보안 침해사고 대응을 위한 컴퓨터 포렌식스 기술 동향

고 병 수* 박 영 신** 최 용 락***

목 차

1. 서 론

불과 2-3년 사이에 급격히 증가한 사이버 테러가 범국가적으로 이루어지고 있으며, 인터넷의 활용성 증가와 함께 컴퓨터 범죄의 수법이 보다 지능적이면서 다양화되어 발전하고 있다. 따라서, 미국을 중심으로 한기술 선진국들은 보안침해사고에 대하여 디지털 전자적 증거분석 및 대응기술 개발에 집중하고 있으며, 이러한 기술들의 개발을 통하여 다양한 보안침해사건의 법의학적 분석 및 복구는 물론 안전한 비즈니스 커뮤니케이션의 제도적 정착을 위하여 국가 전략산업화하고 있다.

따라서 자국의 컴퓨터 포렌식스(Computer Forensics) 기술이 확보되지 않는다면 국내외에서 일어나는 모든 보안침해사고에 대하여 국가 자존적 해석이나 사실증명이 불가능하고 외국에 의뢰하여 결과를 통보 받아야 하는 안타까운 현실을 초래할 수밖에 없다. 그러므로, 적기에 디지털 전자적 증거물을 분석, 제시 할 수 있는 컴퓨터 포렌식스 기술을 개발하여 각종 보안침해사고로 발생하는 역기능들에 대해서 법적인 구속력을 제공하고, 재해로부터 복구해낼 수 있는 대응기술의 개발이 시급하다.

보안침해사고로 인한 산업적 손실은 소프트웨어의 특성상 한번 노출되면 상품가치를 상실하게 되고, 최근 첨단기술의 발달과 더불어 전략적 해킹행위 또한 증가하고 있으므로 발생될 수 있는 산업적 피해는 산출 불가할 정도이다. 이러한 사례는 국내 S사의 고급기술 해외 유출, MS사의 불법적 내부파일 전송사건 및 금년도 국내 "1.25 인터넷 대란"사건 등은 매우 짧은 시간에 엄청난 산업손실을 가져온 경우이다. 산업재해로부터 사건을 분석하여 원인을 규명하고, 본래의 디지털 내용을 복구함과 동시에 법적인 증거까지 제시하는 컴퓨터 포렌식스 산업은, 새로운 비즈니스 모델로 각광받을 것으로 예측하고 있다.

이미 미국의 경우는 보안침해사고를 분석하여 법의학적인 증거를 제시하고, 이러한 활동들을 뒷받침할 수 있는 핵심적 컴퓨터 포렌식스 도구들을 개발하고 있으며, 이러한 전문적 기술이 인기직종으로 부상하고 있다. 따라서, 외국의 컴퓨터 포렌식스 기술을 조기에 도입하여 국내의 기술로 정착시키고, 국산 우수제품을 사용하여 향상된 Forensics 도구들을 연구 개발함으로써 미래 산업에 대한 적절한 준비가 필요하다.

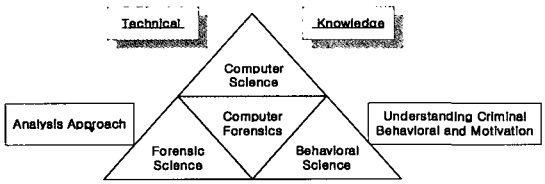
2. 컴퓨터 포렌식스

2.1 컴퓨터 포렌식스 정의

오늘날 비즈니스 커뮤니케이션의 70%가 전기, 전자적으로 이루어지고 있으며, 이에 따른 모든

* 대전대학교 대학원 컴퓨터공학과 박사과정
** 대전대학교 대학원 컴퓨터공학과 석사과정
*** 대전대학교 컴퓨터공학부 교수

순기능과역기능에 대하여 결정적인 거래증거는 컴퓨터와 네트워크 안에 있다. 이러한 환경으로부터 디지털 전자 컨텐츠의 모든 접근행위에 대하여 전자적 증거물을 수집분석 및 역추적 등의 절차를 수행하고 법적 증거물 제시와 적절한 대응조치를 할 수 있도록 새롭게 출현한 기술이 컴퓨터 포렌식스이다.



(그림 1) 컴퓨터 포렌식스 영역

ESM(Enterprise Security Management)과의 차이점에 대해 의문점을 갖는 사람들도 있으나, ESM의 경우 보안제품간의 상호호환성을 바탕으로 관리할 수 있는 제한된 영역을 통제하는 시스템인 반면에, 컴퓨터 포렌식스의 경우 침해사고대응 방법을 위해 여러 문제점들을 분야별로 구분시켜 놓음으로써 향후 침해사고 발생시 증거를 획득, 보존하여 법적 대응이 가능하도록 하는 시스템이라 할 수 있다.

