情報保護學會論文誌
第 21 卷 第 3 號, 2011. 6

디지털 포렌식을 위한 증거 분석 도구의 신뢰성 검증*

이 태 림,† 신 상 욱‡
부경대학교 대학원 정보보호학협동

Reliability Verification of Evidence Analysis Tools for Digital Forensics*

Tae-Rim Lee,† Sang Uk Shin‡
Interdisciplinary Program of Information Security, Pukyong National University

요 약

본 논문에서는 TTAK.KO-12.0112 문서에 따른 컴퓨터 포렌식을 위한 디지털 증거 분석도구의 일반적인 검증 절차를 살펴보고, 제시된 검증 항목들을 이용하여 실제 증거분석 도구를 대상으로 기능 요구사항들을 테스트한다. 또한 테스트 내용을 바탕으로 대상 도구들에 대한 성능 평가를 수행하며, 각 도구들의 증거 분석 기능에 대하여 향후 성능 개선 방향을 제시한다. 이는 테스트 대상 도구가 수행 가능한 기능들을 파악하고, 요구사항 문서에서 제안된 검증 절차들을 활용하여 각 기능 별로 구체적인 모의 테스트를 설계한 후, 검증 항목의 내용을 포함시킨 가상의 증거 이미지 파일들을 생성하여 도구가 분석한 결과를 검증하고 해석한다. 이 과정을 통해 대부분의 도구들에서 단편화된 삭제 파일에 대한 복구, 국내에서 널리 사용되고 있는 파일 포맷 인식, 한글 문자열 처리 기능 등에 취약점이 존재함을 확인할 수 있다.

ABSTRACT

In this paper, we examine the reliability verification procedure of evidence analysis tools for computer forensics and test the famous tools for their functional requirements using the verification items proposed by standard document, TTAK.KO-12.0112. Also, we carry out performance evaluation based on test results and suggest the way of performance improvement for evidence analysis tools. To achieve this, we first investigate functions that test subjects can perform, and then we set up a specific test plan and create evidence image files which contain the contents of a verification items. We finally verify and analyze the test results. In this process, we can discover some weaknesses of most of analysis tools, such as the restoration for deleted & fragmented files, the identification of the file format which is widely used in the country and the processing of the strings composed of Korean alphabet.

Keywords: Reliability verification, Evidence analysis tools, Digital forensics, Computer forensics

I. 서 론

오늘날 우리는 광범위한 네트워크 속에서 고도로 첨단화된 장비 및 관련 기술들을 이용하여 다양한 서비스를 제공받을 수 있게 됨으로써, 과거의 여가 활용 방식이나 비즈니스 방식에서 탈피하여 보다 윤택한 삶을 영위하기 위한 많은 혜택들을 누릴 수 있게 되었다

접수일(2010년 9월 25일), 수정일(2011년 2월 11일), 게재확정일(2011년 3월 16일)
* 본 연구는 2009학년도 부경대학교 연구년 교수 지원사업에 의하여 연구되었음(PS-2009-025).
† 주저자, taeri@pknu.ac.kr
‡ 교신저자, shinsu@pknu.ac.kr

[1]. 하지만 이에 반해, IT 장치 및 기술들이 새로운 범죄의 수단으로 악용됨에 따라 사이버 범죄라는 커다란 사회적 문제가 발생하게 되었다. 이는 전 세계적으로도 매년 급증하는 추세로 그 수법 또한 나날이 다양해지고 있으며, 개인용 컴퓨터는 물론 노트북, PDA, 스마트 폰 등은 이미 우리의 일상 속에서도 널리 사용되어 일반적인 범죄에서도 주요 증거 또는 단서가 컴퓨터를 포함한 각 종 디지털 장치들에 보관되어 있는 경우가 많아졌다[2]. 이에 법 집행 기관은 전통적인 수사 방식을 탈피하여, 전자 매체를 이용한 관련 범죄 수사의 새로운 법적 절차와 수사법을 필요로 하게 되었고, 이를 위한 해결책으로 제시할 수 있는 것이 디지털 포렌식이다. 포렌식이란 범죄수사 또는 증거를 수집하기 위해 과학적이거나 기술적인 기법을 사용하는 것을 의미하며, 이를 위한 도구는 법과 기술 간의 매개체가 될 수 있는 핵심 요소라 할 수 있다[3]. 이는 효율적인 관련 범죄 수사를 위해 디지털 포렌식 기술 및 도구 개발이 필수적임을 의미하지만, 현재 국내 포렌식 관련 실정은 과도기적 단계로 수사 절차 확립 및 개선 단계에 있으며, 국외의 포렌식 기술과 도구들에 대한 의존성이 강하다[4]. 이러한 상황은 경제적인 측면에서도 국가적인 낭비이며, 해외에서 개발된 도구들의 사용은 국내 환경에 적합하지 않은 요소들의 존재로 인해 능률적인 수사 진행에 해가 될 수 있다. 또한 포렌식 도구 개발 분야에 대한 국내 시장 자체가 활성화 되지 않은 상황이기에 자체 기술 개발 및 확보를 위한 노력이 미미하며, 다양한 도구들이 경쟁적으로 개발되고 있지 않기 때문에 실무에 적용 가능한 수사 도구 선택에 있어서도 매우 제한적일 수밖에 없다. 이와 더불어 기존의 포렌식 도구들에 대한 성능과 신뢰성을 평가할만한 기준 또한 미흡하기 때문에 독자적인 신기술 개발과 도구 마련을 위하여 체계화된 평가 방안을 활용한 도구 신뢰성 검증 절차와 적용 모델, 실제 도구 테스트를 통한 성능 평가 데이터 확보가 시급하다. 이러한 관점에서 본 논문에서는 TTAK.KO-12.0112 문서에 따른 컴퓨터 포렌식을 위한 디지털 증거 분석도구의 일반적인 검증 절차[5]를 살펴보고, 제시된 검증 항목들을 이용하여 실제 증거분석 도구를 대상으로 기능 요구사항들을 테스트 하였다. 이를 위해 대상 도구의 특징 및 신뢰성 검증 항목들 간 유사성을 고려하여 분류 및 통합 과정을 통해 개 별 테스트를 설계하고, 가상의 증거 이미지 파일을 직접 생성하여 활용하였다. 또한 테스트 내용을 바탕으로 대상 도구들에 대한 성능 평가를 수행하였으며, 각 도구들의 증거 분석 기능에 대하여 향후 성능 개선 방향을 제시하였다. 이는 실제 신뢰성 검증을 위해 일반적인 방법과 절차만을 기술하고 있는 표준의 내용을 보다 적극적으로 활용을 위한 실질적인 도구 테스트 방안 제시로써도 의미가 있다.

