범죄 억제를 위한 컴퓨터 포렌식의 기술과 과제

- Technology and Tasks of Computer Forensics for Suppressing Computer Crime -

이 상 락 *
Lee Sang Rak
신 승 호 **
Shin Seung Ho
박 상 민 ***
Park Sang Min

Abstract

The soaring increase in the number of Internet users combined with the constant computerization of business process has created new opportunities for computer criminals and terrorist. Fortunately, the computer security field is also progressing at a brisk rate. In particular, the field of computer forensics brings new ways of preserving and analyzing evidence related to computer crime.

Computer forensics is a new emerging professions of the 21st century. It is the collection, preservation, analysis, and presentation of computer related evidence. For this reason, the various technology of computer forensics is regarded as a powerful tool for suppressing computer crime.

Our aims is to introduce the overview of computer forensics technology. We also present the survey results of the state of the art of computer forensics in the domestics and of foreign country.

Keyword : Computer Forensics, Chain of custody, Master copy, Second Copy

† 이 논문은 2003년도 교내 학술 연구 조성비 지원에 의해 수행되었음

* 인천대학교 컴퓨터공학과 부교수
** 인천대학교 컴퓨터공학과 교수
*** 인천대학교 산업공학과 교수

1. 서 론

인터넷 기술의 발전은 네트워크 및 컴퓨터 시스템 기술의 발전과 더불어 정보화 사회를 앞당기고 있으나 이에 따르는 역기능 또한 무시할 수 없다. 특히 인터넷을 통한 범죄는 예전처럼 해커의 장난 수준을 넘어서서 의도적으로 특정인 또는 특정기업의 정보를 빼내 악용하거나 파괴하고 있는 수준이다.

컴퓨터 포렌식은 컴퓨터와 관련이 있는 분쟁이나 범죄에서 어떤 주장의 정당성을 입증하기 위한 증거나 자료를 조사 · 수집하는 방법이나 기술을 다루는 학문이다.

우리의 일상생활이나 경제활동 등이 컴퓨터와 밀접한 관계를 가지게 되면서 이것과 관련되는 분쟁이나 범죄도 급격히 증가하고 있다. 2002년도에 발표된 [5]의 자료에 의하면 컴퓨터와 직접적으로 관련이 있다고 볼 수 있는 사이버 범죄가 그 이전 5년간에 걸쳐 무려 275배가 증가하였다고 한다. 그간 컴퓨터의 보급이 더욱 확대 되었고 관련 기술을 가진 사람들도 더욱 증가하였을 것이므로 범죄건수도 대폭 증가하였을 것으로 쉽게 추측할 수 있다.

일반 범죄 수사에서 지문 등의 경우 증거를 획득, 처리, 보관, 분석 등의 처리과정 및 방법이 확립되어 있듯이 컴퓨터 관련 수사에서 있어서도 증거물 처리에 대한 절차와 방법이 확립되어야 하며, 이러한 과정을 통하여 나온 결과 및 결론은 합리적이어서 관련 전문가들뿐만 아니라 법정에서도 동의 할 수 있어야 한다. 따라서 컴퓨터와 관련이 되는 분쟁이나 범죄에서 전자적 증거나 자료의 수집은 매우 중요한 이슈로 대두되고 있으며 따라서 컴퓨터 포렌식의 중요성 또한 설득력을 더해가고 있다.

이러한 맥락에서 본 연구는 컴퓨터 포렌식과 관련되는 국내의 현황을 국외와 비교하면서 살펴본다. 그리고 더하여 향후의 전망과 과제를 진단한 후 과제의 해결방안을 제시한다.

본 연구의 구성은 다음과 같다.

2절에서는 먼저 컴퓨터 포렌식의 유래와 정의를 살펴보고자 한다.

3절에서는 컴퓨터 포렌식의 기능과 방법을 살펴본다.

