情報保護學會論文誌
第20卷 第6號, 2010. 12

디지털포렌식 관점에서의 디지털복합기내 데이터 복구 및 분석

박 일 신,† 강 철 훈, 최 성 진‡
대검찰청 디지털수사담당관실

The Recovery and Analysis of Digital Data in Digital Multifunction Copiers with a Digital Forensics Perspective

Il-Shin Park,† Cheul-Hoon Kang, Sung-Jin Choi‡
Digital Forensic Center, Supreme Prosecutors' Office

요 약

IT 환경의 발전으로 일상생활에서의 임베디드 기기의 사용빈도가 증가하고 있다. 이러한 임베디드 기기중 대표적인 사무자동화기기인 디지털복합기는 복사기, 스캐너, 팩스, 파일서버 기능 등 다양한 용도로 사용되고 있다. 이러한 디지털복합기내에 스캔 등을 통하여 저장되어 있을 수 있는 데이터의 존재여부와 추출방법, 이를 이용한 증거자료로서의 활용방안에 대하여 논하여 보고자 한다.

ABSTRACT

Caused by the development of IT environment, the frequency of using the embedded machines is increasing in our regular life. A typical example of these embedded machines is a Multi Function Copier and it has various functions; it is used as copier, scanner, fax machine, and file server. We would like to check the existence of and the way to abstract the data that may have been saved through using the scanner of the multi function printer and discuss how to use those data as the evidence.

Keywords: Digital Forensics, Digital Evidence, Multi Function Copier

I. 서 론

PC와 같은 범용의 컴퓨터와는 달리 하드웨어내에 특정 목적의 소프트웨어를 탑재하고 특정 목적만을 위하여 정해진 작업만을 수행하는 임베디드 장치들은 우리와 밀접한 관계를 가지고 있다. 네비게이션, 차량용 운행기록장치, MP3 Player, PMP, CCTV, 디지털복합기 등 임베디드 장치들의 종류는 매우 다양하고 생활의 중요한 일부분들을 차지하고 있음을 알수 있다. 일상생활 속에 임베디드 장치의 활용빈도가 높아진다는 것은 해당 기기를 이용한 범죄의 가능성을 역으로 추정할 수 있다. 이러한 데이터들은 사용자의 과거의 사용 내역등을 통한 사용자 편의성을 제공해주는 기능적 요소를 제공 할뿐만 아니라 범죄수사와 같은 분야에 증거자료로 활용할 수 있다는 가능성을 말해준다. 이러한 여러 가지의 장치들 중에 우리의 사무공간에 빼놓을 수 없는 디지털 복합기의 사용내역에 대한 활용도를 생각해보면 많은 양의 문서들을 복사해서 개인이 사용하거나 사무공간 밖으로 이탈하게 됨을 짐작할 수 있게 한다. 이는 디지털복합기를 통한 기술유출 사건이 빈번히 발생하는 하나의 이유이기도 하다. 이에 따라 디지털복합기에 대한 포렌식 관점에서

접수일(2010년 4월 15일), 게재확정일(2010년 7월 26일)
† 주저자, bis123@spo.go.kr
‡ 교신저자, prowilliam@spo.go.kr

의 연구가 절실함을 알 수 있고, 이에 대해 알아 보려 한다.

디지털복합기의 시장은 삼성, 후지제록스, 롯데 캐논, 신도리코 등의 메이저 업체 제품들이 주류를 이루고 있다. 우리가 업무용 사무실에서 흔히 접할 수 있는 디지털복합기는 과거 복사기의 단순 복사 기능을 넘어서 팩시밀리, 스캐너, 복사기, 프린터 등 다양한 기능을 수행할 뿐 아니라, 네트워크를 통한 스캔된 파일의 송수신, 팩스 자동 송·수신, 이메일 발송, 데이터 장기 보관 기능 등 다양한 부가기능을 통하여 사무업무의 자동화에 기여하고 있는 실정이다.

만일 디지털복합기내 저장매체에 저장되어 있을 수 있는 데이터를 복구하여 문서 위·변조 사건, 사기, 무고, 명예훼손, 뇌물, 기술유출 등 문서와 연관이 깊은 범죄의 직접 또는 간접적인 디지털 증거자료로 활용할 수 있다면 그 효용가치는 매우 크다고 할 것이다. 이를 바탕으로 본 연구에서는 수많은 디지털복합기 제품중 내부에 하드드라이브를 장착하고 스캔한 문서파일을 사용자가 계속적으로 출력할 수 있는 기능을 가지고 있는 메이저급 업체의 특정 2개 모델을 선정하여 디지털복합기내의 데이터를 디지털포렌식 관점에서 분석을 수행한다. 또한 이러한 연구를 바탕으로 범죄 수사에의 활용방안에 중점을 두어 소개 한다.

II. 분석의 필요성

범죄에 사용될수 있는 디지털복합기는 부정을 저지른 당사자 및 기업의 입장에서 이를 고의적으로 은폐해야할 대상이라고 인식하기가 쉽지 않다. 또한 미리 만들어진 시나리오에 의해서 디지털복합기내의 데이터를 사용자 인터페이스 및 복합기 자체의 콘솔 등을 이용하여 인위적으로 삭제하였을지라도 이러한 데이터는 디지털복합기의 저장매체에 전체 또는 일부가 남아 있게 된다. 이렇게 각각의 사건과 관련하여 디지털복합기의 저장매체에 존재하는 데이터의 분석을 통해서 수사에 활용할 수 있는 부분은 다음과 같다.

