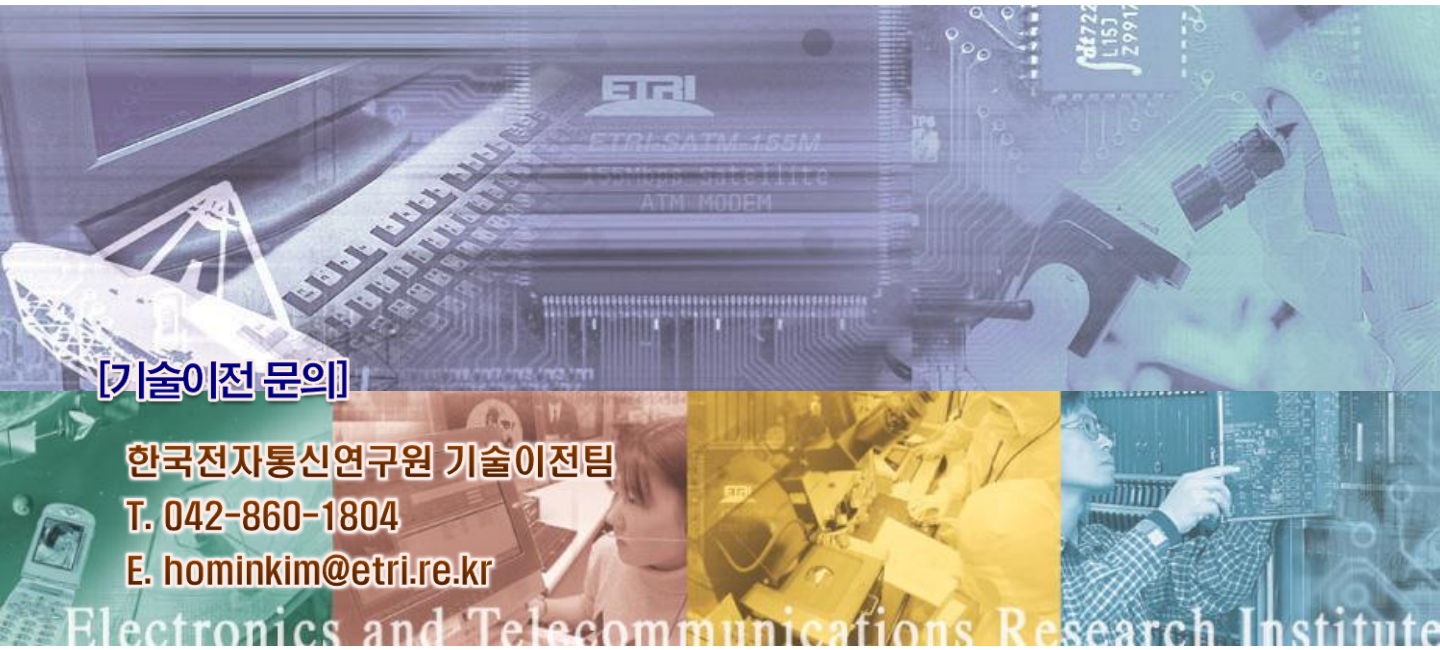
라이브데이터 포렌식v3 기술



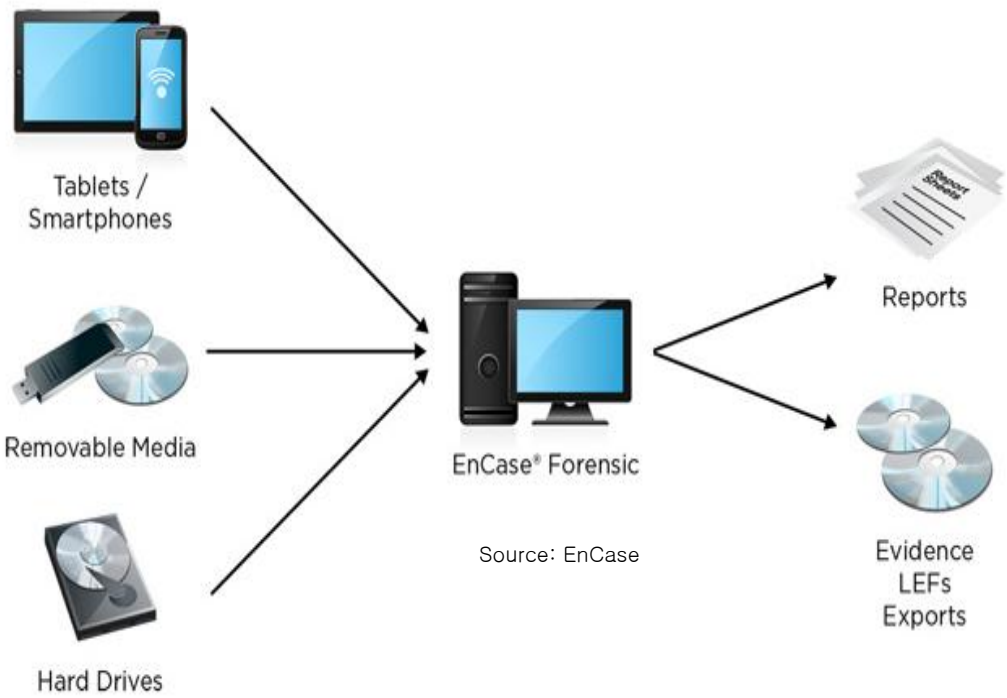
한국전자통신연구원

TECHNOLGY BRIEF 기술소개서

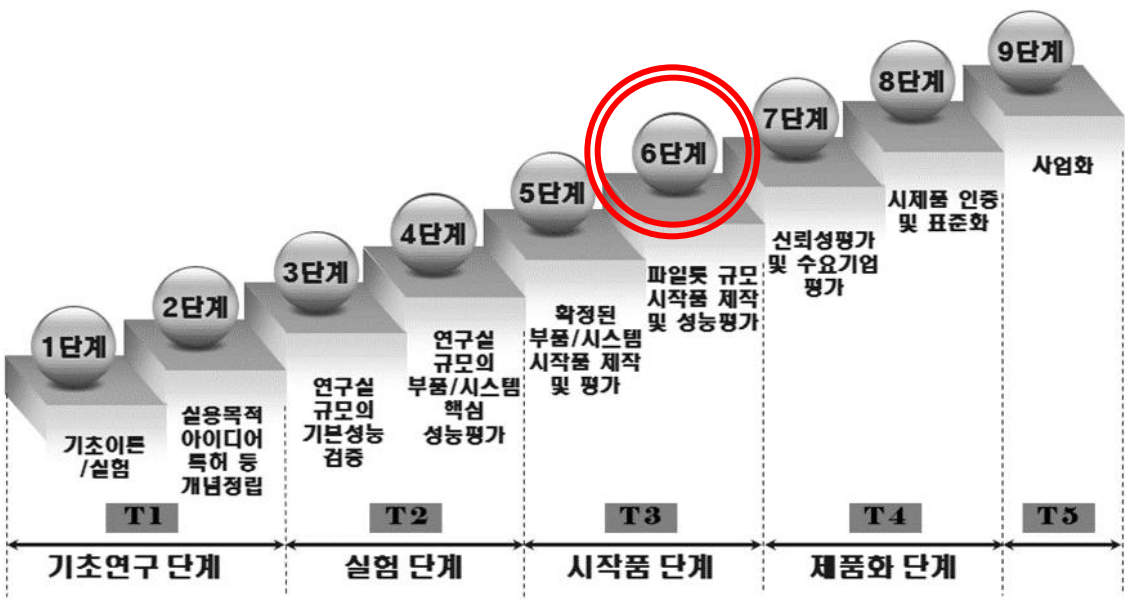
라이브데이터 포렌식v3 기술

기술개요

컴퓨터가 동작중인 상태에서 빠른 시간 안에 얻을 수 있는 자료들을 수집하고 분석하여 증거가 될 수 있는 정보를 찾아내는 기술임



기술 개발 상태 : 6단계



ETRI

TECHNOLGY BRIEF 기술소개서

라이브데이터 포렌식v3 기술

기술설명

▶ 라이브데이터 증거 자료 수집 기술

＊ 시스템 정보 수집 기술

- 프로세스/서비스 목록 수집
- H/W, S/W 설치 목록 수집
- 네트워크 정보 수집
- 사용자 계정 정보 수집
- Page File/ Physical Memory 수집

