국내 수사 환경을 고려한 LiveCD 활용 방법 제안

*이승봉 *최재민 *이상진 *임종인

고려대학교 정보경영공학전문대학원

*{fdc629, koreamath, sangjin, jilim}@korea.ac.kr

Practical Methods of Live-CD usage for Case-Relevance Response in Korea

*Seungbong Lee *Jaemin Choi *Sangjin Lee *Jongin Lim

Graduate School of Information Management and Security, Korea University

요약

디지털 증거의 수집은 컴퓨터 포렌식 수사절차에서 매우 중요하다. 디지털 증거는 특히 용의자가 범죄 과정에서 노출한 증거들을 획득한다는 것에 의미가 있으며, 현재 이러한 디지털 증거 수집을 위한 많은 도구들이 활용되고 있다. 그 중 LiveCD는 대상 운영체제의 영향을 받지 않고, CD 자체를 통해 저장된 다양한 포렌식 툴을 사용 할 수가 있다. 또한 여러 종류의 파일 시스템을 지원하기 때문에 초기 대응에 아주 유용하게 사용되며, 위 과정을 통해 수집된 데이터는 무결성 검증을 통해 증거 수사에 활용된다. 현재 여러 가지 LiveCD를 수사에 활용하고 있으나, 각 도구들 마다 지원하는 포렌식 툴이 다르고 지원하는 운영체제도 다양하다. 따라서 상황에 따라 적절한 LiveCD를 활용하는 것은 매우 중요하며, 이를 통해 증거의 수집을 용이하게 할 수 있다. 따라서 본고에서는 국외의 포렌식용 LiveCD 현황에 대한 조사 및 비교 분석하여 국내 수사 환경을 고려한 LiveCD 활용 방안에 대해 제시 한다.

1. 서론

'컴퓨터 포렌식'이란 컴퓨터를 매개로 이루어지는 행위에 대한 법적 증거 자료 확보를 위하여 컴퓨터 저장 매체 등의 컴퓨터 시스템과 네트워크로부터 자료(정보)를 수집, 분석 및 보존하여 법적으로 유효한 증거물로 제출할 수 있도록 하는 일련의 행위를 의미한다.

컴퓨터 포렌식에서 디지털 증거는 본질적으로 훼손되기 쉬우며, 부적합한 취급이나 조사를 통해 변경, 손상, 파괴될 수도 있다. 이러한 이유로 인해, 증거의 특성을 보존할 수 있도록 사전에 세심한 주의를 기울여야 한다. 즉 증거가 무결성을 상실하게 되는 경우에는 증거로서 사용하지 못하거나 부정확한 결과를 초래할 수 있으므로 증거보존에 유의해야 한다[1]. 따라서 대상 시스템의 운영체제와 독립적으로 증거수집이 이루어져야하며, 이를 통해 무결성이 보장되어야 할 것이다.

*본 연구는 정보통신부 및 정보통신연구진흥원의
IT신성장동력핵심기술개발사업의 일환으로 수행하였음.
[2007-S019-01, 정보투명성 보장형 디지털 포렌식 시스템 개발]

현장에서 디지털 증거를 수집하는 경우 포렌식 LiveCD를 활용하여 간편하고 빠르게 증거를 수집 할 수 있다. 그러나 국내에서 개발한 포렌식 LiveCD는 존재하지 않기 때문에 국내 수사 환경에 잘 맞지 않는 외국 포렌식 LiveCD로 수사를 하는 것은 한계가 있다. 따라서 본 논문에서는 수사에 많이 활용되고 있는 외국 LiveCD을 비교·분석하고 장단점을 파악하여 국내 수사 환경에 맞는 포렌식 LiveCD의 구성을 제안한다.

2. 관련 연구

가. LiveCD

LiveCD는 별도의 설치 과정 없이 응용프로그램이나 운영체제를 CD-ROM으로 부팅하는 것만으로 사용할 수 있도록 특수하게 제작된 CD-ROM 디스크를 말한다[2].

