는 범죄자를 빠른 시간 안에 정확히 찾아내고, 행위에 이용된 증거확보를 통한 법적 대응을 가능하게 하여 컴퓨터 범죄를 지속적으로 감소시키는데 목적을 두고 있다.

2. 종류

일반 범죄 수사와 마찬가지로 컴퓨터 포렌식스는 범죄에 대한 정보를 획득할 수 있는 모든 것들을 대상으로 수행된다. 어떤 것을 대상으로 수사를 행하는가에 따라 컴퓨터 포렌식스의 종류를 구분할 수 있는데, 그 유형은 다음과 같은 것들이 있다[2].

- 디스크 포렌식스(Disk Forensics)

비휘발성 저장 장치인 디스크로부터 증거물을 획득 및 분석하는 컴퓨터 포렌식스이다. 여기에서는 대상 디스크의 내용이 변경되지 않도록 하고, 내용이 변경된 경우에 이를 발견할 수 있는 기술을 필요로 한다.

- 네트워크 포렌식스(Network Forensics)

네트워크 트래픽에서 증거물을 획득·분석하는 포렌식스 유형이다. 여기에는 프로토콜을 해석할 수 있는 기술이 필요하며, 특히 불법적으로 취득한 자료에 대해서는 법적 증거력이 없음에 주의하여 수사를 진행하여야 한다.

- 전자메일 포렌식스(E-mail Forensics)

이메일로부터 내용 및 수신자와 발신자 정보 등을 획득·분석한다.

- 웹 포렌식스(Web Forensics)

웹을 통해 방문자 및 방문 시간, 방문 경유지 등을 분석한다.

- 원시코드 포렌식스(Source code Forensics)

프로그램의 원시코드에서 작성자 등을 확인하여 (해킹 또는 바이러스) 실행코드와 원시코드의 상관관계를 규명한다.

- 모바일 포렌식스(Mobile Forensics)

PDA, 전자수첩, 휴대폰 등 모바일 기기를 통한 컴퓨터 포렌식스로서, 전원이 차단되면 내장된 기록이 소멸되므로 증거물 보존에 유의하여야 한다.

• 멀티미디어 포렌식스(Multimedia Forensics)

디지털 이미지, 오디오, 비디오 등 멀티미디어를 대상으로 하는 포렌식스로서 Digital watermarking과 Steganography 기술이 활용된다.

• 데이터베이스 포렌식스(Database Forensics)

방대한 데이터베이스 자료를 통해 증거자료를 추출하는 컴퓨터 포렌식스이다.

본 논문에서는, 이 중에서 '디스크 포렌식스'에 초점을 맞추어 컴퓨터 포렌식스의 절차 및 기술에 대해 서술하고자 한다.

3. 절차

컴퓨터 포렌식스의 일반적인 절차는 크게 수집, 복사, 분석, 제출의 단계로 이루어진다. 각 절차에 대하여 살펴보면 다음과 같다[3].

1) 수집

디지털 증거물의 수집 단계에서는 증거물로서 합당하고 수집이 허용된 정보가 어떤 것들인지를 결정한 후, 증거물 획득의 과정에 있어서의 현장 상황이나 시스템 구성 등을 여러 가지 방법으로 기록한다. 특히 법적 증거력이 있는 정보를 잘못 취급하여 디지털 증거물로서의 가치를 상실하지 않도록 주의해야 한다.

2) 복사

디지털 증거물을 분석하기에 앞서 가장 먼저 수행되어야 할 절차가 복사 단계이다. 복사는 증거물을 확보한 후에 원본과 동일한 복사본을 만드는 단계로서, 원본 데이터에 대한 변경 및 훼손을 막음과 동시에 조사 과정에서 원본이 가지고 있는 정보를 상실하는 것을 방지하기 위한 과정이다. 따라서 복사는 포렌식스 절차에 있어서 디지털 증거물을 보존하기 위한 가장 기본적이며 필수적인 단계가 된다.

3) 분석

분석은 수집된 자료를 분석 도구를 이용하여 추출, 처리, 판단하는 단계이다. 디지털 증거물의 분석은 그 과정이 명확하고, 결과도출이 논리적이며 재현이 가능하여야 한다. 특히 결정적 증거물의 경우 논리적·물리적 주소를 확보해야 하며, 분석 과정에서 증거물이 훼손 또는 내용이 변경되지 않아야 한다. 디지털 증거물의 분석은 다음과 같은 과정으로 이루어진다[2].

