디지털 포렌식 관점에서의 오픈소스 도구 적용 방안 연구

윤수진* · 김종배** · 신용태**

*숭실대학교 SW특성화대학원 · **숭실대학교 IT정책경영학과 · ***숭실대학교 컴퓨터학부

A Study of Applicable Strategies on the Open Source Tool in Digital Forensics

Su-jin Yoon* · Jong-bae Kim** · Yong-tae Shin***

Soongsil University

E-mail : ysjin0506@ssu.ac.kr, kjb123@ssu.ac.kr, shin@comp.ssu.ac.kr

요 약

범죄 수사에서 디지털 증거물이 증가됨에 따라, 법적으로 효용성이 큰 데이터를 추출할 수 있는 디지털 포렌식 도구에 대한 중요성이 높아지고 있다. 디지털 제품들은 빠르게 성장하고 있고, 포렌식 도구는 사용자와 사건에 맞도록 용이하게 구현 되어야 한다. 포렌식 업계나 정부에서는 소요 비용이 큰 포렌식 도구를 사용하고 있지만 메모리 한계, 사후 감사의 한계 등 한계성이 제시되고 있다. 이러한 문제를 해결하기 위하여 다양한 포렌식 도구가 빠르게 구현 할 수 있도록 오픈소스 포렌식 도구 개발이 필요하다. 본 논문에서는 현재 상용화 되고 있는 디지털 포렌식 기술들에 관해 연구하고, 이들의 한계성을 극복하기 위한 오픈 디지털 포렌식 기법들을 제시하고, 적용 방안에 대해 제안한다.

ABSTRACT

As E-discovery in criminal investigation is increasing, the importance of Forensic Tools which can legally extract data with high effectiveness is getting higher. Digital products are growing fast. Therefore, Forensic Tools should be implemented readily to suit users and events well. Although forensic industry and governments use expensive forensic tools, some have suggested limitations to its use, such as memory limitations and the limits of post-audit. We need to develop open source forensic tools that can implement a variety of forensic tool fast. This research studies digital forensics technical skills which are commercialized currently and suggests applicable strategies of the open digital forensics to help overcome these limitations.

키워드

EnCase, 오픈소스, 컴퓨터 포렌식, 디스크 이미지, Advanced Forensic Format(AFF)

Ⅰ. 서 론

디지털 포렌식은 디지털 증거 자료의 수집, 보존, 분석, 문서화, 그리고 재판 과정에서 증거로 제출하기까지의 모든 과정을 포함하는데, 지금까지는 컴퓨터의 하드디스크에 있는 개인 데이터를 확보하는 것이 주류였으나 디지털 기술의 발달로 그 증거자료가 네트워크, 인터넷, 데이터베이스, 모바일, 휘발성 메모리 등 다양한 곳에서 존재함으로써 그 전문성이 더욱 심화되고 있다[1]. 전 세계적 으로 디지털 포렌식 서비스에 대한 수요는 증가 하지만, 그 속도를 유지하는 측면에서는 실패에 직면하고 있다. 현재 상용화 포렌식 도구들은 수요를 맞춰가기 위해 빠르게 구현되었으며, 사후 감사 한계 등의 문제점이 제시되고 있다. 기업이나 정부 등에서 사용하는 상용화 포렌식 도구는 고가이기 때문에 교육적인 측면에서 본다면 부담이 크다. 본 논문에서는 상용화 디지털 포렌식 기술 중 EnCase 기술 과 오픈소스 디지털 포렌식 기술 중 AFF 기술에 대해 알아보고, 상용화 디지털 포렌식 기술 문제점에 대한 적용 방안을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 상용화 포렌식 도구와 오픈소스 도구에 대해 논한다. 3장에서는 오픈소스 파일타입을 연구하고 적용 방안에 대해 제안한다. 마지막으로 4장에서는 본 논문의 결론과 향후 연구를 논한다.

Ⅱ. 관련 연구

디지털 포렌식 도구 중 Computer forensics, Memory forensics, Mobile device forensics, Network Forensics 등이 있으며, 상용화 포렌식 도구는 EnCase., FTK 기술 등이 있으며, 오픈소스 포렌식 도구는 AFF, SMART, PyFlag 등이 있다. 본 장에서는 상용화 포렌식 도구 중 EnCase로 하고, 오픈소스 포렌식 도구에서는 AFF에 대해 연구한다.

2.1 상용화 디지털 포렌식 기술 EnCase

Guidence Software에서 만든 디지털 포렌식 수사 기술의 표준 이며, 세계 점유율 1위이다. 디지털 포렌식 도구를 사용하는 기업이나, 정부에서 효과적인 디지털 조사를 할 수 있는 도구 이다. eDiscovery 요청 등을 대규모 데이터를 신속하게 수집하며, 결정적으로 외부 공격을 방어를 해준다[2].