II. 디지털 포렌식 도구

일반적인 디지털 포렌식 조사 절차는 증거 평가, 수집, 조사, 문서화 및 보고의 4단계로 진행된다. 관련 사건이 발생하게 되면 위 단계에 따라 최초 사건 현장에서 범죄에 직접 사용되었거나 연관가능성이 있는 디지털 정보를 포함할 것이라 예상되는 시스템을 평가하고, 이를 대상으로 디지털 데이터를 수집하며, 수집된 데이터를 이용하여 분석한 후 법적 효력을 지니는 형태의 증거로 추출한 다음 수행하였던 모든 조사과정과 최종 증거물을 보고하는 일련의 과정들이 이에 포함된다[6]. 이 때, 대부분의 과정은 각 단계에서 필요한 작업을 수행하는 디지털 포렌식 도구들을 사용하여 이루어진다. 도구들은 그 특징에 따라 조사 절차상의 각 과정을 독립적으로 수행할 수도 있으며, 전체 과정을 포함하는 하나의 통합 시스템 형태로 존재할 수도 있다. 이에 비추어 볼 때, 성공적인 증거 추출 가능 여부는 조사 과정에서 데이터 획득 및 분석에 사용되는 포렌식 도구의 성능에 따라 좌우된다고 말할 수 있으며, 조사 기관 혹은 조사자는 존재하는 다양한 포렌식 도구들의 기능 및 신뢰성에 대해 명확한 정보를 확보해야 하며, 상황에 적합한 도구를 선택할 수 있는 능력을 갖추어야 한다. 다음은 대표적인 디지털 포렌식 도구들이다.

2.1 상용 디지털 포렌식 도구

상용화되어 국내외에서 널리 사용되고 있는 대부분의 디지털 포렌식 도구들은 증거 수집부터 분석 및 문서화 과정을 모두 포함하는 통합 도구의 형태를 갖추고 있는 것들이 많다. 대표적인 도구로는 Guidance Software의 EnCase와 AccessData의 FTK(Forensic ToolKit), ILook Investigator v8, Microsoft의 COFEE(Computer Online Forensic Evidence Extractor) 등이 있다. 국내에서 개발된 도구들로는 Final data의 Final Forensics와 A3Security의 A3-AutoWatch 등이 있으며, 상용화된 도구들은 아니지만 검찰청의 D.E.A.S(Digital

Evidence Analysis System for computer forensics), 한국전자통신연구원(Electronics and Telecommunication Research Institute, 이하 ETRI)의 ETRI Forensics가 있다. 이 밖에도 모바일 기기에 대한 조사를 목적으로 하는 Paraben의 Cell Siezure, PDA Siezure 등의 소프트웨어와 각종 휴대용 기기들과의 연결을 지원하는 툴박스 형태의 상용 제품들이 제공되고 있다.

2.2 오픈 소스 형태의 디지털 포렌식 도구

기술 개발 및 학문적인 연구를 목적으로 특정 기능이나 운영체제, 장치들을 대상으로 하여 개발되는 오픈 소스 형태의 디지털 포렌식 도구들은 크게 데이터 획득을 위한 것과 데이터 분석을 위한 도구로 분류되며, 대부분 단일 기능만을 수행하는 형태로 제작된다. 이는 보다 효율적인 기능 구현과 도구 능력 향상을 위함이며, 지속적인 연구와 업데이트가 이루어지고 있다. 데이터 획득 도구는 기반이 되는 운영체제의 종류에 따라 Windows 기반의 Forensic Acquisition Utilities, Liveview 등이 있으며, Unix 기반의 AFF(Advaced Forensic Format), Rdd-2.0.7 등이 있다. 데이터 분석 도구는 주요 분석 대상 및 기법에 따라 세 가지로 분류된다. 그 첫 번째는 미디어 관리 분석 도구로써 TSK(The Sleuth Kit), CDfs, CDrecord 등이 있으며, 두 번째는 파일 시스템 기반의 분석 도구로 웹 브라우저를 기반으로 한 Autopsy Browser, File System Investigator, pyflag 등이 있다. 끝으로 어플리케이션 기반의 분석 도구로는 Event Log Parser, FAUST(File AUdit Security Toolkit) 등이 있다. 이 외에도 오픈 소스 형태이지만 통합 도구로써 대부분의 기능을 갖추고 있는 네트워크 기반의 포렌식 도구인 F.I.R.E (Forensic and Incident Response Environment)가 대표적이다.

2.3 디지털 포렌식 도구 신뢰성 검증

앞서 소개한 바와 같이 다양한 포렌식 도구들이 존재함에도 불구하고 이들은 여러 가지 제한적인 요소들로 인해 실제 포렌식 조사에서 사용되지 못하고 있으며, 그 중 가장 결정적인 이유는 해당 도구를 통해 얻게 되는 디지털 증거가 법적인 증거력을 갖추기 위해 도구에 대한 신뢰성 검증이 필요하지만, 이를 가능하게 하는 제도적인 장치나 표준 등이 마련되어 있지 않다는 점이다[7]. 이를 극복하기 위한 노력으로 수행되었거나 진행 중인 프로젝트들은 다음과 같다.

2.3.1 NIST의 CFTT 및 CFReDS 프로젝트

미국 상무부 산하의 NIST(National Institute of Standards and Technology)에서 진행되고 있는 CFTT(Computer Forensics Tool Testing) 프로젝트[8]는 포렌식 조사에서 사용되는 모든 도구들에 대해 신뢰성 기준을 제공하기 위한 방법을 연구하며, NIJ(National Institute of Justice)와 법무부 산하 연구 개발 조직 및 OLES(Office of Law Enforcement Std.), ITL(Information Technology Lab.)에 의해 공동으로 진행되고 있다. 또한 FBI, 사이버 범죄 예방 센터 및 U.S Security Service를 포함한 여러 관련 기관들에 의해 지원되고 있다. 연구에 대한 결과물로는 2008년 1월에는 포렌식 수사 시 사용되는 문자열 검색 도구를 위한 요구사항들을 정의한 Forensic String Searching Tool Requirements Specification[9]을 발행하였으며, 2009년 3월에는 삭제된 파일에 대한 인식과 복구를 위해 파일 시스템의 메타데이터를 조사하는 포렌식 도구들의 요구사항을 정의한 Active File Identification & Deleted File Recovery Tool Specification[10] 문서를 발행하였다.

CFReDS(Computer Forensic Reference Data Sets) 프로젝트[11]는 실제 범죄 수사에서 획득 가능한 일련의 가상 디지털 증거 이미지들을 개발하며, 제공된 이미지 세트들은 실무 수사 인력 양성 훈련 및 포렌식 도구 적합성 테스트에 사용된다.

