디지털 포렌식 현황과 대응 방안

임경수[1], 박종혁[2], 이상진[3]

Trends and Challenges of Current Digital Forensics

Kyung-Soo Lim[1], Jong Hyuk Park[2], Sangin Lee[3]

요 약

유비쿼터스 시대가 도래함에 따라, 우리는 개인 컴퓨터에서부터 휴대폰까지 다양한 디지털 장비들과 함께 생활하고 있다. 하지만 디지털 장치의 대중화는 이를 활용한 사이버 범죄의 다양화로 발전하였고, 디지털 포렌식 분야에 대한 일반인의 인식 증대는 안티-포렌식 기술의 유행이라는 새로운 문제를 낳고 있다. 이러한 흐름을 반영하듯 포렌식 학계에서는 다양한 분야에 대한 연구가 활발히 진행중이다. 휴대폰/ PDA와 같은 휴대용 전자 장치에서부터 비디오 게임기, 차량의 EDR (Event Data Recorder) 등의 임베디드 시스템에 대한 수사 절차나 분석 방안을 연구하는 임베디드 포렌식, 수사 과정에서 발견된 안티-포렌식 기술에 효과적으로 대응하기 위한 안티-안티 포렌식(Anti-anti-Forensics) 등이 최근의 주요 이슈이다. 본 논문에서는 디지털 포렌식의 최근 현황을 살펴보고, 임베디드 포렌식과 안티 포렌식에 대한 동향 및 대응 방안을 제시한다.

핵심어 : 디지털 포렌식, 임베디드 포렌식, 안티-포렌식, 라이브 포렌식, 포렌식 동향 보고서

Abstract

As ubiquitous Age is arrived in our life, we are living together with more various digital devices such as mobile phone, Ipod, PMP, GPS Navigation etc. But popularization of digital devices has influenced to diversity of cyber crime and moreover growth of understanding digital forensics in the general public takes effect to anti forensic techniques. These movements corresponds to vigorous research in forensic community and law enforcements. For example, embedded forensics which study procedure and analysis techniques about mobile phone, PDA, video game console, EDR(event data recorder), etc. And anti-anti-forensics study countermeasures of anti-forensic techniques and widespread usage of anti-forensic tools. In this paper we report trends of current digital forensics, such as embedded forensics and anti-forensics. and suggest countermeasures for effective digital crime investigation.

Keywords : Digital Forensics, Embedded Forensics, Anti-Forensics, Live Forensics, Trend Forensics Reports

접수일(2008년09월19일), 심사의뢰일(2008년09월20일), 심사완료일(1차:2008년10월10일, 2차:2008년10월30일)

게재일(2008년12월31일)

[1]136-713 서울시 성북구 안암동 5가 1번지, 고려대학교 정보경영공학전문대학원 박사과정
email: lukelim@korea.ac.kr

[2]631-701 경남 마산시 월영동 449번지, 경남대학교 컴퓨터공학부 교수.
email: jhpark1@kyungnam.ac.kr

[3](교신저자) 136-713 서울시 성북구 안암동 5가 1번지, 고려대학교 정보경영공학전문대학원 교수.
email: sangjin@korea.ac.kr

1. 디지털 포렌식 소개

IT 기술의 발전과 정보화 사회가 고도화됨에 따라 사이버 범죄가 증가하게 되었고, 이에 대처하기 위해 과학수사와 수사과학 분야에서 필요한 새로운 형태의 범죄 과학이 디지털 포렌식이다. 디지털 포렌식의 정의는 검찰, 경찰 등의 수사 기관을 기준으로 정의하면 디지털 범죄 수사라고 부를 수 있으며, 광의의 의미로 증거 수집/증거 분석/보고 까지의 수사 절차 및 관련 기술을 연구하는 학문 및 응용 분야로 정의된다. 이러한 디지털 포렌식은 범죄 현장에서 확보한 개인 컴퓨터, 서버 등의 시스템에서 수집할 수 있는 디지털 증거물에 대해 보존, 수집, 분석, 기록, 재현, 보고 등을 과학적으로 도출되고 증명 가능한 방법으로 수행하는 것이다. 디지털 포렌식 연구 분야는 컴퓨터 포렌식에서 점차 확대되어 네트워크 포렌식, 임베디드(모바일) 포렌식 등과 같이 다양한 정보보호의 응용 분야로 그 분야를 넓히고 있다.

컴퓨터 포렌식은 Windows나 Unix와 같은 운영체제를 탑재한 범용 컴퓨터를 대상으로 디지털 포렌식을 수행하는 것을 말한다. 네트워크 포렌식은 기존의 네트워크 보안에서 수행하였던 침입 탐지 방지를 위한 시스템 보호 차원에서 나아가, 실제 범죄를 수행한 범인 검거를 위한 다양한 정보 분석으로 발전한 것이 네트워크 포렌식이다. 이와 같이 범죄에 사용된 모든 디지털 장치에서 필요한 정보를 수집하여 수사에 이용할 수 있도록 도와주는 역할이 디지털 포렌식 기술의 목적이다. 최근에는 기업의 회계 부정이나 분식 회계 등을 탐지하기 위한 포렌식 어카운팅 (Forensic Accounting) 분야에 까지 범위를 넓혀가고 있다.

