정 보 보 호 학 회 지
제26권 제5호, 2016. 10

NIST의 디지털 포렌식 도구 검증 체계 소개

박 정 흠*, James R. Lyle*, Barbara Guttman*

요 약

정보 통신 기술이 빠르게 발전하고 디지털 기기가 보급됨에 따라 다양한 유형의 사건을 해결하는데 있어서 디지털 증거가 핵심적인 요소로 활용되고 있다. 이에 잠재적인 디지털 증거를 수집, 추출, 복구, 분석하기 위한 디지털 포렌식(Digital Forensics) 기술의 연구 개발이 전 세계적으로 매우 활발하게 진행되어 왔다. 활발한 연구 개발의 결과, 보다 효율적인 디지털 포렌식 활동을 지원하기 위해서 여러 도구(S/W, H/W)들이 공개되고 있으며 현재 다양한 목적으로 널리 활용되고 있다.

이와 같이 디지털 포렌식 도구의 활용이 일반화되었고 특히 동일(또는 유사한) 기능을 제공하는 여러 도구가 존재함에 따라서 각각의 도구가 제공하는 기능의 범위와 구현의 정확성 등에 대한 검증의 필요성이 제기되었다. 이러한 요구에 맞춰 1999년 미국 국립표준기술연구소(NIST)에서 디지털 포렌식 도구 검증 체계를 구축하였고, 현재까지도 활발하게 진행되고 있다.

본 논문에서는 NIST에서 수행 중인 CFTT와 CFReDS 프로젝트를 소개하고, 진행 현황과 향후의 발전 방향을 설명한다.

Ⅰ. 서 론

첨단 과학 수사 기법 중의 하나로 알려진 디지털 포렌식(Digital Forensics)은 디지털 증거가 사건 해결을 위한 핵심적인 요소로 활용됨에 따라서 그 중요성이 점차 높아지고 있다. 현재 민사/형사 사건에서 뿐만 아니라 데이터 복구, 내부 감사, 침해 사고 대응, 회계 정보 분석 등 디지털 데이터를 수집하고 분석할 필요가 있는 여러 분야에서 매우 폭넓게 활용되고 있다.

최근 정보 통신 기술의 발전과 보급에 발맞춰서 다양한 디지털 기기 및 서비스에 대응하기 위한 기술 개발의 요구가 높아지고 있다. 특히 임베디드 기기의 광범위한 보급과 함께 클라우드, 빅 데이터, 사물인터넷 등과 같은 새로운 개념이 등장하면서 보다 다양한 관점에서 디지털 포렌식 기술의 연구와 개발이 요구되고 있는 상황이다.

이처럼 디지털 포렌식에 대한 관심이 높아지고 관련 기술의 연구 개발에 투자가 활발해짐에 따라서 다양한 오픈 소스, 무료, 상용 도구들이 개발 및 보급되고 있다. 일반적인 유틸리티나 게임 애플리케이션과는 달리 디지털 포렌식 도구는 잠재적인 디지털 증거를 다루기 때문에 객관적인 평가를 통해서 제공되는 기능을 정확히 이해하고 성능을 정밀하게 파악할 필요성이 꾸준히 제기되어 왔다. 이에 1999년 미국에서는 국토안보부(DHS, Department of Homeland Security), 연방수사국(FBI, Federal Bureau of Investigation) 등의 지원으로 국립표준기술연구소(NIST, National Institute of Standards and Technology)에서 디지털 포렌식 도구 검증을 위한 체계를 마련하기 시작하였다. 참고로 NIST는 미국 상무부(DOC, Department of Commerce) 산하의 연구 기관으로 국가 측정 표준 개발, 기초 기술 연구, 각 세부 분야별 표준 및 가이드라인 제정 등을 통해 미국의 산업 경쟁력을 증진시키기 위한 목적의 연구를 수행하고 있다.

본 논문에서는 NIST의 법과학(Forensic Science) 연구 동향을 간략히 알아보고, 디지털 증거 관련 프로젝트인 CFTT와 CFReDS를 중심으로 현재 NIST 내에서 구축 및 운영 중인 디지털 포렌식 도구 검증 체계를 소개한다.

Ⅱ. NIST의 법과학 연구 동향

NIST는 과거 국립표준국(NBS, National Bureau of Standards, 1901~1988) 시절부터 법과학 분야에서 활

* National Institute of Standards and Technology (NIST), Information Technology Laboratory, Software and Systems Division ({jungheum.park, james.lyle, barbara.guttman}@nist.gov)

발한 연구를 진행해 오고 있다. 필적(Handwriting), 총기, 폭발물 등과 같은 전통적인 분야를 비롯하여 과학기술의 발전에 따라서 DNA, 화학 물질, 디지털 데이터에 이르는 폭넓은 연구가 진행되고 있다.