• 시스템 외관 및 구성 조사

• 혐의에 따른 검색 및 폴더 브라우징

• 삭제된 파일의 복구

• 패스워드 복원

• 시계열(timeline)분석, MACtime(Modification, Access, and Creation times) 분석

• 시스템 및 응용 서비스 로그 조사 및 분석

• 피의자의 행위 판단

• 피의자의 IP주소, 도메인 이름, 라우팅 경로, 웹 정보 등을 조사, 이를 근거로 시스템 관리자 정보 확보

• 전자우편 정보(내용, 주소 등) 분석

4) 제출

제출 단계는 수집된 디지털 증거물의 분석 결과를 바탕으로, 증거물이 법적 효력을 가질 수 있도록 작성한 보고서를 법원에 제출하는 절차이다. 제출될 보고서는 일반인이 이해할 수 있도록 증거물의 수집, 복사, 분석 과정을 명백하게 기재하여야 하며, 증거물의 위치, 크기, 시간 등의 정보를 정확하게 포함하여야 한다.

4. 컴퓨터 포렌식스의 소요기술 및 도구

이 절에서는 컴퓨터 포렌식스에 소요되는 기술과 이를 수행하는 포렌식스 도구에 대하여 소개한다. 표 1은 현재 상용화 되어있는 포렌식스 도구들 및 그 기능을 나타내고 있다.

1) 디스크 이미지 복사 기술

디지털 증거물의 이미징(imaging) 도구는 파일이나 대용량 저장 장치에 저장된 자료를 비트 단위로 복사하는 도구이다. 이러한 도구들은 반드시 원천 정보의 변경이나 자료의 손상 및 손실이 없이 정확히 복사하는 능력을 필수 조건으로 갖추어야 한다. NIST는 Computer Forensics Tool Test(CFTT) 프로젝트를 통해 컴퓨터 포렌식스 도구를 평가할 수 있는 방법론을 제시하였는데, 현재 Disk Imaging 도구가 갖추어야 할 요구사항을 정리하여 몇몇 도구들에 대한 테스트 결과를 발표한 바 있다(IV장 참조). 디스크 이미지 복사에 자주 사용되는 도구로는 Encase, SafeBack, Linux "dd", SnapBack DatArrest 등이 있다.

표 1 컴퓨터 포렌식스 도구 및 해당 기술

도구	디스크 이미징	쓰기 방지		데이터 검색	데이터 복원		데이터 분석					증거물 검증
		SWB	HWB		삭제된 파일	패스워드	서명	해쉬	MACtime/ Timeline	로그	프로세스	
www.accessdata.com												
Forensic Toolkit(FTK)	o			o	o		o	o	o	o		
Password Recovery Toolkit(PRTK)						o						
www.digitalintel.com												
DriveSpy	o			o			o	o	o	o		o
FireFly			o									
SCSIBlock			o									
FireBlock			o									
PDBlock		o										
Image	o											
www.encase.com												
EnCase Forensic Edition	o			o	o		o	o	o	o		
FastBloc			o									
www.ilook-forensics.org												
ILook Image Investigator	o			o	o		o	o	o	o		o
www.dmares.com												
Maresware	o			o			o	o	o	o		
www.forensics-intl.com												
Advanced Password Recovery Software Tool Kit						o						
AnaDisk											o	
CopyQM	o											
CRCMd5								o				
DiskSig												o
FileList				o								
GetFree				o	o							
GetGif				o								
GetSlack				o								
GetTime									o			
NTI-DOC				o								
PTable											o	
SafeBack	o											
Seized		o										
ShowFL											o	
www.fish.com/tct												
The Coroner's Toolkit				o	o		o	o	o	o		
www.wetstonetech.com												
Time Check											o	
Time Lock											o	
DETS											o	
NEXT Witness											o	
www.dibsusa.com												
DIBS Mobile Computer Forensic Laboratory	o			o			o	o	o	o		
DIBS Advanced Forensic Workstation	o						o	o	o	o		
DIBS Rapid Action Imaging Device (RAID)	o											
DIBS Analyzer 2				o					o			
DIBS Mycroft V 3		o		o								
www.atstake.com												
@stake LC4						o						
www.winhex.com												
WinHex	o			o	o		o	o			o	
www.funduc.com												
Search and Replace				o								
www.finaldata.com												
FinalData					o							

