국내 디지털 포렌식 기술 현황과 발전 방안

손정환* · 김귀남**

요 약

정보통신기술의 발전과 인터넷 보급·확산의 영향으로 디지털 범죄는 해마다 증가하고 있다. 고도화·전문화되어 가고 있는 디지털 범죄를 해결하기 위해서는 디지털 포렌식 프로세스 표준화, 전문가 양성 및 교육, R&D, 정부의 정책적인 지원 등 디지털 포렌식 기술 발전을 위한 노력이 필요하다. 이에 본 연구에서는 에서는 국내 디지털 포렌식 기술의 현황을 파악하고 발전방안을 제시하고자 한다.

The present of state Domestic Digital Forensics and Development Methodology

Jung Hwan Shon* · Kuinam J Kim**

ABSTRACT

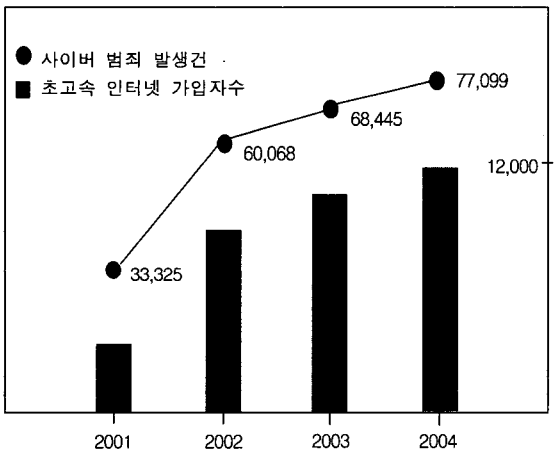
With the develoment of IT(Information Technologies) in Internet, Digital crime are increasing explosive every year. Recently, digital crime is taken advantage of technical and expert skill. It is necessary to investigate a digital crime that Digital forensic process standardization, Specialist training & education, R&D, Government support. So in this paper we proposed device of the grow of digital forensic that make analysis of the present state domestic digital forensic technique.

Key words : Digital Forensics, Digital Forensics(Model · System · Process Standardization)

* 사이버테러정보전학회
** 경기대학교 정보보호기술공학 교수

1. 서 론

경찰청 사이버테러대응센터(www.ctrc.go.kr)의 최근 통계에 의하면 지난 2004년의 사이버범죄가 77,099건에 달하는 것으로 집계되었으며 사이버범죄는 2000년 이후 해마다 폭발적으로 증가하는 추세이다. 이러한 사이버범죄는 정보통신기술의 발달 및 인터넷의 보급·확산과 밀접한 관계가 있으며 PC보유 및 초고속 인터넷 가입자수의 증가와 사이버범죄 발생률이 비례함을 알 수 있다.(그림 1)



구분	2001	2002	2003	2004
PC보급수 (1,000대)	22,495	23,502	26,741	미집계
초고속인터넷 가입자수 (1,000명)	7,806	10,405	11,178	11,921

자료 : 경찰청 사이버테러대응센터, 정통부 2004 정보화백서

(그림 1) 사이버범죄와 PC보급률/인터넷 이용자수

첨단 정보통신기기와 전문기술을 바탕으로 한 사이버범죄는 범죄 수법이 날로 다양화·지능화되고 있는데 특히 해킹, 바이러스 유포뿐만 아니라 사기, 성폭력(매매), 명예훼손, 자살 등 오프라인의 범죄들이 온라인에서도 그대로 재현되고 있는 실정이다.

사이버 범죄는 새로운 유형의 범죄로 컴퓨터, 인터넷 등 사이버·디지털 세상을 배경으로 하고 있어 기존 범죄와는 다른 수사방법이 요구된다. 하지만 새로운 유형의 사이버 범죄 또한 범행 흔적이 남게 되고 남겨진 흔적을 수집하고 보존하여 증거로 제시하는 방법을 필요로 하는데 이에 대한 연구가 디지털 포렌식(학)(Digital Forensics)이다. 디지털 포렌식은 컴퓨터를 비롯한 PDA, Digital Camera 및 광범위한 디지털 장비를 그 대상으로 범죄와 범죄자를 빠른 시간내에 정확히 찾아내고 범죄 증거를 확보하여 법정에 제출하는데 목적을 두고 있다.

