컴퓨터 및 네트워크 환경 하에서 Forensics 적용 동향 및 구현 기술

박연규* 이필중*

* 포항공과대학교 정보통신대학원

Implementation technique and tendency of Computer Forensics in Network and Computer Environment

Yeon Kyu Park*, Pil Joong Lee*

*GSIT of POSTECH

요 약

컴퓨터와 인터넷의 발전과 함께 컴퓨터 범죄가 급속히 증가하고 있는 추세이다. 이에 대응하기 위해 시작된 분야가 컴퓨터 포렌식스(Computer and Network Forensics)이다. 본 논문에서는 컴퓨터 포렌식스의 몇 가지 예를 통해 일반적인 단계와 각 단계에서 이루어지는 절차에 대해 알아본다. 그리고 컴퓨터 포렌식스의 중요한 구성요소로써 사용되는 IDS와 IDS를 적용한 컴퓨터 포렌식스 절차에 대해 살펴보며 마지막으로 보다 효율적이고 체계적인 컴퓨터 포렌식스 준비를 위한 로컬 정책 수립에 기본적인 기준을 제시한다.

I. 서론

1. 컴퓨터 포렌식스

기술이 발전함에 따라 컴퓨터는 더욱 강력한 성능을 갖게 되었으나 불행이도 이러한 발전으로 인해 컴퓨터를 이용한 범죄가 증가하고 있는 추세이다. DDoS(Distributed Denial of Service) 공격, 바이러스(Viruses), 트로이 목마 프로그램(Trojan Horses), 네트워크 도청(Sniffing) 등이 그 예이다. 급증하는 컴퓨터 범죄에 대응하기 위해 대두된 분야가 바로 컴퓨터 네트워크 포렌식스(Computer and Network Forensics, 이후 컴퓨터 포렌식스로 표기)이다.

간단히 말하면, 컴퓨터 포렌식스는 '컴퓨터를 매개로 이루어지는 보안사건(Security incident)에 대한 법적 증거 자료가 법적 증거물로써 제출될 수 있도록 증거물의 확인, 보존, 분석, 제출하는 일련의 행위'를 의미한다. 컴퓨터 포렌식스 조사원이었던 Judd Robbins[1]는 컴퓨터 포렌식스를 다음과 같이 정의하였다.

" Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. "

컴퓨터 관련 범죄(Cyber Crime, Crime related computer)는 2개의 카테고리(Categories)로 나누어질 수 있다[2]. 첫 번째 형태는 컴퓨터를 이용한 범죄이며 두 번째 형태는 컴퓨터가 대상이 되는 형태이다. 전자의 형태에서는 컴퓨터가 범죄 행위를 돕는 도구로써 사용될 수 있고 이는 위조 레코드의 저장, 거짓 신원(False Identification) 생성, 저작권 및 판권의 재생산 및 분배, 아동을 대상으로 제작된 포르노그래피의 수집 및 분배, 그 외 다른 여러 컴퓨터를 이용한 범죄가 여기에 속한다. 후자의 경우 전통적인 범죄, 살인, 강간, 사기 등과는 다른 컴퓨터 자체가 범죄 행위의 대상(Target)이 된다. 컴퓨터와 네트워크 기술이 발전함에 따라 누가, 무엇을, 어디서, 언제, 어떻게 범행했는가에 대한 단서를 찾기 어렵게 되었다. 따라서 전자전기적인 환경에서의 디지털 증거물은 이전의 방식과 다르게 수집, 처리되어야 한다.

II. 본문

1. 컴퓨터 포렌식스 절차

컴퓨터 포렌식스 전문가들은 범죄 발생 이후 컴퓨터에 남아 있을 수 있는 잠재적인 디지털 증거물을 복구하기 위해 다음과 같이 몇 가지 절차를 취한다[1].

가) 범죄가 발생한 컴퓨터는 컴퓨터 포렌식스 조사가 이루어지는 동안 발생할 수 있는 정보

※ 본 논문은 (주)인젠과 '정보보호에 관한 연구 과제 및 산학 프로젝트'의 지원을 받아 작성된 것임.

의 변경, 손상, 또는 바이러스의 침입 등에 대해서 보호된다.