2.1 수사에 직접적으로 관련된 디지털 증거확보

중요데이터의 사용여부, 이는 중요데이터에 대한 활용내역을 복구하므로써 데이터의 사용여부와 복사본 확보만으로도 범죄에 대한 직접적인 관련성을 특정할 수 있다. 또한 이러한 데이터의 사용시점 및 규모를 추정 가능케 하여 사건의 전체적인 윤곽을 잡을 수 있게 해주는 중요한 역할이기도 하다. 설계도면 등의 기술유출건 수사에 있어서 유출된 회사의 원본 설계도면에 대한 사본을 디지털복합기내에서 찾았다면 이보다 더 중요한 증거는 없다고 할 수 있다.

2.2 수사에 간접적으로 관련된 디지털 증거확보

범죄와 직접적인 관련성이 없으나 간접적인 추론을 가능하게 해줄 수 있는 사용시점, 사용규모, 관련자 특정 가능성 부분을 통하여 수사에 간접적인 영향을 줄 수 있다. 즉, 사용자의 PC에 남아있을 수 있는 스풀파일, 레지스트리내의 기기정보, 복합기의 ip주소와 같은 사용자 설정정보, 복합기내 하드드라이브에 저장되어있는 특정 파일들의 속성정보들을 파악하여 개인 컴퓨터에서 추출된 동일 데이터 및 유사한 데이터간의 비교를 통하여 데이터의 이동경로, 시계열 분석 등의 여러 가지 가능성을 제시 할 수 있을 것이다.

이와 같이 디지털복합기에 남아있는 데이터를 통하여 수사에 활용될 수 있는 범위는 매우 크며, 이런 데이터들을 확보하기 위한 절차 또한 중요하다고 할 수 있다.

III. 디지털복합기에 대한 압수수색

3.1 증거수집 준비단계

디지털복합기에 대한 압수수색 준비단계로서 일반적인 디지털증거 압수수색과 같이 증거수집을 위한 적절한 권한의 유무확인, 영장 등의 기재내용 숙지, 증거수집대상 관련 정보의 파악, 적절한 인원의 구성 등은 당연히 확인되어야 하는 사항이다.

여기서 제기될 수 있는 의문점은 과연 디지털복합기가 압수수색 영장에 기재된 '사건과 관련된 디지털 증거를 저장하는 저장매체'로서 압수수색의 대상이 될 수 있느냐는 것이다. 그러나 이는 저장매체의 개념을 단순히 PC나 서버와 같은 전통적인 디지털기기에 지나치게 한정하고 있는 처사이며 이미 네비게이션, CCTV와 같은 장치들이 수사의 중요한 증거자료 확보를 위한 압수수색의 대상이 되고 있는 실정에서 현실을 무시한 발상이라고 할수 있다.

또한 디지털 증거의 특징인 '매체 독립성'의 측면에서 보면 압수수색의 본연의 대상은 디지털저장매체 그 자체가 아니라 매체내에 저장된 디지털자료가 그 대상

이 된다할 것이므로 그 자료가 어떠한 형태의 저장매체내에 존재하고 있는 가는 크게 문제가 될 것이 없다고 할 것이다.

3.2 증거수집

디지털포렌식의 일반적인 절차에 의거하여 디지털복합기에 대한 압수수색 역시 증거능력 인정을 위한 증거의 진정성, 증거의 동일성, 증거의 무결성을 확보할 수 있도록 진행되어야 한다.

디지털복합기에 대한 압수수색 방법을 크게 나누면,

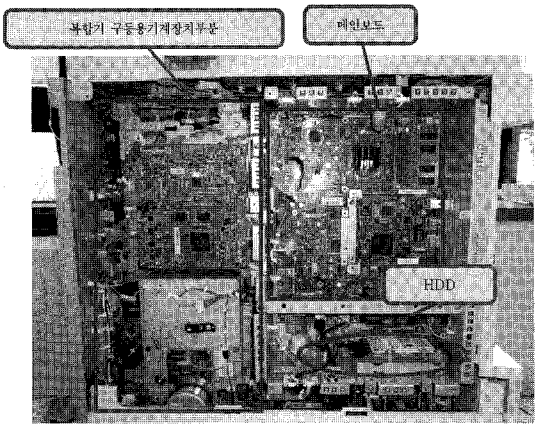
3.2.1 디지털복합기 자체에 대한 압수

이는 압수수색 영장에 원본자체에 대한 압수가 가능하다는 것이 적시되었을 경우, 압수수색절차가 진행되는 현장에서 단순 저장매체내 데이터의 수집이나 저장매체의 분리가 여의치 않을 경우 진행할 수 있는 방법이지만 기기자체의 크기가 커서 운반에 곤란함이 있을 수 있고, 충격 등으로 인한 파손의 가능성으로 인해 실제적으로 집행함에 있어서는 매우 그 가능성이 낮다고 할 것이다. 만일 기기자체를 압수할 경우 전원케이블 연결부위, 기기의 후면 등 저장매체를 분리하기 위하여 분해하여야 할 부위에 적절한 봉인조치를 취하여 추후 증거의 조작시비를 원천적으로 차단하여야 할 것이다.