앞서 설명한 기술적인 면 외에, 디지털 범죄 수사를 통해서 발생할 수 있는 법적인 면의 디지털 포렌식 연구도 진행되고 있다. 최근 이슈가 되고 있는 개인정보보호와 관련하여 디지털 범죄 수사 시에 발생할 수 있는 개인 프라이버시 침해에 대해 어떻게 법적으로 대응할 것인지에 대한 연구가 한 예이다. 또한 미국의 Sarbanes-Oxley Act, HIPAA (Health Insurance Portability and Accountability Act), GLBA (Gramm-Leach-Bliley Act), E-Discovery 와 같은 법안이 상정되면서 기업의 회계 투명성, 개인정보 보호 등과 관련된 기업의 규제 안이 국제적으로 보편화되는 실정이다. 이러한 규제 법안중에서, 기업 간 민사 소송 시에 피고/원고 간의 상대방에게 제출을 요구하는 증거 자료 중 전자메일과 같은 디지털 증거에 대한 제출을 의무화하는 e-Discovery 법안이 통과됨에 따라 이에 관련된 법적/기술적인 연구도 활발히 진행되고 있다.

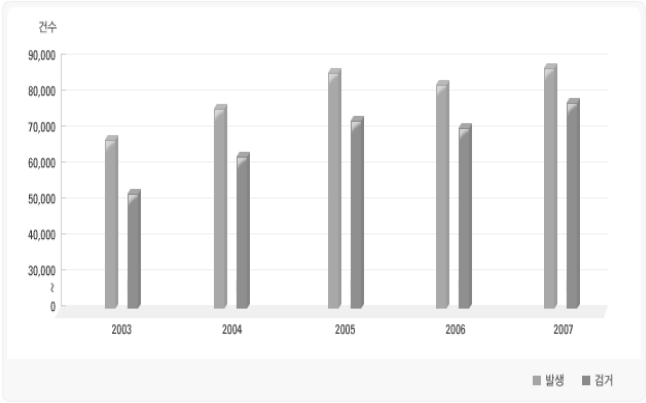
2. 디지털 포렌식 국내외 동향

2.1 사이버 범죄

경찰청 사이버테러대응센터의 공개 자료에 따르면, 사이버 범죄는 2001년에 이후로 급격하게 성

장하였다[1]. 하지만 사이버테러대응센터 및 지방 경찰청 산하 사이버 수사대를 중심으로 적극적인 대응에 힘입어 그 증가 경향은 둔해지고 있는 추세다. 이처럼 사이버 범죄는 새로운 이슈가 되지 않을 만큼 보편화된 하나의 범죄의 형태로 자리를 잡아 가고 있다[그림 1].

또한 디지털 포렌식을 일반적인 형태의 범죄 수사에 대해서도 수행하는 보편화된 수사 과정으로 발전하고 있다. 특히 용의자의 휴대폰에서 사건과 관련된 정보를 수집하고 삭제된 데이터를 복구하는 과정은 필수적인 수사 과정으로 자리 잡았다. 이에 대한 예로 성폭행 살인 사건과 같은 일반 형사 사건에서는 용의자의 개인 컴퓨터와 개인 휴대폰에 대한 포렌식 수집/분석을 수행한다. 특히 웹 브라우저에 대한 사용 내역을 수집하여. 검색했던 내용이나 채팅 사이트의 접속 기록을 수집/분석하여 용의자가 커뮤니티 사이트 또는 채팅 사이트를 통해 피해자와의 접촉을 시도했는지 파악할 수 있다. 또한 용의자의 휴대폰에서 이미지 파일을 탐색 또는 복구하여 피해자의 사진이나 성폭행을 촬영한 사진이 없는지 조사한다. 이처럼 디지털 포렌식은 이제 사건의 해결에 필요한 실마리를 찾는 기본적인 수사 단계로 자리 잡고 있다[2-3].



[그림 1] 사이버 범죄 현황[1]
[Fig. 1] Situation of Cyber Crime[1]

2.2 디지털 포렌식 분야의 성장

IDC의 통계에 따르면 디지털 포렌식 시장은 2001년의 1억 3,300만 달러에서 2004년 2억 8,400만 달러로 급속히 성장하였다. 미국의 경우 순수 디지털 포렌식 시장에서 그 규모가 2001년 2,400만 달러에서 2004년 6,900만 달러로 성장하였다. 이는 디지털 포렌식이 형사 사건의 수사에만 활용되는 기술이 아니라 기업의 기밀 유출이나 기업에 손해를 끼치는 행위와 같은 민사사건에도 활용되고 있음을 보여주는 것이다.