＊ 레지스트리 정보 수집 기술

＊ MFT 정보 수집 기술

＊ 웹페이지 접속 기록 수집 기술

- Internet Explorer v6,7,8 접속기록, 임시파일, 쿠키 정보 수집
- Firefox v2,3 접속기록, 임시파일, 쿠키 정보 수집
- Chrome v2 접속기록, 임시파일, 쿠키 정보 수집
- Safari v4 접속기록, 임시파일, 쿠키 정보 수집

＊ 메신저 사용 기록 수집 기술

- NateOn, BuddyBuddy, MSN, Yahoo, Mi3 메신저 사용 기록 수집

▶ 라이브데이터 증거 자료 분석 기술

＊ 시스템 정보 분석 기술

- 프로세스/서비스 목록, H/W, S/W 설치 목록, 네트워크 정보, 사용자 계정 정보 출력 및 검색

＊ 레지스트리 정보 분석 기술

- 레지스트리 트리, 키속성, 키값 출력
- 타임라인, 북마크, 검색결과 출력
- 사용자 계정정보, 최근 접근 파일, USB 장치 접속 기록 등 분석

＊ MFT 정보 분석 기술

- 시간/속성/크기/클러스터/파일/이름/확장자 필터링 출력 기능

＊ 웹페이지 접속 기록 분석 기술

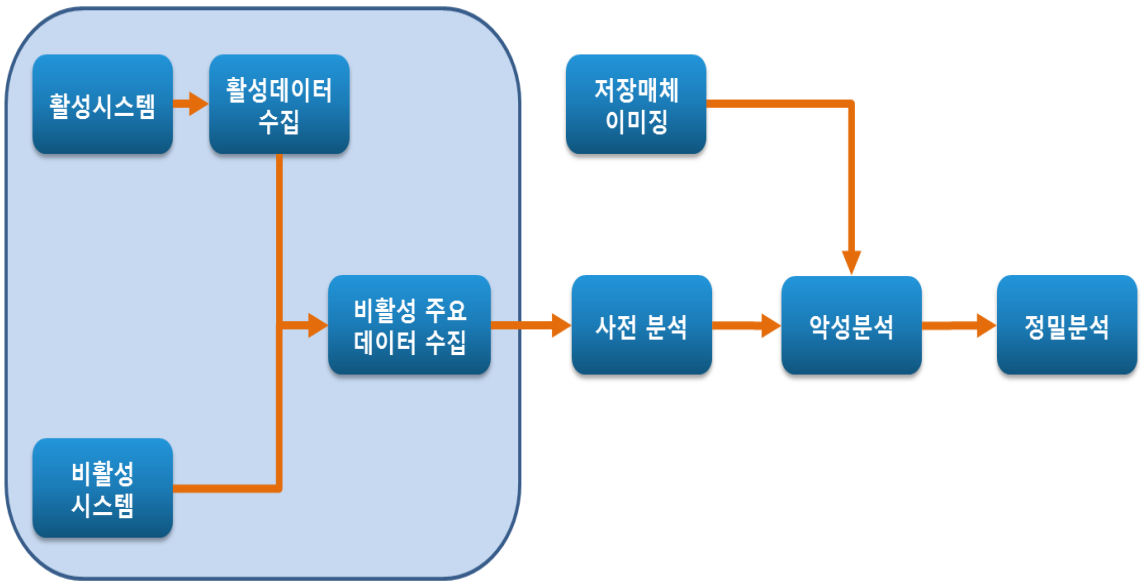
- Internet Explorer v6,7,8 접속기록, 임시파일, 쿠키 정보 출력
- Firefox v2,3 접속기록, 임시파일, 쿠키 정보 출력
- Chrome v2 접속기록, 임시파일, 쿠키 정보 출력
- Safari v4 접속기록, 임시파일, 쿠키 정보 출력
- 타임라인 분석 기능

＊ 메신저 사용 기록 분석 기술

- NateOn, BuddyBuddy, MSN, Yahoo, Mi3 메신저 사용 기록 출력

＊ 보안 USB 우회 기술

- 패스워드 설정 보안 USB의 패스워드 추출 및 기능 해제



▶ 활성 데이터 수집

- 가장 많은 시간이 소비되는 작업은 물리메모리 덤프임. 그러나,가장 많은 시간에도 불구하고 물리메모리를 앞쪽에 배치한 이유는 뒤에서 수집하는 모든 정보가 결국은 물리메모리에서 나오기 때문이며, 물리메모리 덤프가 뒤쪽에 위치하면 수집 명령을 실행하면서 물리메모리의 흔적이 손상될 수도 있기 때문임. 또한, 현재 진행형인 사건의 영향을 정확히 판단하기 위해 마지막에 네트워크 패킷을 수집하는 것이 필요함