이와 같이 NIST를 비롯한 미국 내 여러 기관에서 법과학 분야의 연구가 활발하게 진행되어 왔지만, 최근 법과학의 중요성이 확대되고 과학이 잘못된 유죄 (또는 무죄)를 선고하는 위험을 감소시키기 위해서 보다 체계적인 법과학 분야의 발전을 지원하기 위한 조직적인 연구 개발의 필요성이 대두되었다. 이러한 노력의 일환으로 2014년 NIST는 미국 법무부(DOJ, Department of Justice)와 공동으로 국가 차원의 법과학 정책/기술의 발전과 보급을 지원하기 위한 국립 법과학 위원회(NCFS, National Commission of Forensic Science)와 과학 분야 위원회 조직(OSAC, Organization of Scientific Area Committees)을 설립하였다[1].

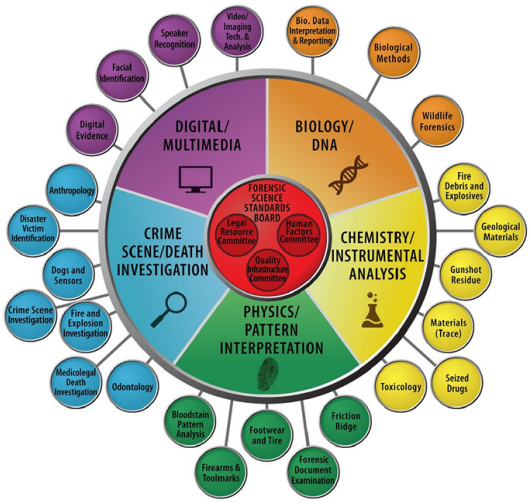
NCFS는 정책(Policy)적인 관점에 초점을 맞춰서 운영되는 조직으로, 2013년 최초 설립된 이후 2014년 2월 첫 공식 회의를 시작으로 현재까지 두세 달에 한 번씩 회의를 개최하고 있다. 주요 설립 목적은 법무 장관에게 과학수사 관련 법률/정책을 제안하고 향후의 방향을 권고하는 것이다.

한편 실무(Practice) 중심의 조직인 OSAC에 대해서는 다음 소절에서 보다 상세하게 설명한다.

2.1. OSAC

OSAC은 법과학 분야의 표준과 가이드라인을 개발하고 보급하며, 각 분야의 현황을 정확히 파악함으로써 연구 개발이 시급하게 요구되는 부분을 도출하고 이를 지원하기 위해 설립된 조직이다.

[그림 1]은 OSAC의 상세한 조직 구성을 나타낸다. 그림과 같이 OSAC에서는 법과학을 생물학/DNA, 화학/기기분석, 물리/패턴해석, 범죄현장/사인조사, 그리고 디지털/멀티미디어 분야로 구분하고, 각 분야별로 유관기관(정부, 수사기관, 법조계, 학계, 산업계 등을 모두 포함)의 전문가 및 연구원들이 참여할 수 있도록 하였다. 현재 25개 하위 위원회에 750여 명이 OSAC에 참여하고 있다. NCFS와 마찬가지로 두세 달에 한 번씩 정기적으로 회의를 개최하여 현안을 논의하고 있으며, 각 세부분야 별로 워크샵도 개최하고 있다.



〔그림 1〕 OSAC 조직 체계

한편 NIST에서 주최하는 공개 학술회의로 각 분야의 연구 개발 현황과 향후의 연구 방향을 토론하기 위한 Forensics@NIST가 2014년에 첫 번째로 개최되었으며, 2016년 11월에 두 번째 회의가 개최될 예정이다.

2.2. 디지털 증거 관련 연구 동향

OSAC의 디지털/멀티미디어 위원회는 [표 1]에 나타낸 것과 같이 디지털 증거(Digital Evidence), 비디오/이미지 분석(Video/Imaging Technology and Analysis), 얼굴 인식(Facial Identification), 그리고 화자 인식(Speaker Recognition) 연구를 수행하는 네 개의 하위 위원회로 구성된다. 특히 멀티미디어 분야의 중요성을 강조하여 세부 기술을 구분하고 활발한 연구를 지원하

〔표 1〕 NIST 내 디지털 증거 관련 연구 분야

연구 분야 구분	연구 목표
Digital Evidence	디지털 데이터의 증거 능력 관련 표준과 가이드라인 개발
Video/Imaging Tech. & Analysis	비디오/이미지 정보 분석 관련 표준과 가이드라인 개발
Facial Identification	디지털 이미지 내의 얼굴 인식 관련 표준과 가이드라인 개발
Speaker Recognition	화자 인식, 음성 데이터 세트, 음성 측정 및 검색 등과 관련된 표준과 가이드라인 개발

고 있다.

