情 報 保 護 學 會 誌
第 12 券 第 5 號, 2002. 10

컴퓨터 포렌식스 기술

이 형 우*, 이 상 진**, 임 종 인***

요 약

컴퓨터 범죄는 급격히 증가하고 있으나 일반적인 범죄에서와는 달리 컴퓨터 파일과 같은 무형의 정보는 증거물로 확보하는 것이 어렵기 때문에 기술적인 측면과 함께 법적 효력을 갖춘 증거물을 확보하기 위한 수집, 확보 및 효과적인 분석 기법이 제시되어야 한다. 이에 본 연구에서는 컴퓨터 포렌식스 기술을 정의하고 유형별로 분류하며, 컴퓨터 범죄 등에 대한 증거물 확보와 분석을 위한 절차 및 방법론 등을 고찰한다. 또한 효율적인 분석을 위해 국외에서 개발된 컴퓨터 포렌식스 도구에 대해 고찰하여, 인터넷 기술이 발전하고 정보화가 급속도로 확산되면서 그 중요성이 날로 증대하고 있는 컴퓨터 포렌식스 기술의 발전 방향을 제시하고자 한다.

Ⅰ. 서 론

인터넷 기술의 발전은 네트워크 및 컴퓨터 시스템 기술의 발전과 더불어 정보화 사회를 앞당기고 있으나 이에 따르는 역기능 또한 무시할 수 없다. 특히 인터넷을 통한 범죄는 예전처럼 해커의 단순 장난 수준을 넘어서서 의도적으로 특정인 또는 특정기업의 정보를 빼내 악용하거나 파괴하고 있는 수준이다.

해킹 등 컴퓨터 관련 범죄는 매년 급격히 증가하고 있다. 예를들어 전자문서 위·변조, 전산업무 방해, 컴퓨터 사용사기 등 각종 컴퓨터 관련 범죄는 기하급수적으로 증가하고 있다. 이와 같은 현상은 컴퓨터와 인터넷 보급이 빠르게 진행되면서 최근 2~3년 사이 컴퓨터 범죄가 급증하고 있으며, 그 수법도 점차 다양화·지능화하고 있는 추세이다[1,2]. 특히 근래에는 해킹과 바이러스 유포로 대표되는 신종 IT 범죄가 급증하고 있다. IT의 발달은 사기·명예훼손·성폭력·협박공갈 등 이른바 오프라인 범죄들이 온라인에서 그대로 발생하고 있다.

해킹 및 바이러스 등과 같은 컴퓨터 범죄는 그 특성상 쉽게 증거물로 확보할 수 없다는 측면을 갖는다. 따라서 일반적인 범죄와 달리 컴퓨터 정보와 같은 무형의 정보를 증거물로 확보하고, 법적 효력을 갖는 증거물로 채택할 수 있도록 하기 위해서는 과학적인 수사 기법 및 체계가 제시되어야 한다.[3,4,5]

왜냐하면 컴퓨터 또는 인터넷상에서 일어나는 행위는 대부분 전자적 현상으로 이벤트의 연속이며 휘발성을 가지거나 광/자기 기록매체에 남겨지는 정도이기 때문이다. 또한 기록매체에 남겨진다 하더라도 피의자가 손쉽게 이를 삭제하거나 훼손할 수 있으므로, 이를 근거로 피의자를 기소하는 등의 사법 절차를 유지하는 것이 매우 어렵다. 컴퓨터는 잠재적으로 순식간에 대규모의 데이터를 처리할 수 있으므로 초등 수사에서 수사관의 간단한 실수도 중요한 증거를 인멸하거나 무력화될 수 있으므로 상당한 주의가 필요하다.

일반 범죄 수사에서 지문 등의 경우 증거물 획득, 처리, 보관, 분석 등의 처리과정 및 방법이 잘 확립되어 있듯이, 컴퓨터 관련 수사에 있어서도 증거물 처리에 대한 절차와 방법이 확립되어야 하며, 이러한 과정을 통하여 나온 결과 및 결론은 대단히 합리적 이어서 관련 전문가들뿐만 아니라 법정에서도 동의할 수 있어야 한다.

본 연구에서는 컴퓨터 범죄에 대한 법적 증거물을 확보하고 이를 통해 컴퓨터 범죄에 대처하는 컴퓨터 포렌식스 기술에 대해 고찰하고자 한다. 2장에서는 컴퓨터 포렌식스의 개념, 유형 등에 대해 살펴보고, 3장에서는 컴퓨터 포렌식스 절차와 세부단계로 나누

* 천안대학교 정보통신학부 조교수 (hwlee@cheonan.ac.kr)
** 고려대학교 정보보호대학원 부교수 (sangjin@korea.ac.kr)
*** 고려대학교 정보보호대학원 교수 (jilim@korea.ac.kr)

어 설명한다. 4장 및 5장에서는 컴퓨터 포렌식스 방법론 및 도구에 대해 세분화하여 제시하고, 6장에서는 결론을 제시한다.

