한국컴퓨터정보학회 하계학술대회 논문집 제19권 제2호 (2011. 6)

Smart Phone에서 삭제된 회계장부의 포렌식 복원 수사 기술

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

Forensic Investigation Restoration Technique from Deleted Accounting Book In Smart Phone

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

● 요 약 ●

기업들의 비자금 수사를 받기 전에 압수수색 대상 회계 파일의 삭제, 파손 및 은닉하고 있다. 2010년 H 그룹 비자금 조성 사건에서도 삭제된 파일에서 회계처리, 비자금 문제를 발견 하였다. 최근에는 Smart Phone의 활성화와 함께 주요 증거물을 Smart Phone에 저장하고 업무를 진행하고 있다. 본 논문에서는 압수수색된 Smart Phone에서 기업의 회계장부를 찾아내고, 삭제한 회계장부를 복원하는 포렌식 수사기술에 관한 연구이다. 기업에 대한 압수수색 준비와 압수 수색, 획득 증거 분석 등의 절차와 포렌식 도구들을 분석한다. Smart Phone 압수수색 후 포렌식 증거 자료 추출 과정과 포렌식 도구를 이용하여 실험하고 포렌식 증거자료를 추출한다. 본 논문을 통해서 Smart Phone 포렌식 기술발전에 기여 하고자 한다.

키워드: Samrt Phone, 포렌식(Forensic), 수사기술(Investigation technique), 회계장부복원(Accounting book Restoration)

I. 서론

검찰이 2010년 H그룹의 비자금 조성 의혹이 제기되어 H 그룹의 본사와 H증권 사무실을 압수수색[1] 했다. 또한 H그룹 비자금 조성의 창구로 추정되고 검찰의 H 그룹의 압수수색을 방해를 하여 증거[2]를 인멸할 시간을 벌어준 S&S 경비업체를 압수수색 하여 조사 중에 있다. 2009년에 벌어진 교하 복합커뮤니티 센터의 입찰비리 사건의 경우에도 590억원의 프로젝트에 연루된 수백 명의 관계자, 거액의 로비금액은 당연하게도 K건설 본사가 연루되어 있다는 것이 예측 가능했지만, 압수수색결과 본사와의 연결고리 외에 정확한 증거를 찾지 못해 의혹만 남긴 채 상무급 임직원의 개인비리로 사건이 마무리 되었다.

위 두 사건에서 압수수색 시에 검찰에서 사건 수사 시 현장에서 빠르게 대상물을 압수수색 하더라도, 기업들의 증거 인멸 행위로 인해 회계장부 등의 증거 자료를 포렌식[3] 수사도구 없이 추출해 찾아내기 어렵다는 점을 알 수 있다.

또한 최근 운영체제[4]를 탑재한 Smart Phone[5]이 등장하여 모바일[6] 시장에서 활성화됨에 따라, Smart Phone 사용자[7]가 증가하고 기존의 휴대폰이 Smart Phone으로 대체 되어가면서 Smart Phone 보안[8]에 대한 관심도 증가하고 있다.

또한 검찰의 압수수색에서 기존의 휴대폰 대신 Smart Phone이 증거물로 나올 수 있음을 예상 할 수 있다. 따라서 압수수색 후 포렌식 분석 과정에서 Smart Phone에서 삭제되거나, 은닉 된 회계장부를 찾아 복원하기 위해 포렌식 도구의 사용과 포렌식 기술 연구가 필요하다.

본 논문에서는 기업의 압수수색 준비와 압수 수색, 획득 증거 분석 등의 절차와 포렌식 수사 도구인 EnCase 및 FinaData 등을 분석하고, 압수수색한 Smart Phone에서 회계장부의 복원을 위해 포렌식 도구를 사용하여 삭제되거나, 은닉된 자료를 복원하는 기법을 실험, 분석하여 Smart Phone 포렌식 기술 발전에 기여할 것이다.

II. 관련연구

2.1 포렌식 수사 도구 FinalData

FinalData[10]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.

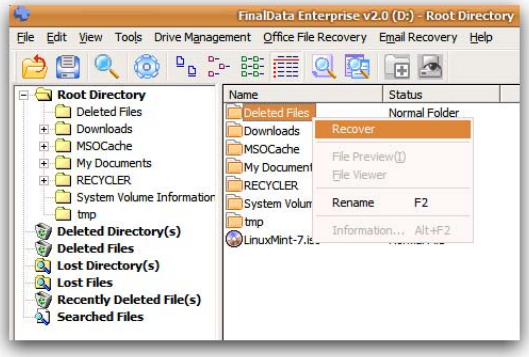


그림 2. FinalData
Fig. 2. FinalData

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 포렌식 수사 도구 EnCase

EnCase[9]는 포렌식 수사 도구로서 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.