LiveCD는 이동성을 지원하고 외부 기억 장치를 지원하여 자료의 저장이 가능하기도 하다. 현재 CD뿐

만 아니라 DVD는 물론이고 USB Flash 메모리(Live USB Flash)형태로 진화하였고 저장 용량의 제한을 넘어 LiveCD 내에서 구동되는 운영체제만으로 거의 모든 작업이 가능하다. 이러한 기능을 발전시켜 포렌식 수사용 LiveCD가 개발 되었다.

(그림 1) 디지털 포렌식의 주요 연구분야

나. 디지털 포렌식과 포렌식 LiveCD

포렌식 LiveCD란 LiveCD의 확장된 개념으로써, 검증된 포렌식 도구들을 CD내에 삽입하여 디지털 수사 전문 도구로 활용할 수 있도록 개발된 것을 말한다.

현재 국내에서 제작한 포렌식 LiveCD는 존재하지 않으며 외국에서 제작한 포렌식 LiveCD에는 Helix, Penguin sleuth Bootable CD, Fire, FCCU Gnu/Linux Forensic Boot CD, PLAN-B 등이 있다[3-7].

다수가 활용하고 있는 LiveCD에는 dd와 같은 디스크 이미징 도구를 비롯하여, Sleuthkit/Autopsy와 같은 파일 시스템 분석 도구, Foremost/Scalpel과 같은 파일 카빙 도구, John The Ripper와 같은 패스워드 크랙 도구, Chkrootkit/Rkhunter와 같은 루트킷(rootkit) 탐지 도구, Snort/Dsniff와 같은 네트워크 관련 도구와 기타 포렌식 수사에 필요한 여러 도구들을 지원하고 있다.

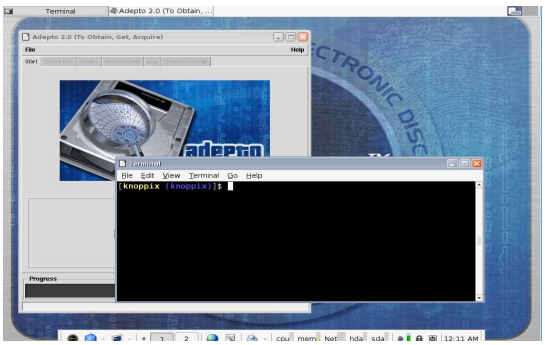

그림 2) GUI 환경의 Helix 구동 장면

하지만 각 LiveCD별로 지원되는 기능이 다르다. LiveCD들 중에서는 디스크 이미징과 파일 시스템 분석에 기능을 집중적으로 지원하는 것들이 있는 반면, 네트워크 관련 분석도구에 기능르 집중적으로 지원하는 것들이 있다. 따라서 다음 절에서는 이러한 LiveCD들을 비교 분석하여 각각의 장단점을 파악한다.

3. LiveCD 구성 분석

가. 운영 체제

운영체제는 Solaris를 사용하는 Fire, 레드햇(Redhat)을 사용하는 Plan-B를 제외하고는 모두 Debian으로 되어 있었다. 대부분의 포렌식 LiveCD가 운영체제를 Debian을 사용하는 것은 기반이 되는 LiveCD를 Knoppix를 사용하기 때문이다. 이것은 레드햇(Radhat) 기반의 리눅스 환경에 익숙한 국내 조사자들에게는 다소 친숙하지 않은 점이 있다[8].

나. 포렌식 기능 분석

각 LiveCD에는 디스크 이미징, 파일 시스템 분석, 네트워크 분석과 관련된 기본 도구들이 포함되어 있다. 하지만 각 LiveCD마다 중점적으로 다루는 도구는 서로 다르므로 [표 1]을 통해 주요 특징을 살펴볼 필요가 있다.

LiveCD	주요 기능
Helix	디스크 이미징 파일 시스템 분석
penguin sleuth Bootable CD	네트워크 관련 분석
Fire	파일 시스템 분석 네트워크 관련 분석
FCCU GNU/LINUX Forensic Boot CD	디스크 이미징 파일 시스템 분석 네트워크 관련 분석
Plan-B	네트워크 관련 분석

[표 1] LiveCD에 따른 주요 기능 분석

[표 1]의 내용과 같이, 대부분의 LiveCD가 포렌식 수사에 필요한 모든 기능들을 지원하는 것은 아니다.

