韓國 컴퓨터情報學會 2008 제38차 하계학술발표논문집
第16卷 第1號, 2008. 06.

안티 디지털 포렌식에 대한 대응 기술 연구

이 규 안*, 박 대 우**, 신 용 태***

A Study on Rivalry Technology of Anti-Digital Forensic

Gyu-an Lee*, Dae-woo Park*, Young-Tae Shin***

요 약

디지털 포렌식이 활성화 되고 수사에서 활용하는 사례가 증가함에 따라 기업과 개인을 비롯한 범죄혐의자들의 이에 대응하기 위한 기술도 증가하고 있다. 이를 안티포렌식 또는 항포렌식이라고 하는데 이는 디지털 자료의 변조, 파괴, 은닉 등으로 나누어 볼 수 있다. 본 논문에서는 범죄 수사현장에서 필요한 안티포렌식에 대응하는 기술인 위·변조된 데이터 추출 기법, 슬랙 영역의 숨겨진 데이터 추출 기법, 스테카노 그래픽 추출 및 분석 기법, 암호 복호화 기법, 삭제된 데이터 및 파괴된 데이터 복원 기법을 소개하고, 이에 대한 대비책을 제시한다. 본 연구를 통하여 첨단 범죄 수사관들이 안티디지털포렌식에 대한 새로운 디지털 증거의 추출과 분석에 기여하여 컴퓨터 및 첨단 범죄에 대한 디지털 포렌식 기술로 새로운 수사의 방향을 제시 할 수 있을 것이다.

▸ Keyword : 안티-디지털포렌식, 디지털 증거, 디지털 범죄. Digital Evidence, An-ti Forensics. Computer Crime

• 제1저자 : 이규안
* 숭실대학교 대학원 컴퓨터 학과 **호서대학교 벤처 전문대학원 ***숭실대학교 컴퓨터 학부

Ⅰ. 서 론

지난 세월동안 범죄 수사의 압수·수색은 범죄자의 범죄행위를 입증하는 증거로서 물증을 찾아내는데 이는 보통 도구, 장부, 부책 등의 형태를 가지고 있는 것들이었다. 시대가 변함에 따라 기존에 장부, 부책등에 사용하던 내용들이 눈에 보이지 않는 이진화된 숫자로된 데이터 정보화됨에 따라 압수·수색의 범위는 디지털 증거가 대부분을 차지하게 되었으며, 이는 범죄 혐의자들의 유비쿼터스 시대를 이용한 첨단 범죄에 대한 법적인 증거 자료로 포렌식[1]을 사용한다.

하지만 불법적인 범죄자들이 범죄에 대한 모의를 하고, 준비를 하거나 다른 범죄자에게 연락을 하는 등, 행동반경을 나타내는 여러 가지 정보들이 디지털화 되어 저장되고 이러한 디지털증거들은 공판주의[2]와 인권주의에 입각한 결정적인 증거로 채택되어 지고, 범죄자들도 이러한 디지털 증거로 인하여 재판에서 활용된다는 사실을 알게 되어 디지털 증거를 없애거나 위변조하는 안티포렌식을 이용하게 된다.

안티포렌식 또는 항포렌식은 포렌식에 대응하는 말로써 디지털 증거를 사용하지 못하게 되거나 또는 사용되더라도 자기에게 유리한 부분만 사용되도록 하는 기술로서, 데이터의 위·변조, 은닉, 암호사용, 파괴 등을 말한다고 할 수 있다[3].

따라서 범죄자들이 불법적인 행위로 인하여 안티포렌식 또는 항포렌식을 통하여 범죄 사실이나 불법적인 활동 등을 은익하거나, 재판의 증거로 채택되지 못하게 조작을 가할 수 있다. 따라서 불법적인 증거자료나, 재판에서의 증거 자료로서의 채택을 위한 포렌식 자료로 상용되기 위해서는 안티포렌식 또는 항포렌식에 대한 실증적인 연구가 필요한 시점이다.

본 논문에서는 이러한 안티 디지털 포렌식의 일반을 소개하고, 이에 대응하는 기술을 제시함으로써 범죄 혐의자들에게 디지털 정보는 꼭 증거를 남김으로 완전범죄는 없으며 범죄자는 잡힌다는 인식을 심어줌으로써 범죄의 동기를 줄이고, 수사관들에게는 첨단 디지털 포렌식 기술로 새로운 수사의 방향을 제시 할 수 있을 것이다.