2.2 컴퓨터 포렌식스 방법론

일반적으로 컴퓨터 범죄 관련 증거자료를 대상으로 한 컴퓨터 포렌식스 분석 방법론은 크게 역추적을 통한 방법과 증거물 복원을 통한 컴퓨터 포렌식스로 구분할 수 있다.

역추적을 통한 컴퓨터 포렌식스 방법에서는 이벤트가 발생한 근원지 또는 위치를 찾아가는 방법에 관한 사항을 제공한다. 컴퓨터범죄와 관련된 증거를 수집하고 이를 분석하여 근원지에 해당하는 IP 주소 등을 역추적한다. 그리고 근원지가 파악되면 이를 문서화하여 최종적인 증거물로 채택한다. 본 방법론에서 수행되는 과정을 단계별로 제시하면 다음과 같다.[1]

·1단계: 관련된 증거 자료 수집
·2단계: 키워드 분석
·3단계: 출처,위치,저장장소 및 근원지 파악
·4단계: 증거물에 대한 문서화

증거물 복원을 중심으로 한 컴퓨터 포렌식스 방법은 관련 증거자료를 수집하여 데이터 복구 과정을 수행하고, 필요로 할 경우 암호화된 데이터에 대한 복호과정을 수행하여 증거물에 해당하는 데이터의 특성에 따라 수사하는 방식이다.

·1단계: 관련된 증거 자료 수집
·2단계: 데이터 복구 및 암호 제거
·3단계: 포맷 분류 및 은닉 자료 검색
·4단계: 증거물 정리 및 문서화

2.3 방법론에 의한 포렌식 분석

방법론에 의한 포렌식 분석들은 세계 표준화가 되어 있지 않지만 대략 역추적 대응분석과 포렌식 위험분석, 관리적 위험분석, 포렌식 대응분석 등 4가지로 구분하고 있다[4].

2.3.1 역추적 대응분석

(그림 2) 역추적 대응분석과 포렌식 위험 분석

(1) 상황실: 관련기관에서 실시간으로 보안 관련 사건들을 조사하고 분석.
(2) 제보접수: 사이버 신문고제도와 비슷한 경우.
(3) 탐문수사: 해커들이 자주 들어가는 웹사이트 내부 게시판자료를 직접 검색하는 방법.
(4) 증거수집: 키보드로 입력 로그 확보 방법.
(5) 키워드 분석: 일반 웹브라우저를 통한 검색 엔진에서 얻는 방법.
(6) 사용 IP 파악: 해당 IP의 국적을 파악하여 국내외로 구분하여 공조수사와 연관성.
(7) 공조지원: 사용 IP 파악 단계에서 요구하는 수작업에 의한 추적을 하드웨어 및 프로그램을 이용해 피해자가 쉽게 접근할 수 있는 방법을 제시.
(8) 해킹범죄의 출처확인: 공조지원 단계에서 조사한 자료를 근거로 잠정적인 결정에 도달하는 과정.

2.3.2 포렌식 위험분석

(1) 증거자료수집: 증발된 자료 확보 단계.
(2) 데이터 복구: 이미 실행되어 지워졌거나 겹쳐진 자료 파일들을 최대한 복구하는 과정.
(3) 암호제거: 의도적으로 암호가 걸려 있는 자료에 대한 비밀키를 무작위 공격으로 구하거나 인위적으로 프로그램 상에 숨겨진 제어명령을 정상 동작하도록 다시 소프트웨어 역공학으로 복구하는 단계.
(4) 파일포맷 정리: 이전 단계들에서 조사해 오던 자료 파일들을 통일된 규격 및 형식으로 전환하는 포맷 작업을 한 후 지정한 저장 장치에 정리해 두는 단계.
(5) 수사자료 검색: 실행 파일에 암호키가 숨겨있는 경우 및 일반화 되어 있지 않은 확장자를 가진 파일을 분석할 경우 내부 파일 키워드 검색을 통해 2진 숫자를 제외한 단어들만을 검출하는 작업.
(6) 범행시간 추적: 해킹범죄가 발생했던 당시의 시간 검증 및 파악된 파일의 디렉토리 구조파악을 통하여 인위적으로 숨겨지거나 증발한 파일들의 정보를 알아내는 단계.
(7) DB 정리: 자료파일의 무결성을 검사하여 지금까지 조사해 오는 과정에서 변조여부를 구별하는 과정.
(8) 산출물 보안조치: 대응 분석에서 나온 산출물의 보안관리용 최종백업 디스크를 제외한 기타 사용해 왔던 시스템의 자료들은 모두 삭제하여 재생이 불가능하게 만드는 단계.