나) 범죄가 발생한 컴퓨터의 모든 파일들, 즉 일반적인 파일들, 삭제되었으나 복구 가능한 파일들, 숨겨진 파일들, 패스워드로 보호된 파일들, 그리고 암호화된 파일들에 대해 조사한다.

다) 가능한 많이 삭제된 파일들을 복구한다.

라) 응용 프로그램이나 운영체제에서 사용된 숨겨진(hidden) 파일, 임시(temporary) 파일이나 교체(swap) 파일의 내용을 조사한다.

마) 가능하다면 패스워드로 보호된 파일이나 암호화된 파일의 내용을 조사한다.

바) 디스크에서 찾을 수 있는 가능한 모든 관련된 데이터를 분석한다.

사) 범죄가 발생한 컴퓨터에서 분석한 내용 그리고 디지털 증거물 등 필요한 모든 것을 결과물로 생성한다.

아) 컴퓨터 포렌식스 디지털 증거물로써 법정에 제출한다.

F.B.I.의 경우, 소속 조직이나 단체의 정책과 절차에 따른 조사를 강조함과 동시에 컴퓨터 사고에 효율적으로 대응할 수 있는 몇 가지 절차를 소개하고 있다[2].

가) 로그 파일, 손상되었거나 변경된 파일, 침입자에 의해 남겨진 파일 등을 백업한 후, 사고 당시의 컴퓨터 상태를 유지한다.

나) 만약 침입이 진행 중이라면, 로그 감사 소프트웨어와 키 타이핑을 기록할 수 있는 소프트웨어를 동작시킨다.

다) 만약 CERT/CC[2]에 사고 사실을 보고할 경우, 디지털 증거물들이 정당성을 고려한다.

라) 다음과 같은 사고로 인해 발생된 모든 손실을 기록한다.

- 사고 대응과 복구에 사용된 시간
- 잠정적인 도움의 비용
- 손상된 장비, 장치의 비용
- 손실된 데이터의 가치
- 사고로 인한 신뢰도의 손실
- 수입의 감소
- 상업적 비밀 정보의 가치

바) 법 집행 기관과 함께 사고 기록을 제시하고 침입자에 대한 정보, 공격 동기 등을 공유한다.

Brezinski와 Killalea[3]는 디지털 증거물 수집에 있어 필요한 원칙을 제시했다. [3]에서는 상세한 내용을 다루고 있으나 여기서는 간단히 살펴보도록 한다.

가) 먼저 해당 사이트의 로컬 보안 정책을 따르며, 적절한 사고 처리 절차를 수립하고 법 집행 부서와 연락한다.

나) 가능한 시스템의 정확한 상태를 포착한다.

다) 시스템의 상태를 상세하게 기록, 유지한다. 이때 날짜와 시간이 포함되어야 한다.

라) 당시 수집했던 정보를 재시현할 수 있도록 준비한다.

마) 정보 및 데이터의 변경을 대비해 외부 접속 경로를 차단한다.

바) 증거 수집은 휘발성 데이터부터 수집한다.

사) 데이터의 복사 시 bit-level 복사를 사용한다.

지금까지 컴퓨터 포렌식스 관련 정보 수집에 대한 몇 가지 절차에 대해 살펴보았다. 일반적으로 컴퓨터 포렌식스 절차는 디지털 증거물의 확인, 보존, 분석, 제출의 단계로 이루어짐을 알 수 있다.

앞에서 살펴보았듯이 컴퓨터 포렌식스의 일반적인 절차는 확인, 보존, 분석, 제출의 단계로 이루어진다. 확인은 저장 장치에 저장된 정보의 유형과 형태를 확인하는 것으로 증거 자료의 확보가 핵심이 된다. 보존의 단계는 전자적으로 저장된 자료를 확인 후 변경 없이 보존될 수 있도록 하는 단계이다. 여기서는 자료뿐만 아니라 자료를 읽을 수 있는 장치의 변경도 포함된다. 분석은 전자 자료를 추출, 처리, 판단하는 단계로써 분석용 도구를 이용하게 된다. 특히 자료의 변경에 주의하여 진행해야 한다. 마지막 제출 단계는 법적 효력을 갖는 디지털 증거물을 법정에 제출하는 것을 의미한다.