2) 하드디스크 쓰기 방지 기술 하드디스크 쓰기 방지(Hard Disk Write Block)

기술은 디지털 증거물의 데이터를 검색, 복원, 분석하기 이전에 각각의 과정에 있어서 데이터의 변경 및 손상을 방지하는 기술이다. 이 도구의 가장 중요한 조건은 쓰기 방지된 드라이브의 데이터를 손상시키는 어떠한 명령에 대해서도 그 명령을 수행하여서는 안되며, 그 드라이브로부터 데이터의 정보를 얻는 것을 막아서는 안 된다는 것이다. 하드디스크 쓰기 방지에 많이 이용되는 도구로는 PDBlock, DIBLock 등이 있다.

3) 데이터 검색 기술

데이터 검색용 도구는 파일과 파일에 연관된 논리적인 정보의 내용을 분석한다. 이를 통해 추출하는 정보는 파일의 생성 날짜, 시간, 소유자, 파일의 특성 등이며 여기에는 EnCase, Forensic ToolKit, The Coroner's ToolKit, Search & Replace 등의 도구들이 이용된다.

4) 데이터 복원 기술

• 파일 복구 기술

이미 손실된 데이터에 대한 복구를 통하여 침입자의 침입 흔적을 확인해야 할 경우 데이터의 복구를 필요로 하게 된다. 어떠한 경우 침입자는 자신이 침입했던 시스템의 임의의 파일을 삭제할 수 있는데, 이런 경우 삭제된 데이터는 침입자 자신의 침입 흔적을 담고 있는 경우가 많으므로 삭제된 데이터의 복구는 침입자에 대한 가장 큰 정보를 담고 있을 수 있다. 이러한 파일 복구에 이용되는 도구로는 FinalData, WinHex 등이 있다.

• 암호 분석 기술

데이터의 암호화 방법은 두 가지 측면으로 나누어 생각할 수 있다. 첫째로 데이터의 접근을 제어하기 위해 패스워드를 설정하는 암호화 방법과, 둘째로 암호 알고리즘을 이용하여 데이터를 암호화하는 방법이 있다. 첫 번째 경우에는 패스워드 크래킹(cracking) 기술을 이용하거나 해당 파일에서 패스워드를 삭제하는 등의 방법으로 우회하여 원래의 정보를 얻을 수 있다. 그러나 두 번째 경우와 같이 암호 알고리즘을 통해 암호화된 데이터를 복호하려면 사용된 암호 알고리즘 등의 정보를 알고있어야 하며 아무런 정보 없이 암호문만 가지고 복호하는 것은 계산이론상 불가능하다. 그러나 암호문이 지니는 의사난수성을 이용하여 데이터의 의사난수 특성을 조사함으로서 그 데이터가 암호문인지를 판별하는 것은 가능하다[7].

패스워드로 암호화된 데이터의 패스워드 크래킹에 이용되는 도구로는 Lc4 등이 있다.

5) 데이터 분석 기술

• 해쉬 분석

해쉬 분석을 통하여 시스템 내의 파일의 변조 유무를 확인할 수 있다. 확인하고자 하는 파일의 해쉬값을 계산하여, 미리 저장된 해당 파일의 해쉬값과 비교함으로써 그것의 변조 유무를 판단한다. 해쉬값은 수사기관이나 각 운영체제의 개발자가 범죄에 자주 이용되는 파일이나 변경이 자주 일어나지 않는 파일에 대하여 주기적으로 저장하여 제공한다. 만약 해쉬값의 데이터베이스가 침입당한 시스템 내에 있다면, 침입자가 해쉬값을 위조할 수 있기 때문에 가능하면 해쉬값은 다른 저장장치에 보관하여야 한다. 해쉬 분석을 지원하는 도구로는 EnCase, Forensic ToolKit등이 있다.

• 서명 분석

서명 분석을 통하여 파일의 종류를 확인할 수 있다. 파일에는 파일의 종류를 나타내는 서명이 포함되어 있는데, 의도적으로 파일의 확장자만 변경하여 파일을 숨기려 했다면 서명 값의 확인을 통하여 원래의 파일을 간단히 파악할 수 있다. 서명 분석을 지원하는 도구로는 EnCase, Forensic ToolKit등이 있다.