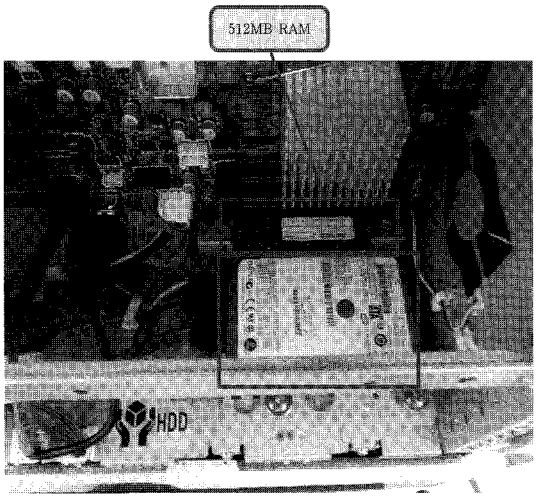
3.2.2 디지털복합기내 하드드라이브의 압수

가장 활용가능성이 큰 방법으로 디지털복합기내의 저장매체를 분리하여 이를 봉인한 후 참관인의 확인서명을 받아 안전하게 이송하여 분석하거나, 또는 압수수색 현장에서 동일 사본을 제작하여 해당 이미지파일을 압수한 후 이를 대상으로 분석작업을 진행하는 것이다.

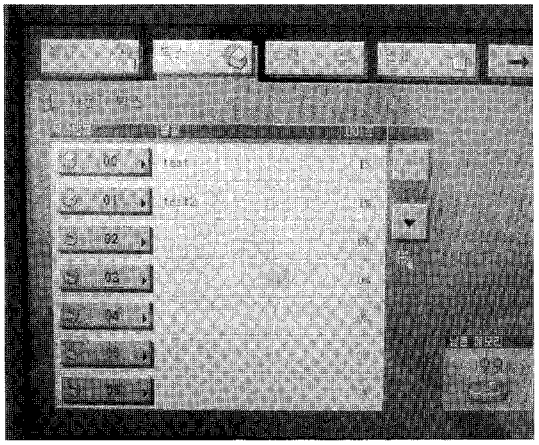
이때 함께 수반되어야 할 작업으로 디지털복합기내 저장매체의 장착형태, 저장매체의 모델명, 시리얼 넘버 등의 기록, 해당 디지털복합기의 콘솔에서 보여지는 각종 설정정보를 아래 〔그림 1~그림 6〕와 같이 함께 촬영하여 추후 분석작업에 있어 필요한 정보를 확보하고, 디지털복합기를 사용하고 있는 사용자의 PC, 서버 등에 설정된 디지털복합기 관련 정보, 프린터 스풀파일, 사용자 인터페이스내 로그기록, 기기 사용설명서 등도 반드시 함께 확보하여야 할 것이다.