Ⅱ. 관련연구

2. 1. 디지털 포렌식

디지털 포렌식은 '디지털'과 '포렌식'의 합성어로서 디지털 증거의 수집과 분석에 관한 일련의 절차와 기술을 통칭하는 것으로서 디지털 증거에 대한 과학적인 조사와 기술을 다루는 분야로서 근래의 공판주의와 더불어 인권을 보호하기 위한 방안으로 급부상하고 있는 학문적이며 실용적인 수사의 한 패러다임이라고 할 수 있다. 디지털 포렌식은 종류를 학문적으로 구분 할 수는 없지만 보통, 디스크 포렌식, 네트워크 포렌식[4], 데이터베이스 포렌식, 모바일 포렌식[5], 해상 디지털 포렌식[6]으로 구분하기도 하고, 휘발성 데이터의 추출하는 기법과 비휘발성 데이터를 추출하는 기법으로 구분 한다[7]. 디스크 포렌식은 보통의 컴퓨터에 저장된 데이터를 추출하고 분석하는 기법으로 하드디스크, 플로피디스크, CD-ROM등에 저장된 정보를 추출하는 것이며, 네트워크 포렌식은 네트워크 상에서 발생하는 범죄에 대한 증거를 추출하고 분석하는 것으로 로그분석, 헤더분석, 접속기록, 전송기록 및 전송내용 등에 대한 정보를 추출하게 된다. 데이터베이스 포렌식은 기업의 전산화가 대형화되고 글로벌 화됨에 따라 기업 회계, 결제 서버 및 메일 서버 등에 저장된 정보를 추출하고 분석하며, 모바일 포렌식은 휴대폰 등의 모바일 장비 속에 저장된 정보를 추출하여 분석하는 기법을 말한다. 근래에는 해상 디지털 포렌식이 등장하게 되었는데 선박에 설치된 컴퓨터 등의 장비에 저장된 항해기록, 통신기록 등이 선박사고가 발생하였거나 국제적인 분쟁에서 중요한 증거가 되기 때문에 디지털 정보를 추출하고 분석하는 분야다[8]. 기본적으로 일상생활 속에서 정보의 디지털 데이터가 증가함에 따라 디지털 데이터의 추출과 분석, 그리고 은닉되거나 삭제된 데이터를 추출하고 복원하는 디지털 포렌식 전문가는 억대의 연봉을 받는등 고급 보안 기술자로 각광을 받고 있다.

2. 2. 안티 디지털 포렌식

2. 2. 1. 디지털 증거 위·변조 기법

통상 디지털로 작성된 문서들은 작업이 진행되거나 완료되는 과정에서 고유한 헤더의 포맷과 확장자를 가지고 있다.

<표 1> 문서의 확장자

문서명	확장자	용도	비고
한글	HWP	한글문서	국내
훈민정음	GUL	한글문서	국내
MS워드	DOC	한글문서	국외
MS파워포인트	PPT	발표문서	국외
MS엑셀	XLS	계산문서	국외

한글 문서의 경우 *.HWP를 확장자를 사용하며, 다른 문서들과 파일들도 고유한 확장자를 통하여 정보를 추출·분석을 하게 되는데 이때 확장자를 변경하게 되면 일반적인 검색을 진행할 수 없게 된다. 통상적인 탐색기의 검색 기능을 이용하여 한글을 검색할 경우 *.hwp를 입력하게 되고 이때 확장자를 변경해 놓은 한글문서는 검색이 되지 않는다. 이러한 특성을 이용하여 은닉하여야 할 문서의 경우 실행파일의 확장자(exe)나 배치파일의 확장자(bat)를 사용하게 되면 전혀 다른 파일로 인식하게 된다.

2. 2. 2. 슬랙영역의 은닉 기법

일반적으로 물리적인 하드 디스크를 사용하기 위해서는 논리적으로 파티션의 작업등을 수행하게 되고 이를 다시 포맷을 하여 사용하게 된다[9]. 이때 만들어진 저장공간인 클러스터에 정보를 저장하게 되는데 이때 클러스터의 영역이 8Kbyte의 영역으로 나누어 진 후 5Kbyte를 사용하게 된다면, 다음 데이터는 다른 영역의 클러스터를 사용하게 되고 실제 3Kbyte의 슬랙영역이 남게 된다. 이러한 남은 공간에 대하여 정보를 저장하게 되면 일반적인 검색기법을 사용하는 기법으로는 데이터를 추출할 수 없게 된다.

