논문 2010-1-4

SW 포렌식과 SW감정에 대한 고찰

김 도 완*

A study of software forensics and software assessment

Do Wan Kim*

요 약

디지털 포렌식은 정보기기에 내장된 디지털 자료의 사실관계를 과학적으로 분석 규명함으로써 법적 증거능력을 보장할 수 있도록 하는 행위이다. 디지털 형태의 증거자료는 간단한 조작만으로도 생성, 복제, 변경, 삭제, 전송 뿐 만이 아니라, 원격지에서도 컨트롤하는 것이 가능하다. 따라서 이들 정보가 법적인 증거능력을 갖게 하기 위해서는 특별한 절차와 방법을 따라야 할 필요가 있다.

SW감정의 주요 대상은 주로 SW 소스코드이다. 이때 감정의 대상이 되는 SW 소스코드는 분쟁의 원인 물증으로써 확인 될 수 있어야 한다. 특히 소프트웨어는 개발단계 및 시험단계, 유지보수단계, 판매 단계에서 수많은 버전이 존재하게 되어, 제출된 증거물에 대한 진위여부가 법적논쟁이 될 소지가 크다. 소프트웨어 포렌식은 이러한 문제에 대처 할 수 있는 방법을 제공한다. 본 연구에서는 SW 포렌식에 대하여 개관하고, SW감정에서 디지털 포렌식의 활용 모델을 제시한다.

Abstract

The digital forensics is activities for assure of legal ability by scientific analysis the facts of digital information in electronic equipment. Evidence in digital form is to create, reproduce, modify, remove, transport with just a simple operation not only, it is possible to control from remote locations as well. Thus, specific procedures and methods are required to achieve legal ability when digital information is examined.

The main target of software assessment is the software source code. At this point, the SW source code as the assessment's object that can be causes of conflict must be confirmed by the legal evidence. Particularly, many versions can be existed in steps of software development, testing, maintenance and sales phase, thus the authenticity of the evidence haven't to be disputed. The software forensics can deal with these issues and offers ways. In this study, we like to introduce an overview about the SW forensics, and then to suggests a model of SW forensics model for SW assessment.

한글키워드 : SW 포렌식, 감정

1. SW 포렌식과 SW 감정의 상관관계 개요

디지털 포렌식의 대상으로는 IT단말기에서 작

* 배재대학교 정보통신공학과
(email: dwkim@pcu.ac.kr)
접수일자: 2010.4.3 수정완료: 2010.5.7

동되는 모든 SW 자체와, IT 단말기에 저장 보관되어 관리되는 모든 자료가 될 수 있다.[2] SW 포렌식은 SW 소스코드 유출에 따른 불법복제 및 개작, 바이러스 프로그램 제작 및 유포, SW 역공학(Reverse engineering) 기술을 이용한 SW 소스코드 생성, SW 저작권 관련 분쟁 등의 문제 해결을 위하여, 증거 능력을 확보하는 것이다.

SW 저작권 침해 분쟁의 경우 50%이상이 "SW 소스코드 불법복제 및 개작"과 관련하여 발생되고 있다[5]. SW 산업의 경우 이직률이 높으며, SW 소스코드는 무형의 특성을 가진 자산이기 때문에 저작권 침해 시 추적이 어려운 특성을 지니고 있다. 또한 판매되거나 공개된 인터페이스로부터 소스코드 생성 및 영업비밀의 유추를 할 수 있다는 취약점을 가지고 있다. 그러나 SW 소스코드 저작권은 개발인력의 인적 이동을 통한 침해, 기술 및 비즈니스 아이디어의 불법적 도용, SW 소스코드에 대한 불법 복제와 같은 다양한 침해 유형으로 확장 증가하고 있는 실정이다. 더불어, SW는 개발단계 및 시험단계, 유지보수단계, 판매 단계에서 수많은 버전이 존재하게 됨으로, 제출된 증거물에 대한 진위여부가 법적논쟁이 될 소지가 크다.

SW 감정에서 유사도 감정은, 원본 SW 소스코드와 복제 또는 개작되었다고 의심되는 SW소스코드를 비교 분석하여, 양 SW 소스코드 중 유사한 부분을 찾아내는 기술이다. 소스코드의 어휘 분석을 통해 토큰(단어)를 비교하는 방식과, 토큰을 특정 심볼 패턴으로 변화해 비교하는 패턴변환 방식이 주로 활용된다. SW소스코드 유사성 비교 도구로는 exEyes, Windiff, Beyond Compare, Compare It, ExamDiff, Xdiff, MOSS, JPlag, YAP등이 존재한다.