2. 디지털 증거물의 확인

디지털 증거물의 확보 및 수집 절차는 가능한 상세히 이루어져야 한다. 특히 법적 증거력이 있는 정보를 잘못 취급하여 디지털 증거물로서의 가치를 상실할 수도 있으므로 항상 주의해야 한다. 이때 사용되는 방법은 반드시 투명성을 유지해야 하며 재시현이 가능해야 한다. 자료의 수집은 다음과 같다[3].

가) 디지털 증거물 수집 위치를 파악, 리스트

---

1) 디지털 형태로 저장 또는 전송되는 정보로 잠재적인 증거물

2) 컴퓨터 범죄와 관련된 법령(미국의 경우) http: // www. usdoj.gov/criminal/cybercrime/fedcode.htm 참고

3) Computer Emergency Response Team Coordination Center, 인터넷 상의 보안관련 정보를 취급하는 주요기관

다.

나) 증거물로서 합당한, 그리고 수집이 허용된 정보는 어떤 것들인지를 결정한다.

다) 외부 접속 경로를 차단한다.

마) 휘발성 데이터부터 수집한다.

바) 시스템 시간과 표준 시간의 차이를 기록한다.

사) 수집하지 못한 디지털 증거물은 없는지 확인하다.

아) 각 단계를 문서화 한다.

자) 자료 수집에 연루된 사람을 기록한다.

자료 수집에 필요한 프로그램들은 읽기전용 매체(예, CD)에 저장한다. 이는 침입자에 의해 프로그램이 변경됨을 막을 수 있다. 다음과 같은 도구를 사용하여 자료를 수집할 수 있다.

가) 프로세스를 검사할 수 있는 프로그램 : ps

나) 시스템 상태를 검사할 수 있는 프로그램 : showrev, ifconfig, netstat, arp

다) bit-level의 복사를 할 수 있는 프로그램 : dd, SafeBack

라) 서명이나 체크섬을 생성할 수 있는 프로그램 : sha1sum, dd, SafeBack, pgp

마) 코어 이미지와 이를 검사할 수 있는 프로그램 : gcore, ddb

바) 자동으로 디지털 증거물 수집을 스크립트하는 프로그램 : The Coroner's ToolKit[3)]

컴퓨터 포렌식스는 공격이 발생한 후에 자료 수집이 중요한 부분이다. 공격 이전의 자료를 남길 수 있는 가장 좋은 방법은 로깅(logging)이다. 로깅의 경우 네트워크를 통해 발생한 모든 정보를 기록할 수 있을 뿐만 아니라 시스템 내에서 발생한 정보도 기록할 수 있어 컴퓨터 포렌식스에 있어 중요한 자료가 된다. Schneier와 Kelsey[4]는 공격자가 읽을 수 없고 수정 및 변경이 불가능한 안전한 감사 로그를 제안하였고, Marcus Ranum[5]은 네트워크를 통한 컴퓨터 포렌식스에 필요한 로그 데이터를 제안하였다. John Ton[6]은 어떻게 로깅이 이루어지는가와 파일 시스템에 따른 로깅 관련 내용을 잘 정리하고 있다. 이러한 로그 파일은 반드시 외부 또는 내부 공격으로부터 보호 받아야 한다.

3. 디지털 증거물의 보존

범죄가 발생한 시스템을 분석하기에 앞서 가장 먼저 수행되어야 할 절차가 백업(back-up)이다. 백업은 보안에 있어 기본적인 조치이며, 보안업체의 전문가나 컴퓨터 포렌식스 전문가 등 제 삼자가 분석할 경우 필수적인 조치가 된다. 만약 피해 시스템을 분석하거나 공격이 모니터링 되는 것을 공격자가 인식한다면 시스템 전체 정보 및 데이터를 삭제하는 경우가 발생할 수도 있다. 예로 리눅스 시스템을 이용한 백업을 [7]에서 잘 설명하고 있다.

만약 공격자의 침입이 진행 중이거나 공격자의 침입 흔적을 알게 된다면 범죄 현장을 손상 없이 그대로 보존해야 한다(Freezing the Scene). 이때, 시스템을 종료시키기나 전원을 차단하는 것보다 네트워크 선을 분리하는 것이 바람직하다. 시스템을 종료시키거나 전원을 차단하는 경우 휘발성 데이터가 손실될 것이다.

