韓國 컴퓨터情報學會 2006동계학술발표논문집&학회지
第14卷 第2號, 2006. 12.

포렌식 자료의 무결성 확보를 위한 수사현장의 연계관리 방법 연구

이 규 안*, 박 대 우**, 신 용 태***

A Study on the Chain of Custody for Securing the Faultlessness of Forensic Data

Gyu-an Lee *, Dea-Woo Park **, Young-Tae Shin ***

요 약

컴퓨터 포렌식은 정보통신 기술의 순기능을 보호하고 역기능에 대한 증거를 추출하여 법정에 제출하는 과정을 다루게 된다. 컴퓨터 수사 현장에서 디지털증거의 무결성이 훼손된다면, 결정적인 증거가 기각당하거나 재판의 증거로서 채택되지 않는다. 본 논문에서는 이 문제점을 해결하는 방안으로 포렌식 자료의 무결성 확보를 위한 디스크 포렌식의 연계방안, 시스템 포렌식의 연계방안, 네트워크 포렌식의 연계방안, 모바일 포렌식의 연계방안, 데이터베이스 포렌식의 연계방안을 연구한다. 제안된 연계방안으로 무결성이 입증되면, 수사 결과물들이 범죄 수사현장과 재판의 중요 증거 자료로 채택하게 될 것이다. 또한 실제 컴퓨터 포렌식 수사 현장에서의 디지털증거의 연계방안의 현장 수사의 문제점의 사례와 대안을 제시함으로서, 컴퓨터 디지털 포렌식의 발전과 정보보호의 현장 연구에 기여하게 될 것이다.

Abstract

Computer Forensics functions by defending the effects and extracting the evidence of the side effects for production at the court. Has the faultlessness of the digital evidence been compromised during the investigation, a critical evidence may be denied or not even be presented at the trial. The presented monograph will deliberate the faultlessness-establishing chain procedures in disk forensics, system forensics, network forensics, mobile forensics and database forensics. Once the faultlessness is established by the methods proposed, the products of investigation will be adopted as a leading evidence. Moreover, the issues and alternatives in the reality of digital investigation are presented along with the actual computer forensics cases, hopefully contributing to the advances in computer digital forensics and the field research of information security.

▸ *Keyword : Chain of Custody, Computer Forensics, Digital Evidence, Integrity.*

• 제1저자 : 이규안, 교신저자 : 박대우(prof1@paran.com)
* 숭실대학교 대학원 컴퓨터학과, **숭실대학교 정보과학대학원 정보보안학과 ***숭실대학교 컴퓨터학부

Ⅰ. 서 론

유비쿼터스(Ubiquitous) 기술이 발전하면서 인터넷을 이용한 업무가 확장되고, 정보전달을 통한 지식정보화 사회가 급격히 확장되고 있다. 하지만 정보화 사회의 부작용으로 나타나는 불법적인 정보의 침해 활동은 정보통신부의 2006년 자료에서 표 1.과 같이 날로 늘어나고 경제적, 금융적인 피해를 수반하고 있다.

표 1. 2005년 공공분야 침해사고 발생현황
Fig. 1 Status of Public Field Intrusion Cases 2005

유형	웜·바이러스감염	경유지 악용	홈페이지 변조	자료훼손 및 유출	기타	합계
국가기관	231	37	16	41	7	332
자자체	599	83	67	11	8	768
연구소	108	51	15	4	5	183
교육기관	1058	944	519	20	5	2,546
산하기관	506	82	68	8	8	672
기타	1	17	2	3	24	47
합계	2,503	1,214	687	87	57	4,548

정보통신망이용촉진및정보보호등에 관한 법률은 "누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입한자"는 3년 이하의 징역 또는 3천만원이하의 벌금에 처하도록 규정하고 있고, "접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위"를 한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처하는 등 법적인 제도[1]가 마련되었다.

제도와 법의 제정에 따라서, 정보의 불법적인 침해와 피해를 다루는 컴퓨터 범죄수사는 컴퓨터 포렌식(Computer Forensic)의 기법과 함께 도입되고 있으나, 아직 컴퓨터를 이용한 범죄의 기법보다는 뒤쳐지고 있는 것이 현실이다.

최근의 컴퓨터 범죄수사는 오프라인 수사에 있어서도, 범죄 현장에서의 DB 압수수색, 시스템 분석 등 컴퓨터 압수·수색 및 디지털 증거의 분석이 범죄의 입증 및 공소 유지를 위한 필수 불가결한 절차로 인식되고 있다. 특히 정보화와 더불어 개인과 기업, 공공기관의 업무가 수 년 사이에 대면결제에서 전자결제로 급속하게 전환되고 있어 정보의 보관방법도 종이 등에서 컴퓨터, PDA, 기타 이동식 저장장치로 다양화되어 디지털증거의 중요성은 더욱 커졌다.

하지만 컴퓨터 범죄수사와 재판에서 디지털증거의 중요성은 인식하지만, 실무에서는 디지털 포렌식(Digital Forensics)이라는 용어에 대한 명확한 규정도 미비한 상황이다. 재판에서 증거주의에 입각한 사법부의 판결에 의해 컴퓨터 범죄수사 기관에서도 과거의 서류철과 회계장부 등 눈에 보이는 증거에서 벗어나, 눈에 보이지 않는 디지털증거의 획득·복원·분석 등의 일련의 과정들이 중요하다. 이러한 디지털 포렌식의 과정들을 절차에 따라 진행하고 법정에 제출하여 증거로 채택될 수 있도록 디지털증거의 무결성(Integrity)을 보장하는 것이 디지털 포렌식[2]이라고 할 수 있다.

컴퓨터와 관련된 증거를 언급할 때, 종전에는 컴퓨터 증거(Computer evidence), 컴퓨터 관련증거(Computer-related evidence)라고 하였고, 현재는 물리적인 증거와 디지털 혹은 전자적 형태의 증거를 구별하기 위하여 전자증거(Electronic evidence)나 디지털증거(Digital evidence)라는 용어를 사용한다.