▶ 비활성 데이터 수집

- 비활성 데이터 중 데이터 크기는 크지 않지만 분석에 매우 중요하게 활용되는 데이터가 있음. 이런 데이터를 라이브 포렌식 시 함께 수집하면 저장매체 이미징 동안 사전 분석 작업을 수행할 수 있음. 따라서, 시스템이 활성 상태가 아닐 경우에도 이미징 전에 쓰기 방지장치를 장착한 상태에서 주요 비활성 데이터를 먼저 수집한다면 전체 분석 시간을 많이 단축시킬 수 있음

▶ 본 라이브데이터 포렌식 기술은 컴퓨터가 동작중인 상태에서 빠른 시간 안에 얻을 수 있는 자료들을 수집하고 분석하여 증거가 될 수 있는 정보를 찾아내는 기술을 포함함

▶ 본 기술은 동작중인 Windows 기반 컴퓨터에서 증거가 될 수 있는 자료를 수집하고 분석하는 방법을 제공함

▶ 본 기술은 시스템 정보, 레지스트리 정보, MFT 정보, 웹페이지 접속 기록 등을 수집하는 라이브데이터 증거자료 수집 기술과 시스템 정보, 레지스트리 정보, MFT 정보, 웹페이지 접속 기록, 프로세스 정보 등을 분석하는 라이브데이터 증거자료 분석 기술로 구성되어 있음

기술적 경쟁력

총 크기 15MB 이하의 실행코드로 생성하여 Flash USB Drive나 외장 HDD에 설치하여 휴가가 간편하고 현장에서 설치 없이 바로 실행하여 빠른 자료 수집을 지원함

▶ 기존 기술의 문제점

- 외산 장비를 사용할 경우 한글 지원이 미비하고 국내법 또는 국내 실정과 맞지 않는 부분이 존재
- 국내에서 개발된 시스템의 경우 외산 장비에 비해 검색 성능, 조사 분석 능력이 떨어짐

▶ 기존 기술과 비교하여 유리한 점

- 선행 기술의 대부분이 미국 업체들에 의해 주도되고 있으며, 외산 장비를 사용할 경우 한글 지원이 미비하고 국내법 또는 국내 실정과 맞지 않는 부분이 존재
- 레지스트리, MFT, 웹접속기록, 메신저사용기록 등 다양한 분야에 대한 간편한 분석 능력 강화
- 디지털 포렌식 연구 수행을 통하여 개발된 기술은 기술이전을 통해 상용화가 적시에 가능

기술 개발 필요성

- 정보화에 따른 컴퓨터 관련 범죄뿐만 아니라 일반 범죄에서도 중요 증거 또는 단서가 컴퓨터를 포함한 다양한 전자 매체 내에 보관되어 있는 경우가 증가하고 있음
- 경찰청 사이버테러대응센터 및 검찰청 인터넷 범죄 수사 센터의 통계자료에 따르면, 아래 표에서 나타난 바와 같이 사이버 범죄의 발생건수가 매년 급속히 증가하고 있으며, 범죄의 유형 또한 공용전자기록손상, 전자문서 관련 죄, 전산업무방해, 전자기록 비밀침해, 컴퓨터 사용사기, 전자기록 손괴, 정보통신망법 및 개인정보보호법 침해 등 갈수록 다양화되고 있음
- 세계적으로 많이 사용되는 포렌식 시스템들은 국내에서 개발된 소프트웨어에 대한 분석 및 복구 기능이 제대로 제공되지 않을 뿐 아니라, 영문 데이터 위주의 분석을 목표로 설계되어 있기 때문에 국문 데이터에 대한 검색 및 분석에 오류가 많으며, 국내 정보 이용환경에 대한 특성이 반영되지 않아 증거 확보 및 활용에 어려움 존재함