디지털/멀티미디어 위원회에 속하는 네 개의 하위 위원회 중, 디지털 증거 위원회는 멀티미디어 분야를 제외한 나머지 디지털 증거 관련 분야를 모두 다루며, 학계의 연구 지원, 관련 분야 간의 융합 지원 등이 주요 활동에 포함된다.

본 논문에서는 디지털 포렌식 커뮤니티에 널리 알려진 프로젝트인 CFTT에서 구축한 디지털 포렌식 도구 검증 체계를 설명한다.

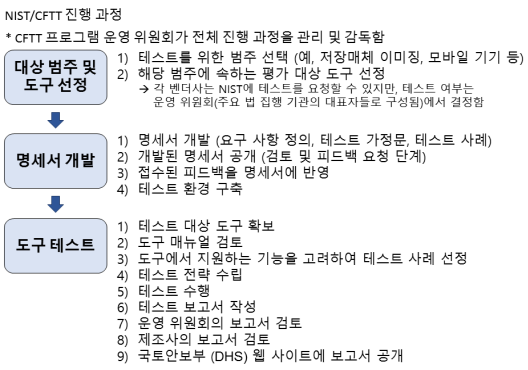
Ⅲ. CFTT 프로젝트

3.1. 프로젝트 개요

NIST의 컴퓨터 포렌식 도구 테스트(Computer Forensic Tool Testing, 이하 CFTT)는 디지털 증거를 다루는 도구의 신뢰성(Reliability)에 대한 이슈가 제기되는 상황에서 객관적이고 공정한 평가의 필요성이 증가함에 따라 1999년 미국 내 디지털 증거와 관련이 있는 유관 기관(정부, 법률, 수사 등)들의 지원으로 시작된 프로젝트이다[2].

3.2. CFTT 진행 과정

CFTT에서는 디지털 증거를 다루는 도구가 신뢰성을 갖추기 위한 요건을 만족시키는지를 객관적으로 측정하기 위해 [그림 2]와 같은 체계를 구축하였다. 그림에서와 같이 특정 범주에 속하는 도구들을 테스트하기 위해 크게 세 가지 단계의 절차를 수행한다. 참고로 모든 과정은 CFTT 운영 위원회(주요 법 집행 기관의 대표자들로 구성됨)의 관리 및 감독 하에 진행된다.



〔그림 2〕 NIST/CFTT 진행 과정

먼저 테스트가 요구되는 범주(디지털 포렌식 분야)가 결정되면 해당 범주에 속하는 평가 대상 도구를 선정하기 위한 절차가 진행된다. 실제 테스트를 수행하는 CFTT 연구원들이 대상 도구 목록을 정리하고, 운영 위원회 회의에서 토의를 거쳐 도구가 새로이 추가되거나 목록에서 제외될 수 있다. 한편 각 벤더 사는 특정 도구에 대한 테스트를 요청할 수 있지만, 테스트 대상으로의 추가 여부는 운영 위원회에서 결정한다[2,3].

대상 범주 및 도구 선정을 완료하면, 그 다음으로 실제 테스트를 체계적으로 수행하기 위한 명세서 개발 과정을 진행한다. CFTT 명세서(Specification)는 크게 세 가지로 구성된다. 가장 먼저 해당 범주의 도구들에게 필수적 또는 선택적으로 요구되는 기능 목록을 정의(Requirements)하고 이를 문서화 한다. 요구 기능 정의서를 작성한 후에는 정의된 각 기능을 테스트하기 위한 가정문(Test Assertions) 목록을 개발하는 과정을 진행한다. 테스트 가정문은 각 테스트가 수행된 이후에 확인될 수 있는 상태들을 기술한 것으로 도구의 반응, 동작 과정, 출력 결과 등이 그 대상이 될 수 있다. 정의된 요구 사항들을 기반으로 하여 필수적 또는 선택적 조건문을 정의하고 이를 실제 테스트에 활용할 수 있도록 한다. 특히 이 과정에서 조건문 목록과 함께 테스트 행위(Test Action)와 적합성 지표(Conformance Indicator)를 정의함으로써 테스트의 결과가 '예상된 결과' 혹은 '예상되지 않은 결과' 인지를 구분하여 표시할 수 있도록 한다. 이렇게 개발된 각 테스트 가정문을 이용하여 하나 이상의 테스트 사례를 생성하게 된다. 여기에서 각 테스트 사례(Test Case)는 테스트 프로토콜(환경 셋업, 결과 측정 등)과 예상되는 결과들을 구체적으로 기술한 것이다[2-5].

이와 같은 과정을 통해서 개발된 명세서는 CFTT 웹 사이트를 통해 공개하여 관련 분야 전문가들의 의견을 반영하는 과정을 거친다. 최종적으로 확정된 명세서를 기반으로 실제 도구 테스트를 수행하기 위한 환경을 구축하게 된다[2,3].