디지털 범죄와 디지털 증거의 독특한 특징으로 인해 증거를 수집·보존하고 분석하여 법정에 증거로 제출하기 위해서는 전문적인 기술과 적절한 절차를 사용하여야만 한다. 특히 디지털 범죄의 초동수사와 증거 수집·분석에 사용되는 디지털 포렌식 기술과 도구들은 수사의 향방을 좌우하는 매우 중요한 열쇠의 역할을 수행한다.

본 연구에서는 국내 디지털 포렌식 기술의 현황을 파악·분석하여 발전방안을 모색하고자 한다. 본문의 구성은 디지털 포렌식의 정의와 유형, 국내 디지털 포렌식 도구와 기술 현황, 전문인력 양성·교육실태 등을 분석하여 국내 디지털 포렌식 기술의 현실태를 파악하고 끝으로 결론에서 발전방안의 도출 등 향후 검토 과제들을 제시하였다.

2. 본 론

2.1 디지털 포렌식 개념

디지털 포렌식은 컴퓨터 포렌식(Computer

Forensics)에서 비롯되었는데 컴퓨터 포렌식은 1991년 미국 오레곤주, 포클랜드의 International Association of Computer Specialists에서 용어가 처음 사용되었으며 당시 컴퓨터 포렌식은 컴퓨터 보안영역 및 법 학회에서 주로 사용되곤 하였다[1].

초기의 컴퓨터 포렌식은 법 집행기관에서 컴퓨터 기기를 압수·수색하는 문제와 압수된 기기로부터 잠재적 증거를 발견하는 것에 중점을 두고 연구되기 시작하였다[2]. 이러한 연구의 방향은 1998년에 이르러 디지털 증거(Digital Evidence)로 관심의 방향이 바뀌었으며 연구의 중점도 미디어 매체나 출력물로부터 디지털 증거 자체에 관심을 갖게 되었다. 따라서 그 명칭 또한 컴퓨터 증거로부터 디지털 증거로 변하게 되었고 디지털 포렌식이라는 명칭도 사용하게 되었다. 즉, 디지털 포렌식은 "디지털 소스로부터 디지털 증거를 Preservation, collection, validation, Identification, Analysis, Interpretation, Documentation, Presentation하기 위하여 과학적으로 이끌어내고 증명하는 방법"으로 정의된다[3].

2.2 디지털 포렌식 유형

디지털 포렌식도 일반 범죄수사와 마찬가지로 범죄에 포함되어지는 모든 것들이 증거 수집의 대상이 된다. 디지털 포렌식의 유형은 어떤 대상을 수사하느냐에 따라 구분할 수 있으며 일반적으로 다음과 같이 구분한다.

디스크 포렌식, 네트워크 포렌식, 시스템 포렌식으로 크게 구분되어지며 인터넷(웹) 포렌식, 이메일 포렌식, 데이터베이스 포렌식 및 최근에는 모바일 포렌식도 등장하였다. 디지털 포렌식 유형의 명칭에서도 알 수 있듯이 디지털 장비나 서비스를 대상으로 유형이 구분되는데 이러한 유형의 구분은 새로운 장비나 서비스의 등장에 따라 유형의 종류도 새로 탄생하게 될 것이다.

2.3 국내 디지털 포렌식 기술 현황

국내 디지털 포렌식 기술의 동향을 파악한다는 것은 매우 어려운 일이다. 왜냐하면 디지털 포렌식 기술이란 디지털 범죄를 다루는 수사관의 전문지식과 개인적인 경험, 범죄 상황 등이 복잡하게 혼합된 소위(所謂) 말하는 '*종합 예술*'이기 때문이다. 또한 국내에서 디지털 포렌식 기술을 개인적으로 활용한다는 것은 제한적이다. 일반 범죄와 마찬가지로 검·경찰 등 수사기관의 수사관 위주로 다루어지고 있기 때문에 국내 수사 관행이나 문화적 요소를 고려할 때 정확한 실태를 파악하기에는 다소 어려움이 있다. 하지만 디지털 포렌식 도구 개발·판매 회사의 기술자료와 판매현황 및 수사기관과 전문 교육기관의 교육과정 분석을 통해 국내 디지털 포렌식 기술의 현황과 수준을 일부 판단할 수 있다.