이러한 디지털증거를 수집하거나 획득하여 유실된 자료를 복원하고, 복원된 자료를 통하여 필요한 정보를 획득하는 일련의 과정들은 전문적인 기술을 가진 디지털 포렌식 전문가에 의하여 진행되어야 하다. 이에 따라 컴퓨터 범죄 수사 전문가들도 컴퓨터 기술의 발전에 따라 연구와 노력으로 새로운 기술을 습득하여야 한다.

하지만 컴퓨터 범죄 수사기관의 경우 통상적인 수사업무와 수사지원 등으로 인하여 새로운 기술의 습득하기 어려운 점이 있다. 또한 기존의 일반적인 압수수색의 방법에 의하여 디지털증거를 압수수색 함으로써 결과적으로 디지털 증거의 무결성이 훼손되어 재판의 증거로서 가치를 상실하는 경우가 발생하고 있다. 또 초등단계인 수사 개시부터 공판에 이르기까지 디지털증거의 절차를 살펴보면 디지털 증거의 무결성 확보를 위한 여러 가지 문제점[3]이 있음을 알게 된다.

본 논문에서는 이러한 문제점을 해결하는 방법으로 포렌식 자료의 무결성 확보를 위한 연계관리 방법을 연구한다. 제안된 연구 방법으로는 디스크 포렌식의 경우 디지털증거의 연계방안과, 네트워크 포렌식의 경우 디지털증거의 연계방안을 연구함으로서, 디지털 포렌식에서 디지털 증거의 무결성을 입증하는 연계방안을 제안하고 이를 현실적인 범죄 수사와 재판의 실무과정에서 제안하는데 그 목적이 있다.

본 논문의 연구를 통해 디지털 포렌식을 통한 디지털 증거의 무결성을 입증함으로써 컴퓨터 범죄에 대한 명확한 증거를 확보하고, 컴퓨터 범죄의 증거자료의 공정성을 유지하여 디지털시대에 발맞춰가는 컴퓨터범죄 수사 및 재판에 대한 컴퓨터기술을 확보하고자 한다.

II. 관련 연구

컴퓨터범죄에 대한 수사와 재판을 위해 디지털증거를 수집하는 일련의 과정들을 디지털 포렌식이라고 한다. 디지털 증거의 무결성을 보장하는 연계방안을 제시하기 위하여 디지털 포렌식의 정의와 절차에 관하여 전반적인 것을 살펴보고 디지털 포렌식의 분야 및 유형을 살펴본다.

2.1. 디지털증거

전자적으로 처리되는 디지털증거는 다음과 같은 특징[4]을 가지고 있으므로 증거자료의 수집·분석·보존 등의 과정에서 특별한 절차와 기법을 따라야 한다.

1) 불가시성(Latent, Invisible and Unreadable)

눈에 보이지 않는 0과 1의 조합인 디지털형태로 저장되어 잠재성, 은닉성, 불가시성, 불가독성을 갖기 때문에 그 적발과 증명이 곤란하다.

2) 취약성(Fragile, Easily altered or destroyed)

변조나 손상이 쉽고 변조사실을 찾아내기 어렵기 때문에 사후에 법정에서 조작여부, 증거 획득절차의 적정성 등이 문제가 될 수 있다.

3) 디지털(Digital)

0과 1의 디지털신호로 되어 있어 원본과 동일한 내용으로 쉽게 복제할 수 있으며, 원복과 복제본의 구별이 쉽지 않다.

4) 대량성(Massive)

기업의 전산 회계자료, 데이터베이스 자료나 파일서버의 문서자료 등은 데이터양이 수백 기가바이트에 이를 만큼 양이 방대하여 특별한 도구나 전문 인력을 사용하지 않고 범죄의 단서나 증거를 찾는 다는 것은 거의 불가능하다.

5) 국경초월성(Trans border)

디지털증거는 인터넷을 통하여 전송되거나 저장되기 때문에 장소의 제한을 받지 않고, 원거리 또는 타국의 서버나 컴퓨터에 존재할 수 있다.

2.2. 디지털 포렌식

1) 디지털 포렌식의 정의

증거법칙과 적법절차에 따라 증거의 무결성을 유지하면서 컴퓨터 시스템, 네트워크, 컴퓨터 저장매체 등으로부터 디지털증거를 수집, 보존, 분석하여 법정에 증거를 제출하는 일련의 과정을 의미한다.

2) 디지털 포렌식의 주요내용

가) 증거수집(Aquisitton)
- 디스크 이미징
- 컴퓨터 하드 디스크 백업

나) 분석(Exams)
- 컴퓨터 하드 백업 및 분석
- 각종 저장매체(USB Memory, Tape backups) 분석
- 데이터베이스, 회계 솔루션 등으로부터 관련자료 추출

다) 추적(Tracking)
- 인터넷사용자의 IP추적
- 네트워크 연결상태, 포트 조사

라) 압수수색현장지원(On site Assitance)
- 압수수색 현장에서의 증거수집

마) 데이터복구(Data Recovery)
- 삭제된 파일 등 복구
- 삭제 메일 복구

바) 패스워드 복구 (Password and Encryption Cracking)
- 마이크로소프트워드, 엑셀, PDF, Zip 파일등 패스워드 복구

사) 조사과정의 문서화
- 조사과정의 기록(Examination Documentation)
- 보관의 연속성(Chain of Custody)

아) 증거의 무결성 유지
- 검증(Authentication)
- 디지털 타임 스탬핑(Digital time stamping)
- 해쉬값의 사용

자) 증거의 법정제출
- 증거의 제출과 법정 증언

3) 디지털 포렌식의 3요소

디지털증거의 분석에 디지털 포렌식을 적정하게 사용하기 위하여는 3가지 요소가 상호 지원되어야 하며, 첫째는 훈련된 전문인력으로 전문가 양성과정이나 학교교육을 통하여 이론과 실무가 겸비한 전문가가 필요하다. 둘째로 디지털 포렌식장비가 있어야 한다. 현재 디지털 포렌식장비의 대부분이 외산장비로서 국내 실정에 맞지 않을 뿐만 아니라 막대한 외화유출의 한 원인이 되고 있다. 외제 장비의 경우 컴퓨터 장비의 발전에 따른 업그레이드가 지연 혹은 지원되

지 않는 경우도 발생하고 전달교육의 부실 등으로 효과적인 장비활용의 걸림돌이 되고 있다. 셋째로는 디지털 포렌식의 표준 지침의 미비로서 현재 수사기관이나 학계에서 어떠한 표준을 제시하지 못하고 있다.