• MACtime/시계열 분석

MACtime 분석을 통하여 파일의 마지막 접근, 변경, 생성 시간 등 파일에 대한 정확한 시간 정보를 확인할 수 있다. 침입자가 시스템 파일의 시간을 수정하였을 경우라도, 파일의 MACtime 분석을 통하면 파일이 마지막으로 변경된 시간을 확인할 수 있으며, 지워진 파일에 대한 시간의 정보를 이용하여 파일의 복구를 가능하게 한다. 주의할 점은 MACtime은 파일에 접근하는 것만으로도 변경되기 때문에, 분석을 시작하기 이전에 MACtime을 먼저 획득하여야 한다. 이러한 MACtime을 시간 순서대로 정렬하여 시계열 분석을 하면 침입자의 행동과 성향을 파악할 수 있으며 침입자의 차후 행동도 추측할 수가 있다. MACtime/시계열 분석을 지원하는 도구로는 EnCase, The Coroner's ToolKit등이 있다.

• 로그 분석

로그 파일에는 외부에서 시스템에 접근한 기록이나 외부에서 보내져온 데이터에 관한 기록, 외부로 보내진 데이터의 기록 등이 남아 있으므로 웹 브라우저 로그, 메일 로그, FTP 로그, 시스템 부팅 로그 등을 통해 수사에 필요한 정보를 구할 수 있다. 로그 파일에 접근하기 위해서는 시스템의 침입흔적을 먼저 찾아내고 침입 시간대를 가능

한 한 근접하게 추측한다. 그리고 나서 로그 파일에서 해당 시간대의 로그를 찾아 침입 방법과 공격 시스템의 IP주소를 정확히 확인할 수 있다. 로그분석에 이용되는 도구로는 Forensic ToolKit 등이 있다.

6) 증거물 검증 기술

수집된 디지털 증거물은 안전하게 보존되어야 한다. 증거물은 컴퓨터 조사 과정에서 손상, 변경, 삭제되어서는 안되며 분석 과정 중 시스템이나 수집된 정보에 바이러스의 침입이 없어야 한다. 또한 이후 처리 과정에서 장치적 또는 전자적 손상으로부터 적절한 방법을 통해 보호되어야 하며 계속적인 연쇄 관리(Chain of Custody)를 유지하여야 한다.

따라서 조사가 완료된 증거물이 안전하게 보존되었는지를 확인하기 위해 원본 데이터와 복사본 데이터의 MD5 또는 SHA등의 해쉬값과 CRC(Cyclic Redundancy Check)값을 지정하여, 이 두 값이 일치하는 것을 확인함으로써 데이터의 보존이 정확하게 이루어졌음을 검증할 수 있다.

IV. 컴퓨터 포렌식스 기술고찰

컴퓨터 포렌식스에서는 해당 절차에 따라 포렌식스를 정확하게 수행할 수 있는 여러 가지 도구를 사용하게 된다. 따라서 컴퓨터 포렌식스가 정확하게 수행되기 위해서는 신뢰성과 안전성을 보장하는 도구의 개발이 우선적으로 이루어져야 한다.

또한 포렌식스 도구가 개발되었다면 그 도구가 필요한 포렌식스 기능을 잘 수행하는지에 대하여 평가할 수 있는 방법이 개발되어야 한다. 이러한 일환으로 NIST에서는 Computer Forensics Tool Test(CFTT) 프로젝트를 수행하고 있으며 현재까지 몇 가지 디스크 이미징 도구(Disk Imaging Tool)에 대한 테스트가 진행되었다.

그러나 현재 우리나라에서는 포렌식스 도구에 대한 개발 및 이에 대한 분석 및 평가가 부족한 실정이므로 앞으로 이에 대한 연구가 활발히 이루어져야 할 것이다,

1. NIST의 컴퓨터 포렌식스 도구 테스트 소개

본 절에서는 NIST의 컴퓨터 포렌식스 도구 테스트(CFTT)에 대해 소개하고자 한다. CFTT 프로젝트는 소프트웨어 포렌식스 도구의 신뢰성을 측정하기 위하여 제안되었다. 이 프로젝트에서 NIST는 컴퓨터 포렌식스에 소요되는 기술에 따라, 그것을 수행하는 도구가 갖추어야 할 요구사항을 설정하고 각 도구를 평가할 수 있는 방법론을 개발하고 있다. 그리고 이에 따라 상용 도구들을 평가하여 테스트 결과를 포렌식 수사관이나 도구 개발자가 활용할 수 있도록 하고 있다.