II. 컴퓨터 포렌식스의 정의

1. 컴퓨터 포렌식스 개념

1980년대 중반부터 디지털 증거의 보존, 신원확인, 증거 확보 등에 관한 기술을 다루기 시작하였으며 법적인 문제와 연관된 학문으로 발전하기 시작하였다. 1991년 IACIS(International Association of Computer Specialists)에서 컴퓨터 포렌식스라는 용어를 처음 사용하였다. 일반적으로 포렌식스(forensics)는 '법정의', '변론에 적합한' 등을 의미하는 것으로 'forensics medicine'은 법의학을 의미한다. 최근 컴퓨터가 일상 생활에 밀접하게 사용되면서 컴퓨터에 저장되어 있는 자료가 법정에서 다루어지는 경우가 많이 발생하여 이와 관련된 분야를 컴퓨터 포렌식스(Computer Forensics)라고 부른다.[5]

'Forensic computing' 또는 'Computer Forensics'가 혼용되고 있으나 이는 법적인 측면에서 고찰하는 방법과 수사학적 입장에서 고찰하는 방식으로 나눌 수 있다. 컴퓨터에서 찾아낸 증거를 가지고 이것이 법적인 효력을 발휘하도록 하기 위해서는 법적인 측면과 기술적인 측면이 조화되어야 한다.

결국 컴퓨터 포렌식스는 '정보처리 기기를 통하여 이루어지는 각종행위에 대한 사실관계를 확정하거나 증명하기 위해 행하는 각종 절차와 방법'이라고 정의할 수 있다. 그러므로 컴퓨터 포렌식스는 단순히 과학적인 컴퓨터 수사 방법 및 절차 뿐만아니라 법률, 제도 및 각종 기술 등을 포함하는 종합적인 분야라고 할 수 있다. 또한 컴퓨터 포렌식스 기술은 '컴퓨터를 매개로 이루어지는 행위에 대한 법적인 증거자료를 확보하기 위하여 컴퓨터 저장 매체 등의 컴퓨터 시스템과 네트워크로부터 자료(정보)를 수집, 분석 및 보존 절차를 통하여 법적 증거물로서 제출할 수 있도록 하는 일련의 행위'로 정의할 수 있다.[6]

2. 컴퓨터 포렌식스 유형

컴퓨터 포렌식스를 유형별로 분류해 보면 적용 대상 및 주요 기술 분야에 따라서 다음과 같이 나눌 수 있다.

- Disk forensics
- Network forensics
- Internet forensics

Disk forensics: 정보기기의 주/보조 기억장치에 저장되어 있는 데이터 중에서 어떤 행위에 대한 증거자료를 찾아서 분석한 보고서를 제출하는 절차와 방법을 말한다. 디스크 포렌식스에서 중요한 점은 획득/분석/보고 등의 전과정에서 증거물인 '디스크'의 내용이 중간에 변경되지 않아야 한다는 것이다. 이를 위한 방법으로는 우선 하드디스크를 똑같이 복사하여 복사디스크에서 분석작업을 수행하도록 하는 방법과 EnCase 등에서와 같이 증거물인 디스크에서 분석컴퓨터로 디스크의 이미지를 읽어서 내부에 파일로 저장한 후에 이 파일상에서 분석작업을 수행하도록 하는 방법이 있다. 두 방법 모두 분석작업 중간 또는 종료 후에는 원본과 복사본 디스크의 전 데이터에 대한 해쉬값을 계산하여, 복사본이 원본과 일치한다는 것을 항상 확인할 수 있어야 한다.

Network forensics: 네트워크상에서 전송되고 있는 데이터를 분석, 보고하는 형태로서 통신비밀보호법을 침해할 위험성이 매우 크며 사전에 필요한 수색영장을 발부 받아서 실행하여야 한다. 트랜잭션 로그 분석 등을 먼저 수행하여 필요한 정보를 확보한 후 스니퍼 등과 같은 네트워크 모니터링 도구 등을 이용하여 수행한다.

Internet forensics: 사용자가 Web상의 홈페이지를 방문하여 게시판 등에 글을 올리거나 읽는 것을 파악하고 필요한 증거물을 확보하는 과정이다. 주로 웹서버 프로그램에서 남기는 로그 등을 분석하거나 네트워크 포렌식스 기술을 이용하여 사용자를 추적하기도 한다. 익명을 사용하는 경우에는 실제의 사용자를 파악하기 위해서는 ISP등의 협조가 필요하다.