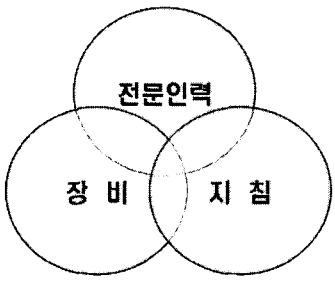

그림 1. 디지털 포렌식의 3요소
Fig. 1 3 Elements of Digital Forensic

4) 연계과정(Chain of Custody)

컴퓨터증거는 다른 증거와 마찬가지로 제출된 컴퓨터증거가 수사기관에서 압수한 증거와 동일하다는 것을 입증할 수 있어야 한다. 전자데이터(Electronic Data)는 변경이 용이하기 때문에 인계인수 책임의 연속성(Hand-to-Hand Chain of Accountability)에 따른 연계과정이 필요하다[5]. 증거에 대한 접근이 엄격하게 통제되어야 하며, 증거를 조사한 사람, 일시, 조사를 위하여 행한 조치와 절차 등에 대한 기록을 문서화 해야 한다.

보관 관리의 연속 또는 보관의 연속성이란 증거가 어떻게 수집되어, 누구에 의하여 분석, 보존되었는가를 보여줄 수 있는 로드맵(Roadmap)을 말하는 것이다.

보관 관리의 연속에 대하여 주의하는 이유는 증거의 무결성을 보호하는 것뿐만 아니라 법정에서 수사기관에서 증거를 다루는 동안 증거가 조작되었다고 주장하는 것에 대처하기 위한 것이다.

5) 자료의 무결성

디지털 증거가 원본 소스(Orignal Source Data)로부터 수집되어 보관, 분석되는 과정에서 부당한 수정(Alteration), 변경(Modification), 손상(Damage or Destruction)이 없도록 유지하는 과정이다.

이를 위하여 컴퓨터데이터를 안전하게 보존하고 원본데이터와 사본데이터가 동일하다는 것을 검증할 수 있어야 한다.

검증이란 원본증거와 현재 증거로 제출하는 증거사본이 동일하다는 것을 입증하는 것을 말한다.

2.3. 디지털 포렌식의 유형

1) 디스크 포렌식(Disk Forensics)

디스크 포렌식은 물리적인 저장매체인 하드디스크, 플로피디스크, 각종 보조기억장치에서 증거를 수집하고 분석하는 포렌식 분야로서 디스크 포렌식은 포렌식의 여러분야중에서 가장 발전되어 있는 분야이다[6]. 이와 유사한 업무를 지원하는 업체로는 파이널데이터사와 명정보시스템[7]이 하드디스크 복원분야에서 활동 있으나, 이는 무결성을 지원하지 않고 다만 데이터의 복원부분에 관하여 지원하고 있다.

디스크 포렌식은 디스크를 검색하여 삭제된 파일을 복구하고, 패스워드나 암호가 설정되어 있는 파일의 경우 패스워드나 암호키를 복구하여 증거를 찾아내는 작업[8]을 말한다. 여러 가지 종류의 파일을 파일 확장자, 부서, 작성자, 작성일시, 사용일시 등을 기준으로 분류하고, 검색 키워드를 사용하여 수사단서를 추출하는 작업을 병행한다. 이때 주의하여야 할 점은 원본데이터를 사용하지 않는다. 복사본을 사용하여야 하며, 부득이 원본데이터를 사용해야 하는 경우에는 디스크의 변경을 방지하기 위하여 그림 2.와 같이 쓰기방지장치를 사용하여 디스크를 분석하여야 한다.

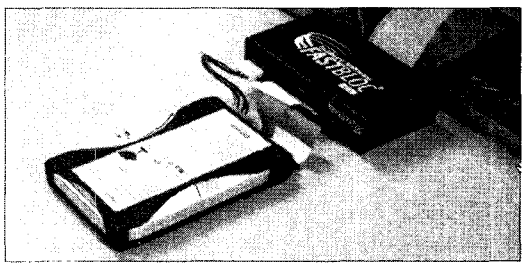

그림 2. 쓰기방지장치가 부착된 디스크
Fig. 2 Hard Disk Equipped with Anti-writing Device

2) 시스템 포렌식(System Forensics)

시스템 포렌식은 컴퓨터 시스템의 운영체제, 서비스, 응용 프로그램 및 프로세스를 분석하여 증거를 확보하는 분야다. 컴퓨터 시스템은 Windows 9×, Windows NT/2000, 리눅스, 유닉스 등 다양한 운영체제를 사용하게 되는데 분석대상의 컴퓨터 시스템에 따라 시스템 포렌식을 윈도우 포렌식, 리눅스 포렌식, 유닉스 포렌식 등으로 나누기도 한다.

3) 네트워크 포렌식(Network Forensics)

네트워크 포렌식은 네트워크를 통하여 전송되는 데이터나 패스워드 등 데이터 트래픽을 분석하거나, 접근·에러 로그,

네트워크 환경 등을 조사하여 수사단서를 찾아내는 분야이다. 네트워크를 통하여 데이터가 전송되는 과정에서 생성되는 자동 로그 기록을 분석하거나 Sniffer와 같은 프로그램[2]을 사용하여 트래픽 데이터를 직접적으로 가로채는 방법을 증거를 획득할 수 있다.