적용분야

▶ 국내 환경에 적합한 포렌식 시스템

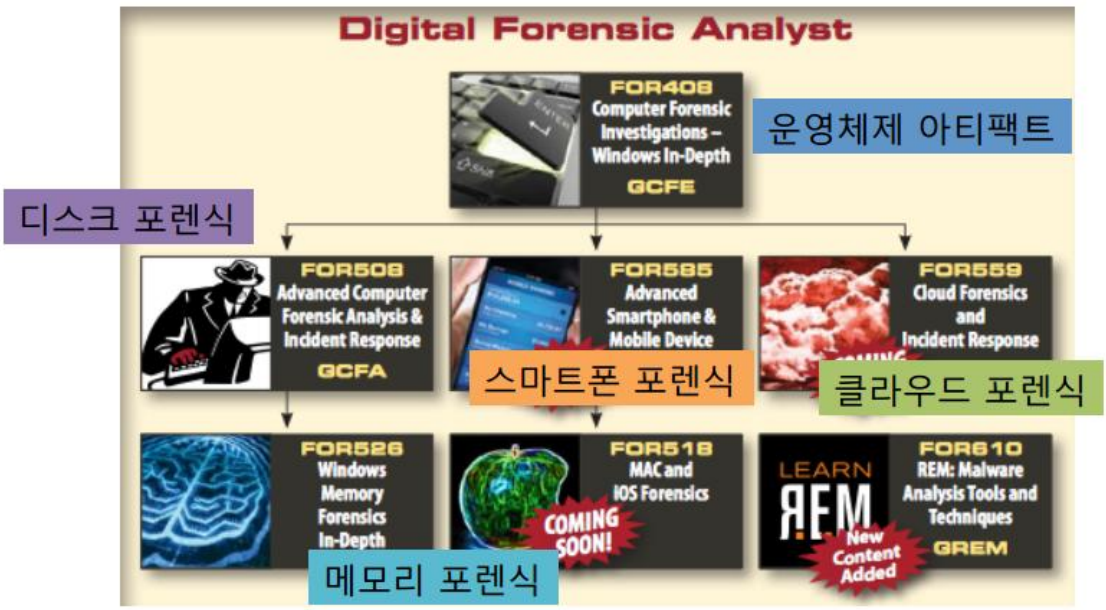
- 디지털 증거에 대한 인덱스 검색을 지원하는 국내 환경에 적합한 포렌식 시스템 개발에 활용

▶ 법률서비스에서 활용

- 검찰, 경찰 등의 국가기관, 디지털 증거 인증 서비스 사업자, 디지털 증거확보가 필요한 법률 서비스에서 활용 가능

기술동향

각 앱스토어에 맞춰 개별적으로 진행되는 현재의 애플리케이션 개발작업이 2014년 경에는 대부분 사라지고 HTML5와 브라우저로 플랫폼에 구애받지 않는 개방적 웹앱 개발환경으로 전환



국내 기술

▶ **파이널데이터사가 유일하게 기술 개발 중**

- 국내에서는 디지털 포렌식 증거분석 솔루션 개발 회사로 파이널데이터사가 유일무이하며 기존에 데이터복구 및 수사관련 포렌직 분야 시장에서 현재 활발한 기술개발을 수행중임
- 관련 제품으로는 Final Forensics, Final Mobile Forensics등이 있음

▶ 국내 인터넷 범죄 수사센터, 사이버 테러 대응센터를 비롯한 대부분의 국가기관들은 해외에서 개발된 컴퓨터 포렌식 절차 및 기술을 사용하고 있으나, 국내 사법 제도와 국산특화 파일 지원 등 국내 환경에 대한 특성이 반영되지 않아 수사상 어려움이 존재함

▶ 국내의 포렌식 기술 개발은 최근에 학교 및 몇몇 산업체를 중심으로 기본 기능 및 초기 수준의 기술 개발을 진행하고 있지만, 국산 파일에 특화된 기능을 내장한 통합 포렌식 도구 개발이 요구되고 있음

▶ 국내의 포렌식 기술 개발 수준은 현재 초기 단계로, 국산 파일에 특화된 기능을 내장한 통합 포렌식 도구 개발이 요구됨

해외 기술

▶ **Guidance Software사와 Access Data 사를 중심으로 매쉬업 개발 도구 개발 중**

- Guidance Software 사는 1997년 설립하여 통합 디지털 포렌식 제품인 Encase를 개발하였으며, 에이전트를 이용해 원격으로 기업 내 모든 개인 컴퓨터의 내부 데이터를 관리하고 검색하는 Encase Enterprise를 상용화하여 포렌식 회계 분야에서도 선도적 위치에 있음

