한국컴퓨터정보학회 하계학술대회 논문집 제19권 제2호 (2011. 6)

기업회계장부 압수수색과 DB파일 포렌식 기술 적용방법 연구

이보만°, 박대우*
°*호서대학교 벤처전문대학원 IT응용기술학과
e-mail: bomans@nate.com, prof1@paran.com

A Study on Forensic Technique Applying Method of Company Accounting Book Data Base File

Bo-Man Lee°, Dea-Woo Park*
°*Dept. of IT Application Technology, Hoseo Graduate School of Venture

● 요 약 ●

검찰과 경찰에서는 압수수색을 통해 조사를 수행하는데, 기업들은 압수수색 수사를 받기 전에 회계 DB 및 회계 관련 파일 삭제, 파손 및 은닉하는 등의 문제점을 발생시키고 있다. 2008년 삼성화재 비자금 조성 사건과, 2009년 교하 복합커뮤니티 센터의 입찰비리 사건 등 기업회계장부의 포렌식 기술적용방법 문제 등이 발생하고 있다. 본 논문에서는 포렌식 수사 도구인 EnCase, FinalData 등을 연구하고, 기업의 회계 서버에 대해 압수수색 준비와 압수 수색, 획득 증거 분석 등의 절차를 연구한다. 기업의 회계 서버 압수수색 후에 디스크에서 포렌식 증거분석에서 실시되는 증거물 원본 파일보관, 원본성이 입증된 사본 생성, 삭제 파일 검사 및 복원, 삭제 내용 확인, 원본 파일과의 대조를 실험을 한다. 본 연구 결과는 포렌식 기술발전에 기여하게 될 것이다.

키워드: Forensic, Forensic Investigation Tool, Company Accounting Data Base, File Restore

I. 서론

2008년 삼성화재 비자금 조성 사건은 1999년부터 2002년 사이 삼성화재 측이 미지급 보험금을 지점에 내려 준 것처럼 회계장부를 조작하고 차명 계좌를 이용해 9억8000만원의 비자금을 조성하였다. 이 사실이 밝혀진 뒤 삼성화재 압수수색 과정에서 회계 자료를 전산에서 삭제한 삼성화재 전무는 특검법 위반과 증거인멸 혐의로 불구속 기소 됐다[1].

또한 2009년에 벌어진 교하 복합커뮤니티 센터의 입찰비리 사건의 경우에도 590억원의 프로젝트에 연루된 수백 명의 관계자, 거액의 로비금액은 당연하게도 금호건설 본사가 연루되어 있다는 것을 예측이 가능했다. 하지만 압수수색결과 본사와의 연결고리 외에 정확한 증거를 찾지 못해 의혹만 남긴 채 상무급 임직원의 개인비리로 마무리 되었다[2][3].

기업회계처리의 비자금 사건의 특징은 압수수색 시에 회계장부가 이미 삭제되어 일반적인 방법으로는 찾을 수 없는 경우에 대해 설명해주고 있다[4][5].

검찰에서 사건 수사 시 현장[6]에서 빠르게 대상물을 압수수색[7] 하더라도, 이미 삭제된 증거자료는 포렌식[8] 수사도구 없이는 포렌식 자료를 추출[9]해 증거물로 찾아내기 힘들다. 즉 검찰에서 압수수색의 조짐을 보인다면, 기업들이 자신들의 회계파일을 그 즉시 삭제할 가능성이 있다. 그렇기 때문에, 위의 비자금 수사 시에는 삭제되거나, 은닉 된 회계장부를 찾아 복원하기 위해 포렌식 도구의 사용과 포렌식 기술 연구가 필요하다.

본 논문에서는 기업들의 삭제된 회계장부 파일과 DB의 복원을 위해, 포렌식 도구를 사용하여 압수 수색된 기업회계장부에서 삭제되거나, 은닉된 자료를 복원하는 기법을 연구, 분석하여 포렌식 기술 발전에 기여할 것이다.