한편, 법률 시장의 경우는 디지털 포렌식 관련 분야의 시장 성장은 두드러진다. 최근 2007년 말부터 미국에서 발효되어 개정된 연방민사소송법에는 Electronic Discovery (e-Discovery)" 법안이 통과에 됨에 따라 전 세계 사건 대응 서비스 시장이 급격하게 성장하고 있다. “e-Discovery" 법안

은 우리말로 번역하면 전자 증거물 개시(開示) 법안이라고 표현할 수 있으며, 민사 소송 시에 피고/원고 각각 상대방에게 요구하는 디지털 증거의 확보 및 제출을 의무화하는 법안이다. 세계적인 시장 분석 기관 IDC에서 발표한 전세계 사건 대응 서비스 시장은 “e-Discovery" 법안의 통과에 힘입어 2005년 17억 달러에서 연 평균 19.3% 씩 증가 41억 $ 추정하였다. 또한 2010년 국내사건 대응 서비스 시장은 2004년 142억원에서 2009년 750억으로 증가할 것으로 발표하였다[2].

2.3 대용량 하드디스크의 보편화

지금의 컴퓨터 포렌식 수사 패러다임은 대상 컴퓨터에서 활성 정보를 수집한 후, 포렌식 이미지를 획득한 뒤 디스크 브라우징 도구를 이용, 다양한 분석 방법으로 이를 조사하는 것이다. 이러한 수사 과정은 하드디스크의 크기에 따라 디스크 이미징 시간과 분석 기법 소요시간이 결정되므로, 증거 분석 소요 시간은 하드디스크의 용량에 따라 결정되는 한계점을 지닌다[4]. [표 1] 대표적인 컴퓨터 포렌식 EnCase Enterprise 4.2[5] 를 이용하여 이미지를 획득하는데 걸리는 시간을 조사한 것이다. 또한 [표 2]는 최근 한 인터넷 쇼핑몰에서 가장 많이 판매되고 있는 하드디스크 순위별 정보를 보여준다. [표 1]과 [표 2]에 근거하여 산술적으로 계산하면, 500 기가 바이트의 하드 디스크의 이미지를 획득하는 데 걸리는 시간은 대략 10시간이 소요된다. 이러한 결과는 수사 영장의 유효 기간이 짧아 신속한 사건 대응이 필요한 경우나, 기업의 보안 사고 조사와 같이 대단위 수사의 경우는 증거 수집 과정 자체가 불가능할 수 있다. [표 2]의 판매 순위가 실제 현장에서 사건이 발생했을 때 대면하는 대부분의 컴퓨터 사양이라고 할 수는 없지만, 향후 수사 대상 컴퓨터의 기본적인 사양일 가능성을 나타내고 있다.

[표 1] EnCase 4.2를 이용한 디스크 이미징 시간
[Table 1] Disk imaging time using EnCase 4.2

시스템 사양	하드디스크 용량	이미징 시간
펜티엄 4 3.2Ghz RAM 2 GB	100 GB	약 2.2 시간
	250 GB	약 4.6 시간
	320 GB	약 6 시간

[표 2] 인터넷 가격비교 쇼핑몰 “다나와”의 데스크탑용 하드디스크 판매 순위
[Table 2] Ranking of desk-top hard-disk in internet shopping mall "Danawa"

판매 순위	제품명	하드디스크용량
1	Seagate SATA2 ST3500320AS	500 GB
2	WD SATA2 WD6400AAKS	640 GB
3	Seagate SATA2 ST3250410AS	250 GB
4	삼성 SATA2 HD252HJ	250 GB
5	WD SATA2 WD5000AACS	500 GB

이처럼 대용량 하드디스크의 보편화는 기존의 포렌식 수사 방식의 한계를 보여주고 있다. 또한 디스크 이미지가 커짐에 따라 분석 과정에서 조사해야 할 데이터의 양 또한 커짐을 나타낸다. 이러한 기존 포렌식의 한계점을 해결하기 위해 다양한 연구가 진행 중에 있다. 고성능 서버 장비를 이용한 고속포렌식수집분석 시스템, 병렬처리를 이용한 포렌식 분석, 고속 데이터 검색 시스템 등이다. 하지만 이러한 연구들은 고성능 하드웨어 장비에 의존해야 하는 단점이 있어, 일선 사이버 수사대나 현장에서 일하는 포렌식 수사관이 사용하기엔 비용이나 환경이 제약이 있을 수 있다.

따라서 최근의 디지털 포렌식 학계는 이러한 문제점들을 개선하기 위해, 디지털 증거 수집의 자동화 기법, 원격지의 분산시스템을 이용하여 현장의 디지털 조사 단계를 수행하는 기법, 프로파일링을 활용한 증거 수집 기법, 데이터 마이닝을 이용한 이상치 탐색 기법, 데이터 검색 시간을 줄이기 위한 사전 처리 기법 등에 대한 다양한 연구가 진행되고 있다[6].