최종적으로 마련된 테스트 전략을 기반으로 실질적인 테스트가 수행된다. 가장 우선적으로 테스트 대상 도구들을 확보한 후, 각 도구의 매뉴얼을 상세하게 검토하여 적용할 수 있는 테스트 사례들을 선정한다. 이렇게 선정된 테스트 사례들을 이용해서 실제 테스트를 수행

하고 발견되는 사항들을 기록하여 결과 보고서를 생성한다. 참고로 보고서는 웹 사이트에 공개되기 이전에 크게 두 단계의 검토를 거치는데, 운영 위원회 검토와 벤더 사 검토 과정이 차례로 진행된다. 모든 검토 및 피드백 과정을 거쳐서 완성된 보고서는 국토안보부(DHS)로 제출되고, 최종 승인 과정을 거친 뒤에 DHS 웹 사이트[1]에 공개된다[2,3].

3.3. 프로젝트 진행 현황

1999년도에 시작된 CFTT 프로젝트는 2016년 현재까지도 활발하게 진행되고 있다. [표 2]는 프로젝트의 진행 현황을 간략하게 나타낸 것으로 디스크 이미징(Disk Imaging), 쓰기방지장치(Write Blocker)와 같은 기본적인 도구를 비롯하여 삭제된 데이터 복구(Deleted File Recovery, File Carving)와 모바일 포렌식 도구에 이르는 다양한 테스트를 수행하고 있다.

현재 가장 활발한 테스트를 수행하는 범주는 모바일 포렌식 분야이며, 기존에 수행하던 테스트들은 새로운 이슈나 요청이 있을 때 테스트를 수행하고 결과를 갱신하고 있다.

참고로 CFTT 프로젝트에서는 디지털 포렌식 도구들을 체계적으로 관리하기 위해서 도구 카탈로그(Tool Catalog)[2] 사이트를 운영하고 있다. 이 사이트의 주 운영 목적은 여러 디지털 포렌식 도구들을 종류별로 분류하고 세부적으로 지원하는 기능들을 목록화해서 간편하게 검색할 수 있는 체계를 마련하는 것이다. 이러한 정보를 관리함으로써 디지털 포렌식 도구의 현황을 파악하고 나아가서 현재 부족한 기술 분야를 도출하는데 활용되기를 기대하고 있다. CFTT에서는 포렌식 도구의 다양한 기능들을 분류하여 각 기능별 기술 변수(Technical Parameters)를 정의하고, 벤더 사(또는 개발자)가 직접 웹 사이트를 통해서 도구의 정보를 입력할 수 있도록 했다. 2016년 6월 현재 26개의 기능으로 분류된 170여 개의 도구(상용, 무료, 오픈소스 포함)들이 등록되어 있다.

〔표 2〕 NIST/CFTT 프로젝트 진행 현황

테스트 구분	내용 및 진행 현황 요약
Disk Imaging	- 이미징 도구 (SW, HW) 대상 - 명세서, 테스트 셋업 문서 공개 - 34개 테스트 결과 보고서 제공
Forensic Media Preparation	- 완전삭제(Wiping) 도구 대상 - 명세서 및 지원 도구 공개 - 10개 테스트 결과 보고서 제공
Write Blocker (SW & HW)	- 쓰기 방지 장치 (SW, HW) 대상 - 명세서, 지원 도구, 테스트 셋업 문서 공개 - 33개 테스트 결과 보고서 제공
Deleted File Recovery	- 삭제된 파일 복구 도구 대상 - 명세서, 데이터 세트 공개 - 6개 테스트 결과 보고서 제공
Forensic File Carving	- 파일 카빙 도구 대상 - 명세서, 데이터 세트 공개 - 18개 테스트 결과 보고서 제공
Mobile Devices	- 모바일 포렌식 도구 대상 - 명세서, 테스트 셋업 문서 공개 - 약 20여 종의 최신 스마트폰으로 테스트 수행 (주기적으로 갱신 중) - JTAG 수집 기능 테스트 준비 중 - 43개 테스트 결과 보고서 제공

Ⅳ. CFReDS 프로젝트

4.1. 프로젝트 개요

NIST의 컴퓨터 포렌식 참조 데이터 세트(Computer Forensic Reference Data Sets, 이하 CFReDS)는 디지털 포렌식 커뮤니티에 참조용 데이터를 제공하기 위한 프로젝트이다. 여기에서 참조용 데이터란 특별한 목적하에 임의로 제작되거나 실제 환경의 디지털 기기로부터 수집된 디지털 데이터로 일반적으로 데이터에 대한 검증을 지원하기 위해 제작(또는 수집) 과정과 결과물에 대한 상세 정보를 함께 제공한다. 이와 같은 참조 데이터는 도구 테스트 및 검증, 교육, 훈련, 능력 시험 등의 목적으로 활용될 수 있다[6].