- Access Data사는 디지털 포렌식 제품인 FTK, 패스워드 복구 제품인 PRTK, 레지스트리 검색 도구인 Registry Viewer를 개발하였으며, 최근 이들을 통합하고 오라클 DB를 탑재한 FTK 2.0을 릴리즈하였음

▶ 현재 상용화되어 있는 컴퓨터 포렌식 소프트웨어는 Guidance Software 사의 EnCase, Technology Pathways 사의 ProDiscover, AccessData사의 FTK, ASR Data사의 SMART 등이 있으며, 그 중 EnCase Edition이 가장 높은 시장 점유율을 차지하고 있음

시장동향

국내 사건 대응 서비스 시장은 2005년 1,100억에서 2010년 2,644억 원으로 증가할 것으로 추정되는데, 이중 20% 수준인 530억원의 수입 대체효과가 기대됨

- **전 세계 사건 대응 시장은 2005년 $22억에서 연평균 19.2%씩 증가하여 2010년에는 $53억에 이를 것으로 추정되는데, 이 중 국내 사건 대응 시장은 세계시장의 5% 수준으로 예측하여 2010년 2,644억 원에 이를 것으로 추정됨**

- **과제 결과물과 직접적으로 연관된 SW 부분은 2010년 전 세계 시장규모가 $10억에 이를 것으로 추정되며, 이 중 국내시장 규모 10%와 해외시장으로의 수출 5%를 예측하여 1,503억 원의 시장창출효과가 있을 것으로 추정됨**

(단위 : 백만불, 억원)

관련 제품/서비스	시장	1 차년도 (2008)	2 차년도 (2009)	3 차년도 (2010)	4 차년도 (2011)	5 차년도 (2012)
민형사 사건의 증거 수집을 위한 디지털 포렌식 시스템	해외	824	939	1002	1072	1147
	국내	758	864	918	978	1042

국내시장

- **검찰은 컴퓨터수사기법을 체계화하기 위한 목적으로 디지털증거 분석시스템인 DEAS를 개발하였고 파이널데이터사는 DEAS를 기반으로 국내 최초로 포렌식 제품을 상용화하였지만, 외산 장비인 Encase나 FTK에 비교하여 검색 성능, 조사 분석 기능이 떨어짐**
- 세계적인 시장 분석 기관 IDC에서 발표한 전세계 사건 대응 서비스 시장은 “e-Discovery” 법안의 통과에 힘입어 2005년 17억 달러에서 연 평균 19.3% 씩 증가 41억$ 추정하였음. 또한, **2010년 국내사건 대응 서비스 시장은 2004년 142억원에서 2009년 750억으로 증가할 것으로 발표하였음**

해외시장

- **Guidance Software사는 제품 개발 외에 eDiscovery Services, Incident Response Services, Forensic Services, Customized Solution Services 등 다양한 포렌식 서비스를 제공함**

- **Access Data의 FTK1.0는 이미지 생성, 데이터 분석 및 복구 기능을 담당하고 PRTK는 파일 복호, 패스워드 클랙등의 기능을 지원하며, Registry Viewer를 통해 PC 내의 레지스트리 정보 분석 기능을 제공함**

  • 유니코드 지원으로 유니코드로 표현된 다양한 언어에 대한 검색이 가능하며, FAT32, NTFS, EXT2, EXT3를 비롯한 다양한 파일 시스템을 지원함