이어서 4절과 5절에서는 국내의 현황을 비교 분석한 후 향후의 과제를 도출하고 과제의 해결 방안을 제시한다.

2. 컴퓨터 포렌식의 정의

2.1 컴퓨터 포렌식의 유래

"컴퓨터 포렌식"이라는 용어는 1991년 미국 오레곤주 포트랜드에서 IACIS (International Association of Computer Specialists)에 의해 열린 훈련 과정 중에 만들어 졌다. 그 이후 컴퓨터 포렌식은 컴퓨터 보안 분야나 법조계에서의 대중적인 주제로 되었다[2]. 다른 법과학(forensic science)과 마찬가지로 컴퓨터 포렌식은 과학에 대한

법의 적용을 다룬다. 이 경우 관련되는 과학은 당연히 컴퓨터 과학이다. 때문에 어떤 사람은 이것을 법 컴퓨터 과학이라 부른다. 컴퓨터 포렌식은 또한 컴퓨터 하드 디스크 드라이브의 검시(autopsy)로 묘사되기도 한다.

그 이유는 컴퓨터 데이터가 저장된 갖가지 수준의 저장 장치를 분석하기 위해서는 전문 소프트웨어 도구와 기술이 요구되기 때문이다.

2.2 컴퓨터 포렌식의 정의

컴퓨터 포렌식은 증거를 위하여 컴퓨터 저장매체(하드디스크, CD, 디스켓, 테이프 등)를 조직적이고 질서 정연하게 조사 하는 과정이다[1].

조사 전문가에 의한 철저한 분석은 컴퓨터 사용자의 어떠한 행동도 재연할 수 있다.

다른 말로 말하면 컴퓨터 포렌식은 컴퓨터와 관련이 있는 증거의 수집, 보관, 분석 및 제시를 의미한다. 컴퓨터 증거는 범죄사건이나 일반인들간의 분쟁 및 고용자와 피고용자간의 분쟁 등에서 유용하게 사용된다.

일반적으로 컴퓨터에는 사람들이 알고 있는 것 보다는 훨씬 많은 정보가 담겨있다. 또 그러한 정보를 완전하게 제거하는 일은 생각보다 훨씬 어렵다. 이러한 이유 때문에 컴퓨터 포렌식은 유실되거나 제거된 정보에 대한 증거를 비롯, 그 정보가 의도적으로 제거되었다 하더라도, 발견하거나 나아가서 완전히 복구 할 수도 있다.

컴퓨터 포렌식은 데이터 복구와 비교하여 같은 종류의 기술이나 소프트웨어를 사용하지만 훨씬 복잡한 과정을 거친다. 데이터 복구에서의 목표는 잃어버린 데이터를 검색하는 것이다. 그러나 컴퓨터 포렌식에서의 목표는 데이터를 검색하고 그것에 관한 정보를 가능한 많이 해석하는데 있다.

2.3 Computer Forensics의 해석

컴퓨터 포렌식에 대한 명칭은 웹에서 "Computer Forensics"라는 단어를 검색하여 보면 영어를 그대로 쓰거나 우리말의 발음나는대로 컴퓨터 포렌식으로 부르고 있다.

"Forensic"은 "법정에서 쓰이는"의 뜻이라고 사전에 기술되어 있다. 또 우리가 종종 듣는 법의학이란 용어는 영어로 Forensic Medicine이다. 앞에서 Computer Forensic은 Forensic Computer Science라고도 불리운다고 하였으므로 이를 곧바로 해석하면 법 컴퓨터 과학이라고 해야 할 것이다. 그러나 이를 더 줄여 법 컴퓨터학이라 하여도 큰 혼란은 없을 것이라 생각된다.

컴퓨터 포렌식이 향후 더욱 보편화 될 것이고 그러면 어차피 우리글로된 명칭을 정하는 일이 필요하다. 따라서 본 연구자는 컴퓨터 포렌식을 법 컴퓨터학이라고 명칭하기를 제안한다.