2.3.2 Brian Carrier's DFTTI

DFTTI(Digital Forensic Tool Testing Images)는 공공 기관에서 이루어지는 포렌식 도구에 대한 테스트 기법 연구와 비영리 단체 또는 개인에 의하여 수행되는 학문적 목표를 지닌 연구들과의 격차를 줄이고자 2003년부터 진행되고 있는 공개 프로젝트이다[12]. 디지털 증거 분석 도구의 핵심 기능에 초점을 두어 각 기능 별로 이를 테스트 할 수 있는 가상의 증거 이미지를 게재하고, 웹 사이트 그룹을 통해 위 이미지를 이용한 도구 테스트 결과, 테스트 이미지에 대한 평가 및 개선점, 효율적인 테스트 방법에 대한 의

견 등을 수렴하는 형태로 진행되고 있다.

2.3.3 국내 TTA 표준 제정

한국정보통신기술협회(Telecommunications Technology Association, 이하 TTA)는 2007년부터 현재에 이르기까지 디지털 포렌식과 관련하여 다양한 국가 표준을 제정하였다. 이들 중 디지털 포렌식 도구들과 관련된 것은 다음과 같다.

- 컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항(TTAS.KO-12.0057)[13]
- 컴퓨터 포렌식을 위한 디지털 데이터 수집도구 검증규격(TTAK.KO-12.0075)[14]
- 컴퓨터 포렌식을 위한 디지털 증거 분석도구 요구사항(TTAK.KO-12.0081)[15]
- 컴퓨터 포렌식을 위한 디지털 증거 분석도구 검증(TTAS.KO-12.0112)[5]

본 논문에서는 디지털 증거 분석도구에 초점을 두어 컴퓨터 포렌식을 위한 디지털 증거 분석도구 검증(TTAS.KO-12.0112) 문서에 기재된 일반적인 검증 절차를 살펴보고, 제시된 검증 항목들을 이용하여 실제 증거 분석 도구를 대상으로 한 기능 별 구체적인 모의 테스트를 설계한 후, 테스트 적용 결과를 분석하여 성능 평가를 수행한다.

III. 디지털 증거 분석 도구 요구사항 및 신뢰성 검증

디지털 데이터는 변경이나 복제가 용이하다는 특수성으로 인해 적법한 형태의 증거로 인정을 받기 위해서는 이를 다루는 증거 획득 및 분석 도구가 정확하고, 결정적이어야 하며, 검증 가능하게 동작해야 함을 의미한다[16]. 하지만 현재 디지털 증거 분석 작업은 도출된 결과에 대한 원인과 방법, 그 특징에 대해 명확히 설명하지 않는 특정 소프트웨어 또는 하드웨어에 의존하고 있으므로, 증거력을 부여하기 위해서는 이를 다루는 조사관 혹은 관련 종사자들이 분석 과정 각 단계의 결과, 도구의 동작 및 원리에 대해 완벽하게 이해하고 있어야 하며, 분석 도구 설계 시 적용된 개발자 고유의 공학적 메커니즘이 공개되어야 한다는 것을 뜻한다. 이는 비현실적인 일이며, 전문가라 할지라도 다양하게 존재하는 디지털 증거 분석 도구들에 대해 모두 파악하여, 그 신뢰성을 판단하기란 쉽지 않은 일이다. 그러므로 디지털 증거 분석 도구에 대한 요구사항 확립을 통해 공통의 필수 기능들을 정의하고, 정의된 기능에 대한 적합성 테스트를 수행하여 신뢰성이 보장된 도구를 이용 가능하게 함으로써 디지털 데이터에 증거력을 보다 효율적으로 부여할 수 있게 하려는 노력이 필요하다. 이러한 관점에서 제정된 컴퓨터 포렌식을 위한 디지털 증거 분석도구 요구사항(TTAK.KO-12.0081) 표준[15]에서는 다음과 같은 내용들을 정의하고 있다.

3.1 디지털 증거 분석 도구의 기능 요구사항

표준에서는 디지털 증거 분석 도구가 시스템 상에서 동작하는 소프트웨어로써 기본적으로 갖추어야 할 일반적인 요구사항 이외에도 포렌식 조사 단계에서 증거 데이터 분석을 수행하기 위한 핵심 요소 3가지에 중점을 두어 해당 기능 별 요구사항을 제시하고 있다.

- 도구는 분석 대상이 되는 증거 디스크 또는 데이터 이미지 내의 모든 영역에 대해 일체 누락 없는 분석을 수행해야 한다.
- 도구는 삭제되거나 변조된 데이터 또는 파일들에 대한 탐지와 복구 기능을 제공해야 한다.
- 도구는 특정 문자열 또는 파일들을 탐색할 수 있어야 한다.

다음 [표 1]은 표준에서 제시된 디지털 증거 분석

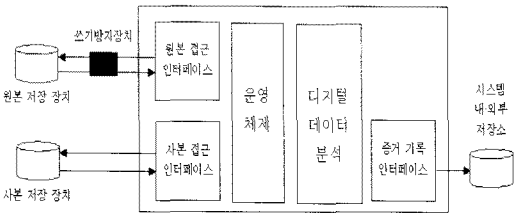
[표 1] 삭제 파일 복구 기능의 필수적인 요구사항

구분	요구사항
DFR_M_01	삭제 파일 복구 기능은 도구에 의해 제공되는 문서들(사용법, 목적, 동작, 시스템 요구사항 등을 기술하는 자료들의 집합)에 의해 확인된 파일 시스템에서 복구 기능을 지원해야 한다.
DFR_M_02	삭제 파일 복구 기능은 파일 시스템 객체가 삭제된 이후에 유지되는 메타데이터에서 복구 가능한 모든 삭제된 파일 시스템 객체들을 식별해야 한다.
DFR_M_03	삭제 파일 복구 기능은 복구된 객체를 구성하는데 있어 발생한 오류를 보고해야 한다.
DFR_M_04	삭제 파일 복구 기능은 잔여 메타 데이터에서 각각의 삭제된 파일 시스템 객체에 대해 복구된 객체를 구성해야 한다.
DFR_M_05	각각의 복구된 객체는 잔여 메타 데이터에서 식별된 모든 할당되지 않은 데이터 블록들을 포함해야 한다.
DFR_M_06	각각의 복구된 객체는 삭제된 블록 풀로부터 데이터 블록들만으로 구성되어야 한다.

도구의 기능 요구사항들 중 삭제 파일 복구 기능에 관련된 요구사항 예시이다.

3.2 디지털 증거 분석 도구 신뢰성 검증

디지털 증거 분석 도구검증(TTAS.KO-12.0112) 표준은 앞서 소개한 요구사항들을 바탕으로 도구의 기능들에 대한 신뢰성 검증을 수행할 수 있도록 여러 가지 검증 항목들과 그에 대한 테스트 절차를 제시한다. 검증 항목들을 선정함에 있어서 요구사항들 중 의미상으로 중복되거나 테스트 방법이 중첩되는 사항들은 통합하여 항목화한 것이며, 다양한 분석 시스템 환경을 고려하여 테스트를 적용할 수 있도록 일반화된 테스트 절차를 기술한다.