현재까지 CFTT는 디스크 이미징 도구에 대한 평가 방법을 개발하고 컴퓨터 포렌식스에 많이 사용되고 있는 EnCase 3.20, SafeBack 2.18, dd에 대한 테스트를 수행하여 그 결과를 발표하였으며[4][5][6], 소프트웨어 하드드라이브 쓰기 방지 도구에 대한 평가 방법과 테스트 계획을 공개한 상태이다. 표 2는 CFTT의 현재까지의 연구 진행 상태를 나타내고 있다.

표 2 CFTT: Current Activity

Identify forensics functions	Develop specification	Test methodology for each function	Report results
Hard drive imaging tools	O	O	EnCase3.20, SafeBack2.18, dd
Software hard drive write protect	O	△ (test plan)	X
Hardware hard drive write protect	X	X	X

이제 도구 테스트가 완료된 CFTT의 디스크 이미징 도구 평가에 대한 내용을 간략하게 요약하고자 한다. CFTT가 제안한 디스크 이미징 도구가 갖추어야 할 요구사항은 다음과 같다.

R1. 도구는 비트 단위로 복사할 수 있어야 하고, 원본 디스크 전체의 이미지를 만들 수 있거나, 분할된 영역에 대한 이미지를 만들 수 있어야 한다.

R2. 도구는 원본 디스크를 변화시키지 말아야 한다.

R3. 도구는 디스크에서의 데이터 입/출력 에러를 로깅할 수 있어야 한다.

R4. 도구에 대한 매뉴얼은 정확해야 한다.

위의 요구사항에 따라 테스트 방법론을 개발하여 각 도구에 알맞은 테스트 케이스를 설정하였으며, 이에 대한 테스트 결과는 아래와 같이 나타났

다.

1) EnCase 3.20

네 가지 요구사항 R1~R4에 대한 EnCase 3.20의 테스트 결과를 다음과 같이 요약하였다.

R1. EnCase 3.20은 세 가지 경우를 제외하면 정확하게 모든 디스크의 영역을 이미지 파일로 복사하고, 다른 드라이브에 복원(restore)했다. 여기에서 제외된 세 가지 경우는 다음과 같다.

• 입출력 시스템(BIOS)이 IDE 하드 드라이브에 접근을 시도했을 경우, 테스트 도구가 드라이브의 일부 섹터에 접근하지 않았다. 만약 ATA를 이용한 직접적인 연결을 시도한다면, EnCase가 모든 섹터에 접근 가능할 것으로 보인다.

• 특정한 분할 형태(FAT32 and NTFS)에 대하여, 분할의 논리적인 복원(restore)이 원본과 정확하게 일치하지 않았다. 물론 개발자 문서에도 원본의 완벽한 복원을 하지 못할 것으로 기술되어 있으며, 비트 단위의 물리적 복사를 할 수 있다면 논리적인 완벽한 복원은 고려하지 않아도 될 것이라는 내용도 기술되어 있다.

• Windows 2000에서는 모든 이미지를 정확하게 복사하지 못하는 경우가 존재한다.

R2. EnCase 3.20은 원본 하드 드라이브를 변화시키지 않았으며, 이미지 파일의 무결성을 체크하였다.

R3. EnCase 3.20은 항상 입/출력 에러를 로깅 하였다.

R4. EnCase 3.20에 사용된 매뉴얼은 "the EnCase Reference Manual, Version 3.0, Revision 3.18."이며, 몇 가지 경우에 있어서 소프트웨어 동작이 기술되어 있지 않거나 모호했다.

2) SafeBack 2.18

네 가지 요구사항 R1~R4에 대한 SafeBack 2.18의 테스트 결과를 다음과 같이 요약하였다.

R1. SafeBack 2.18은 두 경우를 제외하고 정확하고 완벽하게 모든 디스크의 영역을 복사했다. 여기에서 제외되는 두 가지 경우는 다음과 같다.

