Script에서 Forensic 증거자료 확보 방안

김슬기* · 박대우**

*호서대학교 벤처대학원

Generation of Forensic Evidence Data from Script

Seul-gi Kim* · Dea-woo Park**

*Hoseo Graduate School of Venture

E-mail : sgkim_18@naver.com, prof_pdw@naver.com

요 약

최근 발달된 디지털기기들은 사이버로 연결되어 사용되고 있다. 디지털기기 사용자들은 사이버에 연결된 단말기들을 활용하여 금융결제, 전자상거래 등 활동을 하고 있다. 사이버거래의 활성화와 함께 사용자에 대한 사이버범죄가 증가하고 있다. 사이버범죄의 수사에서 Forensic 증거자료를 확보하여야 한다. 하지만, 디지털 포렌식 증거자료를 분석하기에는 많은 정보가 함유되어 있다. 이러한 많은 디지털정보에서, 사이버범죄에 증거를 확보하기 위한 Script가 효율적인 방안이다. 본 논문 연구에서는 Script를 활용하여, Forensic 증거자료를 확보하는 방안을 연구한다. EnCase를 통한 증거자료 추출과 Script를 활용한 증거자료 확보 방안을 연구한다. 본 연구는 안전한 국민생활을 위한 사이버 보안의 기초자료로 활용될 것이다.

ABSTRACT

Recently developed digital devices are being used in cyberspace. Digital device users are engaged in activities such as financial settlement and e-commerce using cyber-connected terminals. With the activation of cyber trading, cyber crimes against users are increasing. Forensic evidence should be obtained from investigations of cybercrime. However, there is a lot of information to analyze digital forensic evidence. In many of these digital information, Scripts are an effective way to secure evidence for cybercrime. In this paper, we study how to secure forensic evidence using scripts. Extract evidence from EnCase and study how to obtain evidence using scripts. This study will be used as the basic data for cyber security for the safe life of the people.

키워드

Forensic, Script, 증거자료, 사이버범죄

Ⅰ. 서 론

정보통신기술이 발달하면서 사이버 공간상에서 범죄가 다양해졌다. 불법 사이트, 불법복제, 악성 프로그램, 해킹 등 다양한 사이버범죄가 존재하면서, 디지털기기들이 사이버로 연결되고 사용이 보편화하면서, 디지털기기를 통한 사이버범죄가 증가했다.

경찰청의 디지털증거분석 현황에 따르면 2009년 11,200건에 불과했던 분석 건수는 2016년 31,144건으로 약 3배정도 늘어났다[1]. 디지털기기에 대한 범죄증거 분석이 매년 증가하는 이유는 사이버에 연결된 단말기들을 활용하여 금융결제, 전자상거래 등 다양한 금융활동을 통하기 때문에 해킹과 같은 온라인 사이버범죄가 늘어나고 있기 때문이다.

사이버범죄에 사용된 디지털기기를 분석을 통하여 수사를 진행하게 되는데, 이때 분석에 사용

되는 Tool은 Guidance Software 사에서 개발한 EnCase를 사용하여 Digital Forensic 분석을 진행한다.

분석 시 EnCase를 통한 증거자료 추출과 Script를 활용한 증거자료 추출이 있는데, EnCase 사용 시 클릭 한 번으로 여러 기능을 수행, 여러 작업을 동시에 가능하도록, EnCase 기능을 좀 더 효율적으로 사용하고 싶을 때 Script를 활용하여 증거를 추출하여 원본성과 무결성을 검증하고 수사에 활용될 수 있도록 한다. 따라서 본 연구에서는 EnCase와 Script를 두 가지 방식으로 활용하여 증거자료를 확보하도록 연구한다.

II. 관련 연구

2.1 디지털 포렌식

디지털 포렌식은 증거 수집, 증거의 포장 및 이송, 조사 분석, 보고서 작성 단계로 이루어진다. 표 1은 디지털 포렌식 수행 과정[2]이다.