이밖에도 소프트웨어 불법복제, 바이러스 프로그램 제작/유포 등의 범인을 색출하기 위한 소스코드 포렌식스, 전자우편을 이용한 사기/공갈협박/불법문서유포 등에 관련된 범죄가 발생하고 있으므로, 송·수신되는 전자메일의 내용뿐만 아니라 실질적인 송신자, 수신자를 식별하기 위한 전자우편 포렌식스 등으로 세분화할 수 있다.

III. 컴퓨터 포렌식스 절차

1. 컴퓨터 포렌식스 적용 단계

전자증거물에 대하여 적용되는 일반적인 컴퓨터 포렌식스는 크게 세가지 단계로 구성된다.[5]

- 1단계 : 원본 데이터에 대한 변형 또는 손실 없이 증거물을 확보하는 과정
- 2단계 : 확보된 증거물이 원본과 동일하다는 것을 확인하는 과정
- 3단계 : 확보된 증거물을 분석하는 과정

첫 번째 단계에서는 증거물에 해당하는 정보 또는 기록 등을 수집하고, 세분화하는 과정을 수행한다. 수집된 정보는 원본과 동일한 형태의 복사본을 확보하게 되는 것으로 손실이나 변형이 나타나지 않아야 한다. 첫 번째 단계는 저장 장치에 저장된 정보의 유형과 형태를 확인하는 확인 단계로 증거자료 확보가 이 단계의 핵심이다. 특히 법적 증거력이 있는 정보를 잘못 취급하여 증거물로서의 가치를 상실하지 않도록 유의하여야 한다.

두 번째는 보존단계로써 전자적으로 저장된 자료를 확인 후 변경되지 않도록 보존하는 단계이다. 만약 변경이 될 경우, 법적 절차에 따라 변경된 원인을 설명해야 한다. 이것은 자료뿐만 아니라 자료를 읽을 수 있는 기기의 변경도 포함한다.

세 번째 분석 단계는 전자 자료를 추출, 처리, 판단하는 단계로 분석용 도구를 이용하여 전자 자료를 분석하는 단계이다. 자료 분석 시에는 검사대상 자료가 변경되지 않도록 주의해야 한다. 이와 같은 분석을 마친 후에는 증거물로 채택될 수 있다.

2. 컴퓨터 포렌식스 세부 절차

1) 준비단계

이 단계는 실제 증거물을 수색/압수하기 전에 준비는 과정으로 매우 주요한 과정 중에 하나로서 아래와 같은 사항들을 점검해야 한다.

- 현장에서 관계자로부터 받을 진술서 양식
- 현장을 기록하기 위한 사진기, 녹음기, 노트 등
- 각종 증거물 획득 및 분석을 위한 하드웨어 및 소프트웨어(하드웨어 및 소프트웨어 도구들을 미리 시험되고 검증되어 있어야 함)

2) 증거물 획득 단계

현장 또는 네트워크상에서 필요한 증거를 확보하는 단계이다. 증거물 유형에 따라 적절한 도구를 사용하여 증거물을 입수한다. 대상 시스템이 네트워크에 연결되어 있거나 또는 복잡하게 구성되어 있는 경우, 그 구성도 등을 사진으로 남기거나 기록으로 남겨서 나중에 재현할 수 있게 하여야 한다. 화면에 나타나는 내용이 단순한 것이 아니면 이들도 사진 또는 화면 캡춰 기능 등의 방법으로 기록을 남긴다. 네트워크 포렌식스 또는 다중 사용자 환경에서 증거물을 확보해야 하는 경우 네트워크 연결을 먼저 제거하여 고의적 또는 우발적으로 각종 사용자파일 또는 로그파일들이 손상이 되지 않도록 한다.

UNIX 시스템 등에서 증거물을 확보하는 경우에는 대표적인 로그파일, 해당 사용자의 home directory 등의 파일 등을 먼저 확보한 후에 이들 파일에 대해서 MD5 또는 SHA 등으로 해쉬를 계산하여 기록으로 남긴다.

3) 증거물 분석 단계

증거물 분석과정은 시스템의 종류, 범죄의 유형, 분석 도구 등에 따라 그 방법이 매우 다르지만, 일반적인 규칙은 다음과 같다.

- 분석과정이 명확하고 기록을 남겨야 한다.
- 제3의 분석자에 의해서도 같은 결과가 나올 수 있어야 한다.
- 분석과정에서 증거물이 변경되지 않아야 한다.
- 삭제된 파일을 복원, 암호화된 파일을 복호화하여 분석한다.