2. SW 포렌식 처리 절차와 SW 감정 절차

SW 포렌식 절차는 디지털 포렌식 처리 절차와 같다.

첫 번째는 준비 단계이다. 증거물 획득 및 분석을 위하여 소요되는 자원을 준비한다. 증거물 획득 단계에서는 본래의 현물을 손상 없이 증거물을 확보하고, 증거물 인증 단계에서 증거물이 본래의 현물에서 획득한 데이터와 동일함을 인증한다. 증거물 분석 단계에서는 증거물의 변형 없이 분석을 수행해야 한다. SW 포렌식의 핵심 절

[그림 1] 디지털 포렌식 처리 절차 [1]

차는 증거물 획득->증거물 인증->분석및 조사라고 할 수 있다. 구체적인 절차의 명세는 주어진 환경과 목적에 따라 달라질 수 있다.[1][7][8][10]

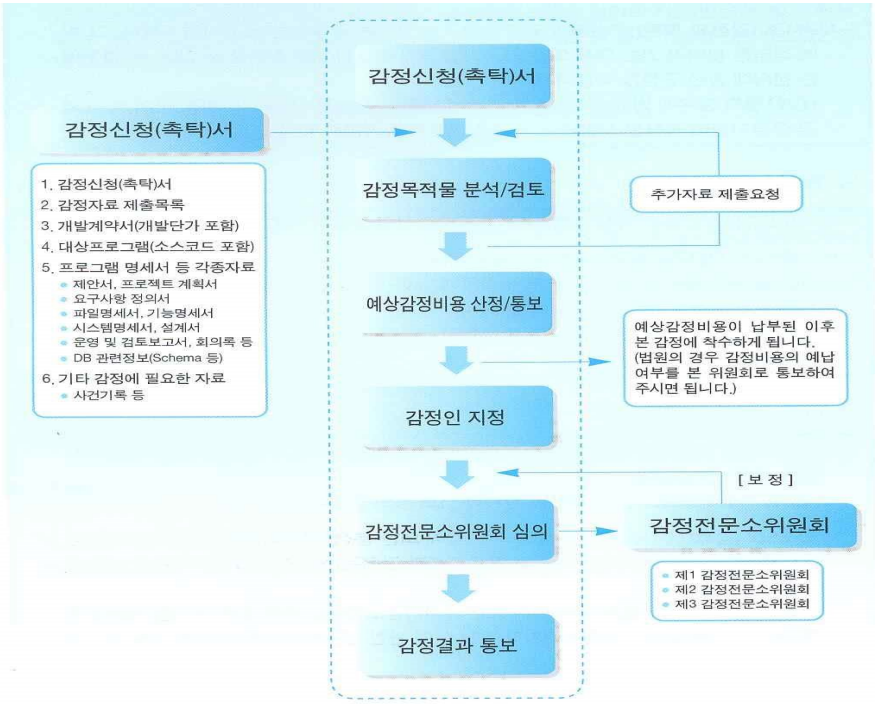
SW 감정은 SW 지적재산권 관련 분쟁이 발생하였을 때, 저작권 침해에 대한 증거 또는 전문가의 소견을 확보할 수 있는 제도로서, 아래 절차에 따라 SW 감정이 이루어진다. SW 감정의 종류 중 하나인 유사독 감정(복제도 감정)은 SW 포렌식의 증거 분석 단계에 해당한다고 할 수 있다.

3. 결론

SW 감정은 SW 포렌식의 핵심 프로세스 중 하나로서, 소프트웨어 관련 증거자료의 분석을 통한 SW지적재산권 침해의 증거를 확보하기 위한 활동이다.[9] 따라서 SW 감정결과에 대한 객관성, 공정성, 정확성 및 신뢰성을 확보하기 위하여 SW감정 절차를 디지털 포렌식 프로세스와 일원화 하여야 할 필요성이 있다.

SW감정 프로세스는 "SW감정신청"으로부터 시작되며, 감정 목적물의 분석/검토->감정대상 및 범위 설정->감정기준 및 방법설정->감정 목적에 따른 물리적/논리적 침해 여부 감정->감정항목 및 영역별 가중치 설정에 따른 침해비율 산출->보고서 작성의 절차를 따른다.