3. 컴퓨터 포렌식의 기술

3.1 데이터 복구

데이터 복구는 각종 저장매체들이 고장이 나서 정상적인 방법으로는 이들로부터 데이터를 읽어 낼 수 없는 경우에도 제거되거나 접근 불가능한 데이터를 추출해 내는 과정이다. 저장 매체들에는 하드디스크 드라이브, 착탈식 매체, 광학식 장치나 테이프 카트리지 등이 포함된다.

데이터에의 접근 불가능의 원인으로는 소프트웨어의 문제, 컴퓨터 바이러스, 기계적 또는 전기적 기능 장애, 그리고 사람의 부주의한 행동이 있을 수 있다. 숙련된 전문가라면 데이터의 손실의 원인이 무엇이던 간에 손실된 데이터의 80~85%를 성공적으로 복구할 수 있다고 한다.[3]

그러나, 하드 디스크 드라이브가 아주 심하게 손상되어 데이터의 복구가 불가능한 경우도 있다. 즉 읽기/쓰기 헤드가 완전히 부서져서 데이터가 파괴될 정도로 저장 매체가 긁혀버린 경우에는 데이터의 복구가 불가능하다.

컴퓨터 포렌식은 범죄현장에서 압수된 컴퓨터로부터 증거자료를 수집하는 일을 다룬다. 주된 관심은 저장매체의 이미 제거된 파일의 복구, 파일 슬랙이나 빈공간의 탐색 및 수집된 정보의 보존 등을 포함한다.

3.2 증거의 보존과 이미징 작업

저장 매체의 이미징이란 컴퓨터 하드 디스크에 있는 모든 저장 공간을 다른 저장 매체에 옮겨서 복제하는 작업을 말한다.

적어도 두 개의 복제품이 증거가 되는 컴퓨터로부터 얻어져야 한다. 하나는 컴퓨터의 소유자가 보는 앞에서 봉인된 후 안전한 장소에 보존된다. 이것은 주복제품(master copy)이 되며 차후에 부복제품(second copy)을 사용하여 분석된 증거에 대한 의문의 생길 때 법정으로부터의 지시하에 조사를 위하여 개봉된다.

만약 법 집행관에 의해 컴퓨터 자체가 압수되고 안전한 장소에 보관된다면 이것이 바로 가장 최선의 증거가 될 것이다. 그러나 컴퓨터가 압수되지 않았다면 주복제품이 가장 최선의 증거가 된다.

이미징 작업은 컴퓨터 매체의 저장용량이 급격하게 늘어남으로서 하나의 난관에 봉착하고 있다. 즉 복제품을 만드는데 많은 시간이 소요된다는 점이다. 따라서 증거를 안전하게 보존할 수 있는 다른 방법이 강구될 필요성이 있다.

컴퓨터 증거는 손상되기 쉬우며 변경이나 삭제 등에 취약하다. 때문에 확보된 증거는 안전하게 보존할 수 있는 방법이 필요하다.

3.3 디지털 증거의 수집

디지털 증거의 수집 과정은 중요한 증거의 소재를 파악할 수 있게 할 뿐만 아니라 그 증거에 대한 무결성과 신뢰성을 유지할 수 있도록 한다. 증거 수집과정에서 중요한 것은 타이밍(timing)이다.

의심스러운 컴퓨터의 압수가 지연되거나 컴퓨터를 계속 사용할 수 있도록 방치 하는 것은 결정적인 자료의 파괴를 가져올 수 있기 때문이다. 이러한 사태를 피하기 위하여 다음과 같은 행동 수칙이 필요하다.

○ 의심스러운 컴퓨터가 있다 하더라도 이를 켜거나 조사하려는 시도는 하지 말아야 한다.
○ 증거를 포함하고 있을 만한 모든 장치를 파악한다.
○ 회사 내부의 모든 컴퓨터를 안전한 장소에 격리한다.
○ 의심스러운 매체에 대하여는 이미징 작업을 한다.