2. 2. 3. 스테가노그래픽 기법

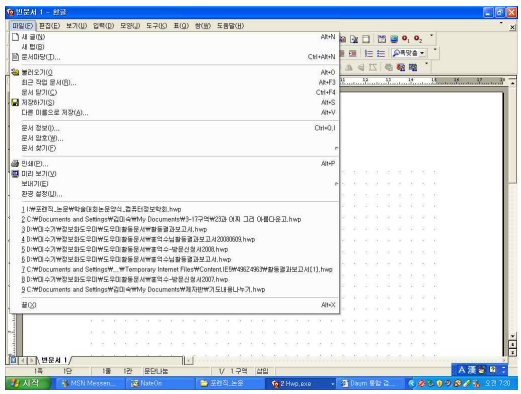
스테가노그래픽는 원래 저작권을 보호하기 위하여 그림파일등의 일정한 빈 공간에 자신의 정보를 심어놓고 보통 사용할 경우에는 표시가 되지 않다가 필요할 경우 추출하는 기법이다. 즉 그림의 경우에는 흰색의 바탕화면은 픽셀이라는 1Bit의 저장 공간에 흑백으로 표시하게 되고, 이러한 흑백의 점들이 모여서 문자나 그림으로 보여지게 된다. 256컬러인 경우에는 이러한 픽셀이 256Bit로 구성되어 다양한 색을 표시하게 되는데 이미지의 픽셀과 픽셀사이에 일정한 데이터를 분산하여 저장하거나, 검은색의 화면에 일정한 정보를 암호화한 후 픽셀 속에 감추기도 하고 음성의 경우 침묵하는 시간동안 발생한 정보의 흐름이 중단되거나 소량의 데이터가 전송되는 간격 속에 정보를 심는 방법이다. 이러한 스테가노그래픽을 사용하는 경우 보통 눈으로 보거나 귀로 들을 때는 아무런 이상 징후를 발견할 수 없게 된다. 빈라덴에 의한 911테러에서 비행기 폭파의 지령으로 사용되었다고 하지만 정확한 정보의 추출이나 분석이 되었다고 확인되지 않을 만큼 고도화된 은닉 기법이다.

2. 2. 4. 암호화 기법

개인정보의 중요도가 높아지고, 네트워크를 통한 침해사례가 증가함에 따라 과거에는 함께 공유하던 패스워드는 좀 더 복잡해지고 완벽한 기능을 제공하게 되었다. 이런 패스워드는 암호의 기능을 가지고 저장하게 되는데 일반적인 문서의 저장 및 압축시에도 암호기능을 이용하게 저장하게 된다. 문서의 경우 기본적인 기능으로 암호화 기능이 첨부되어 있고, 거의 모든 디지털 정보들은 암호화 기능을 이용하여 정보를 보호함에 따라 복호를 하지 못하면 디지털 증거의 추출 및 분석이 불가능하게 된다.

2. 2. 5. 디지털 증거의 삭제 또는 파괴 기법

인터넷을 사용하거나 문서를 작성하는 경우 캐시의 기능을 이용하여 검색의 속도를 높이게 된다. 또 인터넷을 사용하는 경우에는 웹 히스토리 기능이 존재하여 어떤 사이트를 자주 접속하며 이때 검색 등에 사용된 용어들이 Index.dat 파일에 저장하게 되고 이러한 파일들을 검색하면 범죄 혐의를 입증하는 중요한 단서가 되기도 한다[10]. 이러한 웹 히스토리나 캐시에 들어 있는 정보를 삭제하기 위하여 자동 삭제기능을 이용한다. 또 그림 1처럼 사용자들이 문서를 작성하거나 열람을 하게 되면 거의 모든 문서나 실행 프로그램의 임시 저장 공간에는 최근 사용문서나 열람문서를 보관하는 기능이 있으므로 이를 삭제하여 어떤 작업을 하였는지 분석할 수 없도록 한다.