본 논문은 I. 서론에서 기업의 회계장부 삭제 문제와 그에 따른 포렌식 수사 도구를 이용한 복원에 대해 조사하였고, II. 관련연구에서는 포렌식 수사도구인 EnCase 및 FinalData, 기타 포렌식 수사도구에 대해서 조사하였으며, lll. 기업 회계장부 파일과 DB 압수수색에서는 압수수색 준비와 기업 압수수색, 획득 증거 분석에 대하여 서술 하였고, IV. 기업 회계장부의 삭제 파일과 DB 포렌식에서는 분석 환경, 압수수색한 하드 드라이브 복제 및 보관, 압수수색한 DB 분석, 압수수색한 파일 분석, 삭제파일 복원, 삭제파일 내용 확인, 원본과 대조를 실시하였고, V. 결론을 마지막으로 구성되어 있다.

Ⅱ. 관련 연구

2.1 FinalData

Final Data[11]는 그림 2와 같이 복구를 전문으로 하는 포렌식 분석도구로서 휴지통을 비운 경우에 파일 복구, 포맷한 경우 파일 복구, 파티션을 지운 경우 파일 복구, 복구 전 파일 확인 기능, 파일 삭제 관리 마법사, 폴더 보호 기능, 이메일 파일 복구 기능, 손상된 오피스 파일 치료 마법사, Microsoft Access 복구 기능, Linux 파일 시스템 지원 (EXT2 / EXT3), Mac 파일 시스템 지원 (HFS / HFS Plus) 등의 기능을 제공한다.

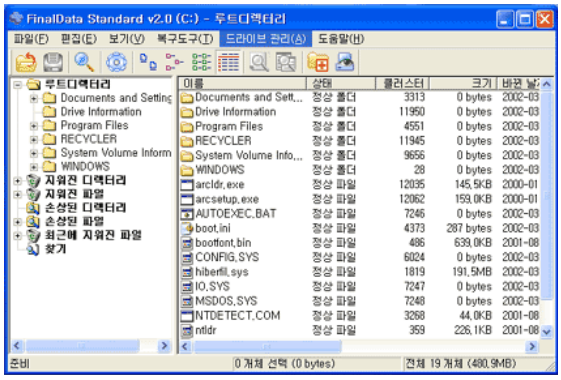

그림 1. Final Data
Fig. 1. Final Data

FinalData의 상세한 데이터 복구 방법은 단순히 윈도우에서 파일이 삭제된 경우에는 [논리드라이브 검색]을, 포맷이나 파티션 손상 등으로 인해 드라이브가 인식되지 않는 경우에는 [물리드라이브 검색]을 해 주어야 하고, [드라이브 선택]에서 복구할 드라이브를 선택한다. [드라이브 선택]에서 [논리드라이브] 탭을 선택한 후 복구할 데이터가 있는 드라이브를 선택한다. [물리 드라이브]탭을 선택하면 복구할 PC에 설치된 물리 드라이브의 목록이 나타나게 되고, 목록에 있는 물리 드라이브 중 복구할 드라이브가 있는 디스크를 선택, 복구할 물리 드라이브를 선택한 후 [선택] 버튼을 클릭하면 FinalData가 자동적으로 파티션을 찾기 시작한다. 논리드라이브 및 물리 드라이브의 검색이 시작되면, 파이널데이터는 해당 드라이브(논리드라이브 또는 물리드라이브)의 FAT 또는 MFT와 디렉터리 엔트리(Directory Entry)를 분석하게 된다. 루트 디렉터리 영역과 데이터 영역에 존재하는 서브 디렉터리 엔트리(Sub Directory Entry)의 정보를 검색하여 삭제된 파일과 폴더를 찾고, 삭제된 파일과 폴더는 디렉터리 엔트리 상의 파일명에서 첫 번째 문자만 삭제된 것이므로, 이것을 검색하여 삭제된 파일과 폴더의 목록이 작성되게 된다. 검색이 끝나면 루트 디렉터리, 지워진 디렉터리, 지워진 파일, 손상된 디렉터리, 손상된 파일, 최근에 지워진 파일, 찾기의 카테고리로 결과가 주어진다. [지워진 디렉터리]와 [지워진 파일]의 항목은 [디렉터리검색]과정까지만 실시하여도 복구가 가능하며, [손상된 디렉터리]와 [손상된 파일]의 항목은 추가적으로 [클러스터 검색]까지 해 주어야 복구가 된다. [디렉터리 검색]이 끝나면 클러스터 검색이 나오는데, 검색할 클러스터의 범위를 설정해주면 설정한 범위에 있는 클러스터를 검색한다. 파일 복구에는 간단한 마우스클릭으로도 복구가 되지만, 드라이브를 복구할 때는 다른 논리 드라이브나 네트워크, CD-ROM으로 저장을 해야 삭제된 정보가 덮어씌워져서 안정된 복구가 된다.