4.2. 프로젝트 진행 현황

CFReDS 프로젝트의 진행 현황을 [표 3]에 간략하게 나타내었다. 현재 삭제된 데이터 복구(Deleted File Recovery, File Carving), 문자열 검색(String Searching), 파일 시스템(File System), 모바일 포렌식(Mobile

1) https://www.dhs.gov/science-and-technology/nist-cftt-reports

2) http://toolcatalog.nist.gov

〔표 3〕 NIST/CFReDS 프로젝트 진행 현황

테스트 구분	데이터 세트 이름	내용 및 진행 현황
Multi-skill holistic Cases	Data Leakage Case	- 가상의 데이터 유출 시나리오 - 하드 디스크, USB, CD 이미지 - Windows 7 (64 bits) 환경 - 교육 및 훈련 목적으로 활용이 가능한 60개의 실전 문제 제공
Data Recovery	Deleted File Recovery	- FAT, NTFS, EXT, HFS 파일 시스템 이미지 - 메타데이터 기반 삭제 파일 복구 기능 테스트에 활용 가능
	File Carving	- 문서, 아카이브, 이미지, 오디오, 비디오 데이터로 구성 - 다양한 단편화(fragmentation) 시나리오를 기반으로 제작된 이미지 - 시그니처, 내부 구조 검증 등을 이용한 데이터 카빙 기능 테스트에 활용 가능
String Searching	Russian Tea Room	- 하드 디스크 이미지 - 영어와 러시아어 문자열로 구성 - UTF-16BE, UTF-8
	Container Files	- 컨테이너 또는 아카이브 파일 - zip, rar, 7z, iso, cpio, dmg 등
Mobile Forensics	Mobile Device Images	- 모바일 기기 / SIM 카드 이미지 - 다양한 종류(현재 6개)의 모바일 포렌식 도구로 부터 생성된 이미지 파일과 결과 보고서 제공
File System	Basic Mac Images	- Mac 파일 시스템 이미지 - OS X 이미지 해석 기능 테스트에 활용 가능
External Data Sets	Rhino Hunt	- DFRWS 2005 Rodeo 이미지 - USB 플래시 드라이브 이미지, 네트워크 로그 파일
	Memory Images	- Windows 2000, 2003, XP, Vista 메모리 이미지
	DCFL	- NTFS 파일 시스템 이미지 - 데이터 복구, 카빙 등의 포렌식 도구 기능 테스트에 활용 가능

Forensics) 등의 데이터 세트가 공개되어 있으며, 대부분 CFTT 프로젝트와 연계되어 제작된 데이터이다.

대다수의 데이터 세트는 NIST에서 제작한 것이며, 일부는 다른 조직에서 제작한 것을 제공하고 있다. 이 중에서 2015년 6월 공개된 '데이터 유출 사건(Data Leakage Case)' 데이터 세트를 CFReDS 활동의 예로써 다음 절에서 보다 상세하게 소개한다.

4.3. CFReDS 예제: 데이터 유출 사건

CFReDS '데이터 유출 사건' 데이터 세트는 가상의 데이터 유출 시나리오를 기반으로 제작된 것으로 용의자 PC의 하드 디스크, USB 플래시 드라이브, 그리고 CD 이미지로 구성되어 있다.

〔표 4〕 NIST/CFReDS '데이터 유출 사건' 구성

항목	설명
시나리오	용의자는 유명 회사의 개발 부서 책임자로 최근 핵심 기술의 유출을 시도하다가 적발됨
압수된 용의자의 시스템 및 장치	개인(사무용) 컴퓨터 HDD 1개, USB 플래시 드라이브 1개, CD-R 1개
실습 문제	교육 및 훈련 목적으로 활용이 가능한 60개의 실전 문제 제공