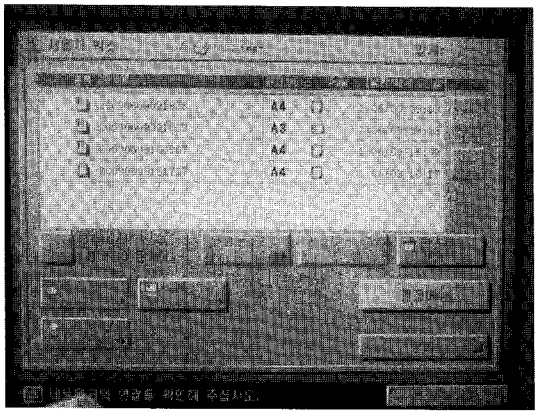
〔그림 1〕 디지털복합기내 하드드라이브 장착형태



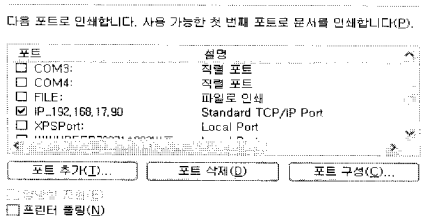
〔그림 2〕 하드드라이브 장착 형태



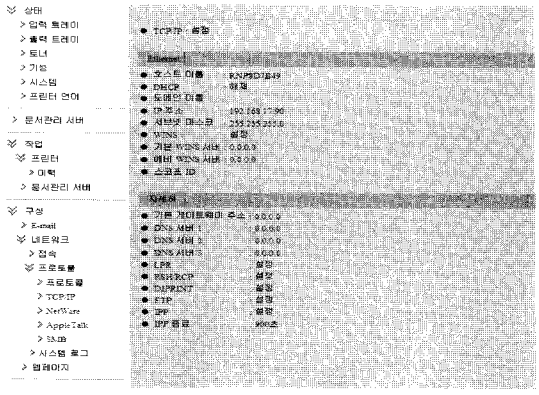
〔그림 3〕 디지털복합기 콘솔에서 보여지는 각종 정보



〔그림 4〕 디지털복합기 콘솔에서 보여지는 각종 정보



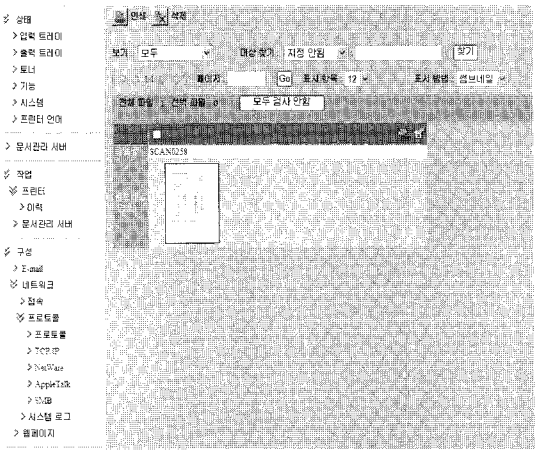
〔그림 5〕 사용자 PC의 프린터 설정정보



〔그림 6〕 사용자 인터페이스내 설정정보

3.2.3 단순 데이터의 압수

디지털복합기 자체의 압수, 저장매체에 대한 압수 또는 현장 사본작성도 불가능한 상황에서 아래 〔그림 7〕와 같이 복합기 제조사에서 제공하는 사용자 인터페이스 등으로 접속하여 현재 보여지고 있는 정보만을 다운로드 받거나 출력하는 등의 방법으로 이루어지는 형태로 확보할 수 있는 정보가 매우 적다는 문제점이 있다.



〔그림 7〕 사용자 인터페이스를 이용한 현재 저장 데이터의 확인

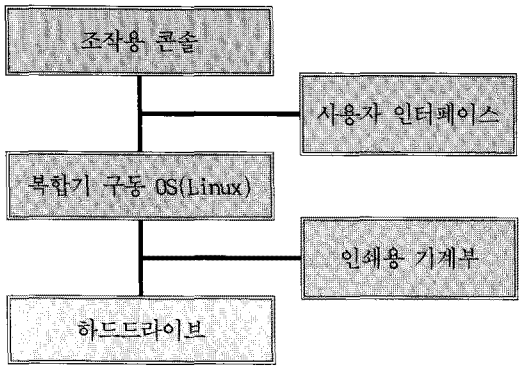
IV. 증거물의 운반 및 보관

디지털복합기 자체를 압수하였을 경우, 기기의 크기, 충격에의 취약성 등을 감안하여 적절한 이동수단을 고려하고 봉인이 훼손되지 않도록 유의하여 분석을 위한 장소로 이동한 후 보관하여야 하고, 저장매체만을 압수하였거나 사본을 작성하였을 경우 역시 충격이나 전자기 등에 의하여 훼손되지 않도록 정전기 방지봉투, 충격방지봉투 등과 같은 안전조치를 취하고 Chain of Custudy의 확보를 위하여 인계인수자의 기록, 비인가자의 접근 차단 등의 조치를 취한 후 운반 및 보관하여야 할 것이다.

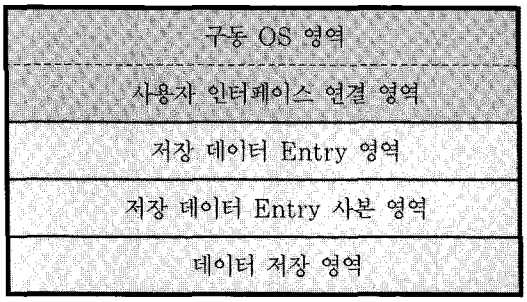
V. 디지털복합기내 데이터 분석

5.1 A사의 디지털복합기내 하드드라이브 분석

디지털증거의 무결성을 확보하기 위하여 원본하드드라이브에 대하여 원본과 동일한 사본 이미지 파일을 작성한 후 이에 대하여 분석작업을 진행하였다. 분석대상이 된 디지털복합기의 개괄적 구조는 아래 〔그림 8~그림 9〕와 같다



〔그림 8〕 디지털복합기 구조



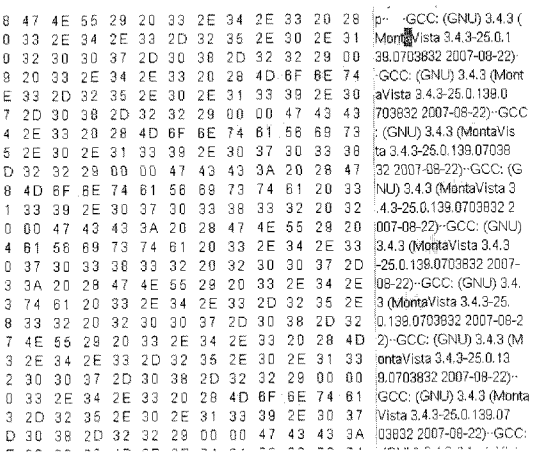
〔그림 9〕 하드드라이브내 구조

분석대상이 된 하드드라이브는 60GB의 용량이었으며 내부 디렉토리 및 파일 등의 정보를 파악한 결과 아래 〔표 1〕과 같이 총 14개의 파티션으로 분할되어 있음을 확인하였다.