2.3.1 국내 디지털 포렌식 도구 사용 현황

디지털 포렌식 기술을 구분한 특별한 기준이나 발표문헌을 발견하지 못해 본 논문에서는 디지털 포렌식 관련 기술을 크게 데이터 복제 기술, 복구 기술, 분석 기술로 구분하였다. 데이터 복제 기술은 범죄 증거로 법정에 제출될 수도 있는 자료를 직접 조작할 경우 훼손의 우려가 있으므로 조사를 위한 복사본의 일부 또는 전부를 생성하는 기술이다. 범죄 증거자료로 사용될 가능성이 있는 하드디스크의 복사본을 만드는 기술과 데이터베이스 또는 저장장치에서 증거가 될만한 자료를 복사하는 것 뿐만 아니라 시스템(또는 디지털장비)에서 휘발성 자료를 복제(추출)하는 기술을 의미한다. 최근의 저장장치는 대용

량 저장능력을 가지고 있어 복제시간이 도구를 선택하는 주요 고려대상이 되기도 한다. 데이터 복구 기술이란 고의나 실수로 삭제되거나 훼손된 데이터를 복원시키는 기술을 말한다. 데이터를 확인하기 위한 암호 복구나 패스워드 크래킹 등도 원래 자료로 복구한다는 측면에서 복구기술의 범주에 포함시켰다. 데이터 분석 기술은 데이터 검색, 로그분석, MAC time 분석, 프로세서 분석, 해쉬분석 등 증거를 찾아내고 범죄 행위를 재조합하는데 이용되는 기술을 말한다.

이러한 디지털 포렌식 기술들은 합법적이고 투명한 방법으로 구현되어야 하고 복제·복구하거나 분석된 범죄 증거로 사용될 자료가 원본과 동일함을 증명할 수 있는 기술이 필수적으로 뒷받침되어야 할 것이다.

앞서 디지털 포렌식 기술들을 기능별로 분류하였다. 하지만 최근 디지털 포렌식 도구들은 부분 기능만을 제공하지 않고 통합·복합적인 기능을 제공하고 있는 추세이다. 국내외에 잘 알려진 몇가지 디지털 포렌식 도구들의 기능과 특징은 다음과 같다.

최근 국내 검·경찰에서도 많이 사용하고 있는 EnCase는 1980년대부터 Guidance Software사에서 개발한 통합기능의 도구이다. 증거의 보존과 분석기능을 모두 갖추고 있으며 Encase로 얻은 내용이 미국 법원에서 증거로 채택되어 더욱 유명해진 도구이다. 미국에서는 1990년대 후반부터 약 600여개의 기관이 이 도구를 활용하고 있는 것으로 알려져 있다. Encase의 주요기능은 원본 디스크의 고속복사, 데이터 탐색 및 획득할 수 있는 증거수집 기능, 훼손된 데이터 복구 기능, 전자우편의 암호를 우회·해독 기능, 하드디스크 쓰기 방지, 레포팅 기능 등을 제공하고 있다.

현재 EnCase를 사용하고 있는 국내 주요기관은 국정원, 경찰청 사이버테러대응센터, 대검찰청, 국방부, 국가보안연구소 등이 있다[4].

국산 디지털 포렌식 도구로 가장 많이 알려진 도구로는 Final Data사의 제품이 유명한데 Final-Data는 강력한 데이터 복구 기능이 특징이다. 이러한 복구 기능을 바탕으로 한 Final forensics은 삭제·손상된 파일을 포함한 검색기능, 전자우편·레지스트리·웹 히스토리(History) 등의 분석 및 보고서 작성 기능 등이 제공된다. 특히 사용자 환경이 한글이라는 점에서 인기를 얻고 있다. 주요 사용기관은 국정원 국가사이버안전센터, 경찰청, 대검찰청, 육군 중앙수사단, 해군 헌병감실 등에서 이용하고 있다[5].