• 특정한 분할 형태(FAT32)에 대하여 분할의 논리적인 복원(restore)이 원본과 정확하게 일치하지 않았다.

• 입출력 시스템(BIOS)이 IDE 하드 드라이브에 접근을 시도했을 경우, 테스트 도구가 드라이브의 일부 섹터에 접근하지 않았다.

R2. SafeBack 2.18은 원본 하드 드라이브를 변화시키지 않았으며, 이미지 파일의 무결성을 체크하였다.

R3. SafeBack 2.18은 항상 입/출력 에러를 로깅 하였다.

R4. SafeBack 2.18에 사용된 매뉴얼은 "the SafeBack Reference Manual, Version 2.0, Second Edition, October 2001"이며, Version 2.18에 대하여 명시된 내용은 없었다. 몇 가지 경우에 있어서 소프트웨어 동작이 기술되어 있지 않거나 모호했다.

3) dd

네 가지 요구사항 R1~R4에 대한 dd의 테스트 결과를 다음과 같이 요약하였다.

R1. dd는 정확하게 모든 디스크의 영역을 이미지 파일로 복사했다. 그러나 홀수개의 섹터를 갖는 원본 디스크에 대해서는 마지막 섹터를 무시하는 오류가 발생했다.

R2. dd는 원본 하드 드라이브를 변화시키지 않았다.

R3. 이 항목에 대한 테스트는 수행되지 않았다.

R4. 매뉴얼의 오류는 발견되지 않았다.

이상 Disk Imaging 도구로서의 EnCase3.20, SafeBack2.18, dd에 대한 도구 평가 결과를 살펴보았다. 이밖에 다른 컴퓨터 포렌식스 도구에 대하여 아직까지 공식적으로 평가된 바는 없으나, 수행되는 소요기술과 관련하여 컴퓨터 포렌식스 도구의 평가를 통한 신뢰성 및 안전성 검증이 지

속적으로 이루어져야 할 것이다.

2. 데이터 복구 기술에 대한 고찰

1) 데이터 복구의 개요

범행에 사용되었거나 범행과 관련된 로그가 남아 있는 파일 등은 컴퓨터 범죄의 대표적인 증거자료가 되기 때문에, 일반적으로 범죄자는 자신의 시스템의 침입 흔적을 지우기 위하여 범행에 사용한 도구와 로그파일 등을 삭제한다. 특히 범죄자가 자신이 추적 당하고 있는 것을 알게 되는 경우에는 시스템의 전체 파일을 손상시키거나 디스크를 포맷시키는 등의 치명적인 피해를 입히는 경우도 발생할 수 있다. 이러한 경우에는 삭제된 파일을 복구하여 컴퓨터 범죄의 증거물을 확보하여야 한다.

또한, 컴퓨터 범죄 수사는 손상된 파일을 복구하여 증거자료로 제출하는 경우가 많을 뿐만 아니라, 복원된 파일도 일반 파일과 같이 법적으로 같은 증거력을 갖는 것으로 법정에서 취급되고(대법원 판례 1999.9.3 건고 99도2317판결)있는 실정이므로, 고의적으로 또는 사용자의 실수로 삭제된 파일을 복구하는 기술은 컴퓨터 포렌식스에 있어서 매우 중요한 부분을 차지한다고 할 수 있다.

본 절에서는, 데이터 복구의 개념 및 삭제의 유형을 구분하고 현재 많이 사용되고 있는 복구 도구를 소개하고자 한다.

2) 데이터 복구 개념 및 삭제의 유형

일반적인 데이터 복구의 개념은 컴퓨터 저장장치에 저장된 데이터가 소프트웨어 및 하드웨어적인 원인에 의하여 손상되었을 때, 이를 손상되기 이전의 상태로 복원시키는 것을 의미한다. 컴퓨터 포렌식스에 있어서 이러한 파일 복구의 개념은 범죄자에 의해 시스템의 데이터가 고의로 손상되거나, 범죄 발생 후 시스템의 사용자에 의하여 실수로 데이터가 손상되었을 경우에 적용될 수 있다. 손상된 데이터가 범죄에 관한 정보를 담고 있을 가능성이 있는 것이라고 판단되면, 이것을 복구하여 증거물을 확보하여야 한다. 여기에서 데이터 손상이라 함은 파일 삭제, 디스크 포맷, 디스크 분할에 의한 시스템 혹은 파일 손상을 일컫는다.