대부분의 네트워크는 사용자의 행위를 감시하고 추적하기 위한 장치를 가지고 있다. IP 헤더는 발신자 및 최종 목적지 IP주소 정보를 포함하고 있으며, 데이터 링크 헤더는 하드웨어 주소 정보를 포함하고 있다. 네트워크의 관문 역할을 하는 라우터에는 routing table, arp cache table, login해 있는 사용자, TCP connection과 관련된 정보, NAT translation과 관련된 정보가 존재하기 때문에 침해시스템을 조사할 때 라우터의 분석은 매우 중요하다. 그림 3.은 해커의 공격 툴인 Sniffer 등을 이용하여 인터넷 사용자의 패스워드를 획득하는 과정[9]을 보여주고 있다.

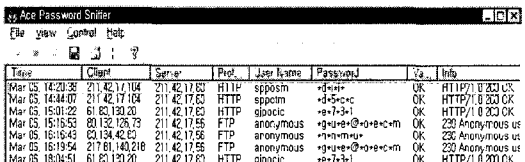

그림 3. Ace Password Sniffer의 실행화면
Fig. 3 Ace Password Sniffer Screen

인터넷을 통하여 서비스되는 웹드 와이드 웹, ftp, Usenet 등 인터넷 응용 프로토콜에서 증거를 수집하고 분석하는 포렌식 분야다. 인터넷상에서 불법행위를 한 해커와 같은 용의자의 DDoS(Distributed DoS) 공격이나 Worm공격[10]를 추적하기 위한 웹 히스토리(WWW history)분석, 전자우편 헤더분석, 전자우편 수신자 추적(E-Mail Tracking), WHOIS 검색 및 IP 추적 등이 인터넷 포렌식의 주요 내용이 된다.

이는 게시판에 불법정보를 업로드 하거나, 명예훼손성 글을 올린 용의자추적, 전자메일 발신자 및 수신자 확인, 인터넷 서핑 내용 추적을 위하여 인터넷 로그기록, 히스토리, 다운로드 받은 파일이나 문서를 분석하는 작업이 필요하다. 현재 많은 사람들이 일반적인 편지를 보내기보다는 전자우편을 사용하여 정보를 주고받기 때문에 이 분야를 전자우편 포렌식 분야로 분류하기도 한다.

2) manpage, tcpdump와 같은 도구가 있음

4) 모바일 포렌식(Mobile Devide Forensics)

모바일 포렌식은 PDA, Laptop, 전자수첩, 휴대폰, 디지털 카메라, MP3 플레이어, 휴대용 메모리카드, USB 저장장치 등 휴대용 기기에서 필요한 정보를 입수하여 분석하는 포렌식 분야다. 휴대폰 및 PDA의 보급이 급속도로 늘어나고 유비쿼터스 컴퓨팅이 활성화 되면서 다양한 종류의 멀티미디어 기기가 개발되어 보급되고 있다. PDA는 일상적인 업무에 사용되어지고 있고, 모바일 포렌식의 증거자료로서 압수수색과 증거확보는 매우 중요한 시점에 와 있다. 특히 이러한 소형화된 기기는 이동성과 은닉성이 뛰어나기 때문에 압수수색 시 데이터가 저장되어 있는 소형저장장치가 은닉되어 있는지 여부를 세심하게 조사하는 것도 관건이다. 최근에 열어보거나 저장한 파일의 드라이브 위치를 조사하거나 링크파일을 분석하여 이동식 저장장치의 사용여부를 확인할 수 있다.

5) 데이터베이스 포렌식(DataBase Forensics)

기업의 회계분석, 횡령, 탈세 등 각종 범죄를 수사할 때 기업의 정보시스템에 저장되어 있는 데이터베이스를 분석하는 사례가 증가하고 있다. 데이터베이스 포렌식은 전사적자원관리시스템(ERP), 전산 회계자로에서 증거자료를 추출하고 분석하는 분야로서 통상 이루어지고 있는 일반 컴퓨터 압수수색과는 달리 기업의 전산자료 압수수색은 여러 가지 어려운 점이 있다. 대용량과 실시간 업데이트 등으로 인하여 그림 4.와 같은 기업전산자료 분석 시스템[11]을 이용하며 전문적인 기술과 지식을 필요로 한다.

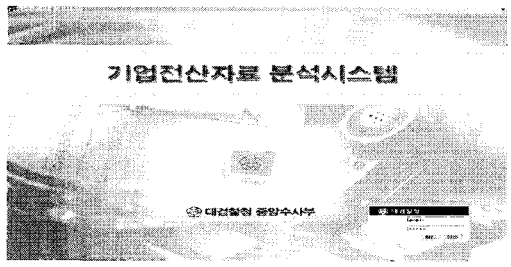

그림 4. 기업전산자료 분석시스템
Fig. 4 Business Computing Data Analysis System

2.4. 디지털 포렌식 절차

1) 증거확보

디지털 저장장치에 저장된 정보의 유형과 형태를 확인하는 확인단계로, 증거자료 확보가 관건이다.

2) 증거입증

보존단계로서 디지털로 저장된 자료를 확인 한 후, 변경되지 않도록 보존하는 단계이다. 만약 변경이 될 경우에는 법적 절차에 따라 변경된 원인을 설명해야 한다. 이것은 자료뿐만 아니라 자료를 읽을 수 있는 기기의 변경도 포함한다.

3) 증거분석

디지털자료를 추출, 처리, 판단하는 단계로 분석용 도구를 이용하여 디지털자료를 분석하는 단계이다. 자료분석 시에는 검사대장 자료가 변경되지 않도록 주의해야 한다.

4) 증거제출

마지막 단계로서 법정제출을 의미한다. 법정에서 진술방법, 발표자의 전문적인 기술과 위의 세 가지 단계가 법적 증거자료로서, 신빙성있게 서술될 수 있도록 체계적으로 준비하는 것을 의미한다.