〔그림 1〕 디지털 증거 분석 시스템 구성 예

다음 표들은 표준에서 제시된 검증 항목과 각 항목별 테스트 절차에 대한 예시이다. 검증 항목 표에는 기반이 되는 관련 요구사항들이 함께 표기되어 있으며, 테스트 절차 표는 대상이 되는 검증 항목, 해당 항목에 대한 테스트 방법, 테스트 수행 시 예상되는 결과를 명시한다.

〔표 2〕 삭제 파일 복구 관련 기능 검증 항목

구분	검증 항목	관련 요구사항
DFRV_01	도구에 의해 제공되는 문서들(사용법, 목적, 동작, 시스템 요구사항 등을 기술하는 자료들의 집합)에 의해 확인된 파일 시스템에서 모든 파일 타입들에 대한 복구가 가능함	DFR_M_01
DFRV_02	파일 삭제 이후 유지되는 메타데이터에서 복구 가능한 모든 삭제된 파일들을 식별함	DFR_M_02
DFRV_03	삭제 파일 복구 과정에서 파일 재구성과 관련된 오류가 발생한다면, 이를 보고함	DFR_M_03
DFRV_04	복구된 파일들은 원본과 동일함	DFR_M_04, 05, 06

〔표 3〕 검증 항목에 대한 테스트 절차
DFRV_04 복구된 파일들은 원본과 동일함

테스트 방법	테스트 전 이미지 파일 내에 존재하는 삭제된 파일들의 해시 값들을 계산하고, 테스트 대상 도구를 이용하여 삭제 파일 복구 작업을 수행한 후 계산된 해시 값들을 비교한다.
테스트 절차	1. 테스트 대상 도구가 실행 가능한 환경을 구축한다. 2. 테스트에 사용할 일련의 파일들을 준비하고, 각각의 파일들에 대한 해시 값들을 구하여 명시한다. 해시 값 비교를 위해서는 암호학적 관점에서 안전성이 검증된 알고리즘을 사용하여야 하며, 해시 알고리즘으로는 SHA1, HAS160 등이 있다. 3. 준비한 파일들을 테스트 설정에 따라 마운트 시킨 이미지 파일에 복사하고, 삭제한다. 이때, 파일이 복사된 위치와 복사 및 삭제 작업에 관한 상세 절차를 명시한다. 4. 이미지 파일을 테스트 대상 도구를 이용하여 복구하고, 복구된 삭제 파일들의 해시 값을 계산하여 2항의 절차에서 명시한 값들과 비교한다. 5. 최종 복구된 이미지 파일을 분석하여, 3항의 절차를 통해 명시한 내용과 비교한다.
예상 결과	테스트 전 이미지 파일 내 존재하는 사전에 준비한 파일들의 해시 값과 삭제 및 복구 작업 이후 파일들의 해시 값이 모두 일치하며, 파일이 존재하는 위치 및 이미지 파일 구조 모두 동일하다.

IV. 디지털 증거 분석 도구 신뢰성 테스트

본 장에서는 실제 상용 및 오픈 소스 형태의 포렌식 도구를 선정하여 테스트 대상으로 삼아, 앞서 소개한 검증 항목 및 테스트 절차를 활용하여 구체화된 모의 테스트를 설계하고 직접 수행함으로써, 향후 테스트 모델 제시 및 해당 도구 장단점 평가에 대한 내용을 기술한다.

4.1 테스트 대상 도구 선정

테스트 대상은 도구의 인지도 및 보유 기능들을 고려하여, 대부분의 검증 항목들을 최대한 빠짐없이 적용해 볼 수 있도록 포렌식 절차에 필요한 전반적인 기능들을 모두 포함하고 있는 통합 도구들로 선정하였다.

〔표 4〕에서 소개된 도구들 중 ETRI Forensics는 비교적 인지도가 떨어지지만, 국내 연구소에서 독자적으로 개발 중인 고속 포렌식 시스템(High-Speed Forensic System, HSFS)의 일부로써 타 도구들

〔표 4〕 테스트 대상 도구

도구 이름	특징
EnCase Forensic LE ver 6.0	Guidance Software 사의 상용 포렌식 도구, 세계적으로 높은 인지도, 국내에서도 법적 유효성을 인정받은 솔루션
The Sleuth Kit-2.09 & AutoPsy-2.08	오픈 소스 형태의 대표적인 포렌식 도구, Windows 및 Unix 계열의 OS 환경에서도 사용 가능, HTML 방식의 그래픽 인터페이스 지원
ETRI Forensics	ETRI에서 2007년부터 개발해오고 있는 고속 포렌식 시스템, 독자적인 이미징 포맷을 가짐, 고속 데이터 수집 및 검색/분석에 중점을 둔 도구

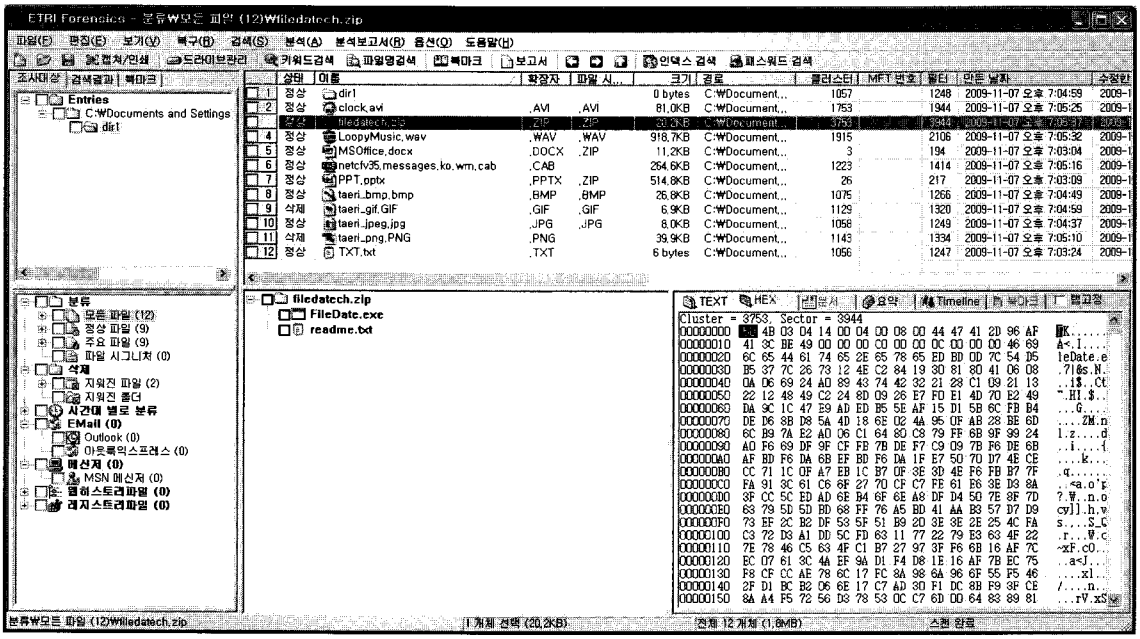
에 상응하는 데이터 수집 및 분석 기능들을 보유하고 있으며, 특히 국내 실정을 고려하여 한글 분석 능력이 강화된 고속 인덱스 생성과 하드웨어 가속을 통한 검색 기술은 매우 뛰어난 성능을 나타낸다[17].