미국 NTI사의 포렌식 툴 킷 중 Safeback은 증거보존과 수집을 위한 원본 대상 이미지 추출 도구로 원격으로 비트스트림 방식의 이미지를 추출하는 기능을 제공한다. NTI사의 포렌식 툴킷은 공개용, 기업용, 미국 정부용으로 제품이 구분되어 있는데 미국 정부용의 경우 핵심적인 내용들은 그 내용조차 공개되지 않고 있다.

이러한 도구들 외에도 잘 알려진 도구로 FTK, @stake, FIRE 등의 통합형 도구들이 있다.

참고로 기존의 컴퓨터 포렌식 도구 및 기술을 <별표 1>에 정리하였다.

국내 수사기관에서는 Encase, Final Data 등 상용 디지털 포렌식 도구와 함께 자체 시스템을 병행 사용하고 있다. 대검찰청에서는 디지털증거분석시스템(DEAS, Digital Evidence Analysis system for Computer Forensic)을 사용하고 있고 경찰청에서는 사이버테러대응센터내 디지털 증거분석센터를 운영하고 있다.

대검찰청의 디지털증거분석시스템은 컴퓨터수사에 대한 표준 개발 및 과학적 수사기법의 도입 등 컴퓨터 수사기법의 체계화와 전문 분석프로그램의 필요성으로 2002~2003년간 개발·도입되었다.

디지털증거분석시스템은 키워드를 통한 정보

검색 및 암호 파일 검색 기능, 파일 포맷·전자우편·웹 히스토리(History) 분석과 디지털카메라, MP3 Plyer, 휴대용 메모리 등 디지털 저장매체에서 삭제·손상된 파일을 복구한후 미리보기(Preview) 기능을 이용하여 현장에서 분석이 가능한 것이 특징이다[6].

경찰청의 디지털증거분석센터는 범죄 수사중 확보된 자료의 검색·복구·분석 기능과 디지털 포렌식 기술, 네트워크 추적기술과 표준화 연구를 목적으로 2004년 12월 21일 경찰청 사이버테러대응센터내에 설치하였다.

디지털분석센터에서는 디지털 범죄 증거수집과 분석 서버, 시스템 포렌식 프로그램, 로그분석 프로그램, 하드디스크(HDD) 복제 및 초기화 장치, 차량형 증거분석 장비와 초동수사용 디지털 현장 증거 분석세트 등이 운용중이거나 운용될 예정이다.

2.3.2 국내 디지털 포렌식 관련 교육 현황

국내의 디지털 포렌식 관련 교육과정은 크게 수사기관 교육과정, 관련 전문기관 교육과정과 맞춤형 교육과정으로 나눌 수 있다. 수사기관의 교육과정으로는 경찰 교육과정이 대표적이며 관련 전문기관은 사이버포렌식협회의 사이버포렌식 조사전문가 과정이 있다. 맞춤형 교육은 행정자치부, 정보통신부 등에서 관련 공무원을 대상으로 실시하고 있는데 민간 교육기관에 위탁하는 방식으로 수행하고 있다. 맞춤형 교육은 교육대상자(초보자, 실무자, 전문가, 관리자 등)에 따라 교육 내용을 적절히 조정할 수 있어 매우 효율적인 교육방식이라고 할 수 있다. 하지만 교육이 비정기적이고 교육 내용이 개설시마다 바뀌어서 본 연구에서는 제외하였다.

대표적인 수사기관인 경찰의 2004년 경찰교육내용중 디지털 포렌식과 관련된 과정을 정리하면 다음과 같다[7].

[경찰수사연수소]

과 정 명	과 목 명	교육기간
수사지휘	사이버범죄수사기법	6시간
조사관리자연수	사이버범죄수사	6시간
조사실무	사이버범죄수사	5시간
디지털분석전문수사	-	59시간
사이버범죄수사	-	59시간
통신추적수사	-	28시간

[경찰종합학교]

과 정 명	과 목 명	교육기간
수사요원 양성	사이버범죄수사	3시간

[국외위탁교육]

과 정 명	대상지/기간
사이버범죄에 대한 효과적인 대응방안	미국 / 1년10개월
사이버범죄 수사기법 및 대응방안 (컴퓨터 포렌식 기법 연구)	3개월

민간의 전문교육으로는 사이버포렌식협회의 사이버포렌식 조사전문가 과정이 있다. 사이버포렌식협회의 사이버포렌식 조사전문가 과정은 다음과 같다[8].