항목	내용
증거수집	-수집 대상 파악 -압수 대상 선정 -증거 목록 작성 -물리적 증거 수집 -관련자 면담 -문서화
증거의 포장 및 이송	-압수물 개별 포장 -전자파 및 충격 방지 포장 -증거물 포장 및 운반
조사 분석	-데이터 이미징 -데이터 추출 및 분류 -데이터 조사 및 증거 검색 -정밀 검색
보고서 작성	-용서 설명 -객관적 설명 -결과 정리

표 1. 디지털 포렌식 수행 과정

2.2 각 기관에서 사용하는 분석도구

법률회사의 경우 수사기관과 반대되는 입장에서 디지털 포렌식을 이용하는 경우가 대부분이기 때문에 일반적으로 수사기관이 사용하는 포렌식 장비와 유사한 것들을 사용한다.

수사기관의 경우 증거 분석 도구 사용 범위에는 제한이 없다. 일반적으로 사용되는 EnCase나 FTK 뿐만 아니라 오픈 소스 혹은 자체 개발 프로그램 등 다양하게 사용한다. 모바일 포렌식에는 경찰에서 자체 개발한 <네모 스마트>라는 프로그램을 주로 이용한다.

기업의 경우에는 기본적으로 자주 사용되고 있는 EnCase 및 FTK를 활용하고 이와 함께 포터블 형태로 휴대가 간편하고 Timeline을 통해 직관적인 분석이 가능한 DFAS라는 도구를 사용한다. Enterpritse DFAS라는 원격 디지털 포렌식이 가능하도록 검토중인데, 이러한 이유는 국내뿐만이 아닌 해외에서도 디지털 포렌식을 통한 업무를 진행함에 따라 보안사고에 대한 회사의 피해를 최소화하기 위함이다[3-보안뉴스 참고 주소].

2.3 EnScript

EnScript는 EnCase에서 여러 작업을 자동화하고, 기능을 충분히 활용하기 위해 설계된 언어이자 API(Applacation Programming Interface)를 뜻한다. EnCase 환경의 전용 프로그래밍 언어이기 때문에 EnScript를 실행하려면 EnCase가 실행되고 있어야 한다. ANSI C++과 JAVA 표준을 따르기 때문에 프로그래밍 언어를 다룰 줄 아는 사람이라면 쉽게 접할 수 있다.

EnScript는 디지털 포렌식 분석 과정에서 데이터 처리 능력을 향상시키고 여러 작업을 자동화하여 새로운 기능을 만드는 중요한 역할을 한다.

EnCase에서는 파일시스템 뷰, 키워드 검색, 파일 추출과 같은 기본 기능 외 사용자가 상황에 맞게 기능을 프로그래밍할 수 있도록 스크립트 언어를 제공하고 있다. 이 언어를 EnScript라하며, EnScript를 사용하면 EnCase의 다양한 기능을 자동화할 수 있으며, 복잡하고 반복적인 동작도 사용자의 편의에 따라 쉽게 처리할 수 있다. 한 마디로 EnCase를 효율적으로 활용할 수 있게 해주는 언어이다[4].

III. 디지털기기에서 포렌식 증거 추출

3.1 포렌식 증거추출 환경

본 논문에서는 다양한 Digital Forensic Tool중에서 EnCase를 사용하여 증거 추출 및 분석을 진행한다.

항목	내용
Name	EnCase
Version	7.10.03.11
Platform	x86
Company	Guidance Software

표 2. EnCase 주요 사양

IV. 디지털기기에서 증거 추출 포렌식

4.1 EnCase 분석

본 논문에서는 다양한 Digital Forensic Tool중에서 EnCase를 사용하여 증거 추출 및 분석을 진

행한다.