2.2 오픈소스 디지털 포렌식 기술 AFF

AFF는 특허 및 기업 기술에 제약 없이 개방적이고 확장 가능한 도구이다. 비슷한 프로그램이나 다른 오픈소스들에게 해당코드를 허용하여 자유롭게 통합 할 수 있다. 순방향 및 역방향 호환성을 유지하는 방식으로 추가하여 새로운 기능을 확장할 수 있다. 새로운 기능의 확장은 부족한 AFF기능을 발전시킬 수 있다[3].

Ⅲ. Advanced Forensic Format

AFF는 유연한 단일 포맷으로 다양한 작업에 사용될 수 있다. 본 장에서는 AFF 도구 버전 중 AFFLIBv3의 파일 타입에 대해 설명하고 AFFLIBv3 도구를 이용하여 증거를 추출한 후 상용화 디지털 포렌식 문제점에 대한 적용 방안에 대해 제안한다.

3.1 AFFLIBv3 파일 타입

AFFLIBv3는 3개의 파일 타입(AFF, AFD, AFM)을 지원 하며 쉽게 변환이 가능하도록 제공한다. 기존의 AFF도구는 100GB이상의 디스크 데이터를 저장 못했지만, AFFLIBv3는 AFF의 파일을 AFD파일로 분할하는 방식으로 용량이 큰 디스크 데이터를 저장한다. AFFLIBv3의 파일 타입은 표 1과 같다.

표1 AFFLIBv3 파일 타입

AFF	232 characters보다 큰 파일을 지원하지 않는 파일 시스템과 함께 사용할 수 있도록, 다수의 파일에서 단일 디스크 이미지를 저장하는 기능을 지원한다.
AFD	AFB 타입을 가진 하나의 디렉토리에 저장되어 여러 파일에 하나의 AFF파일을 분할 한다. AFF 라이브러리 디렉토리에 있는 파일을 관리하고 하나의 파일인 것처럼 호출 할 수 있다.
AFM	AFF파일에 인접하게 저장된 메타 데이터와 함께 하나이상의 원시 파일에 디스크 이미지를 저장한다. AFF타입만 raw images화 함께 장독 할 수 있도록 호환성을 유지하면서 메타 데이터를 저장한다.

3.2 상용화 포렌식 문제점 개선에 대한 적용 방안

상용화 포렌식 도구들은 충분한 검증과 테스트를 거쳐 신뢰성 있는 법적 가이드라인에 맞추어 구축 한다는 장점이 있다. 하지만 데이터 스토리 및 I/O 대역폭의 한계 와 용이하지 못하고 협업이 어렵고 개방적이지 않아 용이하지 않고 디지털 포렌식 교육이 고가라는 단점을 갖고 있다. 이러한 문제점을 개선하기 위한 방법으로 오픈소스 디지털 포렌식 기술들에 대한 교육을 하고 디지털 포렌식 기술 범위 내에서의 법적 가이드라인을 지원한다.

Ⅳ. 결론 및 향후 연구

본 논문에서는 상용화 디지털 포렌식 도구 EnCase와 오픈소스 디지털 포렌식 도구 AFF에 대해 연구 하였고, AFF버전 중 AFFLIBv3에 대한 파일 타입과 적용 방안에 대해 제안하였다. 디지털 제품들의 발달은 디지털 포렌식의 또 다른 도전이 될 수 있기 때문에 상호 협업과 정확한 증거추출이 가능한 디지털 포렌식 도구들이 필요하다. 위 연구를 발전시켜 AFF 도구들을 이용하여 법적 가이드라인에 맞추어 구현이 가능한지 확인하고, 적용방안 과 개선방안에 대해 향후 연구를 계획하여 보강 작업을 진행 한다.

참고문헌

[1] 이종찬, 박상준 “포렌식에서 디지털 증거의 우선순위 스케쥴링“, 한국정보통신학회논문지, 제17권, 제9호, p2055-2062, 2013

[2] Dan Manson, Anna Carlin, Steve Ramos, Alain Gyger, Matthew Kaufman, Jeremy Treichelt, “Is the Open Way a Better Way? Digital Forensics using Open Source Tools“, Journal of Hawaii International Conference on System Sciences, p3-9. 2007

[3] Simson Garfinkel, David Malan, Karl-Alexander Dubec, Christopher Stevens, Cecile Pham, “Advanced Forensic Format: an Open Extensible Format for Disk Imaging“, IFIP international Conference on Digital Forensics, 제222권, p13-27, 2006