포렌식 이미지에서 데이터를 수집한 뒤에 필요한 디지털 증거를 추출하는 방식이 아니라, 활성 상태의 대상 시스템에서 증거의 무결성을 유지하면서 필요한 디지털 증거를 수집/분석하는 기술을 라이브 포렌식(Live Forensics)라고 한다. 이러한 라이브 포렌식 기술은 휘발성 데이터를 비롯한 사건 해결에 필요한 디지털 증거만을 수집하면 수사 시간 절약에 효과적이다. 또한 사건 유형별로 수집해야 할 디지털 증거를 자동으로 선별하고 수집해주는 기능을 제공하면 전문적인 지식이 없는 포렌식 수사관에게 도움을 줄 수 있다[6].

2.4 임베디드 시스템의 범람

초고속 인테넷 시대를 뛰어넘어 유비쿼터스 시대가 도래함에 따라, 우리 주변에는 수많은 디지털 장치나 임베디드 시스템이 넘쳐나고 있다. 여기서 임베디드 시스템은 컴퓨터와는 다르게 사전에 정의된 특정한 작업만 할 수 있는 기기나 장비를 말한다. 이러한 임베디드 시스템의 종류로는 MP3 뮤직 플레이어, 다양한 영상포맷을 재생할 수 있는 PMP, PDA등의 모바일 장비, GPS 내비게이션, 닌텐도DS와 같은 휴대용 게임기, 유비쿼터스 홈 서버 등 다양한 종류의 임베디드 시스템이 있다.

최근에는 Div x Player, IPTV 셋톱박스처럼 동영상 컨텐츠의 재생을 목적으로 한 시스템이나 승용차, 기차, 선박과 같은 운송수단에 탑재되어 주행 기록, 속도 등과 같은 이벤트를 기록하는 EDR(Event Data Recoder, 블랙박스)등 특수한 목적을 가진 다양한 전자 기기들이 임베디드 시스템으로 개발되고 있다. 특히 EDR은 미국에서는 활발히 연구가 진행되고 있다. ICDF 2008에서 발표된 논문[6] 에 따르면 철도회사와 연구기관이 연계하여, 기차 차량에 대한 EDR 수집/분석 방안에 대한 연구 결과가 발표되었으며, 수집 데이터에 대한 보안 프레임워크까지 연구가 발전하고 있다[2]. 또한 일반적인 차량 교통사고에 대해서도 사고 차량에 부착된 EDR 데이터를 추출하여 쌍방의 과실을 가릴 수 있는 솔루션이 개발되고 있다[7].

임베디드 시스템의 범람이 디지털 포렌식 관점에서 주는 시사점은 모든 임베디드 장치가 저장

공간을 가지고 있고, 이는 곧 용의자가 자신하게 불리한 디지털 정보를 전자 기기의 저장 공간에 숨길 수 있다는 점이다. 이처럼 다양한 임베디드 시스템은 그 장치마다 개별적인 분석 방안이 필요하고 체계적인 수집 및 분석 기법이 필요하다. 또한 같은 종류의 임베디드 시스템이라도 제조사별로 특성이 다를 수 있으므로 보급이 많이 된 제조사 별로 각각의 시스템에 대한 포렌식 수사 절차 및 분석 기술에 관한 가이드라인의 제작이 필요하다.

2.5 안티 포렌식 기술의 발전

일반적인 사이버 범죄 기술과 더불어 발전하고 있는 것이 '안티 포렌식 기술' 즉, 디지털 포렌식 수사에 의해 증거가 발견되지 않도록 하기 위한 기술이다. 안티 포렌식 기술은 컴퓨터와 같은 디지털 기기에 대한 일정 수준 이상의 지식과 기술력을 필요로 하며, 이는 사건에 대한 결정적인 증거를 은닉하거나 훼손하는 형태로 발전하고 있다[4]. 대표적인 기술로는 파일 시스템의 특성에 따른 정보의 은닉 및 삭제하는 기술, 스테가노그래피, 메타데이터를 이용한 정보의 은닉 그리고 물리적으로 정보를 파괴하는 것 등이 있다.

증거의 은닉, 삭제 및 파괴 기술에 맞서 증거를 찾아내는 포렌식 기술이 필요하며 이는 디지털 기기에 관한 지식을 바탕으로, 범죄자가 기존에 습득한 기술과 범죄의 의도를 제대로 파악해야만 해당 증거를 찾아낼 수 있다는 점에서 매우 높은 기술력을 요한다. 이러한 대응 기술을 안티-안티 포렌식 기술이라 한다.