2.2 EnCase

Encase[10]는 포렌식 도구로써 그림 1처럼 증거에 대한 조사를 가능하게 하고, 침해사고의 악성 프로세스를 제거, 부정 수단, 정책 위반, 위험한 유틸리티 등을 찾고 디지털 포렌식 증거자료로 만들 수 있다.

Encase의 가장 큰 장점은 법정에서 증거자료로 인정이 된다는 점인데, 이로 인해 전 세계 많은 나라들의 수사기관은 물론 우리나라에서도 사용되는 제품이다.

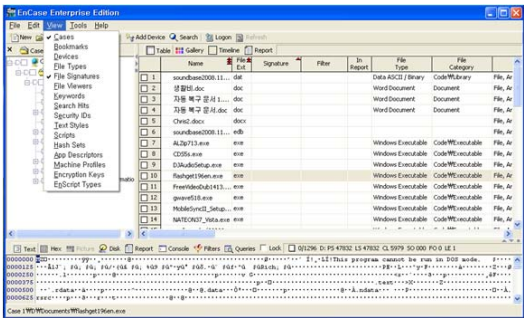

그림 2. EnCase
Fig .2. EnCase

Encase는 고급 기능이 존재하며 이 고급기능은 온라인 타겟노드 미리보기와 증거파일 작성, 암호화 파일보기, 네트워크 사고 대응 및 네트워크 자동 감사, 스냅샷, 동시접속, SAFE, Examiner 등이 있으며, 고급 기능의 유무에 따라 구분된 제품이 출시되어 있다. Encase이 활용되는 곳은 원본 디스크의 고속 복사 및 사본 작성, 데이터복구, 증거자료 보존과 탐색의 동시작업가능, 각종 운영체제의 로그 관리, 분석 및 사용자 패턴 분석, 전자우편 (PST, DBX)복구, 다국어 지원(유니코드 및 한글지원), 동적 디스크 지원(Spanned, Mirrored, Striped, Raid5, Basic) 키워드, 해시, 서명분석, 필터 등의 검색과 분석, 북마크와 발견물 관리, 보고서 작성, 매크로를 이용한 검색 자동화 기능, 이미지 파일 미리보기, 패턴 분석, 암호 복호화 기능(옵션), 휴지통 인덱스 파일 검색기능, 전자우편, IP, 전화번호 등 추출, 인터넷 히스토리 분석 가능, 바로가기 파일 분석, 파티션 파인더(고급 데이터 복구기능), 윈도우 이벤트 로그 분석, 라이브 포렌식 및 원격 데이터 복구 기능, 용의자의 환경으로 부팅하여 조사가능, SCSI, USB, EIDE Device 사본작성 등이 가능하다.

2.3 기타 포렌식 수사도구

기타 포렌식 분석 도구에는 표 1과 같이 ForensicX, MaresWare, The Coronver's Toolkit, ByteBack III, forensic Toolkit 등이 있다[12]. 이 도구들은 상용과 공개용으로 나누어지며, 지원되는 운영체제도 유닉스와 리눅스, 윈도우즈 등으로 구분되어 있으며, 도구에

따라 보조 지원기능도 존재한다.

포렌식 분석 도구가 유사한 기능을 하는 것은 아니기 때문에 포렌식 분석 도구 각각의 기능들이 상이하며 기능의 수준에 맞는 가격이 책정되어 판매 되는 것이 보통이다.