3.4 증거의 규칙

전자적 증거를 수집하는데 유념해야 할 5가지 규칙이 있다. 이들은 증거가 유익한 것이 되기 위하여 갖추어야 할 5가지 성질과 관계된다.

- 인정가능성

증거 자료의 인정 가능성은 법정이나 또 다른 경우에서도 가장 중요한 규칙이다. 이 규칙을 준수하지 못하는 것은 증거를 확보하지 못한 것과 동등하다.

- 정당성

증거를 사건과 밀접하게 결부시키지 못하면 어떤 것을 증명하기 위하여 그 증거를 사용할 수 없다. 그 증거가 사건에 적절한 방법으로 관련되어 있음을 보일 수 있어야 한다.

- 완전성

사건의 한 면만을 보이는 증거를 수집하는 것은 충분하지 않다. 무죄를 증명하려는 사건의 경우 침입자의 행동을 증명하기 위한 자료를 수집해야 하는 것은 물론, 그들의 무구성을 증명할 수 있는 증거도 필요하다. 예를 들어 침입자가 로그인 한 시각에 로그인을 한 또 다른 사람이 있는지 그리고 전자가 사건을 저지르지 않았다고 생각하는 이유를 보일 수 있어야 한다.

- 신뢰성

수집한 증거는 신뢰 할 수 있어야 한다. 증거 수집과 분석 절차가 증거의 정당성이나 진실성에 의심을 받도록 해서는 안된다.

- 신용성

제시하는 증거는 재판관들이 명확히 이해할 수 있고 믿을 수 있어야 한다. 메모리에서 덤프한 이진자료를 그대로 제출하는 것은 재판관이 그것이 무엇을 의미하는지를 전혀 모른다면 아무 의미도 없다. 또, 그 자료를 사람이 이해할 수 있는 형태로 만들어 제출한다면 원본의 이진 자료와의 관련성을 보일 수 있어야 한다. 그렇지 않으면 재판관은 그 자료가 위조되었는지 여부를 알 수 있는 방법이 없기 때문이다.

3.5 훼손의 통제

데이터가 일단 수집되면 그것은 훼손이 되지 않도록 해야 한다. 조사를 할 때는 원본은 절대로 사용하지 않고 검증된 복제본을 사용한다.

데이터가 훼손되지 않은 채 보존하기위한 좋은 방법은 "Chain of Custody"를 유지하는 것이다. "Chain of Custody"란 원래의 복사본이 일단 만들어지면 그 후 그것이 법정에 제출되기 전까지 그에 대해 행해진 모든 일들에 대한 리스트를 작성하는 것을 말한다.

3.6 포렌식 도구

포렌식 도구는 미국과 영국을 중심으로 발전되고 있는 상황이다. 도구들은 하나의 기능만을 갖는 도구도 있으며, 여러 기능을 통합적으로 제공하고 있는 도구도 있다. 컴퓨터 포렌식을 제공하는 도구는 표 1과 같다.[10]

포렌식 도구 개발업체로는 유타 주 프로보 소재의 액세스데이터 디벨롭먼트(AccessData Development), 캘리포니아 주 파사데나 소재의 가이던스 소프트웨어(Guidance Software), 오리건 주 그레샴 소재의 뉴 테크놀러지스 아모(New Technologies Armor) 등이 있으며, 여기에 대학교 연구소의 개발자들과 매사추세츠 주 캠브릿지 소재의 앳스테이크(@Stake)같은 보안 컨설턴트 등도 있다. 이들 업체는 대상 컴퓨터 내부의 저장장치에 남겨져 있는 수 기가바이트의 데이터를 분석하는 강력한 도구를 제공한다.

4. 현황과 전망

컴퓨터 포렌식은, 한때는 일부 법을 집행하는 사람들에게 국한된 분야였지만, 현재는 한창 번창하는 사업으로 자리 잡았다.