〔표 1〕 하드드라이브내 파티션 정보

순번	Name	파티션 타입	총 Sector	크기
1	BOOT	Linux Native	4,209,030	2GB
2	hda2	Linux Native	14,699,475	7GB
3	C	Unknown	41,961,780	20GB
4	D	Unknown	14,699,412	7GB
5	hda6	Linux Native	417,627	204MB
6	E	Unknown	4,208,967	2GB
7	hda8	Linux Native	6,313,482	3GB
8	hda9	Linux Native	10,506,447	5GB
9	hda10	Linux Native	417,627	204MB
10	hda11	Linux Native	2,313,297	1.1GB
11	hda12	Linux Native	224,847	109.8MB
12	hda13	Linux Native	2,586,402	1.2GB
13	ROOT	Linux Native	4,208,967	2GB
14	swap1	Linux Swap	2,120,517	1GB

위 14개 파티션영역 중 'BOOT' 볼륨내 시스템 파일을 분석한 결과 아래 〔그림 10〕과 같이 구동 OS는 MontaVista社의 임베디드 리눅스를 사용하고 있음을 보여주는 정보가 확인되었다.



〔그림 10〕 시스템 파일내에 표시된 OS 관련 정보

위 〔표 1〕와 같이 총 14개의 파티션중 'BOOT', 'hda2', 'hda6', 'hda8', 'hda10', 'hda', 'hda11', 'hda12', 'hda13', 'ROOT', 'swap1' 영역은 Ext (Linux 파일시스템)으로 시스템 구동을 위한 각종 시스템 파일로 구성되어 있고 파일시스템 관련 정보가 파악되지 않는 20GB(볼륨 C), 7GB(볼륨 D), 2GB (볼륨 E)의 3개 영역중 C 볼륨 영역을 대상으로 분석을 진행하였다.

통상적인 파일시스템의 경우 해당 물리 저장매체의 Sector offset 0, 볼륨내 Sector offset 0에 Boot Record 정보가 기재되고 해당 섹터내 byte offset 510~511에 Boot 정보가 기재된 섹터를 의미하는 Magic Number 0x55 AA가 기재되어 있으나 위 3개의 볼륨에는 그러한 정보가 보이지 않으며 위 3개 볼륨 모두 Unallocated area(비할당영역)으로 인식되고 있다.

1) 분석대상으로 선정한 C 볼륨내 Sector offset 5120에서 아래 〔그림 11〕와 같이 사용자가 설정한 문서저장용 폴더의 이름, 순번, 비밀번호 등의 정보가 기재되는 Entry 영역이 보이며,

그 Entry내의 분석된 내용은 아래 〔표 2〕과 같다.

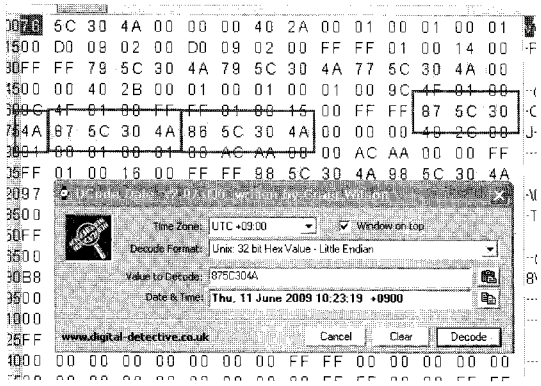
〔그림 11〕 사용자가 생성한 저장용 폴더의 정보가 표시된 Entry 영역

〔표 2〕 사용자 지정폴더 Entry 정보

offset	size	내 용	비 고
10	1	폴더내 파일개수	
24	2	폴더순번	0부터 시작
26	24	폴더이름	영문24자, 한글12자
52	2	비밀번호	

2) 해당 볼륨내 Sector offset 470부터 472까지 아래 〔그림 12〕과 같이 스캔한 문서파일의 생성시간, 위치정보 등을 표시하는 Entry 정보가 발견되고 있으며 Entry의 개수는 저장된 데이터의 용량에 따라 유동적일 것이다.

또한 스캔작업시 자동으로 생성되는 파일이름과 해당파일의 생성시간이 동일하여 생성시간을 파일이름으로 사용하고 있는 것으로 보인다.



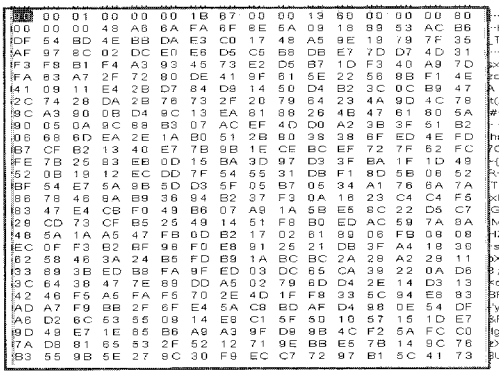
〔그림 12〕 스캔한 파일의 생성시간, 위치정보 등을 표시한 Entry 영역과 시간정보

위 Entry의 분석된 내용은 아래 〔표 3〕와 같다.