따라서 현존하는 다양한 형태의 안티 포렌식 기술에 대한 분석과 도구들에 대한 현황을 조사하고 이에 대한 대응 기술의 연구가 필요하며, 안티-안티포렌식 기술에 대한 정립과 수사관의 기술 습득은 해당 안티포렌식 기술을 이용한 범죄의 동기를 줄일 수 있을 뿐만 아니라 디지털 포렌식 기술의 발전 그리고 디지털 포렌식 수사의 질을 향상시키는 데 큰 도움이 될 것이다

3. 국내환경에 맞는 포렌식 대응 방안

3.1 임베디스 포렌식

임베디드 포렌식 분야는 특정 디지털 장치에 대해 범죄 사건에 필요한 증거를 수집하여 분석할 수 있도록 소프트웨어나 하드웨어적인 방법을 이용하는 조사 방법이다. 최근의 임베디드 시스템의 다양성에 대응하여 학계에서도 활발한 연구를 통해 새로운 범죄 환경에 재빨리 대응해야 한다.

이처럼 다양한 임베디드 시스템의 등장은 디지털 포렌식 관점에서 중요한 시사점을 지닌다. 개괄적인 임베디드 포렌식 분야는 크게 임베디드 시스템에 대한 데이터 수집 및 증거 획득 방안, 안티-포렌식 관점에서 발생할 수 있는 데이터 은닉에 대한 분석/복구 방안 등으로 크게 나눌 수 있다.

안티 포렌식 관점에서의 임베디드 포렌식은 포함된 플래쉬 메모리나 하드디스크와 같은 저장 장치에 대해, 기존 파일시스템이나 운영체제가 사용하는 파티션 외에 사용자가 추가로 파티션을 생성한 다음 여기에 데이터를 은닉하는 방법이 있다. 일반적인 증거 수집 관점에서는 임베디드 시스템의 사용 기록이나 시간 정보를 활용한 타임라인 분석 등에 이용하여 정황 증거를 파악할 수 있는 실마리를 제공할 수 있다. 마지막으로 일반적인 개인 컴퓨터나 데스크 탑과 동일한 기능을 가진 임베디드 시스템은 리눅스 운영체제를 설치하여 해킹 시스템으로 변경하여 이용될 수 있으므로, 이에 대한 포렌식 분석 및 증거 획득 기술이 필요하다.

본 절에서는 기존의 보편화된 모바일 기기 이외에 최근 새롭게 등장한 임베디드 시스템에 대한 디지털 포렌식 연구 동향과 보안 이슈를 다룬다. 앞서 간략히 설명한 임베디드 시스템에 대해 시스템의 종류별로 분류하고 포렌식 관점에서 분석 방안이나 이슈에 대해 설명한다.

3.1.1 비디오 콘솔 게임기

최근에 등장한 가정용 비디오 게임기는 마이크로소프트의 XBOX 가 출시된 이후로, 그 성능과 기능이 일반 개인용 PC와 동일하다. 즉 IDE 방식의 하드디스크를 저장 장치로 지니며 인터넷을 통한 네트워크 통신이 가능하도록 이더넷 카드를 포함하고 있다.

이러한 하드웨어 환경은 게임을 실행하기 위해 설치된 운영체제 외에 리눅스를 설치할 수 있어, 리눅스 기반의 개인 컴퓨터에서 부터 FTP서버나 기타 다양한 서비스를 제공하는 임베디드 시스템으로서 사용될 수 있다. 따라서 학계에서도 이러한 가정용 비디오 게임기에 대한 범죄 수사의 중요성을 인식하고 대상에 대한 증거 수집 및 분석 방안에 대한 연구를 진행하고 있다[8].

또한 최근 출시된 XBOX 360이나 소니사의 플레이스테이션 3는 일반적인 개인 컴퓨터보다 뛰어난 성능을 가져 리눅스 환경 에서 암호 검색 전용시스템으로도 개발되는 등 다양한 목적에 이용되고 있다.

[그림 2] 리눅스 운영체제를 사용 중인 XBOX[4-5]와 하드디스크가 탈착 가능한 최신 버전의 XBOX 360
[Fig. 2] XBOX using linux operating system and XBOX 360

3.1.2 휴대용 게임기

최근에 국내에 발매되어 큰 인기를 끈 닌텐도 사의 닌텐도 DS는 일반적인 휴대용 게임기에 IEEE 802.11 무선통신 기능을 지원하고 두 개의 ARM7과 ARM9 프로세서를 이용한다. 또한 "홈브류"라고 불리는 사용자가 개발한 프로그램을 실행할 수 있는 환경을 제공한다.

닌텐도 DS가 해킹도구로 이용되는 사례는 아직 보고되지 않았지만, 2007년 개최한 POC 2007에는 닌텐도DS의 특징인 터치스크린과 무선랜을 사용하여 닌텐도DS를 해킹도구로 사용할 수 있음을 시연하였다. 이 시연에서 알려져 있는 홈브류 도구를 사용하여 원격지의 PC를 조종하는 공격 방법과 닌텐도용 ARP 스푸핑 도구를 제작하여 시연하였다[9].