전자적 증거가 법정에서 더욱 많이 사용되고 기업은 산업 스파이 활동이나 다른 해악이 되는 활동에 컴퓨터가 사용되는 것에 보다 많은 관심을 가지게 되면서 컴퓨터 포렌식에 대한 서비스의 요청을 폭발적으로 증가하고 있다. [3]에 의하면 범세계적인 컴퓨터 공격을 저지하기 위해서는 적어도 50,000명 이상의 컴퓨터 범죄 대응 인력을 양성할 필요가 있다고 한다. 아마 민간 부분의 수요 인력까지도 감안한다면 향후 전문 인력의 부족 현상은 더욱 심각해 질 것이다.

< 표 1 > 컴퓨터 포렌식 도구

도구 이름	지원 운영체제	기능	공개 여부
chkrootkit	Linux/Unix	루트킷 탐지	공개
TCT	Linux/Unix	데이터 수집	공개
lsof	Linux/Unix	파일 리스팅	공개
CRCMD5	DOS	서명	비공개
DIBS family	DOS	파일 리스팅	비공개
disksearch3	DOS/Windows	디스크 조사	비공개
disksig	DOS	서명	비공개
DriveSpy	DOS	디스크 조사	비공개
FileCNVT	DOS/Windows	파일 리스팅	공개
FileList	DOS/Windows	파일 리스팅	비공개
Filter	DOS	필터	공개
Filter_I	DOS	디스크조사	비공개
ForensiX	Mac/DOS/Windows/Unix	통합	비공개
GetFree	DOS/Windows	디스크조사	비공개
GetSlack	DOS/Windows	디스크조사	비공개
IMAGE	DOS/Windows	이미지생성	비공개
NTAVIEW	DOS/Windows	디스크조사	공개
NTI-DOC	DOS	감시	비공개
PDBLOCK	DOS	증거보존	비공개
ProDiscover DFT	DOS/Windows /NT	디스크조사	비공개
PTable	DOS	파티션테이블 분석	비공개
Seized	DOS/Windows	증거보존	비공개
ShowFL	DOS/Windows	분석시간	공개
TextSearch Plus	DOS	디스크조사	비공개

이러한 배경에서 미국과 우리나라에서의 포렌식과 관련이 있는 기업, 기관 및 교육 현황을 조사하였다. 조사는 인터넷 검색 방법을 이용하였기 때문에 개략적 수준에 불과하다. 조사 결과, 한국 정보보호진흥연구원 기술부에서는 정보통신망을 운영하는 기관의 침해사고 대응팀 및 침해사고 대응팀 협의회(CONCERT)를 운영하여 정보교류, 기술협조 등의 협조체제를 통해 침해사고 예방 및 확산방지를 도모하고 있으나 국내 기업은 몇몇 대기업을 제외하고는 거의 없는 실정이며, 최근 전문가 들이 연합으로 구성한 사이버 포렌식 협회가 발족되어 인력양성 및 연구가 진행되고 있으나, 선진국과는 달리 컴퓨터 관련범죄 발생시 전적으로 외부 용역이나 수사기관에 의존하고 있다. 특히 기업들은 사이버 범죄사고 발생시 보안 유지에만 급급하고 수수방관 하고 있는 것이 현실이다. 따라서 기업에서도 정확한 피해 상황을 조사, 원인을 분석하여 사고를 예방하고 법적 대응을 할 수 있는 사이버범죄 전문조사요원을 양성하여 급변하는 사이버 범죄에 능동적으로 대처하여 기업의 소중한 디지털 자산을 보호하는데 있어 보다 적극적으로 대처하여야 한다.

4.1 미국

1) 기관

미국에서 컴퓨터 포렌식에 관련되는 기관으로는 다음을 찾아볼 수 있다.