(그림 3) 관리적 위험분석과 포렌식 대응분석

2.3.3 포렌식 시스템 분석방법

컴퓨터 포렌식을 이용한 시스템 분석 방법에는 증거 보존 및 분석을 위한 시스템 분석 방법과 해킹과 같은 공격 흔적을 찾기 위한 무결성 도구를 이용한 방법, 그리고 공격기법을 분석하여 침해 여부를 판단하고 로그 파일 분석 및 복구를 통한 증거 수집을 이용한 방법 등이 있다.

- ▶ 분석 시스템을 이용한 분석방법.
- ▶ 공격 흔적을 보존하기 위해 수행중인 프로세스 상태 및 포트, 현재 네트워크정보, 사용자와 터미널에 대한 로그 정보, 현재 사용자, 현재까지 변경된 모든 파일 등을 조사해야 한다.
- ▶ 무결성 도구를 이용한 시스템 변조 유무 확인 방법.
- ▶ 공격기법 및 웜바이러스(바이러스 포함)등을 분석하는 방법.

- ▶ 공격자가 삭제한 파일이나 데이터를 복구하여 증거를 수집하는 방법.
- ▶ 로그파일을 점검함으로써 파일의 유출 및 도난 여부를 확인하는 방법.
- ▶ 디스크 복구를 통한 증거 수집 방법.

3. 보안 침해사고 대응

완벽하게 안전한 보안시스템이란 있을 수 없으며 정보시스템에 대한 침해위협은 항상 존재한다. 침해사고 발생시 피해확산의 방지, 서비스의 신속 안전한 복구, 공격자의 위치와 동기 파악, 재범 발생의 방지를 위하여 발생 가능한 위협에 대하여 미리 조치절차를 수립해 두는 것은 침해사고 대응에 매우 효과적일 것이다[4].

지금까지 우리는 침해사고대응 단계에서 정형화되지 않은 방법과 절차들을 사고분석 절차에 적용하여왔다. 그러나 최근에는 침해분석 대응에 컴퓨터 포렌식스 기법을 적용함으로써 좀더 구체화되고 정형화된 방법론을 가지고 해킹사고에 접근할 수 있게 되었다.

3.1 침해사고 분석 방법

대부분의 조직들은 침해사고에 대응하는데 많은 어려움을 겪고 있다. 이는 우선 어떻게 당하는지 모르고, 어떤 피해를 주는지 모를 뿐만 아니라 누가 했는지, 법적인 문제는 무엇인지, 어떻게 법적 수사를 지원해야하는지에 대한 지식이 없기 때문이다. 그러므로 법적인 프레임워크를 이해하여야 하고, 보안정책, 특히 침해사고처리절차를 갖추어야 하며, 기술적인 도구를 마련하고 있어야 한다.

컴퓨터 증거는 쉽게 변조가 가능하고 변조사실을 알기 어려우며, 처리할 때 다른 관련 없는 정보와 같이 처리되고, 또 여러 가지 형태로 저장되어 관리자가 이해하기 어렵다는 것이 특징이다. 컴퓨터 포렌식스는 'Criminalistics'이며, 지난 사건을 재구축하는 것이다. 즉, 법적인 절차와 규정에 의하여 디지털 증거를 확인하고, 보관하고, 분석하고 제출하는 프로세스인 것이다. 여기서 증거란 사용자나 관리자의 관찰, 시스템 로그, 프로세스, 백업 미디어, TCPWRAPPER 자료, Firewall 로그, 전화 로그, 네트워크 감사 자료 등을 의미한다. 이를 위해, 특히 파일 시스템의 변조유무를 체크하는 방법을 강구하고, 네트워크 통신 발신지는 CISCO NetFlow, Etherboy와 IDS를 이용한다. 사고의 조사(Investigation)는 누가 조사를 결정하며, 담당하는지, 수사기관이 조사할 것인지의 여부를 결정하여야 하며, 동시에 무엇을 얻기 위함인지에 관한 목적과 비용, 그리고 그에 따른 효과를 고려하여야 한다.