수집된 자료들은 안전하게 보전되어야 한다. 그러기 위해서는 다음과 같은 조건을 만족해야만 한다[1].

가) 증거물은 컴퓨터 조사 과정에서 손상, 변경, 삭제되어서는 안된다.

나) 분석 과정 중 시스템이나 수집된 정보에 바이러스의 침입이 없어야 한다.

다) 이후 처리 과정에서 장치적 또는 전자적 손상으로부터 디지털 증거물은 적절한 방법을 통해 보호되어야 한다.

라) 계속적인 연쇄 관리(Chain of Custody)를 유지해야 한다.

4. 디지털 증거물의 분석

디지털 증거물의 분석은 크게 격리 분석, 온라인 분석, 분석 시스템을 이용한 분석으로 나누어진다[7]. 격리 분석은 대체 백업 시스템이 있어 정상적인 서비스에 지장이 없을 경우, 또는 분석할 동안 서비스를 하지 않아도 될 경우에 가능하다. 또한 정확한 정보 보존이 필요한 경우, 그리고 분석 시스템을 이용하여 철저한 분석을 원할 경우에 사용하는 방법이다. 온라인 분석은 대체 백업 시스템이 없거나 정상적인 서비스를 유지해야 할 경우 사용하는 방법이다. 공격자의 공격 프로그램이나 공격 활동을 지속적으로 모니터링 할 수 있다는 장점이 있는 반면 분석 도중 공격자의 침입 흔적 삭제, 변조, 파괴 등의 위험이 따른다. 최소한의 자원으로 최소한의 분석만을 원할 경우에도 사용될 수 있다. 마지막으로 분석 시스템을 이용한 분석의 경우, 피해 시스템의 디스크 이미지를 복사해서 분석 시스템을 이용하여 분석하는 방법으로 증거를 훼손하지 않기 위한 방법이다. 피해 시스템의 자원을 이용하지 않고 분석 시스템의 자원을 이용하기 때문에 보다 정확한 분석이 가능하며, 분석 시스템 준비, 디스크 복사 등 피해 시스템을 분석하기 앞서 준비할 사항이 많으므로 시간이 오래 걸리는 단점이 있다.

디지털 증거물의 수집, 보존, 분석을 보다 정확

3) http://www.fish.com/forensics 참고

하고 체계적으로 하기 위해서 SWGDE(Scientific Working Group on Digital Evidence)는 컴퓨터 포렌식스에 관한 몇 가지 표준과 원칙을 제안했다[8]. 여기서는 SOPs(Standard Operating Procedures)를 제안했으며 이는 반드시 수용 가능한 절차와 장비를 사용해야 한다는 문서화된 안내서를 말한다. SOP의 필요조건, 주기적인 관리, 수행절차의 적합성, SOP 복사본의 유지, 사용되는SW/HW의 적절성, 그리고 모든 활동의 기록 등, SOP에 관한 기준을 제시하고 있다.

컴퓨터 포렌식스에 사용되는 도구는 일반적으로 상업적인 소프트웨어에서 출발하여 지금은 컴퓨터 범죄를 분석하는 도구로 발전하고 있다. 다음은 컴퓨터 포렌식스에 사용될 수 있는 도구들을 분류한 것이다.

복사용 도구(Replication Tool)는 파일이나 대용량 저장 장치에 저장된 자료를 물리적인 복사를 하는 도구이다. 이런 도구의 종류로는 파일 전송프로그램, 이미지 프로그램, 원격 통제 프로그램 등 그 영역의 폭이 상당히 넓다. 이러한 도구들은 반드시 원천 정보의 변경이나 자료의 손상 및 손실이 없이 정확히 복사하는 능력을 필수 조건으로 요구하고 있다.

자료 검사용 도구(Data Examination Tool)는 파일과 파일에 연관된 논리적인 정보의 내용을 분석하는 도구이다. 이때 추출하는 정보로 파일의 생성 날짜, 시간, 소유자, 파일의 특성 등이며 File Viewer, Disk Explorer, File Catalogue 등의 프로그램이 여기에 해당된다.