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.

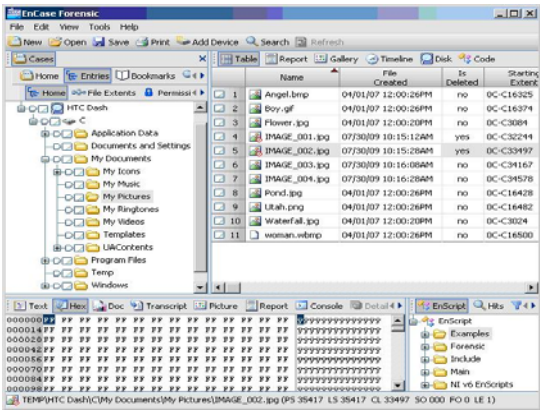


그림 1. EnCase
Fig. 1. EnCase

2.3 Smart Phone에서 회계장부

Smart Phone 회계장부의 예로는 그림 3처럼 LG U+ 가 만든 웹하드[11]의 회계장부가 있다. Smart Phone에서 실행되며 회사의 지출, 수업 등 회계 장부를 쉽고 간편하게 관리, 국세청 간편장부 서식과 예산작성 및 보고서 출력, 사내 구성원별 공유권한 설정, 개인장부로 개인의 지출/수입을 가계부처럼 쉽고 간편한 관리가 가능하다.

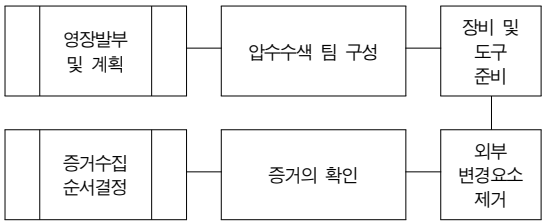
그림 3. Smart Phone 회계장부
Fig. 3. Smartphone Ledger

III. 포렌식 수사 압수수색 준비과정

3.1. 기업의 압수수색 준비

검찰이나 경찰에서 기업의 비자금 단서를 포착, 범죄 혐의가 충분한 것으로 보고 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, 증거확인을 위한 압수수색 대상을 본사의 회계 부서 내부와 우편물, 회계 관련 서류들, 컴퓨터 및 전자정보들과 회계 담당자들의 통화 기록과 휴대폰 및 Smart Phone, 은행 거래내역으로 잡고, 원본의 위/변조가 불가능 하도록 전량 압수조치 과정을 표 1과같이 거친다.

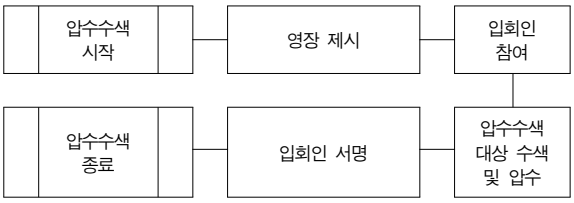
표 1. 압수수색 준비 단계
Table 1. Confiscated search preparation phase



3.2 압수수색 포렌식 적용

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 기록 과 휴대폰 및 Smart Phone을 압수한다. 이 중 우편물이나 서류들에서는 혐의 관련 자료는 입회인의 확인을 받아 압수하고, 정보를 담고 있는 회계용 컴퓨터 서버의 파일을 백업받고, 컴퓨터의 하드 드라이브를 표 2와 같이 수색한다.

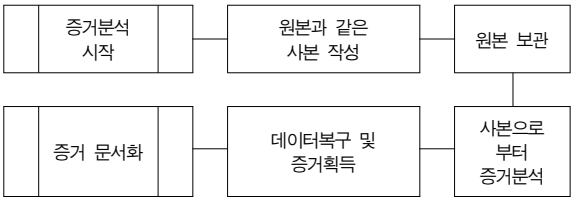
표 2. 압수수색 진행 단계
Table 2. Confiscated search step process