과 정 명	교 육 내 용	교육기간
교 양	정보범죄 동향/윤리	9시간
법 률	사이버 법률	20시간
포렌식 기술	포렌식 총론, 디스크 포렌식, 네트웍/시스템 포렌식 및 추적시스템, 해킹/바이러스 분석	42시간
조사 실무	사이버 포렌식 조사/실습	49시간

2004년 경찰 교육과정의 특징은 사이버 범죄의 증가와 심각성을 인식하고 경찰수사보안연수소에 디지털증거분석전문수사과정, 통신범죄수사과정을 신설하였으며 외국 선진기술 습득을

위한 국외 위탁교육과정이 차별화된 과정이라 할 수 있다. 일반 민간교육으로 사이버포렌식협회의 조사전문가 과정은 2003년부터 현재까지 약 50여명을 교육하는 등 일반인의 디지털 포렌식에 대한 높은 관심을 반영해 주고 있다.

일부 정보보호 관련 전문 교육기관에서도 디지털 포렌식 기술과 유사한 내용을 교육하고 있지만 내용을 분석한 결과 해킹 및 침해사고 대응이 목적이어서 본 연구에서 제외하였다.

3. 결 론

국내에 알려진 디지털 포렌식 도구와 관련 교육과정의 분석을 통하여 국내 디지털 포렌식 기술의 현황을 살펴 보았다. 1장 서론의 (그림 1)에서 알 수 있듯이 디지털 범죄는 매년 증가하고 있고 범죄에 사용되는 기술은 날로 고도화·전문화되고 있다. 이러한 디지털 범죄를 다루기 위해서는 범죄 기술보다 앞선 디지털 포렌식 기술이 요구되어지는데 학계의 연구와 산업계의 발전이 뒷받침되어야 할 것이고 전문인력이 양성과 정책적인 지원도 수반되어야 할 것이다.

3.1 향후 과제

폭발적으로 증가하고 전문화되어가는 디지털 범죄 수사를 위하여 다음과 같은 과제가 논의되어져야 하고 시급히 해결되어야 할 것이다.

3.1.1 디지털 포렌식 기술과 도구의 안전성 확보

2004년 11월 6일 항공관제 레이다시스템의 성능을 향상시키기 위해 미국 록히드마틴사가 제공한 새로운 프로그램을 설치하는 순간 오류를 일으켜 전국 14개 모든 공항이 마비된 일이 있다. 프로그램의 안전성이 확보되지 않아 발생한 일이다.

디지털 포렌식 도구의 개발환경과 실제 범죄 현장의 상황은 매우 다르다. 안전성이 확보되지 않은 기술과 도구는 범죄 증거가 될 원본을 훼손시키거나 그 결과가 일정하지 않고 법정에서 신뢰를 얻지 못 할 것이다.

디지털 포렌식 도구의 신뢰성을 평가하고 테스트 결과를 수사관이나 도구 개발업체에서 활용할 수 있도록 하고 있는 미국 NIST의 CFTT (Computer Forensics Tool Test) project 같은 제도가 디지털 증거의 증거능력을 위하여 도입되어야 하며 공인된 기관에서의 인증이 필수적이라고 판단된다.

3.1.2 디지털 포렌식 절차의 국내 표준 정립

국외에서 디지털 포렌식 모델에 관한 연구가 진행되고 있기는 하나 아직까지 일관성 있는 방법이나 표준으로 자리잡지는 못하고 있는 실정이다. 특히 국내에서는 디지털 포렌식 모델에 관한 연구가 활발히 진행되지 못한 가운데 어떤 검증도 없이 실무 현장에서 여러 기술과 도구들이 도입·사용되고 있다. 범죄 수사 절차에 대한 표준없이 기술적이며 세부적인 기법만을 추구하는 것은 대단히 위험하다. 디지털 범죄를 다루는 수사관마다 자신의 경험과 기술에 따라 증거를 수집하는 방법과 절차가 제 각각 다르고 수집된 증거 또한 매번 다르다면 그 증거는 신뢰성을 잃게 될 것이다[9]. 모델의 정립을 통한 표준화는 디지털 범죄 수사에 지침이 될 뿐만 아니라 훈련과 교육의 정도를 구분짓는 지표로 활용되는 등 파급효과가 매우 크다.