자료 무결성 도구(Data Integrity Tool)는 컴퓨터 포렌식스 검사 과정으로부터 유도된 증거물의 무결성을 제공한다. 이런 도구들은 검사관이 검사받은 자료의 정확성을 독립적으로 검증할 수 있게 한다. 일반적으로 자료 무결성 도구는 주어진 양의 자료로부터 해쉬(hash), 체크섬(Checksum), 전자 서명을 생성하기 위해 고안된 수학적으로 증명된 알고리즘을 이용한다.

시스템 분석용 도구(System Analysis Tool)는 컴퓨터 시스템이나 네트워크를 구성하고 있는 다양한 구성 요소간의 구조와 관계를 분석하는데 도움을 준다.

암호용 도구(Cryptographic Tool)는 암호 알고리즘이나 접근 제어 메커니즘에 의해 보호되어진 자료를 접근하거나 보관된 자료의 접근을 제어하는데 사용된다.

다음은 컴퓨터 포렌식스 전문가들로 구성된 비영리 법인인 IACIS에서 제시한 요구사항을 설명한 것이다.

가) 조사 과정에 사용되는 매체는 기밀 유지 조치가 취해진 것이어야 한다.

나) 조사가 끝난 이후에 원시 매체의 무결성은 유지되어야 한다.

다) 검사 대상 매체에 대한 기록은 인가된 H/W, S/W 사용하여 이루어져야 한다.

라) 검사 결과의 출력 정보 및 기타 결과 내용은 적절히 통제되어야 한다.

5. 컴퓨터 포렌식스 구성요소로서의 침입 탐지 시스템

침입 탐지 시스템(IDS, Intrusion Detection System)은 컴퓨터 포렌식스에 있어 또 하나의 중요한 구성요소이다[6][9][10][11]. IDS를 통한 컴퓨터 포렌식스 절차는 일반적으로 공격의 탐지, 공격의 활동 및 관련 정보 로깅, 마지막으로 공격에 관련된 디지털 증거물을 수집하는 형태이다.

IDS는 침입이 발생하거나 진행 중인 경우 시스템 관리자에게 공격 사실을 통보한다. 침입이 발생한 경우 IDS는 공격의 모든 활동 및 정보를 로깅하고 공격자의 접속을 단절하며 공격 사실을 관리자에게 통보하는 행동을 취한다. 시스템 관리자는 IDS의 침입 통보를 통해 공격에 관련된 디지털 증거물을 확인, 수집할 수 있다. 이때 수집된 정보는 사건 발생 이후에 수집된 정보보다 효율적이고 유용하게 범죄 조사에 사용된다.

일반적으로 공격자는 크게 내부 공격자와 외부 공격자로 나누어진다. 외부 공격자는 시스템에 인가 받지 않은 자가 네트워크를 통하여 공격을 시도하는 형태이다. 외부 공격자는 공격을 하고자 하는 시스템에 직접 공격을 가하지 않고 다른 시스템을 이용하여 공격을 하던지, 공격 시스템의 송수신 정보를 도청하는 등의 우회적인 공격을 취할 수도 있다. 두 번째 형태의 내부공격자는 해당 시스템의 인가를 이미 취득한 공격자로 자신이 소유한 권한 이상의 권한을 취득하려 하거나 접근이 금지된 또는 인가되지 않은 정보를 획득하는 등의 공격형태를 취한다.

IDS에는 크게 네트워크 기반의 IDS(NIDS)와 호스트 기반의 IDS(HIDS)가 있다. 한때 어느 쪽이 더 좋은가에 대한 논쟁이 있었으나 오늘날에는 두 형태 모두를 결합한 혼합 형태(hybrid type)의 솔루션을 취하는 추세이다.

현재 IDS 구현 방법으로 크게 로그를 추적하는 방법, 네트워크 모니터링 방법, 그리고 이상(anomaly) 및 오용(misuse) 탐지 등이 있다. 로그를 추적하는 방법은 가장 오래된 방법이면서도 여전히 많이 쓰이는 방법이다. 이 방법은 네트워크에서 일어나는 모든 활동을 가능한 상세히 로깅 함으로써 공격을 탐지하는 형태이다. 네트워크 모니터링 방법은 네트워크의 트래픽(traffic)을 모니터링 하면서 미리 정의된 규칙과 비교함으로써 공격을 탐지한다. 마지막으로 이상 탐지는 이미 알려진 공격 패턴과 비교하여 공격을 탐지하며 구현 방법이 상대적으로 용이하고 정확성이 높기