2.5. 디지털 자료의 무결성 실패 사례

1) 국내 사례

2001년 10월 경남 진주 00농협 등 7개소에 명예훼손의 내용을 담은 편지가 전달되어 수사기관에 진정을 하였다. 피진정인의 컴퓨터를 압수수색하여 삭제된 문서파일을 복구하여 그 결과로서 각 편지가 발송된 주소록과 동일한 필체의 문서를 추출하게 되어 디지털증거로 채택하게 되었으나, 복구된 #529487.hwp[3]파일의 최초 생성일자가 범행일자 이후라는 근거로 재심을 청구하게 되었고 재판부의 재심결정으로 재심 후 기각결정을 하였다. 이는 수사기관에 디지털 증거물에 대한 이해부족 및 컴퓨터 포렌식의 중요성을 부각시킨 사례로서 디지털증거의 획득, 분석, 이동, 보관 등 절차의 연계표준이 필요한 사례가 되었다.

2) 국제 사례

"Maxim"이라는 해커가 인터넷 쇼핑몰인 CD Universe의 컴퓨터에 침입하여 300,000개의 신용카드 정보를 불법으로 빼내어 간지 6개월간 미 당국은 그 해커를 찾고 있었다. 그러나 그 일에 대해 성공적으로 기소할 수 없었다. 왜냐하면 그 회사로부터 수집한 전자 증거들이 적절히 보호되지 못했기 때문이다. 디지털 증거에 대한 보존의 실패로 그 사건에 대한 기소 가능성을 없애 버렸다.

CD Universe의 증거들이 훼손된 경위는 다소 흥분된 상황에서 FBI이 요원들과, 세 업체의 컴퓨터보안 회사의 직원들이 해커가 어떻게 네트워크에 침입하고 네트워크 보안을 뚫었는지 조사하고 네트워크 보안을 강화하기 위하여 작업하는 동안 발생하였다[12].

3) 복구된 디지털증거는 파일명의 첫 글자가 삭제되어 특수문자로 표시하게 된다.

III. 포렌식 연계관리 방법 연구

3.1. 디스크 포렌식의 연계관리 방법

수사기관에서 수사의 초기단계로서 고소·고발인으로 증거를 제출받거나 다른 이유로 인하여 수사를 시작하여 그림 5.와 같이 일반적인 압수수색의 단계로서 컴퓨터 등 디지털 증거자료를 압수하여 분류작업을 거치게 된다[13].

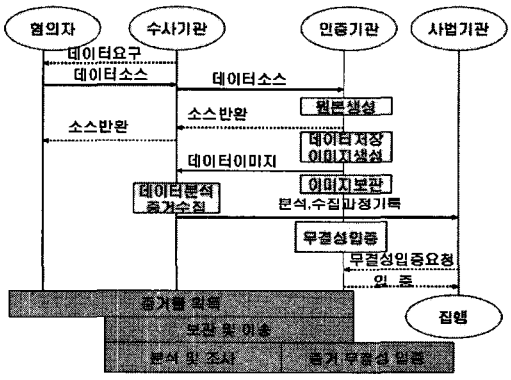

그림 5. 디지털증거의 무결성 입증순서
Fig. 5 Establishment Procedure of Faultless Digital Evidence

이때 컴퓨터 등의 입출력장치에 대하여 통제를 하게 되고 내용물을 검색하기 위하여 컴퓨터가 꺼져 있는 경우에는 동작을 시키는 등의 작업을 해서는 안된다. 동작이 되고 있는 상태라면 컴퓨터 등의 시간이 어떻게 설정이 되어 있는지 확인하고, 디지털 카메라로 촬영하는 등의 증거를 확보해야 하고 네트워크 케이블, 전원케이블, 기타 입출력장치에 대하여 별도의 표시를 하고 장부에 기재를 하여야 한다.

압수된 장비들은 분석팀에 인수인계를 하고, 분석팀은 장부에 인수일시 및 내용 등을 세부적으로 기재한다. 특이사항은 별도로 기재하여 보관하고, 그림 6.처럼 원본과 동일 한 복사본을 제작하여 원본과 사본의 동일성을 유지할 수 있도록 한다.

분석자는 사본을 통하여 분석을 진행하며, 이때 사본은 원본과 동일하다는 것을 입증하는 무결성의 방안으로 해쉬함수,

디지털 타임 스템핑의 작업을 하여 무결성을 보장한다[14].

그림 6. 원본과 동일한 복사본 제작
Fig. 6 Producing Identical Copies of the Evidence

분석자는 사본의 분석 시작일시, 분석프로그램, 분석종료 시각, 분석결과 등을 장부에 기재하고, 분석보고서를 작성한 후 사본을 반환한다. 분석팀에서는 장부에 기재를 하고 사본 및 원본을 법정에 제출할 때까지 보관하며, 이때 디지털 자료의 중요도를 검토하여 귀중품에 준하는 보관방식을 할 것인지를 결정한다.[4)]

법정에서 증거를 필요로 하는 경우 장부에 기재하고 대출받아 제출하며 이때 유실, 파손에 주의하여야 한다.

3.2. 시스템 포렌식의 연계관리 방법

컴퓨터 시스템의 운영체제, 서비스, 응용프로그램 및 프로세스를 분석하여 증거를 확보하는 것으로서, DOS(Disk Operating System), Windows 9×, Windows NT/2000, 리눅스, 유닉스 등 다양한 운영체제를 사용하므로 운영체제에 관한 깊은 지식을 요구한다. 시스템 포렌식에 사용되는 거의 모든 툴들은 윈도우 계열에서 사용되는 것들이고, 유닉스, 리눅스용으로 TCT(The coroner's Toolkit)나 TASK (@stake Sleuth Kit)을 이용하여 증거를 확보하여 분석[15]한다.

