제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

디지털 포렌식 기술 연구 동향 및 고찰

박광현, 박지수, 박종혁
서울과학기술대학교 컴퓨터공학과
{tap100, jisoo08, jhpark1}@seoultech.ac.kr

A Survey on Research and Trends of Digital Forensics Technology

Kwang-Hyun Park, Jong Hyuk Park
Dept of Computer-Science, SeoulTech University

요 약

정보화 시대가 빠르게 진행됨에 따라, 우리는 디지털 기기들을 항상 휴대하고 생활한다. 하지만 디지털 장치의 보급은 사이버 범죄의 수단으로 악용되고 있다. 이런 문제를 해결하기 위해 디지털 포렌식에 대한 다양한 연구가 활발히 진행 중이다. 본 논문에서는 디지털 포렌식 기술 연구 동향에 대해 살펴본 후 최근 문제점 및 이유 사항에 대해 논의 한다.

1. 서론

디지털 포렌식이란 사건 수사의 연장선으로 범죄와 관련된 디지털 증거로부터 옳바른 증거수집 절차를 통해 사건정보를 습득하는 일련의 관련기술을 의미한다. 디지털 포렌식은 디지털 정보기기 안의 내부 디지털 자료를 바탕으로 사건과 관련된 문제행위의 사실 관계를 입증하거나 증명하기위해 과학적 방법을 이용하는 일종의 보안 서비스라 할 수 있다 [1, 2].

스마트폰 1500만 시대를 맞이하여 이 같은 모바일기기에 대한 포렌식 연구도 활발히 진행중이다. 모바일 포렌식 연구는 디지털 포렌식을 모바일 장치에 맞게 바꿔 적용한 것으로 빠르게 진화하고 있을 뿐더러 그 종류가 다양하여 포렌식의 별도 분야로 세분화 하지 않고 디지털 포렌식 연구의 한 부분으로 여긴다 [3].

본 논문에서는 최근 연구되어지고 있는 디지털 포렌식 기술 동향에 대해 살펴본 후 중요 이슈 사항들에 대해 토론 및 고찰한다.

2.관련연구

2.1 디지털 포렌식의 변화

1991년 IACIS에서 디지털 포렌식이란 용어가 처음 사용된 이후로 컴퓨터를 이용한 범죄 수사를 위한 용어로 사용되었다. 최근에는 각종 디지털 기기와 네트워크 전산망 등을 목표로 하는 범죄를 조사, 예방 하는 의미로 확대되었다. 국내에서도 2004년 경찰청에서 디지털증거분석센터를 창설하여 디지털 포렌식 업무를 시작하고 있고, 검찰청도 2008년에 디지털 포렌식 센터를 창설 하였다. 2010년 경찰청에서 발표한 사이버범죄 통계에 따르면 그해 총 108,809건의 사이버 범죄 중 IT기술을 이용한 범죄는 해킹 및 바이러스(17,874), 인터넷사기(35,104)로 약 50%를 차지한다. 이에 따라 효율적인 범죄 사실 확인을 위한 디지털 포렌식 분야의 중요성이 점차 확대되고 관련된 기술이 지속적으로 개발되고 있다 [4, 5].

2.2 디지털 증거의 특징

디지털 데이터는 손쉽게 위, 변조가 가능하다. 눈에 보이지 않는 디지털 데이터의 특징 때문에 디지털 증거가 효력을 가지기 위해선 진정성, 무결성, 신뢰성, 원본성을 충족해야 한다. 사용하려는 증거가 해당 사건에 대한 증거임을 증명하는 진정성, 증거가 원본으로부터 수집되어 보관, 분석하는 과정에서 수정, 변경이 일어나지 않도록 방지하고 이를 지켰음을 증명하는 과정 무결성, 증거 분서 과정에서 증거가 위, 변조 되거나 의도하지 않은 오류를 포함하지 않았음을 증명하는 신뢰성, 법원에 제출되는 가공된 자료가 원본과 같은 증거임을 증명하는 것을 원본성이라 한다 [6, 7].

2.3 디지털 포렌식 대상 저장매체

디지털 포렌식의 대상이 되는 저장 매체에는 하드디스크와 CD, USB, 외장하드디스크, SD카드 와 같은 이동식 디스크와 서버 DB, 네트워크 장비, 디지털 카메라, PDA 등이 있다. 최근 저장 매체의 대용량화 진행됨에 따라 포렌식 수사 과정에 많은 시간이 소요되는 어려움이 있다. 하드디스크를 예로 320GB를 이미징 하는데 약 6시간이 소요, 최근 주로 보급되는 1TB를 이미징 하는데는 약 19시간이 소요 되는 것으로 알려져 있다 [8].

2.4 디지털 포렌식 툴

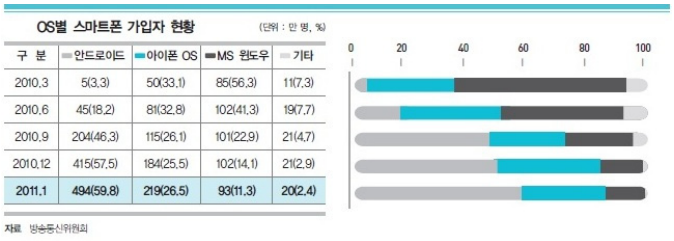
디지털 포렌식 툴 중에 GuidanceSoftware의 Encase와 AccessData의 FTK가 가장 많이 사용되고 있다. Encase의 주요기능은 무결성 보장, 자동화 작업, 삭제 파일 및 폴더의 복구에 특화 되어있고, FTK는 완벽한 한글 지원가능, 대용량 처리 지원, 메모리 덤프 분석기능에 특화 되어있다. 공통적인 특징으로는 유료 프로그램이며, Windows 운영체제를 지원하고, 디스크이미징을 지원한다. 이 디지털 포렌식툴이 주로 사용되는 이유는 국내 포렌식 증거를 이용한 수사, 판결에 이용되어 채택된 판례가 많기 때문이다. 이런 이유로 다른 유용한 포렌식 툴을 이용하여 증거로서의 자격이 있는지 확인 후 주요 툴들로 다시 재증명 하여 증거화 시키는 방법을 선택하기도 한다 [2].