때문에 현재 IDS의 주류를 이루고 있다. 그러나 비정상적인 행위를 통한 침입의 경우 탐지할 수 없다는 단점을 가지고 있다. 이상 탐지는 시스템 자원의 비정상적인 행위나 사용에 근거하여 공격을 탐지한다. 아직 초기 단계이지만 오용 탐지의 단점을 보완할 수 있다는 가능성으로 인해 주목받는 방식이다. 현재 IDS의 모델은 각각의 문제점을 가지고 있으며 완벽한 것이 아니다. Tim Bass는 그의 논문[12]에서 Multisensor data fusion을 이용한 차세대 분산 IDS를 소개했다.

IDS는 침입을 탐지할 수 있다는 장점 때문에 컴퓨터 포렌식스에 있어 중요한 역할을 한다. IDS가 없는 경우 침입 발생 사실을 공격이 종료된 후에야 알 수 있다. 아니면 공격 사실 자체를 모를 수도 있다. 이런 경우 공격자는 자신의 공격 사실을 숨기기 위해 로그 파일에서 자신의 침입 흔적을 지운다든지 차후 공격을 위한 root-kits을 설치한다는 등의 행위를 할 것이다. 그러나 IDS가 정상적으로 동작한다면 침입 상태를 그대로 유지할 수 있다. 다음은 IDS를 이용하여 컴퓨터 포렌식스를 강화할 수 있는 방침이다[13].

가) 정보 유지하기(Retaining Information) : 응용프로그램이나 시스템 로컬 사용자 파일 등을 복사, 유지한다. 그리고 컴퓨터 및 네트워크에 관련된 로그를 복사, 유지한다.

나) 대응 계획하기(Planning the Response) : 포렌식스 팀 구성, 침입에 대한 대응 절차 수립, 그리고 조사 절차를 형식화 한다.

다) 훈련하기(Training) : 대응 팀과 조사 팀이 구성되면 구성원에 대한 대응과 조사에 필요한 교육을 실시한다.

라) 조사에 착수하기(Accelerating the Investigation) : 개인 파일의 암호화나 디스크를 청소하는 도구 그리고 파일을 조각으로 나누는 등의 프로그램 사용을 금지시킨다. 또한 수집한 정보에 인덱스를 부여하여 조사에 누락된 정보가 있는지 검사한다.

마) 익명의 활동 금지시키기(Preventing Anonymous Activities) : 익명의 인터넷 접속을 위한 Onion Routing[4]을 금지하고 수집된 정보의 날짜, 시간, 특성 등을 조사하며 강한 사용자 인증과 접근 제어 메커니즘을 사용한다.

바) 디지털 증거물의 보호(Protecting the Evidence) : 디지털 증거물은 관리자 권한의 강한 통제 하에 유지하며 디지털 증거물을 암호화 하여 보존한다. 암호화를 통한 디지털 증거물의 보호만으로는 충분치 않으므로 데이터 무결성을 제공하는 무결성 검사 기술 등을 디지털 증거물에 적용한다.

4) 공중망을 통한 private communication을 위한 범용 인프라구조이다.

위에서 제시한 방법은 IDS가 설치된 경우만 해당하는 것은 아니나 이는 보다 효율적이고 체계적인 디지털 증거물을 수집, 보존하는 절차를 제시하고 있다.

6. 컴퓨터 포렌식스를 위한 체계적인 기준 제시

본 절에서는 보다 효율적이고 체계적인 디지털 증거물을 확보할 수 있는 기준을 제안한다.

가. 주기적인 백업(Regularly Backup)

백업은 컴퓨터 포렌식스 준비뿐만 아니라 화재, 정전, 기타 사고에 의한 데이터 손실을 방지할 수 있다. 시스템으로부터 수집된 정보는 컴퓨터 범죄가 발생하기 전까지 잠재적인 증거물이 된다. 이러한 특성상 여건이 허락된다면 가능한 많은 정보를 백업하는 것이 좋다. 특히 응용 프로그램의 출력물, 숨겨진 파일, 네트워크 및 감사 로그 파일 등은 반드시 백업을 한다. 이 파일들은 공격을 추적하는데 많은 도움을 준다. 그리고 백업 장소는 가능한 외부로부터 접속이 차단된 장소나 매체를 선택한다. 예로 자기 테이프나 CD-ROM 등에 주기적으로 백업을 하던지 시스템과 로컬 연결만 가능한 백업 머신 등을 이용하여 백업 자료를 보호한다. 추가적으로 중요한 백업 내용은 암호화나 데이터 무결성 메커니즘을 이용할 수도 있다. 마지막으로 백업의 모든 활동(자동화된 도구를 이용하든지 관리자가 직접 백업을 하든지)은 시간, 날짜, 수행자 등의 정보와 함께 문서화하여 유지, 보관한다.