표 1. 기타 포렌식 수사도구
Table 1. Other forensic investigation tools

도구 이름	이미지 생성 및 검사	무결성 검사	저수준 복구
ForensicX	Disk, OS, Traffic	Hard, File, FInger	Delete
MaresWare	Disk	Hard, File	
The Coroner's Toolkit	Disk, OS	Hard	Delete,key
Tom's Rootboot	Disk, OS	X	X
Byte Black III	Disk, OS, Traffic	Hard, File	Raw, Delete
Forensic Toolkit	Disk	Hard, File	Raw, Delete

III. 기업 회계장부 파일과 DB 압수수색

3.1. 압수수색 준비

표 2. 압수수색 준비단계
Table 2. Search confiscated preparation phase

순서	내용
1	영장발부 및 계획
2	압수수수개 팀 구성
3	장비 및 도구 준비
4	외부 변경 요소 제거
5	증거의 확인
6	증거수집 순서결정

검찰이나 경찰에서 기업의 비자금 단서를 포착, 범죄 혐의가 충분한 것으로 보고, 비자금 사건의 중점인 신제품 A의 특허 로열티 관련 자금 흐름을 조사를 위해 압수수색을 하기로 한다. 영장의 내용은 은행거래 내역, 관련자의 전화통화 기록, 기업의 건물, 우편물, 서류철들과, 컴퓨터와 서버 등의 전산 장비 자료를 포함한 압수수색 영장을 청구하여 법원으로부터 압수수색 영장을 발부받는다. 검찰이나 경찰은 기업의 압수수색 날짜 및 인원 편성을 목표인 해당 기업의 본사에 맞춰 편성, 기밀유지에 주의를 기울여 외부변경 요소를 제거하고, 주 증거확인을 위한 압수수색 대상을 본사의 회계 부서 내부와 우편물, 회계 관련 서류들, 컴퓨터 및 전자정보들과 회계 담당자들의 통화 기록, 은행 거래내역 으로 잡고, 원본의 위/변조가 불가능 하도록 전량 압수조치 과정을 거치는데 표 2와 같다.

3.2. 기업 압수수색

표 3. 압수수색 진행단계
Table 3. Search process can confiscate

순서	내용
1	압수수색 시작
2	영장 제시
3	입회인 참여
4	컴퓨터 및 관련 악세서리 압수
5	입회인 서명
6	압수수색 종료

영장을 기업에 제시 한 후 입회인 참여 하에 기업 본사를 압수수색하고, 입회인의 서명을 받는 법적 절차를 거친다. 압수수색에서는 이 기업의 회계를 담당하는 컴퓨터 서버와 회계 부서 내의 컴퓨터들, 회계 부서의 관련 서류와 우편물들을 조사하고, 혐의와 관련이 있는 담당자들의 전화통화 기록도 압수한다. 이 중 우편물이나 서류들에서는 혐의 관련 자료는 입회인의 확인을 받아 압수하고, 정보를 담고 있는 회계용 컴퓨터 서버의 DB와 파일을 백업받고, 컴퓨터의 하드 드라이브를 수색을 하게 되는데 표 3과 같다.

3.3. 획득 증거 분석

표 4. 증거분석단계
Table 4. Analysis phase

순서	내용
1	증거분석 시작
2	원본과 같은 사본 작성
3	원본 보관
4	사본으로부터 증거분석
5	데이터복구 및 증거획득
6	증거 문서화

입회인의 입회하에 압수한 회계용 서버 컴퓨터와 회계 부서의 컴퓨터 하드 드라이브 들을 확인하여 서명을 받고, 사진을 찍은 후에 복사본을 만든다. 포렌식 분석 도구를 이용하여 탐색한 결과, 컴퓨터 하드 드라이브들은 회계 자료가 존재하였고, 회계용 서버 컴퓨터 내의 DB 및 파일을 검사하게 되는데 표 4와 같다.

실험실에서 회계용 서버 컴퓨터의 드라이브는 윈도우 파일과 DB, 회계 장부파일 들이 존재하는 것으로 가정하고, 회계장부 DB와 파일들을 분석하여 증거를 분석하고 포렌식 자료를 생성하는 과정을 거친다.