Helix의 경우에는 디스크 이미징 도구나 파일 시스템 분석 도구는 다양하게 지원하지만, 네트워크 관련 도구는 ethereal과 같은 기본적인 도구만 지원한다. 또한 Penguin sleuth Bootable CD와 Plan-B의 경우는 네트워크 관련 도구는 다양하게 지원하지만, 디스크 이미징 도구나 파일 시스템 분석 도구는 Sluthkit, Autopsy, Foremost, Dcfldd을 지원한다.

참고로 Fire와 Plan-B, Penguin sleuth Bootable CD 경우는 2003년에 개발한 것이 최신 버전이기 때문에, 대상 시스템에서 비정상적인 작동이 발생할 수가 있다. 또한 FCCU Gnu/Linux Forensic Boot CD는 여러 방면에서 다양한 기능을 제공하지만 오히려 너무 많은 도구들을 추가하여 사용자에게 혼란을 야기할 수 있다.

4. 국내 수사 환경을 고려한 포렌식 LiveCD

가. 디지털증거 처리 표준 가이드라인 현황

국내 디지털증거 처리 표준 가이드라인에 따르면 증거 수집 시에 컴퓨터의 전원이 켜져 있을 경우와 꺼져 있을 경우 준수 사항을 다르게 정의한다[9]. 컴퓨터의 전원이 켜져 있을 경우 전원을 종료함으로써 소실되는 휘발성 증거인 해킹, 웜·바이러스등 사건 수사에 중요한 단서가 되는 다음 내용을 기록하도록 명시하고 있다.

- 시간 정보
- 네트워크 연결 상태
- 현재 오픈된 TCP·UDP 포트 정보
- TCP·UDP 포트를 오픈하고 있는 실행파일
- NetBIOS 캐시 정보, 현재 접속 사용자 정보
- 인터넷 라우팅 테이블
- 실행 중인 프로세스 내역
- 실행 중인 서비스 내역
- 예약된 작업 내역
- 현재 사용 중인 파일 내역
- 실행 중인 프로세스의 메모리 내용
- 휘발성 정보가 저장된 파일에 대한 해쉬값을 생성

컴퓨터의 전원이 꺼진 경우에는 컴퓨터 및 기타 장비들과의 연결 상태를 기록하고 하드 디스크 등이 충격을 받아서는 안되므로 안전하게 이송할 수 있도록 명시하고 있다. 이후의 분석 과정에서 증거 디스크의 형태(IDE, S-ATA, SCSI, 플래쉬 메모리)를 확인하고 증거 디스크이 이미지 작업을 수행하며, 만약 증거 디스크의 복구가 필요할 경우 파일 시스템 복구 또는 하드웨어 복구할 수 있도록 하고 있다. 이와 함께 디스크 외에도 인터넷 관련 로그와 전자 우편, 악성 코드 감염 여부 등을 파악한 뒤 기록해야 한다[9].

나. 포렌식 LiveCD 구성 제안

컴퓨터 포렌식 수사에 있어 포렌식 LiveCD는 대상 시스템의 무결성을 유지 할 수 있는 장점이 있고 단 하나의 CD로 대상 시스템의 증거를 확보하고 분석 할 수 있기 때문에 신속성을 요구하는 현장에서 매우 효과적으로 사용 할 수 있다. 또한 Linux 기반으로 이루어진 포렌식 LiveCD는 ext2, ext3, fat, ntfs등의 파일 시스템을 지원하기 때문에 어느 환경에서도 대상의 시스템을 조사할 수 있다.

그러나 현재 국내 LiveCD는 전무한 상태이다. 국내 디지털증거 처리 표준 가이드라인에서 확인한 바와 같이, 디지털 증거 수집은 파일 이미징, 파일 시스템 분석, 네트워크 관련 증거 분석 모두 중요시 하고 있다. 국외 포렌식 LiveCD의 경우 국내 수사 절차 환경에 그대로 적용하기에는 적합하지 않다. 따라서 디지털 증거 처리 표준 가이드라인에 입각하여 국내 수사 환경에 맞는 LiveCD의 제작이 필요하므로, 이에 대한 구성 방법을 [표 2] 같이 제시한다.