<그림 1> 문서의 최근 작업 보기 기능

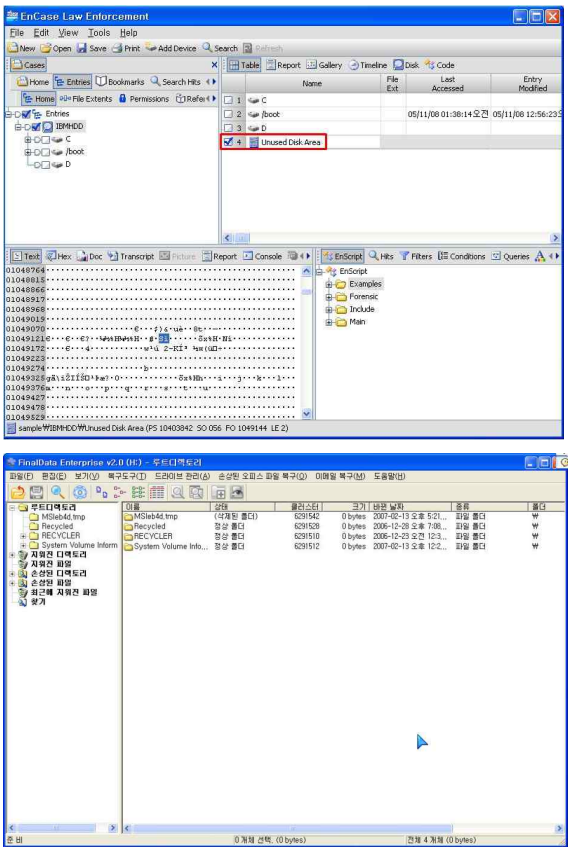
일반적으로 포맷을 하거나, 삭제 작업을 여러 번 반복한 후 덮어쓰기를 함으로써 디지털 증거를 분석을 할 수 없도록 하기도 한다. 또한 물리적으로 완전히 파괴하여 원상복구를 불가능하게 하는 방법이 있다. 데이터는 자성성분을 이용하여 하드디스크나 플로피디스크 등에 저장하게 되는데, 이런 데이터는 전자적으로 강한 자성체 안에 놓이게 되면 정보가 모두 사라지는 단점이 있다. 이러한 메모리기능의 취약점을 이용하여 강한 자석 성분을 접근시켜 자화시키는 방법으로 이러한 방식을 '디가우저'라고 하며, 물리적 파괴하는 방법으로 전기를 통하는 방법, 충격을 가하여 파괴하는 방법이 있다. 자성

체를 이용하는 방법, 전기를 통하는 방법과 충격을 가하여 파괴하는 방법은 모든 정보를 완전하게 없애는 방법으로 복구하기도 불가능 하지만, 차후 업무에 재활용할 수도 없다.

III. 안티디지털 포렌식 대응 기술

3. 1. 위·변조된 데이터 추출 기법

위·변조된 데이터라고 하더라도 헤더부분까지 모두 위·변조를 할 수는 없다. 데이터의 고유한 부분이 존재하므로 이를 비교하여 원래의 데이터와 같은 부분을 추출하게 된다. 현재 EnCase와 DEAS2 등의 종합적인 포렌식 도구에서 그림2와 같이 위·변조된 데이터를 별도로 추출하고 분석할 수 있도록 지원하고 있으며 상당한 수준의 위·변조된 데이터는 추출되고 있다. 이를 통하여 수사에 필요한 정보가 제공 되고 있다.



<그림 2> EnCase 와 DEAS의 데이터 추출 화면

3. 2. 슬랙영역의 숨겨진 데이터 추출 기법

하드디스크는 처음 만들어질 당시 디스크(Disk), 실린더(Cylinder), 트랙(Track), 섹터(Sector)로 구성되어지며, 이를 논리적으로 할당하게 된다. 논리적으로는 파티션(Partition), 파일(File), 레코드(Record), 필드(Field)로 구성되어지는데 이러한 물리적 구조와 논리적 구조 사이에서 발생한 슬랙영역에 숨겨진 데이터를 추출하는 것은 로우레벨 영역에서 가능한 일이다[11]. 이러한 것을 지원하는 것을 디스크 컨트롤로 이므로 이러한 컨트롤러에 접근하고 Live CD와 같은 프로그램을 이용한다면 데이터의 추출이 가능하다[12]. 일반적으로 고도화된 컴퓨터 전문가가 아니라면 이러한 슬랙 영역에 데이터를 은닉하지는 않겠지만, 앞으로 은닉의 한 방법으로 그 사용량이 증가할 것으로 예상되므로 추출하는 기법연구가 필요하다.