4.2 테스트 설계

최초 테스트 대상이 될 도구가 선정되면, 도구가 제공하는 모든 기능들을 파악한 후, 표준의 검증 항목표를 이용하여 테스트 가능한 기능만을 선별한다. 테스트 설계는 선출된 항목들을 각각의 테스트 케이스로 분류하고, 개별 케이스에 적용 가능한 테스트 절차를 확인하여 다양한 수행 환경에 맞게 세부적인 내용을 포함하는 증거 이미지 파일을 생성하고, 관련 사항들을 명시하는 작업을 통해 이루어진다. 다음은 테스트 효율성과 대상 도구의 특성 등을 고려하여 유사성이 존재하거나 동시에 진행 가능한 항목들을 분류 및 통합한 후, 최종 설계한 테스트 케이스들이다. 이 때, MD5 해시가 테스트에서 사용된 것은 암호학적 관점에서 보안 관련 용도가 아니며, 도구가 찾아낸 파일들이 원본과 동일한 것임을 확인하고, 분석 작업 수행 후 내용 변경이 발생하지 않는다는 간단한 무결성 검증을 위한 것이다.

4.2.1 일반적인 기능 검증 항목에 대한 테스트

(1) GV_TEST_01
- 관련 검증 항목 : GV_01, 03, 04, 05, 06, 08
- 이미지 파일(〔표 5〕 참조)
  - GV_TEST_01.dd(FAT, 10MB)
  - MD5:b8a9381adb7a9e296e1ae7d5ee396892
- 확인 사항 목록
  - 분석 작업 수행 후 이미지 파일에 대한 MD5 값 변화 유무



〔그림 2〕 ETRI Forensics 실행 화면

〔표 5〕 GV_TEST_01.dd 내부파일 상세 표

파일	문자열	MD5	설명
file1.hwp	파일1	EC0A60216B692906C9C385778528 49BF	한글 파일
/directory1/file2.txt	file2 in directory1	B228CE4AC7E05CF295426DA91E55DEC3	메모장 파일
/directory1/file3.dat	file3 in directory1	D5DF85E7D05AA6316C8B753D35E3CC3B	
/directory2/taeri.jpg		087BF89B43907BA8711E45290158AA95	JPEG 파일

· 파일 시스템 및 이미지 파일 구조, 내부 구성파일 비교
· 문자열 및 파일 탐색 등 수행 후 이벤트 로그 확인
· 분석 리포트 확인, 복수 테스트 수행 후 각 결과의 동일성 비교

(2) GV_TEST_02
- 관련 검증 항목 : GV_07
- 쓰기방지장치 없이 연결된 USB 메모리 스틱
 · Memorett USB Disk(FAT32, 967.5MB)
 · MD5:4d67bb93c9d8df799e49c0a6af956c7a
- 오류가 있는 분석 작업 수행을 위하여 외부 장치 데이터에 대한 접근을 시도하고, 분석 도중 외부 장치를 제거하여 고의적인 오류를 발생시킨다.
- 확인 사항 목록
 · 분석 작업 수행 중 발생한 도구의 오류보고를 확인

(3) GV_TEST_03
- 관련 검증 항목 : GV_02, 03
- 쓰기방지장치 없이 연결된 USB 메모리 스틱
 · Memorett USB Disk(FAT32, 967.5MB)
 · MD5:4d67bb93c9d8df799e49c0a6af956c7a
- 확인 사항 목록
 · 분석 작업 수행 후 USB에 대한 MD5 값 변화 유무
 · 파일 시스템 및 내부 구조(디렉터리, 파일) 비교

4.2.2 삭제 파일 복구 기능 검증 항목에 대한 테스트

(1) DFRV_TEST_01
- 관련 검증 항목 : DFRV_01, 02, 04
- 이미지 파일(〔표 6〕 참조)
 · DFRV_TEST_01.dd(FAT, 10MB)
 · MD5:1e58db962fa63edff60950766b4df01f
- 확인 사항 목록
 · 해당 이미지에 대한 파일 시스템과 메타데이터 정보 비교
 · 식별된 삭제 파일 및 디렉터리 목록, 구조 비교
 · 원본과 복구된 파일들의 MD5 값 대조를 통한 동일성 비교

(2) DFRV_TEST_02
- 관련 검증 항목 : DFRV_03
- 이미지 파일(〔표 7〕 참조)
 · DFRV_TEST_02.dd(FAT, 5.9MB)
 · MD5:4aeb06ecd361777242ab78735d51ace6
- 확인 사항 목록
 · 원본과 복구된 파일들의 MD5 값 대조를 통한 동일성 비교
 · 비정상적으로 복구된 파일들에 대한 도구의 보고 여부

〔표 6〕 DFRV_TEST_01.dd 내부파일 상세 표

파일	크기 (bytes)	MD5	설명
single_cluster.dat	6	DD5C07036F2975FF4BCE568B6511D3BC	단일 클러스터
multi_cluster.dat	75,303	A89E077ADF8C7B4BC4CA7CEE4608905F	다수 클러스터
single_cluster.txt	6	DD5C07036F2975FF4BCE568B6511D3BC	txt 텍스트
/dir1			삭제된 디렉터리
/dir1/in_deleted_dir1.txt	11,284	6D4C089E8492EEAA3B53AA31AA6C61CF	삭제된 디렉터리 내 파일
/dir1/dir2/			삭제된 디렉터리
/dir1/dir2/한글파일_in_deleted_dir2.hwp	13,824	2F7C17F46EC78B3D20ADDE57C9453C4C	삭제된 디렉터리 내 파일

〔표 7〕 DFRV_TEST_02.dd 내부파일 상세 표

파일	크기 (bytes)	MD5	설명
sing.dat	780	59B20779F69F F9F0AC5FCD2 C38835A79	단일 클러스터
mult1.dat	3,081	FFD27BD782B DCE67750B6B9 EE069D2EF	다수 클러스터
frag1.dat	1,584	7A3BC5B763BE F201202108F4B A128149	단편화된 파일
frag2.dat	3,873	0E80AB84EF00 87E60DFC67B8 8A1CF13E	단편화된 파일
/dir			삭제된 디렉터리
/dir1/mult 2.dat	1,715	59CF0E9CD107 BC1E75AFB737 4F6E05BB	삭제된 디렉터리 내 파일
/dir1/dir2 /			삭제된 디렉터리
/dir1/dir2 /frag3.dat	2,027	21121699487F3 FBBDB9A4B33 91B6D3E0	단편화된 파일