〔표 3〕 스캔된 문서파일 Entry 정보

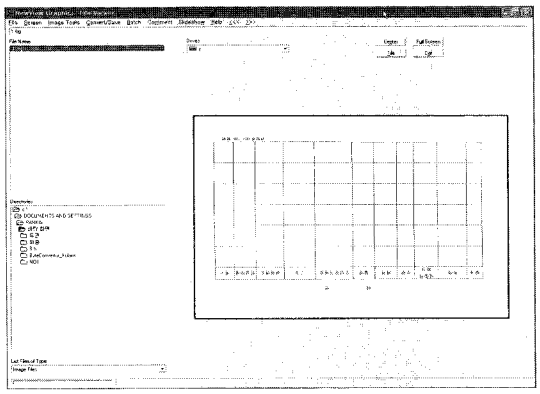
offset	size	내용	비고
0	4	시간정보	작업종료시간으로 추정 (파일이름과 동일)
4	4	〃	〃
8	4	〃	작업시작시간으로 추정(작업종료시간보다 2~3초 가량 빠름
16	2	위치정보	10진수 변환후 2048를 곱한 Sector offset에 데이터 위치

위 〔그림 12〕에서 표시된 0x2C 00(데이터 위치정보)를 십진수로 변환한 값 44에 데이터 블록단위인 2,048 Sector를 곱한 값에 해당하는 볼륨내 Sector offset 90,112로 이동하면 해당 섹터부터 아래 〔그림 13〕와 같이 데이터들이 저장되어 있는 것을 확인할 수 있다.



〔그림 13〕 볼륨내 Sector offset 90,112 부터 저장되어 있는 스캔한 문서파일 Data

이 데이터들은 JBIG 이미지 압축포맷을 사용하고 있으며 Secor offset 90,112부터 데이터의 끝으로

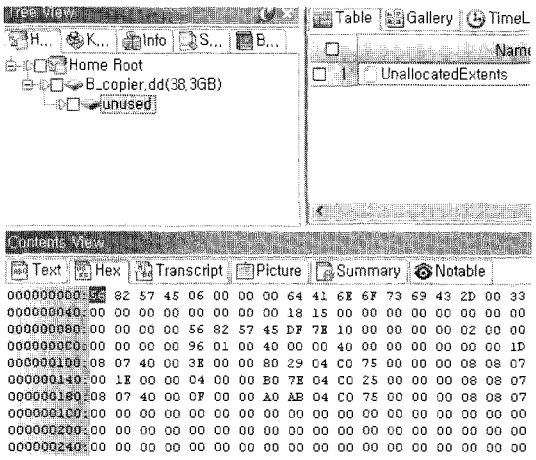


〔그림 14〕 스캔되어 하드드라이브에 저장되어 있는 문서이미지

여겨지는 Sector offset 92,160까지 2,048 Sector (총 1,048,576 byte)를 Export한 후 확장자를 jbg로 설정하고 JBIG 이미지포맷을 볼 수 있는 Viewer 프로그램을 사용하여 해당 파일을 읽어들이면 아래 [그림 14]과 같이 기존에 스캔한 문서 사본을 확인할 수 있다.

5.2 B사의 디지털복합기내 하드드라이브 분석

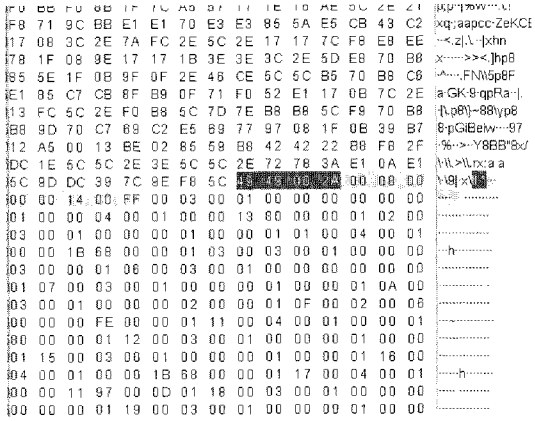
A사의 디지털복합기내 하드드라이브와 마찬가지로 디지털증거의 무결성을 확보하기 위하여 원본하드드라이브에 대하여 원본과 동일한 사본 이미지 파일을 작성한 후 이에 대하여 분석작업을 진행하였다. 분석 대상이 된 하드드라이브는 40GB의 용량이었으나 디스크 전체영역에 대한 통상적인 파일시스템 정보를 확인하지 못하고 Disk 전영역에 대하여 [그림 15]와 같이 Unused Area로 표시되고 있다.



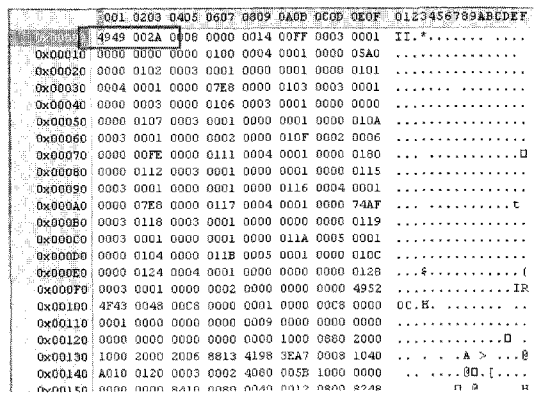
[그림 15] 해당 하드드라이브 전체에 대하여 Unused Area로 인식

해당 사본이미지를 섹터단위로 검색수행한 결과 디스크내 Sector offset 10,279,296부터 스캔한 문서 데이터로 보이는 영역이 발견되어 해당 데이터의 파일헤더로 추정되는 데이터 앞부분 4바이트 0x49 49 00 2A를 이용하여 디스크 전 영역을 검색한 결과 총 392개의 검색결과를 아래 [그림 16]과 같이 얻을 수 있었다.