Ⅳ. 기업 회계장부의 삭제 파일과 DB 포렌식 기술 적용

기업에서 압수수색한 회계장부의 삭제 파일과 DB 포렌식 기술을 적용하는 실험을 실시한다.

4.1. DB 포렌식 실험 환경

삭제 파일과 DB 포렌식 기술 분석에 사용된 컴퓨터 및 도구들의 스펙은 다음과 같다.

4.1.1. MAIN SYSTEM

프로세서 : Intel(R) Core(TM) i3 CPU
RAM : 4 GB
OS : Microsoft Windows 7 - 32 bit
HDD : 500 GB

4.1.2. Virtual Machine Software

포렌식 수사도구 : FinalData Standard 2.0
DB : MySQL

4.2. 압수수색한 하드 드라이브 원본 복제 및 보관

압수한 회계 서버 컴퓨터의 하드 드라이브 원본 보존을 위하여 입회인의 입회하에 원본을 복제하고, 사본의 원본성 입증을 위해 해시값을 사용한다. 원본 하드 드라이브는 증거물 보관소로 옮기고, 복제된 사본 하드 드라이브로 분석을 거치게 된다.

4.3. 복제한 회계 DB의 분석

압수한 회계 서버 컴퓨터의 DB를 분석한 결과, 그림 3과 같은 구조로 판명 되었으며, DB에서는 혐의점과 연관된 자료가 발견되었다.

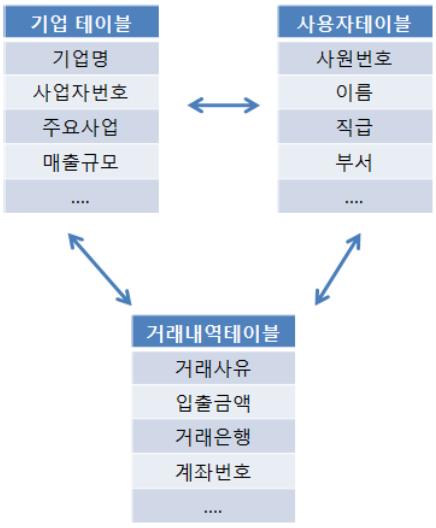

그림 3. 분석한 DB의 구조
Fig. 3. Analysis of the structure of DB

4.4. 회계 파일 포렌식 분석

포렌식 수사 도구인 FinalData를 사용, 복제된 사본 하드 드라이브의 클러스터를 검사한 결과 그림 4와 같이 회계장부 파일을 삭제한 것을 확인 하였다.

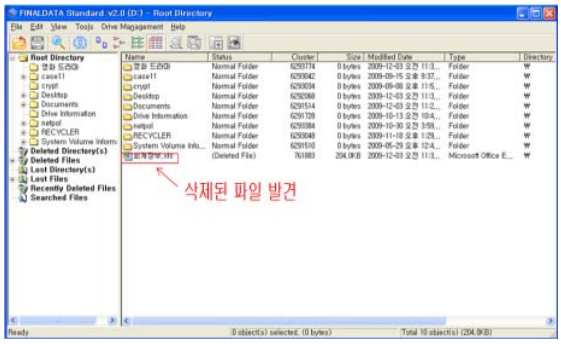

그림 4. 발견된 삭제 파일
Fig. 4. Delete files found

4.5. 삭제된 파일의 복원

FinalData로 발견한 삭제된 회계장부 파일을 복원한 결과 그림 5와 같이 삭제된 파일이 나와 파일이 복원되었다.

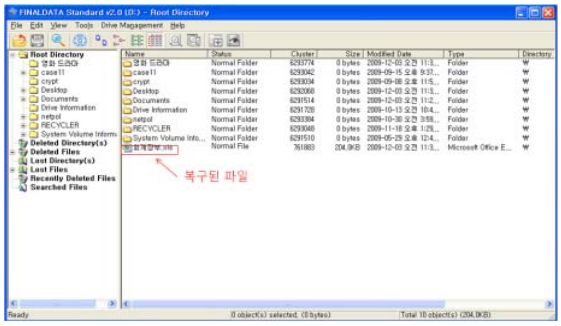

그림 5. 복구된 파일
Fig. 5. Recovered files

4.6. 복원된 파일의 내용 확인

복원된 회계장부 파일을 확인, 그림 6과 같은 혐의점 관련 파일의 내용이 분석되어 혐의점인 신제품 A의 특허 로열티가 존재하는 회계장부임이 확인 되어, 해당 범죄 혐의의 파일인 것으로 확인 되었다.