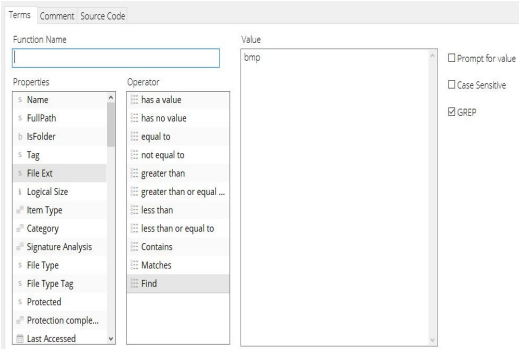

그림 1. EnCase 확장자 찾기 설정

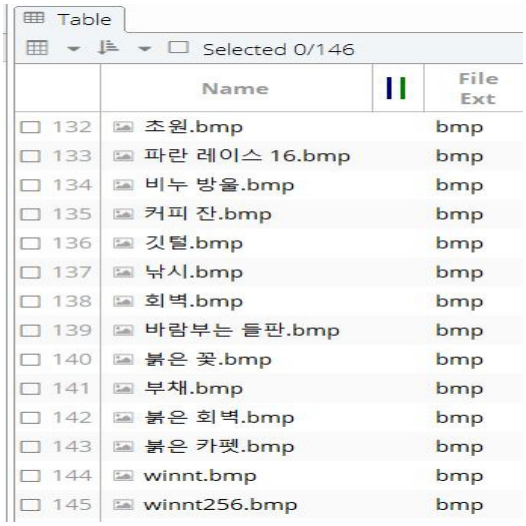

그림 2. EnCase 확장자 찾기 결과값

4.2 EnScript 분석

본 논문에서는 다양한 Digital Forensic Tool중에서 Enscript를 사용하여 증거 추출 및 분석을 진행한다.

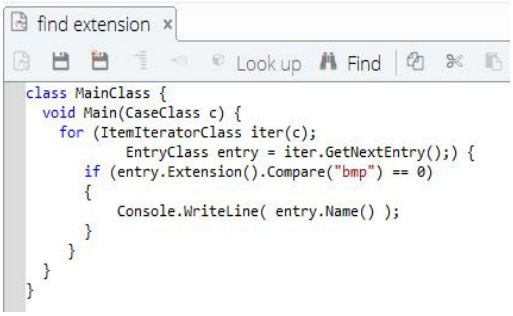

그림 3. EnScript 확장자 찾기

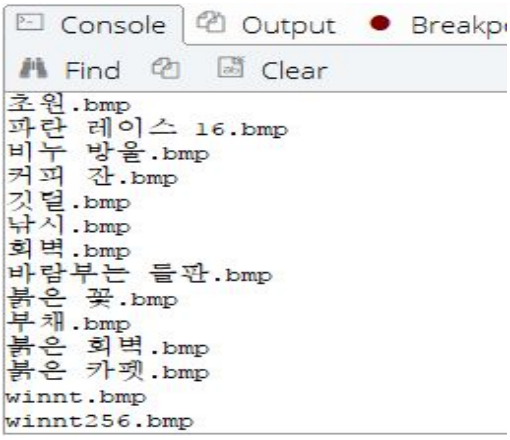

그림 4. EnScript 확장자 코딩 결과

Ⅴ. 결 론

본 논문은 디지털기기에 대한 디지털 포렌식 증거자료 확보 방안에 대해 제안하였다.

디지털기기의 Imaging 작업을 통해 EnCase 자체로 분석해보았으며, EnScript를 이용하여 분석하여 총 2가지 방식으로 분석을 진행하였다.

EnCase를 활용하여 분석하였을 때 다양한 기능을 비교적 편리하고 안정적으로 제공하여 분석 시간을 단축시켜주었다.

반면 EnScript를 이용하여 분석하였을 때 여러 분석 작업을 자동화하여, 빠르고 정확하게 결과값을 나타내주었다.

참고문헌

[1] The Segye Times, “When gathering digital evidence, strengthen the information human rights issue.”, [Internet]. Available: http://www.segye.com/newsView/20170831003650

[2] J. W. Shin, “A Study on Digital Forensic Human Training Method”, *Journal of the Korea Institute of Information and Communication Engineering*, vol. 18, no. 4, pp779~789, Apr. 2014.

[3] boannews, “Three perspectives on digital forensics”, [Internet]. Available: http://www.boannews.com/media/view.asp?idx=42452

[4] “EnScript programming for digital forensics analysis”, bjpublic, Jun. 2017.