이러한 이유로 국내 수사 제도에 적합한 합법적이고 표준화된 수사 절차의 마련이 시급하다고 할 수 있다.

3.1.3 디지털 포렌식 전문인력의 교육 및 양성

수사기관 위주로 다루어지고 있는 디지털 포

렌식은 앞으로 적용범위가 크게 확대 될 것으로 전망된다. 2004년 6월 금감원의 종합검사 직전 전자문서 6만건을 삭제한 「00생명, 금감원 검사 방해」 사건은 디지털 포렌식 기술의 필요성과 확장성을 입증해주는 사례라 할 수 있다. 디지털 범죄의 증가 추세와 관련 분야 전문가의 수요 증가 전망에 비해 관련 디지털 포렌식 전문가는 턱없이 부족한 것이 현실이다. 디지털 포렌식 기술에 대한 연구 개발과 함께 연구인력 및 수사 전문인력의 양성이 시급하다.

3.1.4 디지털 범죄 분석과 범죄 사례 공유 작업반 구축

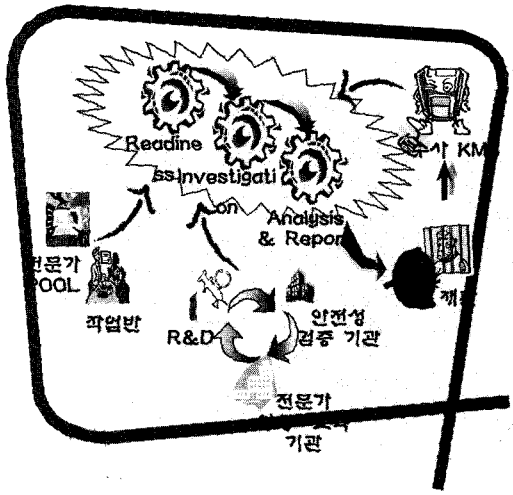
앞서 본론에서 설명하였듯이 국내 수사문화의 특성상 관련기관간 범죄자료의 공유는 대단히 어렵다. 하지만 급속히 발전해가고 있는 디지털 범죄에 대응하기 위해서는 民·官·産·學 등 관련기관의 협조체계가 절실히 요구된다. 특히, 작업반(Working Group) 구축을 통하여 신종 디지털 범죄를 분석하고 범죄 사례를 공유하여 증거 수집과 분석을 위한 기술 개발과 교류가 활발히 이루어져야 할 것이다.

3.1.5 정부의 정책적 지원과 산·학계의 활성화 노력

디지털 포렌식 분야의 발전을 위하여 법·제도 정비 및 국가 예산의 배정 등 정부의 정책적인 지원이 있어야 하며 산업계의 기술 개발과 업계 활성화 노력, 그리고 학계의 학문적인 연구가 활발히 진행되어야 할 것이다.

3.1.6 디지털 포렌식 시스템 구축 및 운용

끝으로 위에서 제안한 요소들이 유기적으로 결합된 (그림 2)와 같은 디지털 포렌식 시스템을 구축, 체계적이고 조직적으로 운용·활용하여야 할 것이다.