4.2.3 파일 및 문자열 탐색 기능 검증 항목에 대한 테스트

(1) FSV_TEST_01
- 관련 검증 항목 : FSV_01, 02, 03
- 이미지 파일(〔표 8〕 참조)
  · FSV_TEST_01.dd(FAT, 10MB)
  · MD5:e4b7a7e7e474981dad87098ef69584e8
- 확인 사항 목록
  · 해당 이미지에 대한 파일 시스템과 메타데이터 정보 비교
  · 인식된 파일 종류 및 관련 정보, 디렉터리 구조 비교

(2) SSV_TEST_01
- 관련 검증 항목 : SSV_01, 02, 03, 04, 05
- 이미지 파일(〔표 9〕 참조)
  · SSV_TEST_01.dd(FAT, 15MB)
  · MD5:cc247d7e2d2b9bd9e0aebe6199e12bfe
- 확인 사항 목록
  · 표기된 문자열에 대해 누락 없는 탐색 여부
  · 탐색 질의 및 탐색 조건 지정에 따른 결과 확인

〔표 8〕 FSV_TEST_01.dd 내부파일 상세 표

파일	크기 (bytes)	MD5	설명
MSOffice. docx	11,475	49C1A7E40CA 3CFBF8D8F72 39A4313F9C	DOC
PPT.pptx	527,240	9B8CF3F55EE 4CFFB9BF7B5 7D977ACA40	PPT
TXT.txt	6	515284BF3426 5A3E4647A520 0D6FC065	TXT
taeri_jpeg. jpg	8,204	087BF89B4390 7BA8711E4529 0158AA95	JPEG
taeri_png. png	40,917	74F2EC576742 891DC8824193 CCA5C132	삭제된 PNG
netcfv35.me ssages.ko.w m.cab	270,954	F59BD607FFF 748B334BD268 33C2EA52C	CAB
clock.avi	82,944	BB516947768F BB05B41A248 7F200716E	AVI
LoopyMusic. wav	940,794	E2FA75ADE39 8C9A44815B11 CC141105C	WAV
filedatach. zip	20,710	BC65324FBAC 4A8974665996 E703391B9	ZIP
FileDate. exe	49,152	7E80E6205C1 EDF29CCCD3 7297049755C	압축된 EXE
readme.txt	3,489	E0C646E43430 725FCDE6E68 DA667FCEE	압축된 TXT
/dir1			디렉터리
taeri_bmp. bmp	27,538	691A35F3CA2 4FFFF10EEF0 283B0A0D79	디렉터리 내 BMP
taeri_gif.gif	7,076	09236F0B6589 B0BA6041BEB 03FD5ACCB	디렉터리 내 삭제 GIF

(탐색 공간 지정, 정규 표현식, 대소문자 지정 영문 검색 등)

4.2.4 기타 기능 검증 항목에 대한 테스트

(1) AFV_TEST_01
- 관련 검증 항목 : AFV_01
- 이미지 파일(〔표 10〕 참조)
  · AFV_TEST_01.dd(FAT, 1.4MB)

〔표 9〕 SSV_TEST_01.dd 내부파일 상세 표

파일	문자열	문자열 위치
file1.dat	first	파일 내
file2.dat	SECOND	파일 내
	SECOND	디렉터리 엔트리 내 파일명
file1 & file2	1cross1	할당된 두 파일 간 교차
file3.dat	2cross2	한 파일 내 섹터 간 교차
	3cross3	비할당영역
file2 & file2 slack	1slack1	파일과 슬랙 영역 간 교차
file3 slack & file4	2slack2	슬랙 영역과 파일 간 교차
file4 slack	3slack3	슬랙 영역
file4.dat	1fragment1	단편화된 섹터 간 교차
file6.dat	2fragment sentence2	단편화된 섹터 간 교차
file5.dat	deleted	삭제된 파일 내
file7.dat	a?b\c*d$e#f[g^	파일 내 정규표현식
ANSIHangul.dat	한글	파일 내
UTF16LEHangul.dat	한글	파일 내
UTF16BEHangul.dat	한글	파일 내
UTF8Hangul.dat	한글	파일 내

· MD5:9fb582f3361ba0bc5a3b0f7c17a082cb

- 확인 사항 목록

· 분석 결과의 파일 생성 시간 정보 비교

(2) AFV_TEST_02

- 관련 검증 항목 : AFV_02, 03, 04, 05, 06, 07
- 이미지 파일(〔표 11〕 참조)

· AFV_TEST_02.dd(NTFS, 4.0GB)

· MD5:0f3206fb0214dc75cb5a04fa5c325410

· 분석 대상이 될 가상 시스템을 구축하기 위해서 VMware workstation을 이용하여 Windows XP를 설치하고, 인터넷 및 이메일 사용 기록과

〔표 10〕 AFV_TEST_01.dd 내부파일 상세 표

파일	파일 생성 시간 정보
winter.txt	2004년 1월 1일 오후 2:00
summer.txt	2004년 6월 1일 오후 3:00

〔표 11〕 AFV_TEST_02.dd 내부파일 상세 표

파일	MD5	설명
file1.jgp	087BF89B43907BA8711E45290158AA95	정상 JPEG
file2.dat	087BF89B43907BA8711E45290158AA95	확장자 변경 JPEG
file3.jpg	59188EAD8BB1FAEE7B455E449D6697B0	확장자만 JPEG인 랜덤 파일
file4.jpg	302A7C427DA0D46EA952F5E6B2133171	JPEG 시그너처 삽입한 랜덤파일
file5.abc	0261963242290FBE6E4DA035AC2E9843	JPEG 시그너처 여러 곳에 삽입
file6.jpg	087BF89B43907BA8711E45290158AA95	삭제된 JPEG
file7.dat	087BF89B43907BA8711E45290158AA95	확장자 변경 후 삭제된 JPEG
file8.dat	087BF89B43907BA8711E45290158AA95	확장자 변경 JPEG
file8.zip	3496F442D30DD2D8E57BCE919560172D	file8.dat를 포함하는 ZIP 파일
file8.abc	3496F442D30DD2D8E57BCE919560172D	file8.dat 포함 확장자 변경 ZIP

아래 표에 기재된 파일들을 저장한다.

· 데이터 수집 도구를 이용하여 전체 디스크를 이미징 한다.