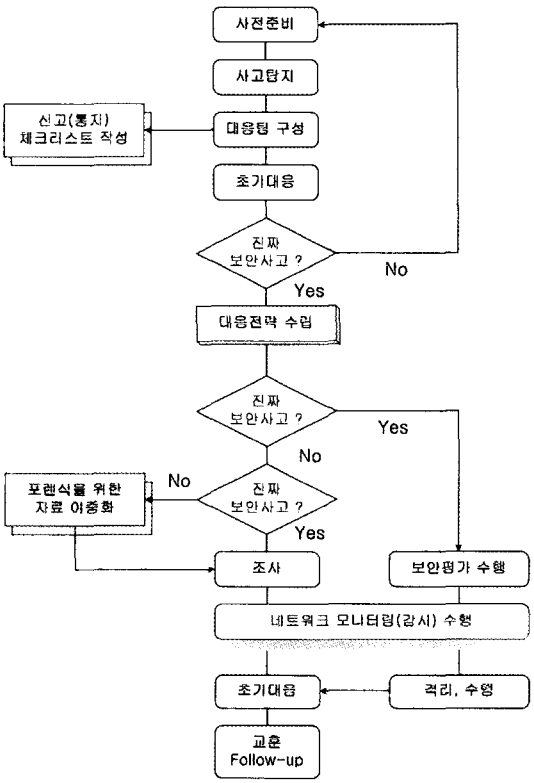
3.2 침해사고대응의 기능과 목적

침해사고 대응의 궁극적인 목적을 다음과 같이 요약 할 수 있다.

- ▶ 침해사고 발생여부를 결정한다.
- ▶ 서비스를 안전하게 복구한다.
- ▶ 침해사고로 인한 비용과 정도를 평가한다.
  손해를 복구한다.
- ▶ 증거의 적절한 핸들링과 복구의 통제절차를 수립한다.
- ▶ 법과 정책에 의해 정해진 개인과 기업의 권리를 보호한다.
- ▶ 적당한 리포트와 유용한 Recommendations을 제공한다.
- ▶ 보안의 중요성을 인식하게 된다.
- ▶ 미래의 보안, 침해사고를 미연에 방지시킬 수 있다.

3.3 침해사고대응 절차

침해사고대응을 할 때 일반적인 접근 방법은 "Incident Response"의 저자 Kevin Mandia과 Chris Prosise는 침해사고 대응의 일반적인 절차와 기능을 사전 준비단계, 사고 탐지단계, 초기 대응단계, 대응전략 수립단계, 포렌식스를 위한 자료 이중화 단계, 조사 단계, 보안평가 수행단계, 네트워크 모니터링 단계, 복구, 보고, 사후조치 단계 등 11단계로 그림 4와 같이 구분한다[5].



(그림 4) 침해사고 대응절차도

(1) 사전준비 단계

향후 과정을 원활히 수행하기 위한 과정으로써 필요한 프로그램과 장비를 준비하거나 사고대응팀을 구성하고 이들의 역할을 정하며, 내부규칙을 마련한다.

(2) 사고 탐지 단계

사고의 인지, 탐지는 사건해결의 첫 시발점이다. 이것들은 주로 IDS, F/W 또는 사용자의 인지에 의해서 알게 되는 것이 보통이며, Tripwire 와 같은 시스템 파일 체크섬을 확인해 주는 프로그램에 의해서도 가능하다.

(3) 초기 대응단계

초기 대응단계에서 사고대응팀이 소집되어야 하며, 모든 작업은 책임자의 책임하에 철저히 통제되어야 한다. 이 단계에서는 컴퓨터의 재부팅시에 사라질 수 있는 휘발성 데이터를 수집하는 것 등이 포함된다.

(4) 대응전략 수립 단계

이 단계는 초기 대응단계에서 파악된 상황을 토대로 구체적으로 어떤 조치를 취할 것인지를 결정하는 단계이다. 사고를 내부에서 처리할 것인지 아니면 수사기관에 신고할 것인지도 이 단계에서 결정해야 할 사항이다.

(5) 포렌식스를 위한 자료 이중화 단계

컴퓨터 포렌식스는 법적인 문제를 해결하기 위한 컴퓨터 법죄 수사 과학이다. 전통적으로 컴퓨터 포렌식스는 하드 디스크의 원본을 완전히 복제하여 분석하는 것으로, 컴퓨터의 부검이라고도 한다.

(6) 조사 단계

조사는 복제된 하드디스크나 운영중인 시스템의 로그파일에 대한 검사를 포함하여 최초 사고발견자, 보안담당자에 대한 면접조사 등 세부적인 사고조사 과정을 말한다. 일반적으로 이 단계는 다른 단계에 비해 가장 긴 시간이 소요되는 것이 보통이다.

(7) 보안평가 수행 단계

보안 평가는 앞의 과정에서 조사된 결과물을 토대로 보안상의 문제점을 평가하는 과정으로, 향후 사고방지를 위한 작업을 뜻한다. 사고의 형태와 원인에 따라 시스템이나 네트워크 차원에서 어떠한 문제가 있었는지 또는 관리상의 실수가 있지는 않았는지, 또는 전반적인 보안정책에 문제는 없는지 등의 항목들이 검토되며, 그 수행결과에 따라 정확한 조치를 취하게 된다.

(8) 네트워크 모니터링 단계

보안평가와 조치 후에 해당 조치의 적절성을 판단하기 위하여 상당기간 네트워크에 대해서 한층 강화된 모니터링이 수행되어야 한다. 안전성이 검증될 때 까지 평상시보다 강화된 보안수준을 적용하여야 한다.