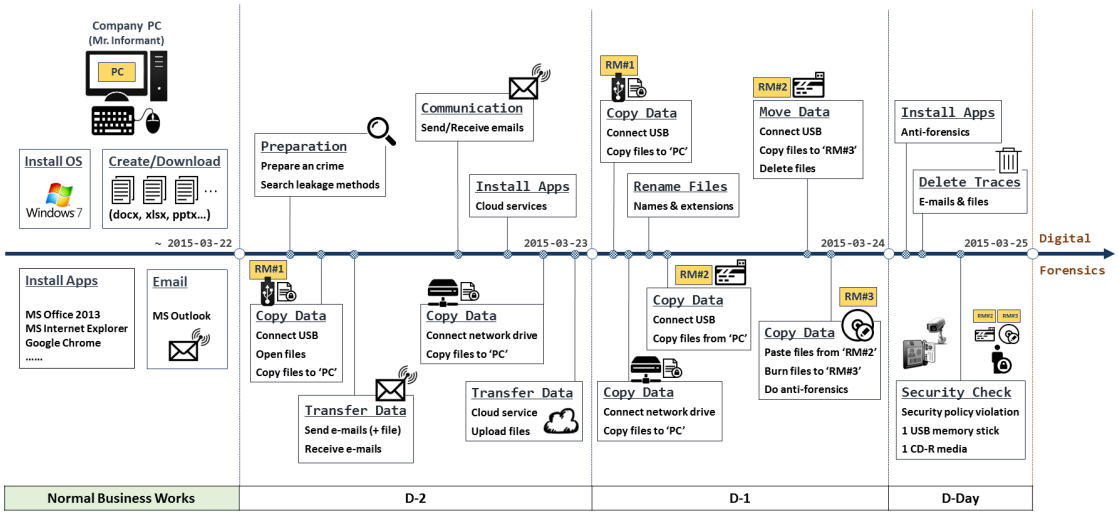
가상의 시나리오에서 용의자는 유명 회사의 개발 부서 책임자로 핵심 기술의 유출을 시도하다가 적발되었으며, 구체적인 용의자의 행위는 [그림 3]과 같다. 그림과 같이 데이터 복사, 네트워크 전송, 이메일 송수신, 응용프로그램 설치, 외부저장장치 연결 등의 일반적인 행위를 비롯하여, 응용프로그램 삭제, 데이터(파일, 이메일) 삭제와 같은 안티-포렌식 행위까지 다양한 사용자 행위가 자연스럽게 포함될 수 있도록 시나리오를 구성하였다.

이와 같이 체계적으로 구성된 시나리오를 바탕으로 제작된 데이터 세트에 대한 상세한 정보에 60개의 실전 문제를 함께 제공함으로써 교육 및 훈련의 목적으로 활용이 가능하도록 했다. 실제로 미국 내 여러 학교와 기관에서 이 데이터 세트를 디지털 포렌식 교육 및 훈련을 위해서 활용하고 있다는 피드백을 받고 있다.

Ⅴ. Federated Testing 프로젝트

5.1. 개요

NIST의 연합 테스트(Federated Testing, 이하 FT)는 CFTT 프로그램을 확장하여 도구 테스트를 위한 자료들(테스트 환경, 테스트 전략, 테스트 절차, 데이터 세트 등)을 통합적으로 제공함으로써 공유가 가능한 테스트 결과물의 생성을 지원하기 위한 프로젝트이다. FT의 핵심 목표는 디지털 포렌식 커뮤니티 누구나 자신들의 작업 공간에서 직접 도구 테스트를 수행할 수 있는 환경을 제공하여 서로 다른 조직으로 부터의 테스트 결과(보고서)를 공유하는 체계를 수립하는 것이다. 현재 기본적인 공통 테스트 환경을 제공하기 위해서 활발한 연



〔그림 3〕 NIST/CFReDS '데이터 유출 사건' 시나리오

구 개발이 진행 중에 있다[7].

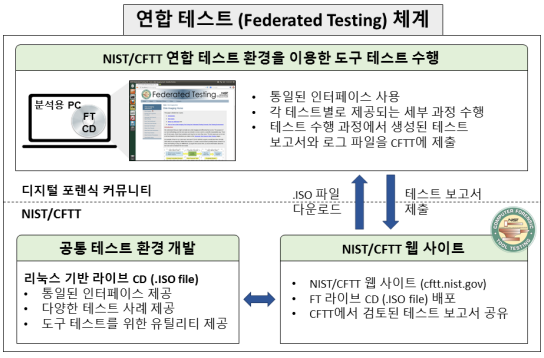
5.2. 연합 테스트 체계와 기대 효과

본 프로젝트에서 기대하는 FT 체계를 [그림 4]에 나타내었다.

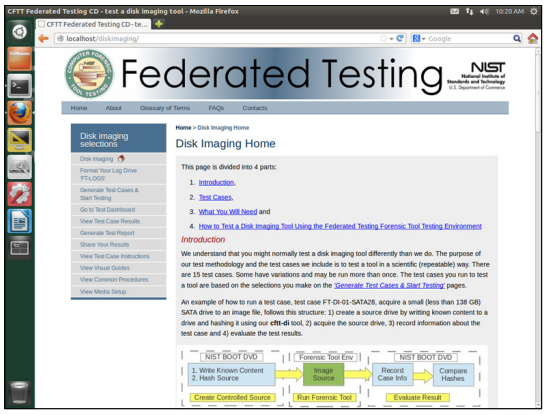
가장 먼저 기본이 되는 공통 테스트 환경은 리눅스 기반 라이브 CD의 형태로 개발을 진행하고 있다. 이 FT 라이브 CD 내에 테스트 사례별 상세 수행 과정과 도구 테스트를 보조하는 유틸리티들을 제공함으로써 연합 테스트 체계에서 공유가 가능한 결과물(보고서)을 생성하는 통일된 인터페이스를 제공할 수 있을 것으로 기대하고 있다. 이렇게 개발된 FT 라이브 CD 이미지(.ISO 이미지 파일)는 CFTT 웹 사이트를 통해 배포되기 때문에, FT 환경을 이용하여 도구 테스트를 수행하기 원할 때 최신 파일을 다운로드하여 활용할 수 있다.