분석 방법을 구분해 보면 크게 네트워크상의 분석, 오프-라인 분석 및 컴퓨터 포렌식스 툴을 이용한 분석 방법으로 나눌 수 있다. 마지막 방식은 증거를 손상시키지 않으며 분석 시스템의 자원을 정확히 분석할 수 있다.

IV. 컴퓨터 포렌식스 분석 방법론

일반적으로 컴퓨터 범죄 관련 증거자료를 대상으로한 컴퓨터 포렌식스 분석 방법론은 다음과 같은 두 가지 방식으로 구분할 수 있다.

- 역추적을 통한 컴퓨터 포렌식스
- 증거물 복원을 통한 컴퓨터 포렌식스

1. 역추적을 통한 컴퓨터 포렌식스 방법

본 방식에서는 이벤트가 발생한 근원지 또는 위치를 찾아가는 방법에 관한 사항을 제공한다. 컴퓨터 범죄와 관련된 증거를 수집하고 이를 분석하여 근원지에 해당하는 IP 주소 등을 역추적한다. 근원지가 파악되면 이를 문서화하여 최종적인 증거물로 채택한다. 본 방법론에서 수행되는 과정을 단계별로 제시하면 다음과 같다.

- 1단계 : 관련된 증거 자료 수집
- 2단계 : 키워드 분석
- 3단계 : 출처, 위치, 저장장소 및 근원지 파악
- 4단계 : 증거물에 대한 문서화

1) 관련 자료 수집

네트워크 포렌식스에 해당하는 것으로 증거 수집 단계에서는 하드웨어적인 증거, 소프트웨어 적인 정보 등 모두를 대상으로 한다. 예를들어 'spyagent'와 같은 도구를 사용하여 컴퓨터 시스템에서 발생하는 로그 정보, 키보드 입력 정보 등과 같은 정보를 수집하게 된다.

2) 키워드 분석

수집된 자료들 중에서 수사와 관련되는 단어 및 정보 등을 조사한다. 역추적 등과 관련된 단서를 제공하는 경우가 많다.

3) 출처, 위치, 저장장소 및 근원지 파악

관련 증거물의 출처 및 저장장소 등을 파악하게 된다. 또한 근원지에 해당하는 시스템의 IP 주소를 파악하는 과정도 포함된다.

4) 증거물에 대한 문서화

조사과정에서 수집된 증거물을 근거로 잠정적인 결정을 수행하고 이를 문서화한다.

2. 증거물 복원을 통한 컴퓨터 포렌식스 방법

증거물 복원을 중심으로한 컴퓨터 포렌식스 방법은 관련 증거자료를 수집하여 데이터 복구 과정을 수행하고, 필요로 할 경우 암호화된 데이터에 대한 복호 과정을 수행하여 증거물에 해당하는 데이터의 특성에 따라 수사하는 방식이다.

- 1단계 : 관련된 증거 자료 수집
- 2단계 : 데이터 복구 및 암호 제거
- 3단계 : 포맷 분류 및 은닉 자료 검색
- 4단계 : 증거물 정리 및 문서화

1) 관련 증거 자료 수집

디스크 포렌식스에 해당하는 것으로 백업 디스켓, 하드 디스크, 자료 등에 대해 의도적으로 파괴하거나 암호화 하였을 경우 이를 복구하기 위해 자료를 수집한다.

2) 데이터 복구 및 암호 제거

이미 실행되어 지워졌거나 겹쳐진 자료 등을 최대한 복구하는 과정으로, 일부 자료만이라도 복구되면 증거 확보에 도움을 줄 수 있다. 만일 논리적으로 파괴된 자료인 경우 복구에 많은 시간이 소요된다.

3) 포맷 분류 및 은닉 자료 검색

복원된 자료에 대해 통일된 규격 및 형식으로 자료를 변환하며, 만일 파일 내부에 은닉된 정보가 있으면 이를 추출하거나 복원하여 증거물로 채택한다.

4) 증거물 정리 및 문서화

복원된 증거물과 관련된 증거물을 정리하여 이를 문서화한다.

이와 같은 분석 방법론을 효율적으로 수행하기 위해서는 적합한 도구를 사용하거나, 필요로 하는 경우 현실에 맞는 도구를 새롭게 개발할 필요가 있다. 컴퓨터 포렌식스 도구를 종류 및 기능별로 분석해 보면 다음과 같다.