각각의 데이터 손상의 유형에 대하여 살펴보면 다음과 같다.(Windows의 경우)

• 파일 삭제의 경우

파일 삭제 명령이 수행되더라도 디스크 안에는 파일의 데이터가 남아있기 때문에 이에 대한 복구를 시도할 수 있다. 삭제된 파일이 Windows의 휴지통에 남아 있는 경우에는 Windows에서 자체적으로 복구 가능하다. 그러나 휴지통에 남아 있지 않은 경우에는 별도의 복구 도구를 이용하여 복구를 시도하여야 한다. 이 때 디스크에서 삭제된 파일이 속해있는 데이터 영역이 다른 파일의 데이터로 완전히 덮어 쓰여진(overwriting) 경우에는 복구가 불가능하지만, 덮어 쓰여지지 않은 데이터 영역이 조금이라도 남아있다면 부분적인 복구가 가능하다.

• 디스크 포맷의 경우

디스크를 빠른 포맷 혹은 보통 포맷하였을 경우, 복구하고자 하는 파일이 속해있는 디스크의 데이터 영역이 덮어 쓰여지기 이전까지는 포맷 후 파일 시스템이 변한 경우라도 복구 도구를 이용하여 파일의 복구가 가능하다. 그러나 디스크 전체가 로우 레벨 포맷된 경우에는 디스크의 데이터 영역이 모두 초기화되어 파일의 데이터가 손상되기 때문에 파일 복구가 불가능하다.

• Fdisk의 경우

디스크 파티션(partition)의 정보를 새롭게 설정한 경우에는 디스크의 정보 영역과 데이터 영역이 모두 손상될 수 있다. 만약 디스크의 손상되지 않은 데이터 영역에 복구하고자 하는 파일의 데이터가 존재한다면 이 부분에 대해서는 복구가 가능하다. 그러나 역시 복구하고자 하는 파일이 속해있는 디스크의 데이터 영역이 덮어 쓰여진 경우에는 복구가 불가능하다.

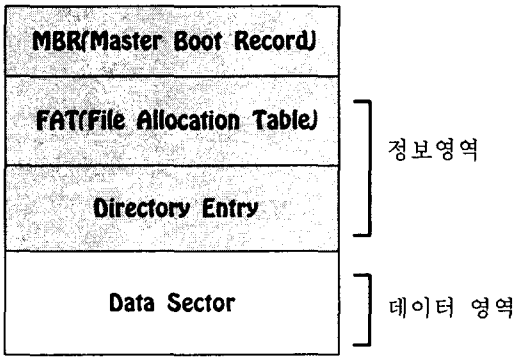

그림 1 디스크 구조의 예 : FAT file system

디스크의 '정보영역'은 파일의 위치 및 이름, 크기 정보 등을 담고 있는 영역이며, '데이터 영역'은 파일의 내용이 저장되는 영역이다. 디스크의 '정보영역'이 손상되더라도, '데이터 영역'이 손상되지 않는다면 파일의 복구가 가능하다.

3) 데이터 복구 도구 소개

현재 많이 이용되고 있는 삭제된 파일 복구 도구 및 사용 환경을 표 3에 정리하였다. 여기에서 음영 부분은 데이터 복구를 전문으로 하는 도구들을 나타내며, 나머지는 복구 기술 이외에 다른 포렌식스 기술을 통합적으로 제공하는 도구들을 가리키고 있다.

V. 결론

컴퓨터 범죄는 날로 지능화·고도화되고 있는 실정이므로 이에 대응할 수 있는 컴퓨터 포렌식스 기술의 발전을 위한 지속적인 연구가 필요하다.

