情 報 保 護 學 會 誌
第21卷 第6號, 2011. 10

디지털 증거 수집과 분석을 위한 스마트폰 포렌식 적용 연구

이 정 훈*, 천 우 성**

요 약

국내 스마트폰의 사용자는 2천만 명에 도달하고 있고, Wi-Fi Zone과 3G망 뿐만 아니라, 4G WiBro와 LTE로 속도까지 향상 되어 스마트폰의 활용은 더욱 높아지고 있다. 또한 일부 스마트폰 사용자들은 본인의 스마트폰 단말기를 해킹과 루팅을 통하여 멀티미디어 콘텐츠를 불법으로 이용하고 있다. 이는 한·미 FTA체결에 저작권의 법적 문제제기가 있다. 또한 기존의 이동통신 2G, 3G 휴대폰들과 스마트폰은 휴대용 이동기기로서, 범죄에 사용되는 직간접 증거들과 관련성이 높아서, 휴대폰과 스마트폰에서 생성·저장된 디지털 증거에 대한 스마트폰 포렌식 적용에 대한 연구가 필요하다. 스마트폰은 휴대폰 보다 다양한 기능을 지원해주기 때문에 스마트폰의 사용정보에는 연락처, 통화기록, 인터넷, 메시지, 사진, 동영상 등의 많은 정보를 가지고 있으며 이러한 정보는 포렌식 수사 과정에서 사용자의 행위를 유추하는데 도움이 될 수 있다. 본 디지털 증거 수집과 분석을 위한 스마트폰 포렌식 적용에서는 법정에서 사용될 포렌식 증거의 수집과 분석을 위한 압수·수색 방법과 주의할 점을 연구하였다

Ⅰ. 서 론

최근 스마트폰(Smart Phone)을 통해서 디지털 멀티미디어 정보의 전달과 이용이 빈번하게 이루어지면서, 이동 중에 업무와 실생활과 관련된 정보를 전달하고, 편리성의 이용하는 도구로서 스마트폰이 범죄에도 이용되고 있다. 스마트폰을 통한 범죄는 디지털 무선 정보에 대한 공격과 침해사고를 유발하고, 사회적 경제적 문화적 피해를 발생시킨다[1].

애플사의 앱스토어(APP Store), 구글사의 안드로이드 마켓(Android Market)과 같이 애플리케이션 소프트웨어 또는 콘텐츠를 판매하는 공개시장(open market)을 운용하고 있다. 앱스토어나 안드로이드 마켓은 일정한 요건을 갖춘 개인이 저작물을 게시하여 거래 할 수 있게 함으로써, 새로운 비즈니스 창출의 기회를 제공하는 매력을 갖추고 있다. 그러나 애플리케이션의 폭발적 증가와 함께 유사한 저작물들이 속출하고 있으며, 특히, 탈옥(Jailbreak)나 루팅(Rooting)을 이용하여 유료로 서비스되는 애플리케이션을 무료로 사용하거나 애플리케이션을 이용해 방송사의 저작물을 실시간으로 스트리밍 서비스 해주는 사례도 등장하고 있다[2].

범죄에 이용된 스마트폰을 압수·수색 하여 증거의 습득과 복원하는 일련의 과정 속에서 원본성과 무결성 검증이 필요하다[3]. 스마트폰의 이동성과 편리성은 범죄자들의 통신수단으로 범죄에 이용되어 지고, 스마트폰에 저장 된 디지털 자료로 부터 증거 수집, 증거 분석, 증거에 대한 무결성 검증이 중요시 되고 있으며, 추출한 증거가 객관적인 증거로 보장하기 위하여 원본성과 무결성 입증하고, 검증을 하여, 불법적인 사용자들을 법적으로 제재하기 위해 디지털 정보 침해범죄 수사 진행 시 사용자의 행위분석 및 침해범죄 행위의 분석에 적용할 수 있도록 수사에 활용할 수 있어야한다[4].

Ⅱ. 휴대폰과 스마트폰을 이용한 범죄 사례

휴대폰과 스마트폰의 높은 보급률과 함께 휴대폰과 스마트폰으로 금융거래까지 가능해 지면서 휴대폰과 스마트폰은 신종범죄에서 사용하는 사례가 발견되고 있

* 한국저작권위원회 디지털정보보호팀(yyyjjhh@paran.com)
** 호서대학교 벤처전문대학원 IT응용기술학과(deux8522@nate.com)

다. 별다른 보안대책이 없는 상태에서 생활필수품으로 자리 잡을 정도의 높은 보급률은 새로운 장비에 대한 빗나간 욕심으로 인하여 휴대폰과 스마트폰 도난범죄가 생겨나고 있고 이러한 휴대폰과 스마트폰을 통한 금융거래가 가능해지자 더욱 다양한 방법의 범죄들이 등장하고 있다.

휴대폰과 스마트폰을 이용한 범죄를 그 양태와 신종범죄에 대한 선행 연구들의 개념규정을 참고하여 정의하여 보면, 이동통신 단말기 및 이동통신 서비스와 관련하여 자기 또는 제3자의 위법적인 이득을 위하여 이동통신 단말기 소유자 및 서비스 활용 자에게 행하는 제반 범법행위라 할 수 있다. 또한 휴대폰과 스마트폰을 수단으로 하거나 또는 그 제도를 이용하여 발생된 것으로서 형사적 제재의 대상이 될 수 있는 반사회적 위법행위라고 정의할 수 있다[5].