V. 컴퓨터 포렌식스 도구

국내에서 공개된 컴퓨터 포렌식스 관련 증거 수집 도구는 거의 전무하며 또한 상업용 증거 수집 도구들 역시 삭제된 파일에 대해 복원 및 복구 기능 등을 주로 제공하기 때문에 상당히 제한적인 분야에만 개발되어 있다. 따라서 우선적으로 국외에서 개발되어 널리 사용되고 있는 공개용이나 상업용 컴퓨터 증거 수집 관련 도구들을 제시하여 국내 컴퓨터 포렌식스 분야에 그 활용성을 높일 수 있는 방안을 마련하고자 한다.

현재까지 제시된 컴퓨터 포렌식스 도구들을 제시하면 크게 두가지 형태로 구분할 수 있다. 첫째는 컴퓨터 포렌식스에 관련된 전반적인 기능을 제공하는 도구가 있고, 둘째는 각 기능별로 포렌식스 과정을 수행하는 부분적인 도구들로 나눌 수 있다.

- 통합 기능을 제공하는 컴퓨터 포렌식스 도구
- 부분 기능을 제공하는 컴퓨터 포렌식스 도구

1. 통합 기능을 제공하는 컴퓨터 포렌식스 도구

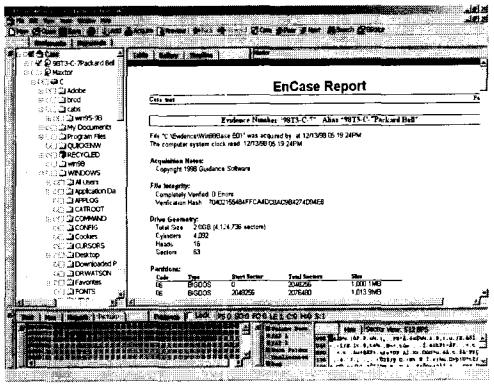
통합 기능을 제공하는 도구인 경우 분석하고자 하는 시스템에 대해 전체적으로 통합 환경하에서 증거물 선택, 수집, 분류 및 증거물 확보 과정을 제공하며 최종적으로 증거물에 대한 문서화 결과까지 제공하는 통합 시스템을 의미한다. 통합형 도구 중에서 대표적으로 아래와 같은 세 가지 도구가 있다.

- EnCase(Guidance Software) - 윈도우즈 환경
- FTK(Access Data) - 윈도우즈 환경
- @stake(Astake) - 유닉스 및 리눅스 환경

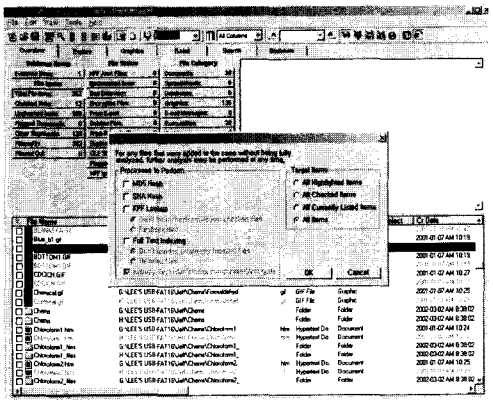
EnCase 또는 FTK 등은 컴퓨터 포렌식스 업무, 즉 증거물 획득(주로 하드디스크)에서부터 다양한 분석 및 보고서 작성에 이르기까지의 업무를 한 소프트웨어에서 수행할 수 있는 기능을 포함하고 있어서 비교적 편리하고 안전하게 작업을 수행할 수 있게 한다. 통합 시스템 중에서 가장 대표적인 도구인 EnCase는 다양한 형태의 디스크 및 파일 시스템을 제어할 수 있으며, 물리적 환경을 정확히 파악하여 이를 증거물로 저장·관리한다.

EnCase 소프트웨어의 특징을 간단하게 나열하면 다음과 같다.

- Intuitive Graphical Interface (GUI)
- Operates directly on image files instead of original evidence
- Search multiple hard drives (and other media) in a single pass
- Search using powerful keyword expressions, UNICODE, and absolute HEX values
- View media at physical or logical level
- Book marking and reporting
- NTFS RAID and Striped Set support
- Unix file system support
- Automatically unzip and search Zip files
- Enhanced recovery of internal files and metadata
- Built-in registry viewer
- Faster acquisitions with more connection options
- Timeline Viewer
- EScript functions



〔그림 1〕 EnCase 도구[15]



〔그림 2〕 FTK 도구[16]

2. 부분 기능을 제공하는 컴퓨터 포렌식스 도구

도구별 기능을 중심으로 컴퓨터 포렌식스 도구를 분류하면 다음과 같이 분류할 수 있다.