(9) 복구

복구는 사고를 당한 시스템과 네트워크를 정

상적인 상태로 환원시키는 작업이다. 해커가 설치한 프로그램과 파일을 제거하고, 백업 파일로 지워지고 흐트러진 자료를 원상 회복시키는 등의 작업이 복구과정에 포함된다.

(10) 보고

사고대응 절차를 종료하는 시점에서 개별사건에 대한 별도의 보고서를 작성하고, 조치결과는 책임자에게 보고되어야 한다. 때때로 이 단계에서 수사기관에 대한 신고가 이루어지거나 법적인 대응이 본격적으로 이루어지기도 한다.

(11) 사후조치 단계

실질적으로 사고대응을 하면서 알게된 필요한 조치를 실무에 반영하는 것이다.

위에서 설명된 방법론은 각각의 중요한 의미를 지니고 있으나, 작업순서가 반드시 설명된 순서대로 진행되어야 하는 것은 아니다. 좀더 이해하기 쉬운 대응절차가 많이 있으며 그 중에 워싱턴 대학의 Dave Dittrich가 제시한 사고대응 6단계 모형은 매우 간결하고 많이 이용되고 있으며 비즈니스 관점에서의 접근방식을 취하였다. Dittrich는 그 단계를 사전준비 인지, 차단, 근절, 복구, 후속조치 등 6가지로 구분하였다.[3]

4. 최근 기술 동향

4.1 컴퓨터 포렌식스 시장 동향

최신 포렌식 도구는 갈수록 늘어나는 디지털 증거 은닉처를 찾을 수 있게 해 준다. 그러나 기업과 법률 집행기관에 유용한 포렌식 가치를 제공하는 전문가를 길러내기 위해서는 많은 돈이 들어간다. 그리고 조사자들이 궁극적인 장소에서 테스트 받기까지는, 다시 말해 법정에서 전문가로서 증언할 수 있기까지는 현장에서 오랜 경험을 쌓아야만 한다.

한국의 경우 정보선진국으로 가기 위한 가장 중요한 부분이 컴퓨터 범죄나 인터넷 테러 등을 사전에 차단하기 위한 사후예방책을 마련해야한다. 더욱이 해킹 경로의 절반이상을 차지하고 있는 한국의 경우 정부뿐만 아니라 민간부분에서도 컴퓨터 포렌식스 기술과 도구에 대한 꾸준한 연구와 개발이 요구된다.

이와 같이 포렌식 서비스에 대한 수요는 아직 작지만 계속 늘어나고 있다. IDC는 사건 대응 서비스 시장(포렌식 서비스 시장 포함)이 2001년의 1억3,300만 달러에서 2004년의 2억8,400만 달러로 성장할 것이라고 예상한다.

4.2 컴퓨터 포렌식스 제품 동향

현재까지 제시된 컴퓨터 포렌식스 도구들은 크게 두 가지 형태로 구분할 수 있다. 즉, 예를 들면 컴퓨터 포렌식스에 관련된 전반적인 기능을 제공하는 도구와 각 기능별로 포렌식스 과정을 수행하는 부분적인 도구로 구분할 수 있다.

국내에서 공개된 컴퓨터 포렌식스 관련 증거수집 방법 및 도구는 거의 전무하며 또한 상업용 증거 수집 도구들 역시 삭제된 파일에 대해 복원 및 복구 기능 등을 주로 제공하기 때문에 상당히 제한적인 분야에만 개발되어 있다.

해커스랩과 KCC정보통신이 부분 기능을 제공하는 컴퓨터 포렌식스 도구를 연속적으로 개발하고 있으며, KDL도 컴퓨터 파일, 이메일, 네트워킹 추적 등을 합법적으로 전자 증거물을 찾을 수 있는 컴퓨터 포렌식스를 개발하고 있다. 그러나, 순수한 국내의 기술력을 바탕으로 개발하는 연구는 매우 미흡하며, 외국에서 발표된 일부 도구돌을 도입 연구하는 수준이다.

외국의 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(예를 들어 엔론 사건과 같은 조사의 경우, 대부분의 윈도우 서버와 PC, 노트북 등) 내부의 저장장치에 남겨져 있는 수 기가바이트의 데이터를 분석하는 강력한 도구를 제공한다.

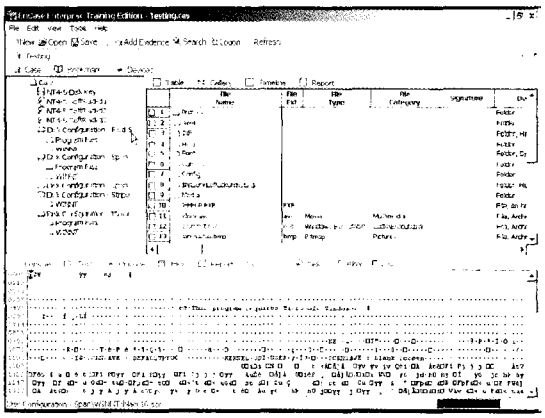
최근 가장 많이 사용되어지는 도구를 나열하면 다음과 같다.