3.3. 네트워크 포렌식의 연계관리 방법

현재 가장 일반적인 네트워크 범죄는 인터넷침해사고, 개인정보 침해, 바이러스 제작 등으로 구분할 수 있다. 이러한 네트워크 범죄는 단순 오락형과 재산형으로 구분해 볼 수 있다. 오락형은 청소년들이 오락 등 게임 아이템을 취득하는 하나의 방안으로 백 도어를 설치하여 개인정보를 취득하여 아이템을 탈취하는 형태이며, 재산형은 재산상의 이득을 취할 목적으로 ID 갈무리, 백 도어 또는 Cain 툴 등을 이용한 스니핑(Sniffing)을 한 후 일반 사용자의 권한을 취득하여 이를 이용하여[9] 홈뱅킹을 시도하거나 취합된 정보를 매매하고, 또는 음란물을 판매하거나 P2P방식을 이용하여 다운횟수에 따른 요금을 부과하는 등 금전적인 이익이 목적이 된다.

이러한 네트워크형 범죄는 범행을 한 용의자의 신원을 확인하고 범행의 흔적을 조사하는 것이 매우 중요하다. 네트워크상에서는 개인의 신원 파악이 어렵게 되는 여러 가지 요인들로 응용프로그램과 기법들이 사용하기 때문에 로그파일 분석 등은 더욱 주의하여야 한다. 이때 수사에 사용되는 증거수집 방법으로는 화면캡처를 이용하여 이미지파일로 변환한 다음 PDF 파일로 변환하여 보관하며 또한 HyperSnap-DX, X-Player, WebZip, Flashget를 이용하기도 한다.

침해사고에 대응하기 위해서는 로그파일을 분석하고, 통신사실 확인 자료를 요청하여 혐의를 입증한다.

이러한 로그파일의 백업 및 자료요구 및 분석하는 일련의 과정들은 수사기관의 공문에 의한 요청이 아니면 진행할 수 없고, 포렌식 전문가에 의한 무결성이 입증된 방법으로 분석되고 보관되어야 한다.

3.4. 모바일 포렌식의 연계관리 방법

모바일을 통한 정보전달이 급속하게 발달하여, 디지털증거를 모바일 장비속에 보관하거나 이동의 수단으로 사용되고 있다. 플래시메모리의 경우에도 8GB이상의 대용량이 사용되어 휴대폰, USB메모리, 디지털카메라 등에 데이터를 저장하게 되었고, 이동성과 은닉성, 대용량화로 인하여 압수수색에 더욱 세심한 주의가 요구되게 되었다.

연계방법은 압수수색을 진행하는 동안에는 모바일장비들의 드라이브, 게이블, 전원부등을 구분하여 압수목록을 작성한 다음 별도의 보관함에 보관하여 관리하여야 한다.

특히 모바일 장비의 경우 전자파의 차단이 되어 있지 않는 장소에서 동작을 시키는 경우에는 데이터가 유입되는 등의 원인으로 인하여 무결성이 훼손되고 특히 증거의 연계과정에서 유실 및 파손이 염려되는 부분이 많다. 현재 모바일 장비의 경우 본체만 압수하여 분석을 진행하는 경우가 있으므로 제작회사에 의뢰하여 연결 케이블과 전원들을 별도 구매하여 분석하는 등 연계과정에 많은 문제점이 있다.

3.5. 데이터베이스 포렌식의 연계관리 방법

데이터베이스는 대용량의 데이터일 뿐만 아니라 실시간 정보를 제공함으로 데이터의 전송이 중단되는 일이 있어서는 않된다.

4) 압수규칙 제2조 제4호

불법 게임서버 등 일반인에게 피해를 주는 경우가 아니라면 운용중인 상태에서 필요한 정보를 백업받는 형식으로 자료를 제공받는다. 일반적인 근무시간 중에는 전문가를 통하여 백업을 받고, 서버 관리자를 통하여 백업요청을 하기도 한다. 대기업 등의 데이터베이스는 다수의 서버들이 서로 연계되어 있으므로 중간에 데이터를 위·변조하는 경우 데이터가 파괴되어 모든 데이터를 유실하게 되므로 백업중간에 데이터를 위·변조하는 일은 드물다. 단 대용량의 데이터를 백업받기 위해서는 수 시간 혹은 수일의 시간이 걸리므로 담당자는 인내와 끈기를 가지고 작업을 임해야 하고, 백업된 데이터의 분석을 위하여 수일간의 기간이 소요되는 단점이 있다.

데이터베이스 포렌식의 경우 증거물의 연계과정은 보통 서버를 압수하는 경우에는 전원부와 네트워크 케이블을 분리한 다음 별도의 보관함에 보관하여 충격을 방지하고, 분석실로 인계를 하게 된다. 이러한 일련의 과정들은 디지털 증거의 연계절차에 따라 진행된다.

Ⅳ. 포렌식 연계관리 방법의 검증

4.1. 디스크 포렌식 연계관리 방법의 검증

일반적인 디스크 포렌식의 경우 수사의 초등단계부터 법정에 제출되는 상황에 이르기까지 연계방법이 통일되어야 한다. 가장 중요한 사항중의 하나는 일련의 과정들이 모두 기재되고 정리되어야 하며 특이한 사항은 비고란에 기재함으로써 디지털증거의 연계성이 훼손되지 않아야 한다.

압수수색을 하는 단계에서는 메시지 인증코드(Message Authentication Code)가 변하지 않도록 사진 촬영을 하는 등 그림 7.과 같은 시스템의 시간을 확인하고, 연결코드, USB메모리의 부착 여부 등을 살펴보고 압수한다.

이때 외장하드를 사용하여 자료를 이동하였는지 여부를 확인하기 위하여 레지스터를 검색하고, 시작 폴더의 최근문서폴더에 저장된 문서 및 한글과 워드문서의 파일창 밑의 최근문서 목록을 참조하여 문서의 보존여부를 확인한다. 이때 USB메모리 등 이동형 저장장치를 이용한 흔적을 발견할 경우 검색장비를 사용하여 증거물을 획득한다.