- 자료 수집 도구
- 자료 복구 도구
- 암호 제거 도구
- 자료 수사(파일 리스팅) 도구

- 필터링 및 자료 추적 도구
- 디스크 조사 및 이미지 복사 도구
- 에이전트 기반 도구

통합 기능을 제공하는 도구와는 달리 부분적인 기능을 제공한다. 부분 기능을 제공하는 도구들은 아래 표와 같다.

〔표 1〕 부분 기능을 제공하는 컴퓨터 포렌식스 도구

도구 이름	지원 운영체제	기능	공개 여부
chkrootkit	Linux/Unix	루트킷 탐지	공개
TCT	Linux/Unix	데이터 수집	공개
lsof	Linux/Unix	파일 리스팅	공개
CRCMD5	DOS	서명	비공개
DIBS family	DOS	파일 리스팅	비공개
disksearch3	DOS/Windows	디스크 조사	비공개
disksig	DOS	서명	비공개
DriveSpy	DOS	디스크 조사	비공개
FileCNVT	DOS/Windows	파일 리스팅	공개
FileList	DOS/Windows	파일 리스팅	비공개
Filter	DOS	필터	공개
Filter_I	DOS	디스크조사	비공개
ForensiX	Mac/DOS/Windows/Unix	통합	비공개
GetFree	DOS/Windows	디스크조사	비공개
GetSlack	DOS/Windows	디스크조사	비공개
IMAGE	DOS/Windows	이미지생성	비공개
NTAVIEW	DOS/Windows	디스크조사	공개
NTI-DOC	DOS	감시	비공개
PDBLOCK	DOS	증거보존	비공개
ProDiscover DFT	DOS/Windows/NT	디스크조사	비공개
PTable	DOS	파티션테이블 분석	비공개
Seized	DOS/Windows	증거보존	비공개
ShowFL	DOS/Windows	분석시간	공개
TextSearch Plus	DOS	디스크조사	비공개

공개용 컴퓨터 증거 수집 및 분석 도구들 중에서 대표적인 몇 가지만을 비교 분석하면 다음과 같다.

- chkrootkit : 대부분의 공개된 루트킷을 탐지해 주는 도구로 대부분의 Unix, Linux 시스템상에서 컴파일되고 실행된다. 피해 시스템을 분석할 때 매우 편리하고 효율적으로 루트킷을 탐지할 수 있는 도구이다.

- TCT(The Coroner's Toolkit) : 경험적인 피해 시스템 분석방법을 프로그램으로 만들어 놓은 도구이다. 피해 시스템으로부터 다수의 정보를 자동으로 수집하는 기능, MAC time 분석 지원, 지워진 파일 복구 기능 등을 포함하고 있다.

- lsof(List Open File) : 현재 실행되고 있는 특정 프로세스가 참조하는 파일에 대한 정보를 알려주는 도구로 특정 포트를 사용하는 프로세스의 정보도 알 수 있다. 피해를 입은 유닉스 시스템을 조사하는데 필수적인 도구이다.

- CRCMD5 : 저장장치에 있는 모든 파일들의 내용에 대하여 유일한 서명을 생성한다. 그러한 서명들은 컴퓨터 파일들의 내용이 변하였는지, 그렇지 않은지를 식별하게 해 준다. 이 프로그램은 컴퓨터 증거를 처리하는 동안 수정되거나, 바뀌지 않았다는 것을 증명하는데 사용된다.

- DIBS Forensic Workstation : 컴퓨터 범죄자에 의한 문제들에 완벽한 해답을 제공한다. 법정 수사 분석가의 실험에 의해 여러 해에 걸쳐서 개발되었고, 오늘날의 진보된 질의들을 충족시켜 주는 장치이다.

- DIBS Mobile Forensic Workstation : 의심되는 컴퓨터들의 내용을 현지에서 분석할 수 있도록 하는 모든 장비들을 제공한다. 펜티엄 기반이지만, 랩탑에서도 충분히 분석 소프트웨어와 함께 설정할 수 있고, 외장형 하드디스크와 세 하드디스크 랙과 드라이브들, 흑백 프린터, PCMCIA 카드, 케이블, 커넥터와 마우스를 재구성한다.

- DIBS Portable Evidence Recovery : 컴퓨터 하드디스크의 모든 내용을 카피하는 능률적이고, 쉬운 방법이다. 법원에서 증거로 인정

될 수 있는 잠재적 증거들을 찾기 위해 수사관들과 함께 일하면서 개발했다.

- DIBS Professional Forensic Software : 특정 태스크를 목적으로 설계된 모듈로 사용할 수 있으며 아주 효율적이고 생산적인 소프트웨어이다.