3. 3. 스테카노 그래픽 추출 및 분석 기법

스테카노 그래픽에 의하여 숨겨진 데이터를 찾는 방법은 프로그램에 의하여 추출할 수 밖에 없다. 또한 통상의 파일등이 스테카노 그래픽이 되어 있다고 확신할 수 없기 때문에 보통의 파일속에서 스태카노 그래픽이 되어 있는 파일을 찾는 것부터 수작업에 의하여 진행된다. 컴퓨터의 압수수색 당시에 스테카노 그래픽을 사용한 흔적이 있거나, 보통의 상식으로 보관하지 않아도 되는 파일들이 전송되거나 보관되어 있다면 일단 의심을 하고 분석 프로그램을 이용한다. 또 이러한 정보가 인터넷 등의 게시판이나 공지사항 등에 첨부된 이미지 속에 정보를 은닉할 수 있기 때문에 인터넷에 업로드한 흔적, 다운로드한 흔적과 업무의 연관성을 비교하는 등 검색을 통하여 의심이 가는 이미지 파일을 분류하게 되고 그 후에 스테크 분석을 통하여 이미지 속에 숨어 있는 정보를 추출하게 된다[13].

3. 4. 암호 복호화 기법

암호화가 진행된 데이터의 추출은 EnCase등의 디지털 포렌식의 분석도구로서 추출될 수 있다. 하지만 복호화를 지원하는 프로그램이 별도로 존재하지 않으므로 복호화 프로그램을 별도로 이용하여야 한다. 통상 4자리의 암호문을 복호화하는 데는 일반적인 컴퓨터를 이용할 경우 수 시간이 걸리지만 숫자이외의 특수문자를 이용하여 암호화를 하였을 경우에는 수 일이 소요되었다. 하지만 일반적으로 128bit이상의 암호화된 데이터가 숫자만으로 구성되었을 경우 이를 복호화하기에는 거의 불가능하며 이를 위하여 클러스터링 기법을 이용

하기도 하지만 실제 수사현장에서 이를 이용한 사례는 없다.

사람의 기억에 의존하는 데이터를 이용하여 암호화키를 만들어 특수한 기호를 이용하여 암호화를 한다면 어느 부분에 그러한 흔적을 남기게 되는데 메모의 흔적이나 가족사항, 생일 등을 조합하여 암호화 키를 추출하기도 한다.

3. 5. 삭제된 데이터 및 파괴된 데이터 복원 기법

삭제된 후 그 위치에 다른 데이터가 덮어 씌여 진 경우에는 이를 복원하기가 사실상 불가능하다. 국가정보원등에서 제공하는 정보시스템불용처리지침에 의하면 정보의 복원을 회피하기 위하여 최소 3회 이상 덮여 쓰기를 요청하고 있으며, 완전한 삭제를 위하여 (주)F사의 삭제프로그램의 경우 7회 이상 덮어쓰기를 지원하고 있는 것으로 되어있다. 하지만 500GBYTE이상의 대용량 하드디스크를 완전히 삭제하였다가 일정 회수 이상으로 덮어쓰기를 하는 것은 많은 시간이 소요되므로 사용량은 많지 않고, 보통 휴지통의 삭제기능과 폴더의 삭제기능의 경우 복원 프로그램을 이용하여 정보를 추출하게 된다. 또 Bit-To-Bit 방식으로 서로의 연관성을 찾아서 퍼즐식으로 연결 고리를 찾아서 문서를 복원하기도 하지만 시일이 많이 걸리는 단점이 있다.

Ⅳ. 결론

안티 디지털 포렌식은 범죄의 혐의를 은닉하고자 하는 심리나 개인의 정보에 대한 보호를 원하는 사람들의 심리를 나타내는 기법이라고 할 수 있다. 컴퓨터 및 네트워크의 발전과 더불어 디지털증거의 중요성은 더욱 높아지게 되었고, 디지털 증거가 법정에서 채택되는 사례가 증가함으로 안티 디지털 포렌식은 일반화 된 경향으로 나타나고 있다. 수사를 하는 입장에서는 이러한 디지털 포렌식의 여러 가지 회피 기법을 이해하고 깊이 있는 연구를 함으로써 이를 대응하여야 한다.

안티 디지털 포렌식에 대한 지속적인 연구를 함으로써 위·변조된 데이터뿐만 아니라 은닉되거나 파손된 데이터 정보를 추출하는 새로운 기법이 나타나야 한다. 이는 수사기관의 환경을 생각하고 컴퓨터 발전 등의 짧은 주기를 고려할 때 주도적인 입장에서 대응기술을 연구하고 실무에 적용하는 것은 매우 어려운 것이며 이를 해결하기 위하여 산학이 함께 하는 연구기관이 필요하며, 이러한 기관을 통하여 개발된 안티 디지털 포렌식 대응기술을 함께 공유하며 새로운 길을 모색하여야 한다. 수사의 목적에서 사용되는 이러한 기술들은 외부에 노출될 수 없는 특수한 환경임을 인식하고 대처할 때 완전범죄를 노리는 범죄자에 대한 경각심과 디지털 강국의 위상을 이어갈 수 있을 것이다.