- 확인 사항 목록

· 해당 이미지의 운영 체제, 시스템/사용자 정보, 설치된 프로그램, 파일 시스템 관련 정보 비교

· 고유 정보 변경 파일에 대한 원래의 파일 타입 인식 여부

· 인터넷 및 이메일 사용 기록, 운영체제의 로그 파일 분석 여부

· 분석 결과에 나타난 내부 파일들과 원본 파일의 MD5 값 비교

4.3 테스트 결과 분석

테스트는 대상 증거 분석 도구를 각각의 동작 환경에 적합한 시스템에 설치 후, 해당 테스트 케이스에 맞게 별도로 사전 파일을 만든 다음 생성한 이미지 파일들을 raw image 타입의 증거물로 등록하여 분석을 수행한 결과이다. 테스트 결과표에서 만족은 테스트 설계 시 명시하였던 확인 사항 목록의 내용들이 분석 작업을 통해 모두 확인되었음을 의미하며, 그 외 누락되거나 내용이 다른 항목이 존재할 경우 불만족으

로 표시하였다. 분석 결과에 대한 상세한 설명은 불만족 된 항목들을 중심으로 기술한다.

4.3.1 EnCase Forensic LE ver 6.0

〔표 12〕 EnCase Test 결과

Test Cases	결과
GV_TEST_01	만족
GV_TEST_02	만족
GV_TEST_03	만족
DFRV_TEST_01	만족
DFRV_TEST_02	불만족
FSV_TEST_01	만족
SSV_TEST_01	불만족
AFV_TEST_01	만족
AFV_TEST_02	만족

- DFRV_TEST_02 : 〔표 7〕에 기재된 파일들을 모두 식별하였으나, 복구 후 단편화 된 파일 frag1.dat, frag2.dat, frag3.dat의 MD5 값이 원본과 일치하지 않았다.
- SSV_TEST_01 : 한글 관련 검색에 있어서 ANSIHangul.dat 파일 내 사항이 누락되었다. 키워드 검색 옵션에 ANSI Latin-1이란 항목은 있었으나 테스트에 포함된 인코딩 타입과는 차이점이 존재하여 나타난 결과라 판단된다.

EnCase의 경우 대부분의 테스트에서 만족스러운 분석 결과를 보여 주었지만 위 2가지 결과를 통해 단편화된 파일 처리 및 복구 기능에 대한 개선이 필요하며, ANSI 인코딩 타입의 한글 문자를 탐색하지 못하는 것에 대한 업데이트가 필요함을 확인하였다.

4.3.2 The Sleuth Kit-2.09 & AutoPsy-2.08

〔표 13〕 TSK & AutoPsy Test 결과

Test Cases	결과
GV_TEST_01	불만족
GV_TEST_02	미 시행
GV_TEST_03	미 시행
DFRV_TEST_01	불만족
DFRV_TEST_02	불만족
FSV_TEST_01	만족
SSV_TEST_01	불만족
AFV_TEST_01	만족
AFV_TEST_02	만족

- GV_TEST_01 : 파일 구조, 파일 시스템, 내부 구성 파일에 대한 정보들이 설계했던 내용과 모두 일치하였으며, 수행한 작업에 대한 이벤트 로그 역시 모두 정확하게 확인 가능하였다. 하지만 file1.hwp 파일을 Microsoft Installer로 인식하며, 한글 문자열 처리에서 불완전한 결과를 나타냈다.
- GV_TEST_02, 03 : 분석 대상을 이미지 파일만으로 제한하는 도구의 특성을 고려하여 테스트를 수행하지 않았다.
- DFRV_TEST_01 : 한글파일_in_deleted_dir2.hwp 파일에 대한 인식과 복구가 정확하게 이루어지지 않았다.
- DFRV_TEST_02 : 단편화 된 파일 frag1, frag2, frag3.dat 의 MD5 값이 원본과 일치하지 않았다.
- SSV_TEST_01 : UTF-8 인코딩 타입의 한글 문자열 외에는 전혀 알아볼 수 없는 형태로 처리하여, 〔표 9〕에 기재된 문자열에 대한 탐색 질의 결과에 누락이 발생하였다.

TSK & AutoPsy의 경우 전반적으로 파일 타입 인식과 브라우징 측면에서 취약점이 나타났으며, 특히 한글 관련 인코딩 타입 및 문자열에 대한 처리가 미흡하여 이에 대한 개선이 필요하다. 또한 EnCase와 마찬가지로 단편화된 파일 처리 및 복구 기능에 대한 개선도 이루어져야 한다.

4.3.3 ETRI Forensics

〔표 14〕 ETRI Forensics Test 결과

Test Cases	결과
GV_TEST_01	만족
GV_TEST_02	만족
GV_TEST_03	만족
DFRV_TEST_01	만족
DFRV_TEST_02	불만족
FSV_TEST_01	만족
SSV_TEST_01	불만족
AFV_TEST_01	만족
AFV_TEST_02	만족

- GV_TEST_02 : 고의로 제거된 외부 장치에 대한 오류 메시지를 정확하게 보고하였으나, 도구가 최초 구동되는 시점에서 분석 시스템에 연결

된 모든 장치에 대한 인식을 시도하는 형태로 동작하기 때문에 사용자 편의를 위하여 실시간으로 추가 또는 제거 되는 외부 장치들에 대한 정확한 인식 여부가 가능하도록 보완될 필요성이 있다.

- DFRV_TEST_02 : [표 7]에 기재된 파일들을 모두 식별하였으나, 복구 후 단편화 된 파일 frag1.dat, frag2.dat, frag3.dat의 MD5 값이 원본과 일치하지 않았다.
- SSV_TEST_01 : UTF16BEHangul.dat 파일 내의 문자열 탐색에 실패 하였으며, 키워드 검색 옵션 내에 존재하지 않는 인코딩 타입이었으므로 이에 대한 추가가 필요하다.

ETRI Forensics의 경우 국내에서 개발 중인 도구답게 다른 도구들에 비해 국내에서 널리 사용되는 파일 타입에 대한 인식과 브라우징 측면에서 장점을 나타내었으며, 특히 한글 관련 처리가 정확하게 이루어졌다. 하지만 문자열 탐색과 관련하여 누락된 인코딩 타입에 대한 추가와 단편화된 파일 처리 및 복구 기능에 대한 개선이 이루어져야 한다.

4.4 테스트 의미

디지털 증거 분석 도구의 신뢰성 검증을 위해 선정된 모든 검증 항목에 대한 테스트를 성공적으로 통과해야만 실무에 적합한 증거 분석 도구가 되는 것은 아니다. 하지만 앞서 기술된 테스트 내용들과 이를 바탕으로 한 도구의 평가는 표준에 명시된 테스트 절차에 대한 구체적인 활용 방법과 하나의 기법 적용 모델 제시로써 의미를 가지며, 국내 실정 및 다양한 기술적 요소들을 고려해 볼 때 향후 보완되어야 할 사항들을 권고함에 의의를 둘 수 있다. 실제 표준의 내용을 살펴보면 증거 분석 도구의 기능들을 중심으로 신뢰성 검증이 필요한 항목들과 그 방법에 대한 일반적인 절차만을 기술하고 있기 때문에, 해당 정보를 활용하고자 하는 다양한 계층의 독자들에게 막연하게 느껴 질 수 있다. 이에 본 논문에서 기술된 테스트 설계 부분과 특히 테스트를 위한 가상의 증거 이미지 파일을 생성하기 위해 수행한 작업 관련 사항들은 포렌식 도구 생산자들에게 자신들이 개발 중인 제품을 테스트 할 수 있는 실질적인 기법 마련에 유용하게 사용될 수 있을 것이며, 추가적인 도구 테스트를 통해 객관적인 성능 평가 자료가 확보된다면 포렌식 관련 종사자들에게 도구 선택 시 활용 가능한 좋은 참고 자료가 될 것이다.