닌텐도DS에 대한 포렌식 수사 방안은 기존의 알려진 홈브류에 대한 해쉬값을 생성하여 변경된 비교/분석하거나 닌텐도DS의 게임 카트리지에서 실행되도록 만들어진 이미지 파일인 롬(ROM)에 대한 분석 방안이 있다.

`

[그림 3] 닌텐도DS Lite와 DSLinux를 가동한 화면
[Fig. 3] Nintendo Ds lite and DSLinux

[그림 4] KT의 IPTV 서비스인 메가TV의 셋톱박스와 분해 하면
[Fig. 4] Capture of set-top box and partition in Mega TV(KT)

3.1.3 IPTV 셋톱 박스

최근 초고속 인터넷 보급(HTTH)과 더불어 HD급의 디지털 컨텐츠를 원하고 싶은 시간대에 보고 싶어하는 시청자의 요구에 부응하여 IPTV의 보급이 늘어나고 있다. IPTV는 인터넷 프로토콜 텔레비전(Internet Protocol Television)의 약자로 초고속 인터넷을 이용하여 정보 서비스, 동영상 콘텐츠 및 방송 등을 텔레비전 수상기로 양방향 통신 서비스로 이용하는 것을 말한다. IPTV를 시청하기 위해서는 셋톱박스를 텔레비전에 연결하여 시청할 수 있다

IPTV의 셋톱 박스는 하드디스크 저장장치와 네트워크 통신이 가능하여 포렌식 수사의 대상으로 인식해야 한다. 가장 기본적인 예로, 안티 포렌식의 정보 은닉 기법을 예로 들 수 있다. 용의자는

하드디스크의 파티션을 조정하여 사용자가 정의한 파티션에 데이터를 은닉하는 기법이 가능하다. 예를 들어 특정 사건의 용의자가 자신의 범죄 행위와 관련된 데이터나 파일을 포렌식 수사관에게 발견되지 않기 위한 목적으로 용의자가 변경한 하드디스크의 파티션에 데이터를 은닉하거나 디스크의 슬랙 공간에 데이터를 삽입하는 소프트웨어를 이용하여 은닉할 수 도 있다.

3.2 안티 포렌식

안티 포렌식 기술은 데이터 영구 삭제, 증거 자동 삭제, 데이터 암호화, Steganography, 물리적인 정보 은닉, 하드디스크 및 와이핑(Wiping), 로그 및 이벤트 삭제 등으로 나눌 수 있다. 본 절에서는 각각의 안티 포렌식 기술에 대해 간략히 살펴보고 이에 대한 대응 방향을 살펴본다.

3.2.1 데이터 삭제

데이터 삭제 기법은 데이터 영구 삭제와 증거 자동 삭제로 나눌 수 있다. 영구 삭제 기법은 하드디스크, 플로피 디스크와 같이 물리적으로 자성을 띠는 자기적 저장 매체에 물리적인 변화를 가해 자성을 제거하여 데이터를 영구히 삭제하는 기법이다. 이러한 기능을 수행하는 장비를 디가우저(Degausser, 소자 장비)라 부른다[그림 5]. 일반적인 디가우저의 기능은 정부 및 정보기관에서 폐기하는 저장 매체에 대해 국가 기밀 정보의 누출을 막기 위한 방법으로 개발되었으나, 개인 사용자가 사용될 경우 증거 은닉의 도구로 이용될 수 있다.

디스크 와이핑(Disk Wiping)은 일반적인 파일 시스템의 파일 삭제 취약점을 해결하기 위한 대안으로 개발되었다. 파일시스템은 파일 삭제시 파일시스템이 내부적으로 관리하는 테이블과 파일과의 연결을 끊는 방식으로 파일을 삭제한다. 따라서 파일시스템이 파일이 삭제되었다고 표시하더라도 파일은 그대로 남아 있을 수 있다. 즉, 파일의 실제 정보는 할당 영역과 해당 클러스터가 덮여 쓰지 않았다면 파일의 이름과 시간정보를 완전히 복구할 수 있다. 이를 방지하기위하여 매체를 '난수' 혹은 '0'으로 중복 덮어쓰는 기법을 와이핑이라 한다[4]. 디가우징 기법과 마찬가지로 디스크 와이핑의 경우도 역시 완벽하게 디가우징 된 디스크에서 데이터를 획득하는 것은 거의 불가능하다. 디가우징은 디스크 상에 존재하는 모든 파일의 완전한 삭제를 가능하게 한다.

증거 자동 삭제는 특정 삭제 응용프로그램을 설치하여 컴퓨터 운영체제에 의해 생성되는 사용자의 개인 정보 또는 증거물이 될 만한 모든 데이터를 삭제하는 행위이다. 웹페이지, 문서, 그림, 동영상, 음성파일, E-mail, 레지스트리, 쿠키 그리고 히스토리 등이 주로 삭제 대상이 된다. 예를 들어 Evidence Elimibator[10] 프로그램은 윈도우 운영체제에서 포렌식적으로 의미 있는 사용자 정보인 웹 히스토리, 그림, 동영상, 음성 파일, E-mail 정보들을 자동으로 삭제하는 기능을 제공한다.