구분	도구
포렌식 수집 도구	AIR
포렌식 분석 도구	Sleuthkit, Autopsy
파일 시스템 및 디스크 복구 도구	Fatback, Foremost, Scalpel
하드웨어 관련 도구	Discover, lshw, Blktool, Scsiadd, Disktype
패스워드 크랙 도구	Cmospwd, John the ripper, Chntpw
안티 바이러스	Clamav, Rkhunter, f-port
MS files 도구	Pasco, Rifiuti, Tnef, Reglookup, grokevt, mscompress
네트워크 관련 도구	Sbd, Arping, Ngrep, Netwox, Lft, Socat, Netdiscover, Weplab, Knocker, Nikto, Nbtscan, Tcpflow, Tcpreplay, Tcpextract, Dsniff, Hunt, Ettercap, Scapy, Hydra, Macchanger
기타 도구	Pipebench, 2hash, Ftimes, md5deep, Curl, Sgrep, Glimpse

[표 2] 국내 수사용 포렌식 LiveCD 도구의 구성

[표 2]의 내용은 본 논문에서 제안하는 포렌식 LiveCD의 도구 구성에 관한 내용이다. 각 도구들은 디지털증거 처리 표준 가이드라인에서 권고하고 있는 디지털증거 수집 절차를 준수하기 위한 디스크 이미징 도구, 파일 시스템 분석 도구, 네트워크 관련 도구이다. 여러 도구를 동시에 지원하게 되면 수사관에게 혼란을 가중시킬 수 있기 때문에, 각 도구별로 검증을 거친 보편화된 도구들을 선택하여, 포렌식 기능을 적절히 수행 할 수 있도록 구성 하였다.

4. 결론 및 향후 과제

디지털 증거 수집에 있어 대상 시스템의 무결성을 유지하고 신속하게 증거를 수집및 분석하는 과정은 매우 중요하므로, 포렌식 LiveCD는 이러한 상황에서 디지털 증거를 획득할 수 있다는 것에 그 효용 가치가 있다고 할 수 있다. 그러나 현재 국내 포렌식 LiveCD는 전무한 상태이므로 국외 포렌식 LiveCD에 의존 할 수밖에 없다. 국외 포렌식 LiveCD는 국내 디지털증거 처리 표준 가이드라인에 적합하지 않으며 국내 수사관이 사용하기에 현실적인 한계가 존재한다. 따라서 본 논문은 국내 디지털증거 처리 표준 가이드라인과 국내 수사관에 적합한 국산 포렌식 LiveCD의 구성을 제안하였다.

향후에는 국산 포렌식 LiveCD에 들어갈 포렌식 도구 검증 방안에 관한 연구와 함께, 국내 디지털 증거 처리 표준 가이드라인에 따라 일선의 수사관들이 효과적으로 사용할 수 있는 포렌식 LiveCD를 제작할 것이다.

참고 문헌

[1] NIJ, “Forensic Examination of Digital Evidence: A Guide for Law Enforcement", NIJ SPECIAL REPORT, 2004

[2] LiveCD list, http://www.livecdnews.com/

[3] Helix, http://www.e-fense.com/helix /index.php, e-fense

[4] Penguin Sleuth, Penguin Sleuth Bootable CD, http://www.linux-forensics.com/

[5] Fire, http://fire.dmzs.com/, dmzs

[6] FCCU Gnu/Linux Forensic Boot CD, http://www .lnx4n6.be/index.php, lnx4n6

[7] PLAN-B, http://www.projectplanb.org/, J. McDaniel

[8] 이하영, 이상진, 임종인, “포렌식 조사용 LiveCD구현”, Korea Crypt 2006, pp. 166~172. Vol.7,2006

[9] 경찰청, “디지털 증거처리 표준 가이드라인”, (사)한국디지털포렌식학회, 2007