압수된 증거물은 분석실로 인계되어 분석담당자, 장비명, 수량, 특이사항, 분석 요구사항 등을 기재하여 분석담당자에게 전달되면 분석담당자는 원본 디스크를 복제하여 사본을 만들고 원본과 사본이 동일함을 해쉬값으로 입증한 다음 원본 디스크는 보관실로 인계하고 사본으로 분석한다.

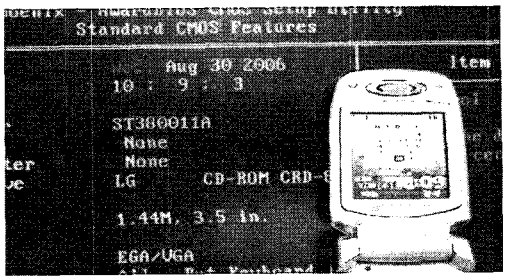

그림 7. 시스템 시간을 휴대폰 시간으로 동일함을 입증
Fig. 7 Time report of the system is identical to that of a cellular phone

분석 시에는 분석에 필요한 장비와 도구 등을 기재하고 필요한 경우에는 사진, 동영상등 필요한 조치를 취하고 분석도중에는 타인의 출입을 삼가고, 자리를 부재중에는 증거물은 보관함에 보관하여 증거의 훼손을 방지한다.

분석을 마친 디스크는 분석보고서를 작성하고 원본과 함께 보관하고, 사본은 법정증거물로 사용하기 위하여 보관하게 된다. 이때 제출된 디스크의 중요도를 심사하여 귀중품에 준한 경우에는 2중 보관함에 보관토록 한다. 이러한 절차는 통일된 규정이 있어야 하며, 이러한 규정을 준수하지 못하는 경우에는 그 사실을 대장에 기재함으로 디지털 증거의 무결성을 보장하여야 한다.

4.2. 시스템 포렌식 연계관리 방법의 검증

운영체제 등은 시스템은 동작 중에 메모리부분에 상주되었다가 전원이 차단되면 사라지게 되므로 시스템이 운영 중에는 전원을 차단하지 말고, 전원이 차단된 상태에서는 전원을 동작시키지 말아야 한다.

디지털 자료는 임의로 제공되거나 압수된 시스템의 캐시메모리, 레지스터 등에 그 자료가 남아 있으므로 장비의 분석 시 세심한 주의를 기울여야 한다.

4.3. 네트워크 포렌식 연계관리 방법의 검증

네트워크 분석과정은 일반 디스크 분석과정과 같이 대상 시스템에 대하여 증거물을 복제하거나 해싱을 전부할 수 없는 경우가 많으므로 경우에 따라서 적절한 판단을 해야 한다. 이러한 판단의 근거는 문서로 기록하여 향후 수사상 연계과정의 문제가 발생할 경우를 대비하여야 한다.

네트워크 포렌식은 운영시스템을 온라인 상태에서 분석하는 온라인 시스템 분석방법과 네트워크를 단절하고 격리시켜서 분석하는 격리 분석방법, 마지막으로 시스템의 전원을 끄고 시스템에 장착된 저장장치의 저장내용들을 분석시

스템에 슬래이브로 부착하여 자료를 분석하는 방법 등이 있다. 경우에 따라서는 온라인과 격리 시스템 분석을 복합적으로 행해질 수 있으며, 이는 시스템 분석을 통하여 네트워크의 침해나 바이러스 감염 등 일반적인 침해사실을 확인하고, 격리해서 필요한 부분을 분석한 다음에 증거물을 확보하는 일련의 과정이 진행된다.

이러한 과정과 절차들은 현재 개인의 경험과 상황에 따라 진행되므로 네트워크 침해사고 분석규정 등을 통하여 통일된 지침을 만들고 지침에 충실하게 진행하면서 상황에 따라 예외적인 상황이 발생할 경우에는 사진, 동영상, 장부에 기재하는 방법 등을 통하여 디지털 증거의 무결성을 입증하여야 한다.

4.4. 모바일 포렌식 연계관리 방법의 검증

모바일 포렌식의 가장 큰 문제점은 초등수사의 단계부터 장비의 이해와 기술이 부족하다는 점이다. 현재 휴대폰의 사용자는 정보통신부 통계에 의해 2006년 9월 현재 3,955만명으로 1가구당 2.5대 전화를 보유하고 있으며 휴대폰 기능의 다양화로 사진, 동영상, 메시지 등은 기본으로 하고 그림8.처럼 작은 크기의 저장메모리의 확장으로 다양한 정보를 저장하고 있다.

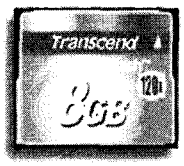

그림 8. 8G. 고용량 플래시 메모리
Fig. 8 8G. High-Capacity Flash Memory

모바일 장비 분야의 데이터의 전달은 무선을 활용하기도 하지만 속도와 요금문제등으로 인하여 컴퓨터에 연결하여 전송되므로 압수수색 시 컴퓨터와 연동관계, 케이블의 보유유무 등을 잘 살펴서 관련 장비와 부품들을 압수해야 한다. 압수 후 임의로 장비의 전원을 켜거나 끄는 등의 행동은 증거의 오염을 가져올 수 있으므로 전자파가 차단된 봉투나 장비를 이용하여 보관하고 분석실로 이동하여 분석하여야 한다. 이러한 일련의 과정들이 규정대로 행하여 지지 않은 경우에는 데이터의 무결성은 심하게 훼손 받는다고 할 수 있으며, 초등수사의 단계부터 세심한 주의와 관리가 요청된다고 하겠다.

분석은 모바일 장비의 데이터를 이미지 덤프를 하여 원본 장비는 보관하고 사본을 사용하여 분석을 진행하며 모든 과정은 대장에 기재하고 필요시 분석과정을 녹화하여 보관하는 것도 연계과정의 무결성을 보관하는 방법이다.