3.3 획득 증거 분석

입회인의 입회하에 압수한 회계용 서버 컴퓨터와 회계 부서의 컴퓨터 하드 드라이브 들을 확인하여 서명을 받고, 사진을 찍어 보관한다. 포렌식 분석 도구를 이용하여 서버 컴퓨터의 하드 드라이브 및 회계 부서의 컴퓨터 하드 드라이브와 휴대폰 및 Smart Phone 등을 분석한다. 분석을 위해서는 무결성 보장을 위해 해쉬값을 첨부하며 파일을 복제하여 분석을 하고, 분석에서 나온 포렌식 증거 또한 해쉬값을 첨부하여 원본성 입증이 가능하게 한다. 분석을 실행하고 포렌식 자료를 생성한 과정을 문서화 하여 기록하는 과정을 거친다[표 3].

표 3. 증거분석 단계
Table 3. Analysis phase



IV. 압수수색된 Smart Phone에서 삭제된 회계장부의 포렌식 복원 기술

4.1 포렌식 기술 분석 환경

Smart Phone 포렌식 분석에 사용된 환경은 다음과 같다. 회계장부는 Smart Phone에 가상의 회계장부 Excel 파일이 있는 것으로 가정하고 실험하였다.

- Smart Phone

  Smart Phone : 삼성전자 갤럭시 S
  통신 프로그램 : Samsung Kies

- System

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

HDD : Samsung HD502IH (500 GB)

- Forensic Software

포렌식 수사도구 : EnCase Enterprise

4.2 Smart Phone에서 자료 추출

그림4 과 같이 제조사에서 제공하는 USB 케이블을 이용하여 갤럭시 S를 컴퓨터와 연결하고, 제조회사의 통신 프로그램인 Samsung Kies와 연결하였다. 그림5에서는 Kies와 연결된 갤럭시 S의 자료인 전화번호부, 일정관리, My 다이어리, 메시지 뷰어, 메모, 시간표 등을 보여주고 있으며, 그림 6에서는 하드 드라이브로 인식이 된 갤럭시 S의 메모리 안의 폴더 및 파일을 보여주고 있다.

그림 4. 컴퓨터와 연결된 갤럭시 S
Fig. 4. Computer is connected to the Galaxy S

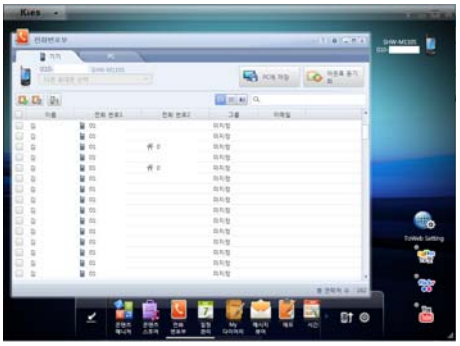


그림 5. 갤럭시 S의 자료
Fig. 5. Galaxy S Base

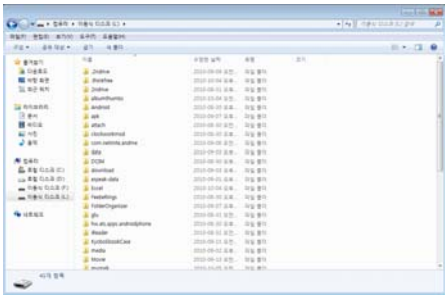


그림 6. 갤럭시 S 메모리의 폴더와 파일
Fig. 6. Galaxy S Memory Folders and Files

4.3 Smart Phone에서 삭제된 회계장부 복원

하드 드라이브로 인식이 된 갤럭시 S는 정상적으로 포렌식 수사 도구의 사용이 가능하기 때문에, 포렌식 수사 도구인 EnCase Enterprise 버전을 사용하여 갤럭시 S의 드라이브인 L 드라이브를 분석하였다. L 드라이브를 분석한 결과, Smart Phone에서 삭제된 회계장부를 찾아 그림 7처럼 Excel 폴더 안에 회계장부 파일이 발견되었다. 발견된 Excel 파일을 복원하여 그림 8처럼 System의 하드 드라이브에 저장 하여 파일의 내용을 확인한 결과, 그림 9처럼 정상적으로 복구가 된 것을 확인 할 수 있다.