향후 연구로는 스테가노그래픽이 된 파일이 보통 파일과 차이점을 비교하여 추출하게 함으로써 분리할 수 있는 방안에 대한 연구 및 추출된 스테가노그래픽 속에 정보를 추출할 수 있는 방안에 대한 연구와 암호화된 파일을 복호화 하는 방법에 대한 다양한 기법 연구, 덮어 씌어 진 데이터라고 하더라고 부분적으로 덮어 쓰여 지지 않는 부분을 추출하여 조합하는 부스러기 추출에 대한 연구가 진행되어야 할 것이다.

참고문헌

[1] 백승조, 심미나, 임종인, “국가 디지털 포렌식 법률체계와 국내외 디지털 포렌식 법제현황” 정보보호학회 논문지, 제18권 제1호, 2008. 2.

[2] 양근원. “형사절차상 디지털증거의 수집과 증거능력에 관한 연구” 경희대학교대학원박사학위논문, 2006. 2.

[3] Ryan Harris, "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensic problem", Digital Forensic Research Workshop, Digital Investigation Elsevier. 2006.

[4] 김혁준, 이상진, “분석사례로 본 네트워크 포렌식의 동향과 기술” 정보보호학회 논문지 제18권 제1호, 2008. 2.

[5] 성진원, 김권엽, 이상진. “국내 휴대폰 포렌식 기술 동향” 정보보호학회 논문지 제18권 제1호, 2008. 2.

[6] 이규안, 박대우, 신용태. “분쟁소지가 있는 공해상에서 디지털 포렌식을 이용한 해결방안” 한국컴퓨터정보학회 논문지, 제12권 제3호 pp138-145. 2007. 7.

[7] 이규안, 박대우, 신용태. “포렌식자료의 무결성 확보를 위한 수사현장의 연계관리 방법 연구” 한국컴퓨터정보학회 논문지, 제 11권 제6호, pp175-184. 2006. 12.

[8] 이규안, 박대우, 신용태. “분쟁소지가 있는 공해상에서 디지털 포렌식을 이용한 해결방안” 한국컴퓨터정보학회 논문지, 제12권 제3호 pp138-145. 2007. 7.

[9] 이홍재. “하드디스크의 이해” 전자신문사, 2003.

[10] 마취제로 남편 살해. 연합뉴스, 2008. 2. 29.

[11] 이석희, 박보라, 이상진, 홍석희. “안티 포렌식 기술과 대응방향” 정보보호학회논문지 제18권 제1호, 2008. 2.

[12] Kyle Rankin, "KNOPPIX HACKS", O'RELLY, 2005.

[13] 테러가 인터넷 속에 숨을 때. ADAM COHEN (TIME). Joins CNN.com 한글뉴스. 중앙일보.

http://news.joins.com/cnn/2001/11/11/20011
11101. html. 2001. 11. 11.

저 자 소 개

이 규 안

2006년 숭실대학교 정보과학대학원 졸업 (공학석사)
2006년 숭실대학교 컴퓨터학과 재학 (박사과정)
2000년 벽성대학 정보통신과 겸임교수
2002년 대검찰청 중앙수사부 컴퓨터 수사과근무
2005년 대검찰청 디지털수사담당관실 모바일 분석 팀장
<관심분야> 유비쿼터스 보안, 디지털 포렌식, 해상 디지털 포렌식, 모바일 포렌식

박 대 우

1998년 숭실대학교 컴퓨터학과(공학석사)
2004년 숭실대학교 컴퓨터학과(공학박사)
2000년 매직캐슬정보통신 연구소 소장, 부사장
2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수
2006년 정보보호진흥원(KISA) 선임연구원
2007년 호서대학교 벤처전문대학원 조교수
<관심분야> 정보보호, 유비쿼터스 네트워크 및 보안, Forensic, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality

신 용 태

1985년 한양대학교 산업공학과 (공학사)
1990년 Univ.of Iowa 전산학과 (공학석사)
1994년 Univ.of Iowa 전산학과 (공학박사)
1994년 ~ 1995년 Michigan State Univ. 전산학과 객원교수
1995년 ~ 현재 숭실대학교 컴퓨터학부 교수
<관심 분야> 멀티캐스팅, 실시간통신, 이동통신, DRM 등