· RCFL(Regional Computer Forensics Laboratory)

미국 최초로 여러 정부 부서에서 공동 설립한 지역 컴퓨터 전문 연구소

· CERT

국제적인 보안 관련 권고안을 발표하고 해결해 주는 전문기관

· IOCE(International Organization on Computer Evidence)

국제적인 법 컴퓨터학과 관련 된 정보를 교환하고 새로운 이슈들에 대해서 토론하는 기관

· IACIS(International Association of Computer Investigative Specialists)

컴퓨터 자문 관련 인증서를 발급한다.

2) 산업계

포렌식 관련 기업은 상당히 많다.

한 가지 특징은 이들 기업이 포렌식 소프트웨어를 공급하고 서비스를 제공할 뿐만 아니라 교육과 훈련 기능도 수행한다는 점이다.

3) 대학

센트럴 플로리다 대학에서 법 컴퓨터학과 관련하여 컴퓨터 자문 분야의 학위를 제공하고 있다.

· Guilford College, Nc Wesleyan College

미국 북 캐롤리나 주에 있는 두 대학에서 컴퓨터 포렌식과 관련되는 코스가 개설되어 있다. Guilford College에서는 Justice and Policy Studies Dept.에서 선택 과목인

Special Topics가 개설되어 있고 Nc Wesleyan College에서는 법학과의 응용 범죄학(Applied Criminology)과목이 개설되어 있다. 법학을 전공하지 않는 학생도 수강할 수 있으며 별다른 선행조건도 요구되지 않고 있다. 이와 관련한 자세한 사항은 [5]에서 찾아볼 수 있다.

4.2 우리나라

1) 기관

우리나라에서 컴퓨터 범죄와 관련되는 기관은 상당수가 있다. 그러나 이들 기관은 현재로서는 그들의 역할이 주로 인터넷 범죄나 침해사고, 사이버 테러와 관련되어 있다.

· 사이버 포렌식 협회

이 협회는 사이버 범죄를 정확히 분석하고 예방차원의 기능을 극대화하고자 보안업계의 전문가들이 모여서 인터넷 사회에서 가장 중요한 정보자산의 보호와 그 피해에 대한 정확한 분석을 위해 서로의 지식과 경험을 공유하며 더 큰 발전을 도모하는 협회이다.

2) 업계

업계 또한 대부분이 컴퓨터 보안과 관련이 있다. 그러나 훼손된 컴퓨터 자료를 복구하는 기술을 서비스하는 업체를 2~3개 검색으로 찾아볼 수 있으며 이들 회사들이 컴퓨터 포렌식과 관련되는 서비스를 제공할 수 있다.

4.3 전망과 과제

우리나라에서도 컴퓨터 포렌식에 대한 관심과 서비스에 대한 요구도 점차 증대 될 것으로 전망된다. 특히 [4]의 자료에 의하면 북한이 사이버 정보전을 위한 인터넷 부대를 조직 운영하고 있다고 한다. 이점에 비추어 우리도 이에 대한 대비책이 시급하다 하겠다.

컴퓨터 포렌식에 대한 업계의 관심은 고조되고 있는데 비하여 학계에서의 이에 대한 관심은 아직 미미해 보인다. 그러나 컴퓨터 보안이나 네트워크 보안, 암호화 등에 대한 학계의 관심이 집중적으로 증가하고 있음에 비추어 조만간 관심의 방향이 컴퓨터 포렌식으로 옮겨올 가능성이 크다 하겠다. 이를 대비하여 컴퓨터 포렌식 전문가를 양성하기 위한 교육훈련 과정의 개발이 필요하며 훈련생들이 저렴한 비용으로 실습할 수 있는 관련 프로그램들이 개발되고 무상 사용이 가능한 환경이 조성 되어야 할 것이다.

5. 결론 및 제언

본 연구에서는 급속히 확대되고 있는 컴퓨터 범죄에 대한 증거물을 확보하고 이를 체계적으로 분석하는 기술인 컴퓨터 포렌식의 기술과 발전 전망에 대하여 연구하였다.