증거 자동 삭제 도구에 대한 대응 방안은 먼저 시장에서 사용되는 증거 삭제 도구들에 대한 분석을 수행하여 삭제된 데이터의 복구 방안이나 동작 환경의 취약점을 분석하여 대응해야 한다. 또한 파일 카빙 기술 이나 슬랙 공간 분석 도구를 활용하여 증거 자동 삭제 도구가 삭제한 정보들을

디스크 전체에서 탐색하여 복구하는 방법에 대한 연구도 연계해서 수행해야 한다.

[그림 5] Degausser 장비 예 (http://www.enetrex.com)
[Fig. 5] Equipment of Degausser

3.2.2 데이터 암호화

데이터 암호화 기법은 문서 파일이나 디렉토리, 압축파일을 암호화하는 것으로, 소요 시간이 중요한 증거 분석 과정에서 가장 어려움을 주는 분야 중에 하나이다. 특정 파일이 암호화되었을 경우, 패스워드를 크랙 하여 파일을 복호화 해야 내부 컨텐츠를 볼 수 있으므로, 패스워드 검색 도구의 성능이나 용의자가 설정한 패스워드의 길이에 따라 대기 시간이 늘어난다. 데이터 암호화 기법에 효과적으로 대처하기 위해서는 암호화 되어있는 대상 파일 포맷에 취약한 패스워드 공격 방법이나 패스워드 검색시간이 빠른 도구를 사용하여 대기 시간을 최소화하는 방법이 필요하다.

3.2.3 스테가노그래피(Steganography)

스테가노그래피(steganography)는 메시지(massage)가 전송되고 있다는 사실 자체를 은닉함으로써 데이터를 숨기는 정보 은닉 기술이다. 데이터 암호화 기법은 패스워드 검색 도구를 이용하여 복호화하면 데이터를 획득할 수는 있지만 스테가노그래피는 데이터 자체를 획득할 수 없다. 주로 스테가노그래피 기술은 어느 정도의 데이터의 변경을 가하여도 가시적으로 변화가 적은 이미지나 동영상 파일에 정보를 숨긴다[4].

스테가노그래피 기술이 특정 데이터의 통신 자체를 은닉하는 것이기 때문에, 데이터가 은닉된 상태로 전송 혹은 전달되고 있다는 것을 관찰자 혹은 수사관들에게 들키지 않을 수 있다. 또한, 수사관들이 스테가노그래피 기법을 이용하여 정보를 은닉한 이미지 파일을 획득하였더라도 은닉된 데이터를 획득하기 위해서는 사용자가 데이터를 은닉할 때 설정한 비밀번호를 알고 있어야 한다. 그렇기 때문에 수사관이 스테가노그래피 기법을 이용하여 은닉된 데이터를 획득하는 것은 어려운 일이다. 최근에 스테가노그래피기법은 문서의 저작권을 보호하는 데에 사용되기도 한다. 만약 이러

한 기법들이 기업의 기밀정보를 유출하는 데에 사용된다면 기업의 경쟁력 약화와 많은 금전적 피해가 발생할 수 있을 것이다[4].

현재 스테가노그래피에 대한 명확한 대응 방안은 없는 것으로 알려져 있다. 통계 분석 등을 통한 스테가노그래피 통신에 대한 탐지를 할 수 있는데, 이러한 탐지를 통해 스테가노그래피가 적용된 고 이미지를 획득하더라도 숨겨진 데이터를 추출해 내는 것은 거의 불가능하다. 만약 해당 이미지를 제작한 도구를 밝혀낸다면, 해당 도구가 변형된 이미지를 제작할 때 생기는 특성을 추출해 낼 수도 있겠지만 그렇지 않을 경우 은닉된 데이터를 추출하는 것은 거의 불가능하다고 알려져 있다.

3.2.4. 로그 및 이벤트 기록 삭제

사실의 증거나 범죄 자체의 은폐를 위해 로그 및 Event 기록을 삭제할 수 있다. 일반적인 win32 시스템에서는 지정 경로에 로그파일이 저장되게 되며 UNIX 시스템에서의 로그는 대부분 /var/log 경로 등에 저장된다. 컴퓨터의 로그를 주기적으로 원격지의 서버에 전송하도록 하는 시스템이 구축되어 있지 않거나 삭제된 로그 파일을 복구해내지 않고는 일반적으로 로그가 모두 삭제된 경우 해당 로그에 대한 기록을 찾는 것은 거의 불가능하다.