3.최신 디지털 포렌식 연구

3.1스마트폰의 발전과 모바일 포렌식

최근 디지털 포렌식의 한 분야인 모바일 포렌식 시장이 스마트폰 1500만 시대에 맞춰 급성장함에 따라 주목 받고 모바일 포렌식 분야가 성장하고 있다. 이전에 모바일기기에 비해 최근의 스마트폰유형의 모바일 기기들은 매우 다양한 개인정보들을 가지고 있다. 스마트폰을 이용한 인터넷뱅킹, 결제서비스, GPS수신 기능을 이용한 위치정보, 인터넷을 통한 웹서핑의 흔적 등 포렌식의 범위에서 사용가능한 많은 정보들을 담고 있다

하지만 아직 체계적인 절차나 수집방법이 부족한 이유는 (그림 1)에서처럼 여러 종류의 운영체제를 기반으로 한 스마트폰이 나오고 있고 각 운영체제별로도 기기마다 약간의 차이가 존재한다 [3].


OS별 스마트폰 가입자 현황 (단위 : 만 명, %)

구 분	안드로이드	아이폰 OS	MS 윈도우	기타
2010.3	5(3.3)	50(33.1)	85(56.3)	11(7.3)
2010.6	45(18.2)	81(32.8)	102(41.3)	19(7.7)
2010.9	204(46.3)	115(26.1)	101(22.9)	21(4.7)
2010.12	415(57.5)	184(25.5)	102(14.1)	21(2.9)
2011.1	494(59.8)	219(26.5)	93(11.3)	20(2.4)

자료 방송통신위원회

(그림 1) OS별 스마트폰 가입자 현황 [3]

2010년 12월 방송통신위원회에서 '모바일 시큐리티 종합계획'을 수립하여 2015년까지 사업을 진행 중에 있다. 정부 자원에서도 모바일분야에 대한 사업을 확장하고 있고 대다수의 사람들이 모바일 기기를 기본적으로 휴대하는 시대임을 감안하면, 이런 흐름에 맞춰 모바일 포렌식 관련 분야 기술도 속속 개발될 것으로 보인다 [9].

3.2 디지털 포렌식 기술의 위기

디지털 포렌식은 현대 기술이 발전함에 따라 다음과 같은 위기를 맞고 있다.

- 분석 대상 장치의 증가 : PC, 노트북, 휴대폰, PMP ,디지털카메라 등의 다양한 전자제품 수 증가
- 저장 장치의 용량 증가 : 하드디스크의 고용량화로 증거 분석시간의 증가
- 웹 기술의 발전 : 클라우드컴퓨팅 같은 기술들은 시스템에 데이터를 저장하지 않아 증거분석에 악영향.
- 안티 포렌식 기술 증가 : 인터넷을 통해 배포된 안티 포렌식 기술로 인해 증거 수집에 악영향.

이러한 디지털 포렌식 기술의 위기상황에서 이를 극복하기 위한 변화되는 상황에 적절한 디지털 포렌식의 절차 및 방법 등에 관한 연구가 다루어져야 한다.

4.결론

본 논문은 디지털 포렌식 기술 동향에 대해 조사하였고, 이를 바탕으로 디지털 포렌식 흐름의 변화와 특징에 대해 연구하였다. 디지털 포렌식 분야가 점차 성장함에 따라 활용 범위에 대한 많은 연구가 필요하다.

모바일 포렌식 시장은 스마트폰의 지속적인 성장세에 힘입어 발전 가능성이 매우 높다. 디지털 포렌식 기술을 모바일 기기에 응용하여 성장시키기 위해선 국가적 차원에서의 모바일 포렌식을 통한 증거 채택 방안을 체계화하고 국내 모바일 단말기들의 특성에 맞춘 포렌식 툴의 개발이 선행될 필요가 있다. 스마트폰 처럼 새롭게 등장하는 디지털 장비들의 특성에 맞춘 포렌식 기술들에 대한 연구가 선행된다면 디지털 포렌식 기술의 위기를 극복 할 것으로 사료된다.

감사의 글

본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2011-C1090-1131-0004)

참고문헌

[1] 경찰청 사이버테러센터, "국내 사이버 범죄 현황", http://www.netan.go.kr

[2] 정익래, 홍도원, 정교일 ,"디지털 포렌식 기술 및 동향, 정보통신동향분석" 제24권 제 1호, 2009

[3] 한국인터넷진흥원, "2011 국가정보보호백서", 2011

[4] 임종인, "유비쿼터스 시대의 컴퓨터 포렌식의 중요성과 향후전망", 수사연구사, 2005

[5] 김진국, "디지털 포렌식 개요 및 절차" http://forensic-proof.com

[6] 길연희, 은성경, 홍도원, "디지털 증거의 신뢰성 확보 방안", 디지털 포렌식 연구 제1권 제1호, 2007

[7] 이상진, "디지털 포렌식 개론", 이룬출판사, 2010

[8] 임경수, 박종혁, 이상진 ,"디지털 포렌식 현황과 대응 방안", 보안공학연구논문지, 제 5권 제 6호, 2008

[9] 방송통신위원회, "Smart Korea 强國 도약을 위한 스마트 모바일 시큐리티 종합계획", 2010