나. 정보 유지하기(Freezing the Scene)

IDS의 침입 사실 통보, 시스템의 이상 발견, 로그 파일 분석 등의 방법을 통해 침입 사실을 확인하게 되면 당시의 시스템 상태를 그대로 유지해야 한다. 특히 휘발성 순서(Order of Volatility)[3]에 따라 사라질 수 있는 레지스터, 캐쉬, 라우팅 테이블, arp 캐쉬, 프로세스 테이블, 커널 상태, 메모리, 임시 파일 등은 반드시 복사, 유지한다. 이 과정에서 수집된 정보는 이후 정보 수집 과정에서 수집된 정보보다 공격이나 침입을 분석, 추적하는데 더 많은 도움을 주게 된다.

다. 공격에 대응하기(Response of Attack)

공격에 대한 정보를 유지했다 하더라고 공격에 대한 대응이 이루어지지 않으면 잠재적인 증거물에 대한 변경, 삭제 등의 위험이 존재하게 된다. 따라서 시스템은 외부로부터 접근 경로를 차단하고 적절한 대응 방안을 수립한다. 서비스를 계속적으로 제공해야 할 경우 로깅을 강화하고 강한 인증과 접근 통제 메커니즘을 사용한다. 침입에 대한 대응으로 시스템의 전원을 차단하는 것은 많은 정보를 잃을 수 있으므로 인터넷 접속 경로를 차단하던지 공격자의 연결을 차단하는 식의 대응을 하는 것이 바람직하다.

라. 정보 수집하기(Acquiring Information)

컴퓨터 포렌식스에서는 컴퓨터에 관련된 모든 정보가 증거물이 될 수 있기 때문에 가능한 많은 정보를 수집한다. 수집한 증거물은 일정 순서(시간이나 저장위치)에 따라 정렬, 인덱스를 부여하여 문서화 한다. 이 정보들은 직접적인 증거물이 될 수도 있고 그렇지 않을 수도 있다. 정보 수집에 있어 필요한 도구나 소프트웨어는 읽기전용 매체에 따라 보관, 유지한 것을 사용한다. 그리고 정보 수집 과정에 있어 [3]에서 제시한 프라이버시(Privacy)와 적법성에 관련된 고려사항은 반드시 만족되어야 한다.

마. 증거물 조사하기(Investigation)

증거물 조사는 전문가가 아니면 피하는 것이 바람직하다. 이는 원천 정보의 손실 방지와 잘못된 결과 유출을 막기 위함이다. 이 단계는 컴퓨터 포렌식스 관련 교육을 받은 관리자에 한해서 진행되어야 한다. 증거물 분석 시에는 분석한 사람, 시간과 날짜, 증거물의 정보, 분석 결과 등을 문서화한다. 분석된 결과는 동일한 방식을 통해 시현이 가능해야 하며 원천 정보를 변경, 손실시켜서는 안된다.

바. 증거물 보호하기(Protecting Evidence)

컴퓨터 포렌식스에 있어 또 하나 중요한 부분 중 하나는 증거물의 보호이다. 이는 법적 증거물로 사용되므로 증거물의 보호는 반드시 이루어져야 한다. 먼저 지금까지의 과정은 문서화하여 유지, 보관하며 증거물과 관련 정보는 암호화 및 무결성 검사용 메카니즘을 이용하여 보관한다. 또한 증거물에 대한 접근 권한을 제한하며 접근 시 접근 내역을 기록한다. 증거물은 읽기전용 매체나 외부 연결이 차단된 매체에 보관하며 증거물의 전송이 필요한 경우 암호학적 기술(전송 데이터 보호, 강한 인증 메커니즘, 데이터 무결성 유지 등)을 적용한다.