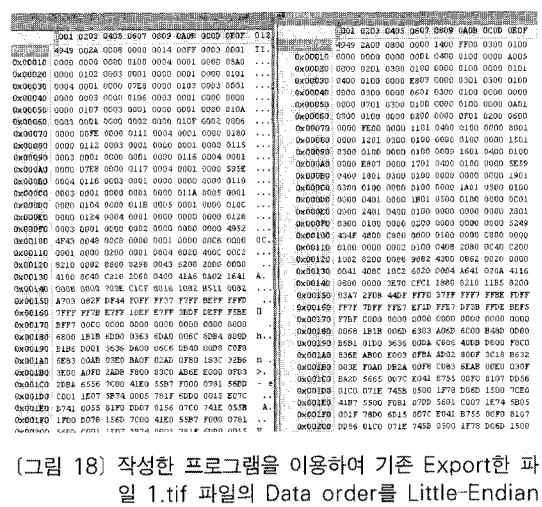
검색결과중 Sector offset 10,280,384에서부터 해당 데이터의 끝으로 보이는 Sector offset 10,280,831까지 448 Sector (총 229,376 byte)를 export한 후 데이터를 분석한 결과 아래 [그림 17]과 같이 tiff 파일 포맷을 사용하고 있는 것으로 확인되었다.



[그림 16] Keyword 검색 수행결과



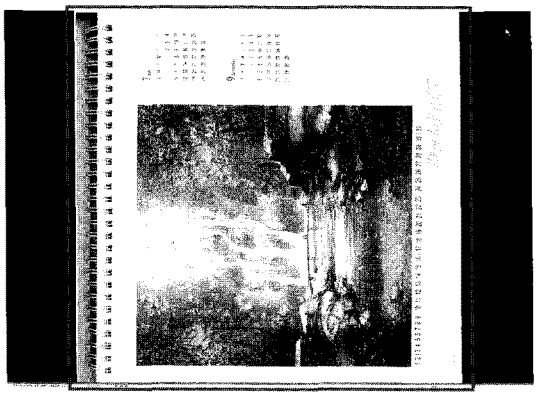
[그림 17] Export한 데이터 내용으로 tiff 파일 포맷과 유사한 구조



[그림 18] 작성한 프로그램을 이용하여 기존 Export한 파일 1.tif 파일의 Data order를 Little-Endian Data order로 변경하여 new.tif 파일로 저장

그러나 현재 이 데이터는 Little-Endian Data order가 아닌 Big-Endian Data order로 나열되어 있어 통상적인 그림파일 Viewer에서는 이를 읽어들일 수 없어 데이터를 Littel-Endian Data order 형태로 변형하기 위하여 2바이트 단위로 내부 바이트 위치를 서로 교환할 수 있는 프로그램을 작성한 후 해당 파일의 내부 바이트 위치를 아래 [그림 18]와 같이 변경시켰다.

Little-Endian Data order로 변경된 new.tiff 파일을 Viewer 프로그램으로 읽어들인 결과 아래 [그림 19]과 같이 기존에 스캔되어 저장된 문서 사본을 확인할 수 있다.



[그림 19] 스캔되어 하드드라이브에 저장되어 있는 문서이미지

VI. 범죄수사에의 적용 가상 시나리오

위 분석과정에서 처럼 디지털복합기로부터 추출한 기존 스캔문서파일의 활용 방안에 관하여 가상 시나리오를 고려하여 보면 아래와 같은 상황을 상정할 수 있다.

피의자 갑은 과거 자신이 근무하던 회사 병에서 첨단 반도체 소자 개발장비의 설계를 담당하던 엔지니어이다. 평소 자신에 대한 회사의 처우에 불만을 품고 있던 중 경쟁업체 정의 대표이사인 을로부터 더 나은 대우와 높은 보수를 약속받고 자신이 근무하던 회사에서 특정 장비 설계도면 20여장을 몰래 인쇄한 후 이를 무단으로 반출하는 방법으로 빼돌린 후 경쟁업체 정으로 직장을 옮긴 후 이를 사무실 디지털 복합기를 이용하여 스캔하고 사무실내 설계업무를 담당하는 팀원들과 공유하여 작업하던 상황이었다.

회사 병의 대표이사는 우연히 거래업체에 납품을 위한 방문을 하던 중 경쟁업체에서 자신들의 고유한 기술로 가능하던 회사제품과 유사한 제품을 생산하기 시작하는 것을 보고 기술유출을 의심하였고 내부적으로 이에 대하여 파악하던 중 피의자 갑을 기술유출 대상자로 지목하여 검찰에 고발하였다.

해당 사건의 고소장을 접수한 검찰은 수사를 개시하여 여러 정황, 참고인들의 진술 등을 토대로 피의자 갑과 을, 그리고 경쟁업체 정에 대한 압수수색을 통한 증거자료의 확보 필요성을 느껴 법원으로부터 압수수색영장을 발부받아 압수수색을 개시하였다. 그러나 이미 주변 참고인들의 검찰소환 등을 통해 기술유출이 문제가 되었음을 직감한 피의자 갑과 피의자 을은 자신들이 보관하던 설계도면을 파기하고 컴퓨터내 하드드라이브를 교체하는 방법 등으로 압수수색에 대비하여 증거의 인멸을 시도하였다.