[표 3] 각 서비스 별 일반적인 로그 파일 저장 경로 및 이름
[Table 3] General log file save path and name of each service

서비스명	파일명	경로명
WWW	·access_log ·error_log ·referer_log	·/usr/local/apache/logs/
Database (MySql)	·localhost.err	·/usr/local/mysql/var/
email	·maillog	·/var/log/

4. 결론

본 논문은 디지털 포렌식의 현황 조사를 통해 앞으로 나아가야 할 방향에 대해 알아보고, 이에 대한 대응 방안에 대해 살펴보았다. 디지털 포렌식 분야의 성장과 활용 범위의 증가는 새로운 분야에 대한 활발한 연구를 필요로 하고 있다. 향후의 디지털 포렌식 수사는 기존의 용의자의 컴퓨터 시스템에 포렌식 수집/분석을 해야 되는 시점에서 벗어나, 다양한 임베디드 시스템을 모두 수사 대상으로 인식해야 될 시점에 이르렀다. 또한 각각의 임베디드 시스템은 그 장치마다 개별적인 분석 방안이 필요하고 체계적인 수집 및 분석 기법이 필요하다. 설령 같은 종류의 임베디드 시스

템이라도 제조사 별로 특성이 다를 수 있으므로 보급이 많이 된 제조사 별로 포렌식 분석을 수행하여 수사 가이드라인 및 분석 도구 개발이 필요하다. 안티 포렌식 기법 또한 다양해지고 사용자가 사용하기 편리한 증거 자동 삭제 프로그램 등이 늘어나고 있다. 각각의 안티 포렌식 기법에 대한 체계적이고 심도 있는 분석 방안과 안티-안티 포렌식 연구의 활성화가 필요하다.

감사의 글

본 연구는 지식경제부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음. [2007-S019-02, 정보투명성 보장형 디지털 포렌식 시스템 개발]

참고문헌

[1] 경찰청 사이버테러대 센터, 국내 사이버 범죄 현황, URL: http://www.netan.go.kr/

[2] World wide Legal Discovery and Litigation Support Infrastructure 2006-2010 Forecast, IDC, 2006 URL: http://www.idckorea.com

[3] 임경수, 이석희, 이상진, 임종인 “지식관리시스템을 활용한 포렌식 수사 정보교환 시스템의 필요성에 대한 연구”, *정보보호학회 동계학술대회*, 상명대학교, P35~38, 07년12월

[4] 이석희, 박보라, 이상진, 홍석희 “안티포렌식 기술과 대응방향”, *정보보호학회지*, 18권, 1호, 11~19, 08년 2월

[5] EnCase Enterprise edition 4.2 http://www.guidancesoftware.com

[6] Kyung-Soo Lim, Seokhee Lee, Jong Hyuk Park and Sangjin Lee , “XFRAME: An XML-Based Framework for Efficiently Acquiring Digital Evidence from Live Windows Systems”, *Fourth Annual IFIP WG 11.9 International Conference on Digital Forensics*, Kyoto, January 2008

[7] Mark Hartong, Rajni Goel and Duminda Wijesekera, “Cryptographic Protection and Recovery of Railroad Event Recorder Data”, *Fourth Annual IFIP WG 11.9 International Conference on Digital Forensics*, Kyoto, January 2008

[8] Jeremy Daily, Nathan Singleton and Gavin Manes, "Automobile Event Data Recorder Forensics", *Fourth Annual IFIP WG 11.9 International Conference on Digital Forensics*, Kyoto, January 2008

[9] Paul K. Burke, Philip Craiger, “Forensic Analysis of XBOX Console”, *Journal of Digital Forensic Practice*, 2006. 12. 01.

[10] Evidence Elimibator, http://www.evidence-eliminator.com

저자 소개

임경수 (Kyung-Soo Lim)

2006년 2월 : 부경대학교 컴퓨터멀티미디어전공 학사 졸업
2006년 3월~2008년 2월 : 고려대학교 정보경영공학전문대학원 석사 졸업
2008년 3월~현재 : 고려대학교 정보경영공학전문대학원 박사과정
관심분야 : 디지털 증거 수집 및 관리, Live Forensics, XML

박종혁 (Jong Hyuk Park)

2001년 2월 : 순천향대학교 컴퓨터공학부 학사 졸업
2003년 2월 : 고려대학교 정보보호대학원 석사 졸업
2007년 2월 : 고려대학교 정보보호대학원 박사 졸업
2002년 12월~2007년 7월 : (주)한화에스앤씨 기술연구소. 선임연구원
2007년 9월~현재 : 경남대학교 컴퓨터학과 교수
관심분야 : 디지털 포렌식, 유비쿼터스 보안, DRM, 상황인식, 홈네트워크 응용 및 서비스,

이상진 (Sangin Lee)

1989년 2월~1999년 2월 : 한국전자통신연구원 선임 연구원,
1999년 2월~2001년 8월 : 고려대학교 자연과학대학 조교수,
2001년 9월~현재 : 고려대학교 정보경영공학전문대학원 교수
관심분야 : 대칭키 암호, 정보은닉이론, 디지털 포렌식