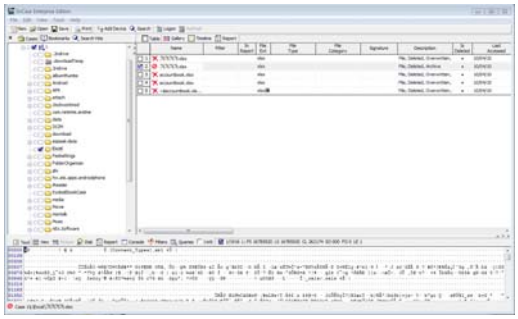


그림 7. 발견된 Excel 파일
Fig. 7. Excel files found

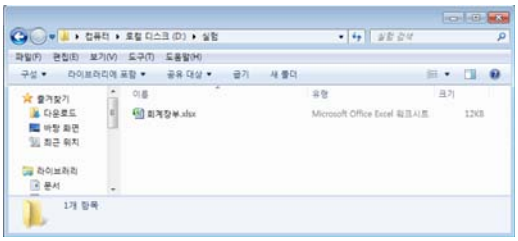


그림 8. 복구 저장한 파일
Fig. 8. Save the file recovery

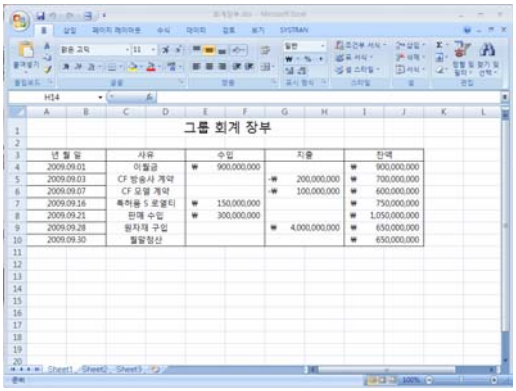


그림 9. 정상적으로 복원된 파일
Fig. 9. Files are restored to normal

V. 결론

기업들이 회계장부를 조작하여 비자금을 조성하고 검찰이 기업들을 압수수색 하고 있다. 하지만 기업들의 증거 인멸 행위로 인해 증거 자료를 추출하기 위해서는 포렌식 수사도구를 사용해야 한다. 기존의 휴대폰이 Smart Phone으로 대체 되면서 검찰의 압수수색에서 기존의 휴대폰 대신 Smart Phone이 증거물로 나올 수 있음을 예상 할 수 있다. 따라서 압수수색 후 포렌식 분석 과정에서 Smart Phone에서 삭제되거나, 은닉 된 회계장부를 찾아 복원하기 위해 포렌식 도구의 사용과 Smart Phone 포렌식 기술 연구의 필요성이 있다.

본 논문에서는 기업의 압수수색 준비와 압수 수색, 획득 증거 분석 등의 절차와 포렌식 도구인 EnCase 및 FinaData 등을 분석하였고, 압수수색한 Smart Phone에서 회계장부의 복원을 위해 컴퓨터와 Smart Phone을 연결하고 포렌식 도구인 EnCase를 사용하여 삭제된 회계장부 자료를 복원하여 확인하여 증거자료를 추출하였다. 향후 연구로는 Smart Phone 포렌식 데이터 추출 과정에서 무결성, 안정성을 보장하는 연구가 진행되어야 할 것이다.

참고문헌

[1] 권양섭, “디지털 포렌식 법률체계 구축 방안,” 한국법학회, 35, 357-382쪽, 2009. 8.

[2] 신용달, “컴퓨터 포렌식 수사절차 모델,” 한국멀티미디어학회 춘계학술발표논문집, 583~586쪽, 2008. 5.

[3] 임경수, 박종혁, 이상진, “디지털 포렌식 현황과 대응 방안,” 보안공학연구논문지, 3(6), 461-473쪽, 2008. 12.

[4] 이상윤, 이환구, 김우식, 이재호, 김선자, “스마트폰 운영 체제 개발 동향,” 전자통신동향분석, 19(6), 2004.

[5] 심승배, 정봉주, “한국 스마트폰 시장의 확산 전략,” 한국경영과학회/대한산업공학회 춘계공동학술대회, 2009.

[6] 김기연, 조성제 “스마트폰 보안 취약점 동향,” 한국정보과학회, 37(2), 90-94쪽, 2010.

[7] 김태한, “스마트폰 시대의 사용자 환경,” 정보과학회지, 28(6), 90-94쪽, 2010.

[8] 제갈병직, “스마트폰 시장과 모바일OS 동향,” Semiconductor Insight, 9-18쪽, 2010.

[9] EnCase, http://www.encase.com/

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

[11] 웹 하드 회계장부, http://www.webhard.co.kr/