이러한 사건의 경우 기존의 통상적인 디지털증거 압수수색 상황에서는 컴퓨터내 하드드라이브의 압수수색후 분석과정에서 유출된 설계도면의 행방을 찾기는 힘든 상황이 될 것이다. 그러나 미처 피의자들이 인식하지 못하고 있던 디지털복합기내 하드드라이브에서 스캔된 설계도면 파일이 복구된다면 이는 기술유출 범죄 수사에 있어 핵심적인 증거자료가 될 수 있는 것은 당연한 사실일 것이다.

이러한 상황외에도 디지털복합기내 저장된 데이터의 적용 가능성은 훨씬 다양할 수 있을 것이고, 특히 기술유출, 문서 위·변조 사건, 명예훼손, 무고 등과 같은 범죄의 증거자료 확보에 기여할 수 있는 바가 크다고 할 것이다.

VII. 결 론

이 논문은 국내시장에서 높은 점유율을 보이는 메이저급 업체중 특정 두 업체의 각각 1가지씩의 모델을 가지고 데이터의 복구 및 분석방법과 그 활용가치에 대한 가능성을 연구해 보았다.

현재 우리나라의 규모를 불문한 기업환경에서 디지털복합기의 사용빈도 및 활용도를 감안한다면 디지털복합기내 저장매체에 저장되어 있는 각종 정보는 그 효용가치는 매우 클 것으로 판단되며 피의자의 자백보다는 오히려 복합기내에 저장되어 있던 과거 문서 사본 한 장이 오히려 더 큰 가치를 가질 수 있다.

이 분석을 통해 범죄에 사용된 데이터의 전체 및 일부의 데이터가 내부적으로 저장 관리되고 있다는 것을 확인하였고, 원본과 동일한 그림파일을 확보할 수 있음을 확인 하였다. 또한 시간정보 및 사용규모 등을

추정할 수 있는 부가적인 데이터도 함께 존재함을 일부 확인하였다. 이러한 정보들은 수사기관의 입장에서 범죄수사에 있어 증거물의 중요도에 따라 직접적인 증거로 활용될 수 있을 뿐만 아니라 시간정보 등을 통한 범죄자의 알리바이를 검증할 수 있는 간접적인 자료로도 활용될 수 있는 가능성을 제시하였다. 이는 또한 수사기관이 아닌 기업의 입장에서도 내부통제의 중요한 수단으로 충분히 활용될 수 있을 것이다.

급속도로 발전하는 정보화 시대에 있어, 이에 대한 부정을 막고 기업의 자산과 이윤을 보호하기 위해서는 IT보안과 부정에 대한 통제방법에 대해 새롭게 구성해야 하고 다양화 시켜야 한다. 디지털복합기에 대한 포렌식 관점에서의 분석은 그 다양한 내부통제 방법 중 하나의 통제 역할을 제시 해주리라 본다.

임베디드 포렌식에 대한 수요는 앞으로 꾸준히 증가 할 것이다. 개인용 컴퓨터 뿐만 아니라 디지털포렌식의 한분야라고 할 수 있는 임베디드 시스템에 대한 데이터의 추출 및 이에 대한 분석의 필요성은 앞으로 꾸준히 증대할 것으로 보이고 계속적인 연구와 분석 작업이 이루어져야 할 영역이라 할 수 있다.

참고문헌

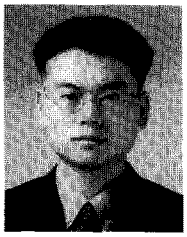
[1] 대검찰청, 대검찰청, "디지털포렌식 매뉴얼," pp. 15-50, Mar. 2008.

[2] Adobe Developers Association "TIFF Revision 6.0,"

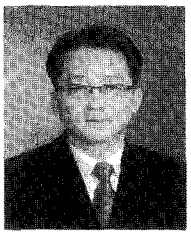
[3] Joint Bi-level Image Eperts Group, http://www.jpeg.org

[4] FileFomat.info The Digital Rosetta Stone "JBIG Compression", http://www.fileformat.info

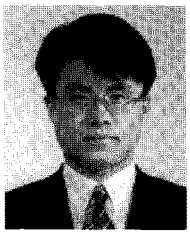
〈著者紹介〉



박 일 신 (Il-Shin Park) 정회원
2000년: 전남대학교 행정학과 졸업
2009년~현재: 성균관대학교 정보보호학과 석사과정
2007년~현재: 대검찰청 디지털수사담당관실 디스크분석팀 검찰수사관
〈관심분야〉 디지털포렌식 관련 법제도, 역공학, 임베디드 포렌식



강 철 훈 (Cheul-Hoon, Kang) 정회원
대전대학교 컴퓨터공학과 졸업
연세대학교 공학대학원 컴퓨터공학과 졸업
2006년~현재: 대검찰청 디지털수사담당관실 데이터베이스 포렌식팀 검찰수사관
〈관심분야〉 Database Forensic and Accounting Forensic



최 성 진 (Sung-Jin Choi) 정회원
1990년: 서울대학교 사법학과 졸업
1997년: 서울대학교 법학 대학원 졸업
2009년~현재: 대검찰청 디지털수사담당관
〈관심분야〉 디지털포렌식, 증거법