사. 법 집행 기관에 연락(Contact with Law Enforcement)

수집된 정보와 분석된 결과를 바탕으로 회사나 단체의 로컬 정책에 따라 법 집행 기관에 연락을 취한다.

지금까지 제안된 기준이 컴퓨터 포렌식스 준비에 있어 완벽한 것은 아니다. 그러나 제안된 절차는 지금까지 언급된 내용들을 정리한 것으로 회사나 단체의 로컬 정책 수립 시 도움을 줄 것이다.

III. 결론

최근 컴퓨터 관련 범죄는 인터넷과 컴퓨터의 발전에 따라 급속히 증가하고 있다. 대부분의 기업, 관공서, 학교 등은 컴퓨터 범죄나 보안 취약점을 탐지, 감소시키는데 초점을 맞추고 있다. 그러나 현재 보안 솔루션들은 완전한 보안을 제공하는 것이 아니므로 컴퓨터 포렌식스에 대한 인식이 필요하다. 많은 사람들이 컴퓨터 포렌식스는 컴퓨터 관련 범죄가 발생한 이후 이루어지는 범죄 조사 과정이라며 전문가에 의해서만 이루어진다고 생각한다. 그러나 이는 잘못된 생각으로, 앞에서 살펴보았듯이 비록 컴퓨터 포렌식스 전문가가 아니더라도 필요한 정보를 수집해야 하며 이에 적합한 교육을 관리자는 받아야 한다. 또한 컴퓨터 포렌식스에 필요한 정보 또는 증거물은 범죄가 발생하기 전에 수집되어야 한다. 즉 컴퓨터 포렌식스는 사건이 발생하기 전 발생할 사건에 대한 증거물 수집으로부터 시작된다고 볼 수 있다. 컴퓨터 관련 범죄의 특성상 컴퓨터 관련 모든 정보는 잠재적 증거물로써 수집되어야 하며 사건 발생 시 이 잠재적 증거물을 토대로 법적 증거물을 분석, 추출할 수 있게 된다.

본 논문에서는 컴퓨터 포렌식스에 대한 개념과 몇 가지 예를 통하여 일반적인 준비 절차에 대해 살펴보았다. 또한 보다 체계적이고 효율적으로 컴퓨터 포렌식스를 준비할 수 있는 로컬 보안 정책 수립에 도움을 줄 수 있는 기준을 제시하였으면 이 기준이 많은 도움을 줬으면 한다.

참고문헌

[1] Judd Robbins, "An Explain of Computer Forensics", http://computerforensics.net/forensics.htm

[2] CERT Coordination Center, "How the FBI Investigate Computer Crime", http://www.cert.org/tech_tips/FBI_investigates_crime.html

[3] Dominique Brezinski, Tom Killalea, "Evidence Collection and Archiving", [RFC3227], February 2002

[4] Bruce Schneier, John Kelsey, "Secure Audit Logs to Support Computer Forensics", ACM Transactions on Information and System Security, v. 2, n. 2, May 1999, pp. 159-176.

[5] Ranum M., "Network Forensics: Network Traffic Monitoring", Network Flight Recorder Inc. 1997.

[6] John Tan, "Forensic Readiness", http://www.atstake.com/research/reports/, July 2001.

[7] 이현우, 김영직, 전숙, "UNIX 피해시스템 분석 및 침입자 모니터링 : Part I v1.0", http://www.certcc.or.kr/paper/paper-1.htm, 07, 2001

[8] "Digital Evidence: Standards and Principles", Forensic Science communications,

April 2000 Vol 2

[9] 임채호, "중요정보통신망 해킹시 침입자기법 분석과 대응", 한국정보보호센터, 01. 1999

[10] Christopher Patrick Murray "Network Forensics", http://mrs.umn.edu/~lopezdr/seminar/fall2000/Murray.htm, 2000

[11] University Of Melbourne, "Intrusion Detection Systems and A View To Its Forensic Applications", 1999

[12] T. Bass, "Multisensor data fusion for next generation distributed intrusion detection systems", In Proceedings, 1999 IRIS National Symposium on Sensor and Data Fusion, May 1999.

[13] Alec Yasinsac, "Policies to Enhance Computer and Network Forensics", Proceedings of the 2001 IEEE, June, 2001