표 3 Deleted File Recovery 도구 소개

Tool	OS	File System	Drive
FTK	Windows, Linux	NTFS, NTFS compressed, FAT 12/16/32, Linux ext2/3	
EnCase Forensic Edition	Windows 95/98/NT/2000/XP/2003 Server, Linux, Unix, BSD, DOS, PALM OS, Macintosh	NTFS, FAT 12/16/32, EXT 2/3, UFS, FFS, Reiser, CDFS, UDF, JOLIET, ISO9660, HFS, HFST	different dynamic disk configurations including RAID 0, RAID 1, RAID 5, Spanned and Basic
ILook Image Investigator	Windows NT/2000, Linux, Macintosh	FAT 12/16/32/32x, VFAT, NTFS 4/5/4 Compressed/5 Compressed, Mac HFS/HFS+, Linux Ext2FS/Ext3FS(journaling variant of Ext2FS), SCO Sys V AFS/EAFS/HTFS, CDFS, Novell Netware NWFS	
GetFree	DOS, Windows 3.x/95/98	FAT 12/16/32	
TCT	Unix		
WinHex	Windows	FAT 12/16/32, NTFS	HDD, FDD, CD-ROM, DVD, ZIP, Smart Media, Compact Flash memory cards, and more
FinalData 2.0 (for window)	Windows 95/98/Me, Windows NT Workstation/2000 professional/XP home/XP professional	FAT, NTFS	HDD, FDD, CD-ROM, DVD-ROM, 플래쉬 메모리, 스마트 미디어, MO, ZIP, Jaz 드라이브 등
FinalData 2.0 (for Unix)	(Solaris) 2.6/2.7/2.8/2.9	UFS/VxFS 3.33,3.4	
	(AIX) 4.3/5L	JFS(JFS2는 지원안함)	
	(HP-UX) 11.0/11i	HFS/VxFS	
FinalData 2.0 (for Linux)	Linux	EXT2/3	
EasyRecovery 6.0	DOS, Windows 3.x/95/98SE/Me/NT/2000/XP systems	FAT, NTFS	IDE/EIDE/ATA and SCSI hard drives, FDD, Zip and Jaz removable media
Data Medic	Windows XP/95/98/Me/NT Workstation 4.0/Server 4.0, Windows 2000 Professional/Server/Advanced Server	FAT 12/16/32, NTFS	IDE, SCSI

본 논문은 컴퓨터 포렌식스에 대한 소개와 소요기술에 대한 분류를 통하여 법·집행기관의 컴퓨터 포렌식스 수사에 도움을 주고자 하였다. 또한, CFTT를 소개함으로써 도구 평가에 대한 필요성을 언급하였고, 특히 컴퓨터 범죄에 의한 데이터 손실의 유형과 삭제된 파일 복구 도구에 대한 고찰을 통해 향후 신뢰성 있는 컴퓨터 포렌식 도구를 개발하고 분석하는 데 기반이 되고자 하였다.

향후, 상용 컴퓨터 포렌식스 도구에 있어서 데이터 복구 도구에 관한 세부 기술을 분석하여 그로부터 개선점을 도출하고, 복구된 증거물의 신뢰성을 제고하기 위한 법·집행기관 간 프로토콜을 개발하는 것이 필요할 것이다.

참고문헌

[1] 이대기, 김태성, 노종혁, 진승헌, 정교일, "국내외 컴퓨터범죄관련 처벌법규 분석", *WISC2002*, 2002. 9.

[2] 이성진, "컴퓨터 포렌식스 기술", *NETSEC-KR 2003*, pp.739-762, 2003. 4.

[3] 박연규, 이필중, "컴퓨터 및 네트워크 환경 하에서 Forensics 적용 동향 및 구현 기술", *CISC2002*, 2002. 11.

[4] National Institute of Justice, "Test Results for Disk Imaging Tools: SafeBack 2.18", *NIST*, http://www.ojp.usdoj.gov/nij/sciencetech/ecrime.htm, 2003. 6.

[5] National Institute of Justice, "Test Results for Disk Imaging Tools: dd GNU fileutils 4.0.36, Provided with Red Hat Linux 7.1", *NIST*, http://www.ojp.usdoj.gov/nij/sciencetech/ecrime.htm, 2002. 1.

[6] National Institute of Justice, "Test Results for Disk Imaging Tools: Encase 3.20", *NIST*, http://www.ojp.usdoj.gov/nij/sciencetech/ecrime.htm, 2003. 6.

[7] 박홍구, 차경준, 장호종, 송정환, 박성준, "실험계획법을 이용한 평문, 암호문 식별방법의 표본크기 선택에 관한 연구", *Journal of The Korea Institute of Information Security and Cryptology Vol.9*, No.4, pp.71-84, 1999. 12.

[8] Warren G. Kruse II, Jay G. Heiser, "Computer Forensics : Incident Response Essentials", *Addison-Wesley*, 2002.