4.5. 데이터베이스 포렌식 연계관리 방법의 검증

데이터베이스에서 디지털 증거의 수집은 데이터베이스의 기술과 업무기술(Business Technology)이 동시에 필요한 분야로서 다양한 업무에 대한 이해와 실수가 있어서는 않된다. 특히 규모가 큰 기업의 대용량 데이터베이스의 압수수색의 경우 수 시간 혹은 수일의 기간이 소요되고, 분석의 과정에서는 더욱 많은 시간이 필요하다.

데이터베이스의 특성상 기업 혹은 전산실에서 데이터의 무결성을 훼손하기 위한 임의적인 자료삭제 및 변경을 불가피하므로 전문가에 의한 자료의 백업 및 분석하는 연계과정에 데이터가 훼손되거나 오염되지 않도록 주의하여야 한다. 진행 등의 모든 절차는 기록하여야 하고 필요시 녹화하는 방법을 이용하기도 한다. 필요한 데이터는 프린트 혹은 CD(DVD)로 저장하여 수사팀에 제공하고 백업본 데이터 및 분석 데이터의 보관은 증거번호를 부여하여 보관하고, 진행상황 보고서도 별도로 보관하여 연계과정에서 무결성이 깨어지지 않도록 한다. 이러한 진행과정은 한 사람에 의하여 분석되어야 한다. 데이터를 추출하고 법원에 제출하는 일련의 과정들은 일반적인 디스크 포렌식의 경우 수사의 초등단계부터 법정에 제출되는 상황에 이르기까지 연계방법이 통일되어야 한다.

V. 결론

본 논문은 디지털 포렌식을 수행함에 있어, 디지털증거가 훼손되어 수사를 진행하지 못한 외국사례와, 국내 재판에서의 재심리를 통하여 시간과 인적낭비를 초래한 사례를 통하여 디지털 포렌식 자료의 무결성의 중요성과 무결성이 훼손되지 않아야 함을 살펴보았다.

또한 컴퓨터 범죄 수사에 있어서 증거 자료를 습득하는 과정에서부터 법정에 제출하여 증거로 채택되는 때까지의 일련의 연계과정을 실제 컴퓨터 수사 상황에서 연구하였다. 그 결과로 디지털 증거의 무결성을 보장하기 위한 포렌식의 연계과정에 대한 현 실태를 살펴보고, 수사상 일어날 수 있는 디지털 증거의 오염가능성 영역을 검토하였다.

따라서 현재 디지털 증거의 포렌식 연계과정의 문제점과 이에 대한 해결방안을 컴퓨터 포렌식을 위한 수사현장에서 실무적인 차원에서 제시하였으며, 이는 표준화된 절차와 지침이 컴퓨터 범죄의 수사 초기단계부터 지켜져야 함을 의미한다고 하겠다.

향후 연구 되어야 할 과제로는, 디지털 포렌식의 각 분야에 대한 정의와 표준화된 지침, 그리고 새롭게 등장하는 신기술에 대한 포렌식의 절차 등에 관하여 연구해야 하며, 실무에 적용함으로써 발생하는 새로운 문제점들을 발굴 보완해야 할 것이다.

참고문헌

[1] 법제처종합법령정보센터. http://www.klaw.go.kr 2006.10.

[2] Kanellis, P., Kiountouzis, E., Kolokotronis, N.,& Martakos, D. (Eds.). "Digital crime and forensic science in cyberspace". Journal of digital forensic practice. Hershey: Idea Group. 2006.

[3] Adelstein, F. "Live forensics: Diagnosing your system without killing it first". Communications of the ACM. V.49, N.2, 63-66. 2006.

[4] 컴퓨터 수사교육. 대검찰청. 2006.

[5] 인터넷과 컴퓨터수사. 한국정보통신대학교부설정보통신교육원. 2002.

[6] Burdach, M. "Digital forensics of the physical memory". http://forensic.seccure.net/pdf/mburdach_ digital_forensics_of_physical_memory.pdf. 2005.

[7] http://www.myung.co.kr/dr/menu01_01.php

[8] Brain Carreier. "File System Forensics Analysis." Addison-Wesley. 2005.

[9] 박대우, 윤석현. "VoIP 서비스의 도청 공격과 보안에 관한 연구." 한국컴퓨터정보학회논문지, 제11권 제4호, pp1-10, 2006. 9. 30.

[10] 박대우, 서정만. "TCP/IP 공격에 대한 보안 방법 연구." 한국컴퓨터정보학회논문지, 제10권 제5호, pp217-226, 2005. 11. 30.

[11] 기업전산자료분석기법. 대검찰청, 2003

[12] http://rr.snas.org/incident/camp-forensics3.php

[13] 디지털증거의 무결성유지를 위한 절차와 시설에 관한 연구. 대검찰청/숭실대학교. 신용태. 2006

[14] 국가정보보호백서, 국가정보원/정보통신부, 2006.

[15] Luoma, V. "Forensics and electronic discovery: The new management challenge". Computers & Security, 25(2), 91-96. 2006.

저 자 소 개

이 규 안

2006년 숭실대학교 정보통신학과 졸업 (공학석사)

2006년 숭실대학교 컴퓨터학과 재학 (박사과정)

2000년 벽성대학 정보통신과 겸임교수

2002년 대검찰청 중앙수사부 컴퓨터수사과 근무

2005년 대검찰청 과학수사2담당관실 근무

〈관심분야〉 유비쿼터스 보안, 컴퓨터 포렌식, 이동통신 보안

박 대 우

1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)

2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)

2000년 매직캐슬정보통신 연구소 소장, 부사장

2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수

2006년 정보보호진흥원 선임연구원

〈관심분야〉 유비쿼터스 보안, 네트워크 보안 시스템, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality

신 용 태

1985년 한양대학교 산업공학과 학사

1990년 Univ.of Iowa 전산학과 석사

1994년 Univ.of Iowa 전산학과 박사

1994년 ~ 1995년Michigan State Univ. 전산학과 객원교수

1995년 ~ 현재 숭실대학교 컴퓨터학부 교수

〈관심 분야〉 멀티캐스팅, 실시간통신, 이동통신, DRM 등