- DiskSearch32 : 파일에 있는 텍스트에서 문자열을 찾을 때 사용한다. 파일이 아무렇게나 되어있고, 공간이 할당되어 있지 않은 텍스트에서 문자열을 찾을 때 사용할 수 있다. 또한 맞춤법이 틀린 단어나 유사 단어를 찾을 수 있다. 물리적 레벨에 있는 저장장치를 검사하도록 사용될 수 있다.

- DiskSig : 이 프로그램은 컴퓨터 하드디스크 드라이브의 내용을 위한 유일한 서명을 수학적으로 생성한다. 이런 서명은 컴퓨터 하드디스크 드라이브의 비트 스트림 이미지를 백업해서 정확한 법정증거로 사용할 수 있다.

- FileCNVT : 새로운 기술들로 FileList 프로그램을 보충하는 프리웨어이다. FileList는 하나 또는 그 이상의 컴퓨터 하드 디스크 드라이브들의 내용을 빠르게 목록으로 저장하는데 사용하는 포렌식 툴이다. FileList의 결과는 프로그램과 관계된 출력이 플로피 디스크에 맞도록 압축된다.

- FileList : 하나 또는 그 이상의 컴퓨터 하드디스크 드라이브와 다른 컴퓨터 저장 장치에 저장된 파일들에 대한 정보를 빠르게 문서로 만든다. 이 다목적 툴은 은밀한 사용, 기밀 재조사, 컴퓨터 증거의 실험용 처리증거로 사용된다.

- GetFree : 이 프로그램은 포렌식 분석과 조사를 위해 DOS 또는 윈도우 기반의 컴퓨터 시스템에서 할당되지 않은 파일 공간의 모든 것을 캡춰한다. 이 프로그램의 사용은 컴퓨터 하드디스크와 플로피 디스크에 있는 수백, 수천개의 파일들을 잠재적으로 복구한다.

- GetSlack : 이 프로그램은 다른 NTI 포렌식 툴들과 함께 분석을 위해 논리 도스/윈도우 하드디스크 드라이브 또는 플로피 디스크 드라이브의 파일 슬랙의 캡춰를 하는데 사용한다.

- IMAGE : 플로피 디스크의 물리적 이미지를 생성하는 유틸리티이다. IMAGE에 의해 생성된 파일들은 디스크의 완전한 물리적 이미지를 담고 있다. IMAGE는 포렌식 분석을 위해 "flat"한 이미지 또는 많이 압축된 이미지들을 만들 수 있다.

- PDBLOCK : 물리디스크 드라이브에 예기치 않은 것들이 쓰여지는 것을 예방하는 유틸리티이다. 표준 인터럽트 13과 인터럽트 13 익스텐션 모두를 조작해, 컴퓨터 증거의 오버라이트를 예방할 수 있다.

- ProDiscover DFT : 분석, 수집, 관리를 위한 완전한 무결성의 윈도우 어플리케이션이고, 컴퓨터 디스크 증거의 보고를 한다. 압축된 이미지 파일들을 생성하고, 포렌식 워크스테이션에 저장한다. 정확한 비트스트림 카피를 생성해서 오리지널 증거를 안전하게 지킨다. 윈도우 NT/2000 양쪽 데이터 스트림에서 숨긴 것을 찾을 수 있다. 강력한 검색 능력을 포함한다.

- PTable : 하드디스크 파티션 테이블 분석 툴이다. 이 소프트웨어는 컴퓨터에서 하드디스크에 할당된 파티션 테이블의 포렌식 조사와 분석을 위해 사용된다. 이 툴은 네트워크 포렌식에 관계되고, 혹은 여러개의 OS가 하나의 하드디스크에 여러 파티션에 들어있을 때도 필요하다. 이 소프트웨어는 또한 파티션 갭이 "Unknown"으로 되어있는 부분도 검출한다.

- Seized : 증거 보존 툴이다. 이 간단한 프로그램은 증거로 잡혀있는 컴퓨터들로의 접근을 제한한다.

- ShowFL : 컴퓨터 사용의 분석시간을 위한 프리웨어 툴이다. 그것은 또한 여러 컴퓨터와 컴퓨터 사용자들이 포함될 때 공모에 대한 조사를 돕기도 한다.

- TextSearch Plus : 하드디스크, zip 디스

크, 플로피 디스크(텍스트의 키워드 도는 특정 패턴)를 빠르게 조사할 수 있다.