그림 6. 혐의점 관련 파일의 내용
Fig. 6. Related to the contents of the file

4.7. 원본 파일과 비교 검증

복원된 파일이 원본 파일과 일치하는지를 입회인의 입회하에 그림 7의 원본 파일의 내용과 그림 8의 복원된 파일의 내용을 대조하여 원본파일과 동일함을 확인하였다. 입회인의 사인을 받고, 동일 자료임을 증명하는 자료를 작성하였다.

그림 7. 원본파일의 내용

Fig. 7. The contents of the source file

그림 8. 복원된 파일의 내용

Fig. 8. The contents of the restored files

V. 결론

기업 성장과 함께, 기업들이 수익에 대한 비자금을 조성하는 문제가 발생하게 되었고, 검찰과 경찰의 압수수색과 포렌식 분석 조사가 이루어지고 있다. 하지만 기업들이 비자금 압수수색을 받기 전에 회계 관련 DB를 조작하거나 회계 장부 파일을 삭제 및 은닉하는 문제가 항시 존재하게 되었다.

본 논문에서는 회계 관련 DB와 파일을 압수수색하고, 원본 증거자료를 보존하고 원본과 똑같은 사본으로 회계 DB를 분석하고, 포렌식 수사 도구를 사용하여 삭제된 기업의 회계장부를 원본성을 확보하여 복원하고, 혐의점에 대한 증거물을 찾아내는 포렌식 기술을 연구함으로서 문제에 대해 대처법을 제시하였다.

향후 연구로는 인터넷을 이용하여 네트워크상에서 회계 처리를 조작하거나, 삭제를 할 때, 삭제된 정보를 복원하는 방법에 관한 연구가 진행 되어야 할 것이다.

참고문헌

[1] 중앙일보, '삼성 특검 주요내용,' http://article.joinsmsn.com/news/article/article.asp?ctg=12&Total_ID=3102985, 2008. 6.

[2] MBC뉴스, '파주 교하 신도시 입찰비리 현장 포착.' http://imnews.imbc.com/replay/nwdesk/article/2515888_5780.html, 2009. 12.

[3] 매일경제, '[경기] '교하' 입찰 비리', http://mbn.mk.co.kr/pages/news/newsView.php?news_seq_no=473504&category=mbn00007, 2009. 12.

[4] 네이트 리포트, '수사상 압수 및 수색에 관한 연구', 'www.kalgas.or.kr/download.php?category=research&filename...pdf', 2005. 10.

[5] 원혜욱, "과학적 수사방법에 의한 증거수집-전자증거의 압수.수색을 중심으로" 비교형사법연구, 제5권제2호

[6] 대검찰청-숭실대학교, "디지털증거의 무결성 유지를 위한 절차와 시설에 관한 연구," 2008.

[7] 신이철, "수사기관의 압수수색영장 집행절차와 제한 규정," 한국통신학회논문지, 중앙법학,11권2호, 2009.

[8] 이광열, 최윤성, 최해랑, 김승주, 원동호, "현행 증거법에 적합한 디지털 포렌식 절차" 정보보호학회지 제18권 제3호, 2008,6.

[9] 姜信澤, "行政學 硏究方法의 變遷 過程과 앞으로의 方向" 한국행정학보 제21권 제1호, 1987,6. page(s) 3-367

[10] Encase, http://www.guidancesoftware.com/, 2009.

[11] FinalData, http://www.finaldata.co.kr/, 2009.

[12] 고병수, 박영신, 최용락, "보안 침해사고 대응을 위한 컴퓨터 포렌식스 기술 동향" 인터넷정보학회지 제4권 제1호, 2003.3