최근 연구 개발의 노력과 함께 새로운 도구가 지속적으로 개발(또는 기존 도구가 갱신)됨에 따라서 테스트의 대상이 되는 도구의 수가 증가하여 단일 기관의 노력만으로는 모든 테스트를 수행하기 어려운 상황이다. 이러한 상황 속에서 FT 체계는 현재의 어려움을 해결하고 나아가서 디지털 포렌식 분야가 더욱 발전될 수 있는 토대가 될 수 있을 것이다.

한편 FT 환경을 이용한 테스트의 결과물은 목적에 따라서 유관 기관들 간의 정보 공유에 활용하거나 디지털 포렌식 커뮤니티 전체에 공유될 수 있을 것이다. 만약 공개적으로 공유하기를 원하는 경우에는 CFTT에 테스트 결과물을 제출할 수 있고, 검토 과정을 거친 후



〔그림 4〕 Federated Testing 체계



〔그림 5〕 Federated Testing 지원 시스템 실행 화면

에 웹사이트를 통해 게시될 예정이다.

5.3. 프로젝트 진행 현황

현재 공통 테스트 환경 구축을 위한 FT 라이브 CD의 연구 개발이 진행되고 있다. [그림 5]는 FT 라이브 CD의 구동 화면을 보여주며, 리눅스(Ubuntu) 환경에서 웹 인터페이스를 제공하는 형태이다. 테스트를 지원하기 위해 완전삭제(Wiping), 해쉬값 계산, 테스트 사례 관리 등을 위한 유틸리티들이 제공되며, 웹 인터페이스와 리눅스 콘솔 등을 활용해서 편리하게 이용할 수 있다. 2016년 7월 현재 FT 라이브 CD 버전 1.1이 CFTT 웹 사이트에 공개되어 있다[7].

FT 라이브 CD 개발의 진행 현황과 계획된 일정을 [표 5]에 간략하게 정리하였다. 현재까지 디스크 이미징 도구에 대한 FT 테스트 환경 구축을 완료하였다. 디스크 이미징 도구가 지원하는 세부 기능, 저장매체 종류, 저장장치 인터페이스, 파티션, 파일 시스템 등을 고려한 다양한 테스트 사례들을 제공한다. 또한 올해 안으로 쓰기방지장치와 모바일 포렌식 도구에 대한 FT 환경을 구축하는 것을 목표로 연구 개발을 진행하고 있다.

〔표 5〕 Federated Testing 프로젝트 진행 현황

테스트 구분	현황	내용 요약
디스크 이미징	완료	- 15개 테스트 사례 - 세부 기능, 저장매체 종류, 저장장치 인터페이스, 파일시스템 등을 고려한 하위 테스트 사례 제공
쓰기방지장치	진행 중	- 공통 테스트 환경 개발 중
모바일 기기	예정	- FT 전략 수립 중

Ⅵ. 향후 진행 방향 및 계획

이상에서 NIST의 디지털 포렌식 도구 검증 체계인 CFTT와 CFReDS 프로젝트를 소개하였다. 이 장에서는 현재 진행 중인 프로젝트의 향후 진행 방향과 계획을 간략하게 설명한다.

6.1. 대상 도구의 범위 확대

CFTT 프로젝트에서는 향후에 다양한 디지털 포렌식 기술 분야들로 테스트의 대상을 확대할 계획을 수립하고 있다. 새로운 디지털 기기, 소프트웨어, 서비스 등이 계속해서 출현하는 상황에 맞춰서 효율적이고 체계적인 테스트 방법론을 개발하고, 도구 테스트에 적용할 예정이다.

특히 기존에 수행 중인 임베디드(모바일) 기기와 관련된 테스트를 발전시키는 노력과 동시에 그 동안 다루지 못했던 세부적인 기술 분야들(운영체제 아티펙트, 데이터베이스, 멀티미디어, 휘발성 메모리 등)로 테스트의 범위를 확대할 계획이다.

6.2. 다양한 참조 데이터 세트 개발

CFReDS 프로젝트에서는 디지털 포렌식 분야의 발전을 지원하기 위해 다양한 참조 데이터 세트를 지속적으로 개발하고 공개할 예정이다.