V. 결론

본 연구에서는 컴퓨터 관련 범죄의 급증에 따라 중요시 되고 있는 디지털 포렌식 도구들 중 증거 분석 기능에 초점을 두고, 이와 관련하여 제정된 디지털 증거 분석 도구 요구사항 및 신뢰성 검증에 대한 표준을 살펴보았다. 또한 이를 바탕으로 실제 포렌식 도구인 EnCase 와 The Sleuth Kit & AutoPsy, ETRI Forensics 를 대상으로 구체적인 모의 테스트를 설계하고 직접 수행하여 각 도구 별 성능에 대한 장단점을 분석하였다.

그 결과 3가지 도구 모두 많은 부분의 테스트를 성공적으로 통과한 반면, 단편화된 삭제 파일 복구 및 처리에 있어서 기능 개선이 필요함을 확인하였다. 또한 EnCase 와 The Sleuth Kit & AutoPsy 같은 국외 도구들은 국내에서 널리 사용되고 있는 파일 타입에 대한 인식과 한글 문자열 처리가 미숙하여 이에 대한 보완이 필요함을 알 수 있었으며, ETRI Forensics는 국내 개발 중인 도구답게 이러한 부분에서 강점을 나타내었으나 다양한 인코딩 타입을 추가적으로 고려해야 할 필요성이 있음을 발견하였다.

위와 같은 결과들을 통해 본 연구는 포렌식 관련 종사자 및 도구 개발자들에게 보다 상세한 정보를 제공하며, 다양한 도구들을 대상으로 신뢰성 검증을 수행하고 평가가능하게 함으로써 도구 선택의 자유도를 높여줄 수 있을 것이다. 더불어 국내 실정을 고려한 평가 기준 마련은 독자적인 디지털 포렌식 도구 개발과 관련 기술 발전에 이바지할 것이라 사료된다. 이를 토대로 국외 포렌식 기술 의존으로 인한 국가적인 낭비를 줄이고, 자체적으로 새롭게 개발되는 미래의 포렌식 도구들은 다양한 측면에서 국제적인 경쟁력을 지니며, 관련 범죄를 처벌하고 예방하기 위한 핵심 도구로써 사용될 수 있을 것이다.

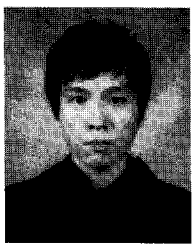
향후 연구 과제로는 다양한 도구들을 대상으로 추가적인 테스트를 수행해보면서 보다 효율적인 테스트 설계 방법을 모색하고, 개별 생성한 이미지 파일들을 보완하여 상황에 따라 유용하게 적용 가능한 증거 이미지 파일 셋을 확보할 계획이다.

참고문헌

[1] Amber Schroader and Tyler Cohen, Alternate Data Storage Forensics, Syngress, May. 2007.

[2] Albert J. , Marcella, Menendez and Doug, Cyber Forensics:A Field Manual for Collecting, Examing, and Preserving Evidence of Computer Crime, CRC Press, Aug. 2007.
[3] Anthony Reyes and Jack Wiles, The Best Damn Cybercrime and Digital Forensics Book Period, Syngress, Oct. 2007.
[4] 손정환, 김귀남, "국내 디지털 포렌식 기술 현황과 발전 방안," 한국사이버테러정보전학회, 정보보안 논문지, 제5권 제1호, pp.11-18, 2005년 3월.
[5] 한국정보통신기술협회, "컴퓨터 포렌식을 위한 디지털 증거 분석도구 검증," 표준번호: TTAK.KO-12.0112, 2009년 12월.
[6] 길연희, 홍도원, "디지털 포렌식 기술과 표준화 동향," TTA Journal, IT Standard & Test, No.118, pp.75-81, 2008년 8월.
[7] Brian Carrier, "Open Source Digital Forensics Tools : The Legal Argument," @stake Research Report, 2002.
[8] Computer Forensics Tool Testing(CFTT) Project, http://www.cftt.nist.gov/
[9] NIST CFTT, "Forensic String Searching Tool Requirements Specification," Public Draft 1 of Version 1.0, January 24, 2008.
[10] NIST CFTT, "Deleted File Recovery Tool Specification," Draft for SC Review of Version 1.0, January 19, 2005.
[11] Computer Forensic Reference Data Sets (CFReDS) Project, http://www.cfreds.nist.gov/
[12] Digital Forensic Tool Testing Images(DFTTI), http://dftt.sourceforge.net/
[13] 한국정보통신기술협회, "컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항," 표준번호: TTAK.KO-12.0057, 2007년 12월.
[14] 한국정보통신기술협회, "컴퓨터 포렌식을 위한 디지털 데이터 수집도구 검증," 표준번호: TTAK.KO-12.0075, 2008년 12월.
[15] 한국정보통신기술협회, "컴퓨터 포렌식을 위한 디지털 증거 분석도구 요구사항," 표준번호: TTAK.KO-12.0081, 2008년 12월.
[16] National Institute of Justice, "Forensic Examination of Digital Evidence: A Guide for Law Enforcement," NIJ Special Report, April 2004.
[17] 김건우, 홍도원, "고속 디지털 포렌식 기술," 한국정보보호학회, 정보보호학회 논문지, 제19권 제5호, pp.45-51, 2009년 10월.

〈著者紹介〉



이 태 림 (Tae-Rim Lee) 학생회원
2008년 3월: 부경대학교 컴퓨터멀티미디어학과 학사
2010년 2월: 부경대학교 정보보호협동과정 석사
2010년 3월~현재: 부경대학교 정보보호협동과정 박사과정
〈관심분야〉 정보보호, 디지털 포렌식, e-Discovery

신 상 욱 (Sang Uk Shin) 정회원
1995년 2월: 부경대학교 전자계산학과(학사)
1997년 2월: 부경대학교 전자계산학과(석사)
2000년 2월: 부경대학교 전자계산학과(박사)
2000년 4월~2003년 8월: 한국전자통신연구원 선임연구원
2003년 9월~현재: 부경대학교 IT융합응용공학과 부교수
〈관심분야〉 디지털 포렌식, 모바일네트워크보안, 암호프로토콜, 멀티미디어콘텐츠보호