VI. 결 론

본 연구에서는 급속히 확대되고 있는 컴퓨터 범죄에 대한 증거물을 확보하고 이를 체계적으로 분석하는 기술인 컴퓨터 포렌식스 기술에 대해 고찰하였다. 컴퓨터 포렌식스 기술은 증거 자료에 대한 확보 과정에서부터 시작하며 변형 및 손실 없이 증거물을 확보해야 한다. 이때 법적인 측면에서 많은 부분을 고려해야 하며 전체적인 절차 역시 재고찰할 필요가 있다. 이제 확보된 증거물에 대해서는 분석 과정을 통해 근원지를 역추적하거나 원본 데이터를 복원하여 증거물로 최종 채택하는 방식 등을 수행하게 된다.

사이버 환경이 구축되면서 사이버 범죄 역시 급증하고 있고, 특히 해킹 및 바이러스의 위협은 급속도로 증가하고 있는 시점에서, 컴퓨터 포렌식스 기술을 적용한다면 정보화로 인한 역기능을 방지할 수 있는 도구가 될 것이라고 판단된다. 이와 같은 토대를 구축하기 위해서는 우선적으로 컴퓨터 포렌식스 도구에 대한 조사 및 분석을 통해 우리 현실에 적합한 도구를 선정하고, 최종적으로는 개선된 포렌식스 도구를 개발하는 것이 바람직하다고 판단된다.

참고문헌

[1] Eoghan Casey, *Digital Evidence and Computer Crime*, Academic press, 2000

[2] Eoghan Casey, *Handbook of Computer Crime Investigation*, Academic press, 2002

[3] Albert j. Marcella etc., *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, Auerbach, 2002

[4] Micheal A. Caloyannides, *Computer Forensics and privacy*, Artech House, 2001

[5] Warren G. Kruse II, etc., "Incident Response Essentials", Computer Forensics, Addison-Wesley, 2002

[6] Kevin Mandia & Chris Prosise, "Investigating Computer Crime", Incident Response, Osborne/McGraw-Hill, 2001

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

[8] Deborach Russel and etc., *Computer Security Basics*, O'Reilly & Associates Inc., 1991

[9] Warwich Ford "Principles, Standard protocols and Techniques", Computer Communication Security, Prentice-Hall Inc., 1994

[10] D. Brezinksi and T.Killaea, *Guidelines for Evidence Collection and Archiving*, RFC 3227

[11] J. Ashcroft, "Electronic Crime Scene Investigation - A Guide for First Responders", Electronic Crime Scene Investigation, NIJ, 2001

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

[13] Stephen Northcutt, Judy Novak, *네트워크 침입탐지와 해킹분석 핸드북*, 인포북, 2001

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

[15] *EnCase V3.0 User Manual*, Guidance Software, 2001

[16] *Forensic TOOLKIT User Guide*, AccessData Corp, 2000

〈者著紹介〉

이 형 우(Hyung-Woo Lee)
종신회원

1994년 2월 : 고려대학교 전산과학과 졸업(이학사)
1996년 2월 : 고려대학교 전산과학과 졸업(이학석사)
1999년 2월 : 고려대학교 전산과학과 졸업(이학박사)
1996년~현재 : 컴퓨터과학기술연구소 연구원
1999년~현재 : 천안대학교 정보통신학부 조교수

2001년~현재 : 한국정보보호학회 논문지 편집위원
관심분야 : 전자서명, 암호 프로토콜, 네트워크 보안, 스테가노그래피, DRM, 컴퓨터 포렌식스 기술

이 상 진(Sang-Jin Lee)
종신회원

1987년 2월 : 고려대학교 수학과 졸업(이학사)
1989년 2월 : 고려대학교 수학과 졸업(이학석사)
1994년 8월 : 고려대학교 수학과 졸업(이학박사)
1989년 2월~1999년 2월 : 한국전자통신연구소 선임 연구원
1999년 3월~현재 : 고려대학교 자연과학대학 부교수, 고려대학교 정보보호대학원 겸임교수, 고려대학교 정보보호기술연구센터 연구실장
관심분야 : 블록 암호 및 스트림 암호 분석 및 설계, 암호 프로토콜, 공개키 암호 알고리즘 분석, 스테가노그래피, 컴퓨터 포렌식스 기술

임 종 인(Jong-In Lim)
정회원

1980년 2월 : 고려대학교 수학과 졸업(이학사)
1982년 2월 : 고려대학교 수학과 졸업(이학석사)
1986년 2월 : 고려대학교 수학과 졸업(이학박사)
1986년 3월~현재 : 고려대학교 수학과 정교수
1999년 2월~현재 : 고려대학교 자연과학대학 정교수, 고려대학교 정보보호대학원 원장, 고려대학교 정보보호기술연구센터장
관심분야 : 블록 암호 및 스트림 암호 분석 및 설계, 암호 프로토콜, 공개키 암호 알고리즘 분석, 스테가노그래피, 컴퓨터 포렌식스 기술