① 전문가 POOL
디지털 포렌식 관련 民·官·産·學 전문가로 구성, 디지털 범죄 수사 관련 법률적·기술적 조언
② 작업반(Working Group)
범죄 분석·사례 연구·기술 공유
③ R&D
디지털 포렌식 관련 신기술 및 도구에 대한 연구
④ 안전성 검증기관
디지털 포렌식 기술과 도구가 법정에서 인정받을 수 있도록 기술과 도구의 투명성, 공정성 등 신뢰도 검증기관
⑤ 전문가 양성·교육기관
디지털 포렌식 관련 전문가 양성 센터
⑥ 디지털 포렌식 절차
㉠ Readiness(수사 준비 단계/훈련과 교육·장비 확보·기동수사팀 대기 등)
→㉡ Investigation
초동수사 (상황판단·휘발성자료 추출·보존)
→ 수사(압수·수색·수집)
→㉢ Analysis & Report
분석 → 검증 → 문서화 → 증거 제출
⑦ 수사 KMS
사건 개요, 수사 기법, 증거 수집 및 증거 능력 등 수사 관련 일련의 과정을 지식 DB에 저장, 유사 사건에 참조, 사례 교육 등에 활용
⑧ 디지털 포렌식 시스템 모델
①~⑨항까지의 구성요소들이 유기적으로 연계, 상호 작용하여 효과가 극대화되는 체계

(그림 2) 디지털 포렌식 시스템

〈별표 1〉 포렌식 도구 기능 분석

도 구	복제	보존	검색	복원	분석
DIBS Mobile Computer forensic Laboratory	O		O		O
DIBS Advanced forensic Workstation	O				O
DIBS Rapid Action Imaging Device(RAID)	O				
DIBS Analyzer 2			O		O
DIBS Mycroft V3		O	O		
@stake LC4				O	
WinHex	O		O	O	O
Search and Replace			O		
FinalData				O	
dd	O				
SnapBack DatArrest	O				
SnapBack Live	O				
Forensic toolkit(FTK)	O		O	O	O
Password Recovery Toolkit(PRTK)				O	
DriveSpy	O		O		O
FireFly			O		
SCSIBlock		O			
FireBlock		O			
Image	O				
Encase Forensic Edition	O		O	O	O
FastBloc		O			
Ilook Image Invetgator	O		O	O	O
Maresware	O		O		O
Advaced Password Recovery Software Tool Kit				O	
AnalDisk					O
CopyQM	O				
CRCMd5					O
DiskSig					
FileList			O		
GetFree			O	O	
GetGif			O		
GetSlack			O		
GetTime					O
NTI-DOC			O		
PTable					O
SafeBack	O				
Seized		O			
ShowFL					O
The Coroner's Toolkit			O	O	O
Time Check					O
Time Lock					O
DETS					O
NEXT Witness					O

자료 : 홍성욱, 컴퓨터 포렌식스 기술의 고찰, 한양대학교, 2004.

참 고 문 헌

[1] Michael G. Noblett, Mark M. Pollitt, Lawrence A. Presley, "Recovering and Examining Computer Forensic Evidence", *Forensic Science Communications*, Vol.2, No.4, Oct. 2000, http://www.fbi.gov.

[2] Carrie Morgan Whitcomb, "An Historical Perspective of Digital Evidence: A forensic Scientist's Views", *International Journal of Digital Evidence*, Spring 2002, Vol.1., Available:www.ijde.org/archives/carrie_article.html.

[3] Gary Palmer, "A road Map for Digital Forensics Research", DFRWS, Nov. 2001. Available:www.dfrws.org.

[4] 제이엔아이인터내셔널(주), www.kdl.co.kr.

[5] FinalData, www.finaldata.com.

[6] 헌병기, 디지털증거분석시스템, 사이버테러대응공동 심포지엄 2004.

[7] 2004 경찰교육훈련계획, 경찰청.

[8] www.cfpa.or.kr.

[9] 손정환 외, 디지털포렌식 절차 모델, 제2회 추계학술발표대회, 사이버테러정보전학회, 2004.

손 정 환

1993년 경기대학교 전자계산 (학사)
1995년 경기대학교 전자계산 (석사)

김 귀 남

University of Kansas, U.S.A.(학사)
Colorado State University, U.S.A. (석사)
Colorado State University, U.S.A. (공학박사)
2000~현재 경기대학교 정보보호기술공학 교수
2001~현재 한국사이버테러정보전학회 회장
2001~현재 경찰청 사이버치안위원회 자문위원
2002~현재 KT 정보보안기술협의회 회장
2002~현재 국정원 국가정보보안협의회 위원