(1) Foundstone Forensic Toolkit

Foundstone 포렌식 도구는 권한이 없는 행위에 대해 NTFS 디스크 파티션 파일을 조사하는 것으로 몇몇 Win32 명령 라인의 도구를 포함한다.

이러한 공개 소스 툴은 숨은 파일과 데이터 스트림을 찾기 위해 디스크를 스캔하고 디스크의 데이터 속성을 변경하지 않고 MAC 시간과 함께 그것들을 기록한다.

(2) EnCase(Guidance Software)



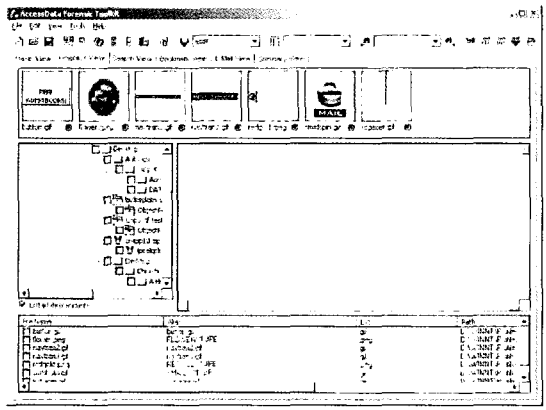
(그림 5) EnCase의 Disk Forensics

EnCase는 조사자가 많은 양의 컴퓨터 증거를 쉽게 관리하고 파일 스택과 할당되지 않은 데이터를 볼 수 있는 GUI(GraphicalUser Interface)의 특징을 가진 강력한 컴퓨터 포렌식 도구이다.

통합된 기능의 EnCase는 목표로 하는 드라이브의 초기 사전 검토, 증거의 이미지를 획득하고, 데이터를 검색하고 복구해서 기록하고, 모든 같은 애플리케이션에서 컴퓨터 포렌식 조사 처리의 기능을 모두 수행하도록 조사자에게 제공한다.

(3) AccessData Forensic Toolkit

AccessData 포렌식 툴킷(FTK)은 컴퓨터 시스템의 포렌식 조사를 수행하기 위한 완벽한 방식을 제공하는 편리한 컴퓨터 포렌식 도구이다. 전체 텍스트 색인은 신속한 기능을 제공하며, 삭제된 파일 복구와 파일 슬랙 분석이 뛰어나다.



(그림 6) AccessData의 Forensics Toolkit

또한, FTK는 비밀번호 복구와 암호화 파일 식별 프로그램들 같은 다른 AccessData 유틸리티들과 함께 상호 작용이 가능하다. 그리고, FTK는 255 개의 다른 파일 형식으로 접근가능 하도록 Stellent의 Outside In Viewer 기술을 결합하였다. FTK는 EnCase, Snapback, SafeBack 그리고 리눅스 DD에 의해서 얻어진 증거 파일들을 지원할 수 있다.

(4) Windows Event Log Analysis

마이크로소프트의 WinNT/2K는 시스템 이벤트와 애플리케이션 이벤트, 그리고 보안 이벤트를 기록하기 위하여 바이너리 파일로 이벤트 로그를 구성할 수 있다. 이러한 이벤트 로그는 동적 라이브러리 파일을 링크하거나 기록 및 실행을 통하여 서술적 메시지를 저장한다. 이벤트 뷰어는 이 파일들의 정보를 결합시켜 표시하고 데이터를 볼 수 있는 편리한 방법을 제공한다.

따라서, 원격 시스템에서 이벤트 로그 파일을 볼 때, 조사를 위해 어떤 시스템에서 다른 곳으로 이벤트 로그 파일을 복사하는 것은 오역의 결과를 가져올 수 있다. 이벤트 뷰어는 원격의 로그 파일로부터 이벤트가 기록된 데이터를 읽는다. 하지만 이벤트 메시지 파일에 대응시키기

위해서 는 로컬 시스템의 기록을 탐색한다.

(5) DumpEvt(somarSoft)

원격의 포렌식 PC에서 윈도우즈 이벤트 로그 분석을 메뉴얼로실행하는 불편을 미리 조사하여 용이하게 한다. 스프레드시트로 다중 기계의 로그 파일들의 내용을 가져와 연대순으로 이벤트를 분류하고 동시에 로그를 탐색하는 것을 더 간단하게 한다.