관련기업

- **Guidance Software, Access Data, 파이널데이터**

수요처

기술 수요	디지털 증거 인증 서비스 관련 기업
적용처	검찰, 경찰등의 국가기관, 디지털 증거 인증 서비스 및 법률서비스

기술이전 내용 및 범위

▶ Open Source Software 사용 내역

OSS 라이선스 정보				
*라이선스명	*오픈소스 SW	출처(URL)	*주요기능	비고
Public Domain	SQLite	http://www.sqlite.org/	DB Handling	라이선스 사용 고지
PUblic Domain	TinyXML	http://www.grinninglizard.com/tinyxml/	XML 문서 생성	"
BSD2.0	Zuume Scripting Engine	http://sourceforge.net/projects/zuume/	GUI	"
"	Efficient Shader Compiler	http://sourceforge.net/projects/efficientshader/	GUI	"
Code Project Open 1.02 License	A PIC C Code Wizard	http://www.codeproject.com/	Template	"
"	Adobe ActiveX Control with MFC	"	ActiveX Control	"
"	CppSQLite - C++ Wrapper for SQLite	"	DB Handling	"
"	Detecting Hardware Insertion and/or Removal	"	USB Detection	"
"	Driver to Hide Processes and Files	"	Process Hiding	"
"	How To get the usbdisk's drive letter properly	"	USB Detection	"

OSS 라이선스 정보				
*라이선스명	*오픈소스 SW	출처(URL)	*주요기능	비고
"	MFC Grid control 2.26	"	Table Generation	"
"	Print Previewing without the Document/View Framework	"	Print	"
"	Protected Storage	"	Registry Hide Copy	"
"	Translating logical offsets into physical offsets	"	USB Detection	"
"	Using CodeProject - A Day In the Life of an Application - Part 1 of 5	"	USB Detection	"
"	Using the Grid Control in a Doc/View framework	"	Table Generation	"
"	WebReplay - an automated software testing tool for Web applications	"	Web Preview	"

▶ 라이브데이터 증거 자료 수집 기술

- MD5/SHA-1 Hash 값 생성
- Report 생성
- Windows XP/Vista 지원

▶ 라이브데이터 증거 자료 분석 기술

- 프로세스 정보 분석 기술
- Physical Memory내 프로세스 추출 기술
- Windows XP/Vista 지원

예상 응용 제품 및 기대효과

▶ 예상 응용 제품 및 서비스

- 디지털 증거에 대한 인덱스 검색을 지원하는 국내 환경에 적합한 포렌식 시스템 개발에 활용
- 검찰, 경찰 등의 국가기관, 디지털 증거 인증 서비스 사업자, 디지털 증거확보가 필요한 법률서비스에서 활용 가능

▶ 기대효과

- 국가 기관 및 민간 기업에서 사용하는 외산 포렌식 장비 및 소프트웨어에 대한 수입 대체 효과 발생
- 일상에서의 포렌식 기술 활용 빈도 증가가 예상됨에 따라 본 이전 기술은 이용한 다양한 제품 개발을 통해 새로운 보안 서비스 시장 창출

▶ 테스트 기준

테스트 항목	세부
기능테스트	각 단계별 기능 테스트
	통합 테스트
비기능테스트	성능 목표

▶ 테스트 방법

＊ 다중 호스트를 사용한 패스워드 탐색 기능 시험

- GUI에서 서버설정 아이콘을 눌러 서버 IP, 포트 등의 정보를 입력함
- PICASSO 시스템에서 88대의 계산노드를 구동함
- GUI에서 새작업 버튼을 눌러 대상파일을 선택함
- 찾고자 하는 파일의 예상 패스워드 최소 암호길이와 최대 암호길이를 설정함. 예상이 어려우면 최소 길이를 1로 함
- 문자열을 선택함. 사용자가 직접 문자를 설정할 수도 있음
- 작업시작 버튼을 누름
- 패스워드 발견이 되면 원도우가 팝업되는데, 그 노드에 대한 패스워드 발견 정보를 확인함
- GUI 화면에서 88대 노드의 상태와 패스워드 발견 정보를 확인함

＊ 복수의 GPU를 사용한 패스워드 탐색 기능 시험

- GUI에서 서버설정 아이콘을 눌러 서버 IP, 포트 등의 정보를 입력함
- 리눅스 머신에서 4대의 C1060 GPU 가속 프로그램을 구동함
  - 4개의 GPU 동작여부는 CUDA 에서 제공하는 deviceQuery 명령어로 확인 가능함
- GUI에서 새작업 버튼을 눌러 대상파일을 선택, 암호길이 선택, 문자열 선택을 함
- 작업시작 버튼을 누름
- 패스워드 발견이 되면 원도우가 팝업되는데, 그 노드에 대한 패스워드 발견 정보를 확인함
- GUI 화면에서 노드의 상태와 패스워드 발견 정보를 확인함