SW감정 프로세스는 독립된 사법기관의 범죄사실 인지로부터 시작되는 것이 아니라, 감정신청인의 감정신청촉탁서 제출로부터 시작된다. 이때 감정신청인과 피신청인은 감정을 위하여 요구



[그림 2] 감정 절차

되는 자료(SW소스코드, 개발계약서, 프로그램 명세서 및 각종자료 등)를 제출하는데 있어서, 강제성을 가지지 않는다. 따라서 감정 목적물의 무결성이 보장되지 않는다는 문제가 있다. 이와 달리, 디지털 포렌식 프로세스 중 증거물획득 단계는 디지털 포렌식 대상의 무결성을 보장하는 것을 전제로 하고 있다. 즉, 소프트웨어 포렌식에서 SW 감정 프로세스 중 감정목적물의 무결성을 보장할 수 있는 방법이 강구되어야 한다. 예를 들어, 강제적 감정목적물 확보(증거 수집)를 위한 법적 제도정비, SW 저작권 보호를 위하여 SW등록, SW임치 의무화와 같은 제도가 필요하다.

증거분석 단계와 관련하여, 현재 SIM, Yap, Windiff, Plague 및 exEyes와 같은 다양한 소프트웨어 감정 툴 들이 이용되고 있다. 이러한 감정 도구들이 가지고 있는 취약점은 신뢰성이라 할 수 있다. 따라서 공신력 있는 검증 기관의 인증을 거친 소프트웨어 감정 도구를 확보하려는 노력이 필요하다.

결과보고서 작성 단계에서도, 감정 결과에 대한 가중치를 어떻게 부여할 것인가는 중요한 문제이다. 소프트웨어 소스코드, 자료구조 및 알고리즘, 인터페이스 디자인, 부가적 자료 등 하나 하나가 중요한 factor라고 할 수 있으며, 소프트웨어 소스코드 자체에서도 핵심 소스코드와 일반적 소스코드 사이에 어떻게 가중치를 부여하여 결과보고서를 작성할 것인지는 문제가 되고 있다. 따라서, 이에 대한 표준화 작업은 추상적 레벨부터 시작하여, 사례 중심의 하위 레벨까지 이루어 져야 할 것이다.

소프트웨어 포렌식은 인간의 창작 작업에 의하여 만들어진 지능적 창작물을, 작게는 수만 라인에서부터 크게는 수천만 라인에 이르는 방대한 자료를 분석하여, 법적 증거를 확보하는 작업이다. 따라서 단순히 범주화 시킬 수 없는 특성을 가지고 있다. 그러나 소프트웨어 포렌식 결과에 대한 객관성-공정성-신뢰성을 확보하기 위하여 디지털 포렌식이 추구하는 표준화 대열에 적극적으로 참여하여야 할 것으로 보인다.

참 고 문 헌

[1] 홍도원; 디지털 포렌식 기술; 한국전자통신연구원; 2007
[2] 임경수, 박종혁, 이상진; 디지털포렌식 현황과 대응방안; 보안공학연구논문지, 2008. 11
[3] 류희수; 정보보호: 디지털 세상의 CSI, 그 가능성은?, 정보통신진흥협회, 2007
[4] 조용현; 디지털 포렌식을 위한 절차와 도구의 중요성; (주)시큐아이닷컴 CERT팀, 2007
[5] 김도완, 윤영선; SW소스코드 저작권보호를 위한 통합 가이드; 컴퓨터프로그램보호위원회, 2009. 4
[6] 길연희, 홍도원; 디지털 포렌식 기술과 표준화 동향; IT standard & test TTA journal, 2008, 8
[7] 정익래, 홍도원, 정교일; 디지털포렌식 기술 및 동향; 전자통신동향분석 제22권; 2007. 2
[8] 변정수; 한국형 디지털 증거분석 표준화: 경찰청 디지털 증거처리 표준가이드라인 및 증거분석 전문매뉴얼의 고찰; 디지털 포렌식 연구 창간호, 2007. 11
[9] 방효근, 신동명, 정태명; 소프트웨어 포렌식: 프로그램 소스코드 유사성 비교 및 분석을 중심으로; 디지털 포렌식 연구 창간호, 2007. 11
[10] 전상덕, 홍동숙, 한기준; 디지털 포렌식의 기술 동향과 전망; 정보화정책; 2006. 11

저 자 소 개

김 도 완

1990년 독일 Regensburg 대학교 전산정보공학 학사
1993년 독일 Regensburg 대학교 전산 정보공학 석사
1996년 독일Regensburg 대학교 전산 정보공학과 박사 (Ph. D.)
1996년 한국전자통신연구원 선임연구원
2004년 Southampton Uni. (영) 방문교수
1997~현재 배재대학교 정보통신공학과 교수

<주관심분야 : Semantic Web Service, Information Management, Knowledge -based System>