DumpEvt는 더 많은 로그 분석을 용이하게 사용하기 위하여 DB에 적합한 포맷으로 다중 이벤트 로그를 저장하도록 디자인된 유틸리티이다.

(6) Unix Log Analysis

Unix는 컴퓨터 보안 전문가를 위한 교육으로 알맞다. 이것은 객체의 접근 허용에 대해 다루고, MS-DOS의 지식을 기반으로 MS-DOS를 보완하고 수정하여 기능을 확장하였다.

DOS 배치 파일과 유사한 기능의 Unix 스크립팅을 사용하여 조사자는 보안 감사를 수행하고 많은 파일을 검색하기 위하여 전문 프로그램으로 명령들을 결합할 수 있다. 또한 Unix 시스템은 정보의 가치가 없는 소스로 판단될 수 있는 시스템 구성 파일들로 설정된다.

(7) Network Analysis

분석자는 Win32 환경에 대한 전체의 구성된 네트워크를 분석하는 프로그램을 가지고 있다. 이것은 네트워크에서 패킷을 추출하여 사용하기 쉬운 그래픽 인터페이스를 통하여 나타낸다. 분석자는 실시간 모니터링으로 네트워크 패킷을 추출하고 추출된 파일을 생성하는 능력이 있다.

프로토콜 포맷을 기술하고, 패킷들의 표시를 만들고, 통계치를 평가하고, 그래프를 계획하고, 분석엔진으로 질의를 설정하고 MAC, 네트워크, 트랜스포트 또는 애플리케이션 계층에 기록된 패킷의 필터를 설정하는 조사자를 지원한다.

그 외 부분 기능을 제공하는 포렌식스 도구들을 처리내용별로 분류하면 표 1과 같다.

기능	제품
디스크 조작, 포맷팅, 파티션	-**ACARD**: SCSI 와 IDE 어댑터 관련 도구. -**CPR**: *Toolsthatwork.com*의 도구 -**Digital Intelligence**: DriveSpy software 와 F.R.E.D 포렌식하드웨어 도구. -**Encase**: Guidance Software의 컴퓨터 포렌식 도구. -**Expert Witness**: ASR Data의 포렌식 도구 -**FTK**: Access Data의 포렌식 툴 킷. -**iLook** 포렌식 도구. -**Digital Detective**: 데이터 컨버젼 유틸리티. -**IMAGE MASTER**: 디스크 이미지 도구. -**IMAGECAST**: 디스크 복제 도구. -**Maresware**: 디스크, 파일 관련 도구. -**Norton Utilities** : 시만텍 도구. -**NTI** : 컴퓨터 포렌식스 소프트웨어. -***Ontrack***: 데이터 복구 소프트웨어. -**Powerquest**: 파티션, 디스크 이미지, 디스크 카피 도구. -**SnapBack**: 이미지 소프트웨어. -**Sydex**: Safeback 소프트웨어. -**System Commander Also**: Partition Commander from V-Com. -**WINHEX**: 편집기.
데이터 복구	-**AcoDisk**: CD 데이터 복구. -***Atlanta Computer Resources***: 데이터 복구 -**Computer Conversions**: 데이터 복구.
Disk /text /hex editing	-**Disk**: 데이터 분석과 복구 도구. NTFS 디스크 지원. -**EditPro**: 윈도우 환경의 에디터. -**Hex Workshop**: Excellent editor. -**File Maresware**: Maresware 에디터. -**VEDIT**: text/hex 에디터 -**WINHEX**: Excellent editor. -**NTFS**: 디스크 에디터.
다양성 있는 소프트웨어	-**ASR Data**: "SMART" 시리즈 컴퓨터 포렌식 도구. -**AccessData**: FTK(Forensic Toolkit). -**Digital Intelligence**: DriveSpy 소프트웨어와 F.R.E.D 포렌식스 하드웨어. -**Encase**: Guidance Software의 컴퓨터 포렌식 도구 -**Expert Witness**: ASR Data의 컴퓨터 포렌식 도구. -**FTK**: Access Data의 포렌식 툴킷. -**Maresware**: 컴퓨터 포렌식과 데이터 분석 도구. -**NTI**: New Technologies의 컴퓨터 포렌식스 도구. -**SysInternals**: NT와 Windows 계열을 위한 소프트웨어.