사이버 환경이 구축되면서 사이버 범죄도 증가하고 있고, 특히 해킹 및 바이러스의 위험도 급속히 증가하고 있는 실정이다. 이런 시점에 컴퓨터 포렌식은 정보화로 인한 역기능을 방지할 수 있는 방법이 될 것이라 판단된다.

컴퓨터 포렌식은 컴퓨터 증거에 관한 학문이다. 구체적으로 말하면 법정에서 받아질 수 있도록 증거를 검출하고 보존하고 문서화 하는 작업이다.

컴퓨터 포렌식은 폭발적으로 성장하는 산업으로 자리잡아가고 있다. 따라서 이 분야의 전문가에 대한 수요 또한 폭발적으로 증가한 것으로 예상된다. 이에 대비하여 학계는 전문가를 양성하기 위한 교육계획을 수립하고 필요한 환경을 조속히 조성할 필요가 있다.

특히 운영체제가 디스크를 쓰고 파일을 관리하는 데 있어 독자적인 방식을 갖고 있기 때문에, 포렌식 도구는 PC 형태의 그래픽 인터페이스를 통해 분석용 디스크 복사본을 만들어 거기에 무엇이 있는가를 조사하여야 한다.

향후 연구로는 법과학과 컴퓨터 기술자들의 협력으로 컴퓨터 과학을 법에 적용하기 위한 컴퓨터 포렌식에 대한 철저한 분석 및 어떤 운영체제에도 적용 가능한 개선된 포렌식 도구 개발을 위한 연구가 선행되어야 한다.

8. 참 고 문 헌

[1] John k. Vacca, "Computer Forensics : Computer Crime Scene Investigation", CHARLES RIVERS MEDIA, INC, 2002

[2] "Computer Forensics," Rehman Technology Services, Inc., 18950 U.S. Highway 441, Suite 201, Mount Dora, Florida 32757,2001.

[3] Judd Robbins, "An Explanation of Computer Forensics," National Forensics Center, 774 Mays Blvd. #10-143, Incline Village, NV 89451,2001.

[4] Peter Sommer,"Computer Forensics: An Introduction," Virtual City Associates, PO Box6447, London N4 4RX, United Kingdom,2001. Academic URL: http://csrc.lse.ac.uk.

[5] David Icove, Karl Seger, William VonStorch, "Computer Crime", O'Reilly & Associates, Inc.

[6] Neil Barrett, "Digital Crime", Kogan Page

[5] http://user.chollian.net, "사이버 범죄 관련정보", 2002. 1. 18

[6] http://www.forensics-intl.com/def.html, "Computer Forensics Defined".

[7] http://faculty.ncwc.edu/toconnor/4261

[8] 정계옥, "감사로그를 이용한 포렌식 시스템 설계 및 구현" ,전남대 대학원, 2003.02

[9] 강유, "사이버 범죄 소탕작전 컴퓨터 포렌식 핸드북", 에이콘출판사, 2003.

[10] 황현욱, 김민수, 노봉남, 임재명, "컴퓨터 포렌식스: 시스템 포렌식스 동향과 기술", 한국정보보호학회, 2003

[11] 이형우, 이상진, 임종인, "컴퓨터 포렌식스 기술", 정보보호학회지, Vol.12, No.5

저 자 소 개

이 상 락 : 현재 인천대학교 컴퓨터공학과 부교수로 재직 중이며,
(주)시큐리티 테크놀리지스 부설 정보보호기술연구소장 역임
관심분야는 컴퓨터 그래픽스(그래픽 알고리즘, 기하모델링) 등이다.

신 승 호 : 현재 인천대학교 컴퓨터공학과 교수로 재직 중이며,
관심분야는 컴퓨터 그래픽스이다.

박 상 민 : 현재 인천대학교 산업공학과 교수로 재직 중이며,
관심분야는 경제성공학, 설비관리, 신뢰성공학, 원가공학