단기적으로는 CFTT에서 계획하고 있는 세부 기술 분야들에 대한 도구 테스트를 지원하기 위해서 새로운 데이터 세트를 개발할 것이다. 특히 효율적인 참조용 데이터 개발 체계를 구축하기 위해서 자동화된 프레임워크를 개발하고 발전시켜 나갈 계획이다. 또한 앞에서 소개한 '데이터 유출 사건' 데이터 세트와 유사한 유형으로 여러 가지 관점의 시나리오를 개발하고 이를 이용한 참조 데이터 세트를 확대해 나갈 것이다.

6.3. Federated Testing 체계 구축

이전 장에서 언급한 것과 같이 NIST는 연합 테스트(Federated Testing) 체계가 디지털 포렌식 커뮤니티에 확대되기를 기대하고 있다. 디지털 포렌식 커뮤니티 내에서 공유가 가능한 테스트 결과를 생성함으로써 도구 테스트 활동의 어려움을 해결하고 나아가서 디지털 포렌식 분야가 더욱 발전될 수 있는 토대를 구축하기 위해 노력을 계속해 나갈 계획이다.

Ⅶ. 결 론

이상에서 NIST의 법과학(Forensic Science) 연구 활동 중에서 디지털 증거 관련 프로젝트인 CFTT와 CFReDS를 중심으로 현재 NIST 내에서 구축 및 운영 중인 포렌식 도구 검증 체계를 소개하였다.

현재 NIST에서는 본 논문에서 소개한 CFTT와 CFReDS 프로젝트 이외에도 다양한 프로젝트를 활발하게 수행하면서 법과학 분야의 발전을 지원하고 있다. 특히 디지털 증거와 관련된 CFTT, CFReDS, NSRL 등의 프로젝트는 10년 이상의 장기적인 지원을 바탕으로 꾸준한 연구 개발이 수행되어왔으며, 이러한 노력을 통해서 현재의 체계를 갖출 수 있었다.

NIST의 디지털 증거 관련 프로젝트들은 연구 개발의 결과물을 적극적으로 공개하고 피드백을 반영하고 있다. 이와 같이 NIST는 '디지털 포렌식 기반 기술'을 커뮤니티에 제공함으로써 다양한 목적의 디지털 포렌식 활동을 지원하고 관련 분야가 지속적으로 발전할 수 있는 토대를 구축하고 있다. 최근 새로운 기기와 서비스가 빠르게 출시됨에 따라 디지털 포렌식 활동의 어려움이 커지고 있는 상황에서 이와 같은 '기반 기술'에 대한 연구 개발 및 보급의 노력은 지속적으로 확대되어야 할 것이다.

참 고 문 헌

[1] OSAC (Organization of Scientific Area Committees), http://www.nist.gov/forensics/osac, [Last visited: July 2016].

[2] Computer Forensics Tool Testing (CFTT) Project, http://www.cftt.nist.gov, [Last visited: July 2016]

[3] B. Guttman, J. R. Lyle, R. Ayers, "Ten years of computer forensic tool testing", Digital Evidence and Electronic Signature Law Review, Vol 8, 2011.

[4] NIST, "Mobile Device Tool Specification Version 2.0", March 2016.

[5] NIST, "Mobile Device Tool Test Assertions and Test Plan 2.0", March 2016.

[6] Computer Forensic Reference Data Sets (CFReDS) Project, http://www.cfreds.nist.gov, [Last visited: July 2016]

[7] Federated Testing Project, http://www.cftt.nist.gov/federated-testing.html, [Last visited: July 2016]

〈저 자 소 개〉

박 정 흠 (Jungheum Park)

2007년 2월 : 한양대학교 정보통신대학 컴퓨터전공 공학사
2009년 2월 : 고려대학교 정보경영공학전문대학원 공학석사
2014년 2월 : 고려대학교 정보보호대학원 공학박사
2014년 3월~2014년 12월 : 고려대학교 정보보호대학원 연구교수
2015년 1월~현재 : National Institute of Standards and Technology (NIST), Guest Researcher
관심분야 : 디지털 포렌식, 사이버 보안, 사이버 물리 시스템

James R. Lyle

1972년 : East Tennessee State University, BS in Mathematics
1975년 : East Tennessee State University, MS in Mathematics
1982년 : University of Maryland at College Park, MS in Computer Science
1984년 : University of Maryland at College Park, PhD in Computer Science
1993년~현재 : National Institute of Standards and Technology (NIST) Computer Scientist

Barbara Guttman

1984년 : Trinity College (Hartford, CT)
1989년~현재 : National Institute of Standards and Technology (NIST) Group Leader [Software Quality Group]