5. 결 론

컴퓨터와 인터넷의 활용증가와 더불어 어린이

그래픽 뷰어 및 처리	-CompuPic: 파일 뷰어. -Conversions Plus: DataViz software의 MAC 포맷을 지원하는 데이바 컨버젼 소프트웨어. -DiskJockey: 파일 뷰어. -IrfanView: 그래픽 뷰어. 쉐어웨어. -Quick View: Inso의 파일 뷰어. -Thumbs Plus: 파일 뷰어. -Thumber: 디지털 이미지 처리 소프트웨어. -U.S. Navy: NCIS 소프트웨어.
Hashing (CRC, SHA) 계산	-AccessData: SHA. -Digital Intelligence: DriveSpy. -Mares: Hash, Crckit, Diskcat, Disk_crc, MD5. -NTI: DiskSig, CRCMD5.
Unix /Linux	-ForensiX: 리눅스 포렌식스 도구. -eXaminer: 디지털 증거 분석 도구. -NeoWorx: traceroute 보다 더욱 다양한 기능 제공. -SMART: ASR Data의 리눅스 컴퓨터 포렌식스 도구. -Maresware
Windows 9X 관리자 툴	-Applog: 히스토리 검사 툴.

포르노, 각종 음란 사이트 개설, 내부인의 불법적 계좌이체, 위협 편지, 사기, 지적재산 도난 등의 전자적 증거를 추적하고 법적인 책임을 부과하는 것이 새로운 사회적 문제가 되고 있다. 이러한 문제들은 사용된 컴퓨터를 면밀히 전자적으로 조사하고, 특정 키워드 탐색, 로그파일분석 등을 통한 불법적인 행위의 시간 및 방법을 구체적으로 증명해내야 하는 대단히 난해한 작업이다.

컴퓨터 포렌식스는 각종 보안침해사고에 대하여 법의학적으로 인정받을 수 있는 미래사회의 고도로 발달된 새로운 업종이다. 현재, 사이버테러 및 각종 보안침해사고에 대하여 사회적 인식의 제고와 함께 '공인탐정관련법'등 국내외적으로 정보보호 정책 및 사회적 규제가 강화되는 추세이나, 이에 대한 기업의 연구인력 및 기술수준은 매우 미흡한 실정이다.

컴퓨터 포렌식스는 전자적 증거를 제공하는 법의학적 측면 및 보안침해사고를 기술적으로 복구하는 산업재해 복구 측면에서 새로운 업종의 탄생에 대한 흥미로운 연구주제가 될 것이다.

그러나, 컴퓨터 포렌식스 기술이 발전한다는 것은 인간이 범죄 심리에 취약하다는 것이므로 보안기술을 개발하기보다는 보안을 침해하지 않도록 의식을 진화시키는 일은 더욱 시급하고 중요하다.

참 고 문 헌

[1] 이형우, "컴퓨터 포렌식스 기술", 한국정보보호학회 제 12권 제 5호, 2001.10. PP.8-16.

[2] Warren G, Kruse II & JayG.Heiser, Computer Forensics - Incident Response Essentials.

[3] Kevin Mandia & Chris Prosise, Incident Response - Investigating Computer Crime.

[4] 김종필, '컴퓨터 포렌식스를 기반으로한 침해사고 대응 방법론 연구', 석사학위 논문, 2002.

[5] Alfred C., 해킹과 포렌식 입문 - 사이버테러 대응분석시리즈 001, 2002.

[6] Chris Prosise, Kevin Mandia, Incident Response: Investigating Computer Crime, 2001.

[7] Eoghan Casey, Handbook of Computer CrimeInvestigation: Forensic Tools & Technology, 2001.

[8] Albert J. Marcella Jr (Editor), Robert S. Greenfield, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2002.

[9] The Honeynet Project (Editor), Lance Spitzner(Preface), Bruce Schneier, The Honeynet Project, Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community, 2001.

[10] John R. Vacca, Michael Erbschloe, Computer Forensics: Computer Crime Scene Investigation(With CD-ROM), 2002.

[11] Eoghan Casey, Digital Evidence and Computer Crime, 2001.

[12] 박재홍, Network Hacking & Security (네트워크 해킹과 보안), 2003.

◐ 저 자 소 개 ◑

고 병 수

2000년 호남대학교 대학원 컴퓨터공학과(석사)
2000년~현재 : 대전대학교 대학원 컴퓨터공학과 박사과정
관심분야 : 침해사고대응 기술, Secure OS, PKI 응용 보안

박 영 신

2002년 대전대학교 컴퓨터공학과(학사)
2002년~현재: 대전대학교 대학원 컴퓨터공학과 석사과정
관심분야 : 보안 컴포넌트, 컴퓨터 포렌식스

최 용 락

1989년 중앙대학교 전자계산학과(박사)
1982년~1986년 한국전자통신연구원 선임연구원
1986년~현재 : 대전대 컴퓨터공학부 교수
1997년~1999년 한국정보보호학회충청지부 초대지부장
2001년~2003년 대전대학교 공과대학 학장
2000년~현재 : 대전지검 컴퓨터수사자문위원
관심분야: 컴퓨터통신보안, 컴퓨터 포렌식스, DRM, 보안 API