2.1 사기 · 공범관계 사건

사기 범행의 공범관계임에도 불구하고, 피고소인을 상대로 자신도 피해자라고 주장하며 고소를 하였다. 수사기관은 피고소인과 고소인 사이에 오고간 핸드폰 문자 메시지를 입수하기 위해 피고소인의 핸드폰을 압수하였으나 이미 문자 메시지는 삭제되어 있었다. 수사기관은 압수한 핸드폰의 삭제된 문자 메시지를 복구하고, 이를 근거로 고소인에 대해 무고와 사기를 인지하여 공범인 피고소인과 병합 기소하였다[6].

2.2 살인 사건

2010년 5월, 피의자가 경남 소재 피의자 집에 찾아온 피해자와 다투던 중 피해자를 부엌에 있는 칼로 찔러 살해한 사건이 발생하였다. 피의자가 동생에게 보낸 휴대폰 문자메시지에서 살해도구 '칼'과 관련된 내용을 복구여 범행 사실 자백에 활용한 사건이다[7].

2.3 기업 영업비밀 누설 사건

2009년 12월, 경기 소재 연구소를 방문해 회사 허락 없이 개발 중에 있는 자동차를 휴대폰을 이용해 촬영하고, 외부로 유출해 자동차 개발사의 영업비밀 누설 사건 발생하였다. 피의자가 촬영 후 삭제한 개발 중인 자동차 사진 7매를 휴대폰에서 복구해 범행 사실을 입증한 사건이다[7].

2.4 과금 유발형 악성코드 유포 사건

2010년 8월, 발견된 트로이목마 'SmsSend'는 구글 안드로이드 운영체제(Operating System, OS)에 감염되는 최초의 악성코드로 'MoviePlayer'와 'PornoPlayer'란 이름의 동영상 애플리케이션으로 위장·유포됐다. 이 코드가 설치된 스마트폰은 특정 상용서비스 번호로 문자메시지(SMS)를 지속적으로 전송하고 과다 요금을 발생케 하며, 사용자 몰래 자동으로 6달러가 유료로 과금 되었다[8][9].

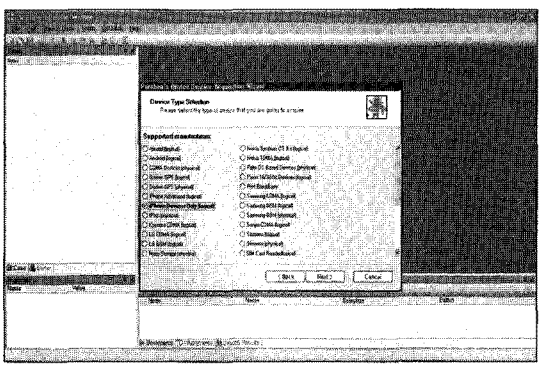
2.5 사생활 침해 사건

2010년 9월, 주택에 필터교체 등 정수기 점검을 위해 방문한 정수기 점검 기사가 여성의 치마 속을 스마트폰으로 동영상 촬영하는 등 같은 수법으로 모두 5차례에 걸쳐 여성들의 특정 부위를 촬영한 혐의(성폭력 범죄의 처벌 등에 관한 특례법 위반)를 받고 불구속 입건하였다[10].

Ⅲ. 스마트폰 포렌식 수사 도구

3.1 Device Seizure

현재 시장에 나와 있는 도구 중 가장 많은 휴대폰 모델을 지원하고 있으며 수사에 필요한 다양한 정보를 수집 할 수 있다. Device Seizure는 논리적인 수집과 물리적인 데이터 수집도 지원한다. 물리적 수집과 유니코드



〔그림 1〕 Device Seizure 메인화면

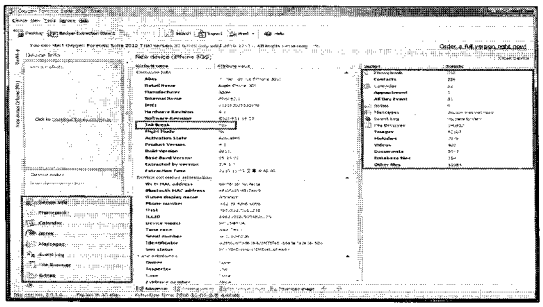
및 핵사 검색 기능이 가능하며, SIM 카드 복제, Windows CE 레지스트리 뷰어 및 핵사 뷰어가 가능하다[11]. [그림 1]은 Device Seizure 메인화면이다.

3.2 Oxygen Forensic Suite 2

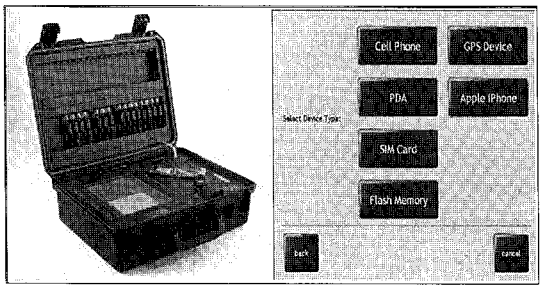
OXYGEN SOFTWARE에서 제작한 Oxygen Forensic Suite 2는 1350개의 휴대폰을 지원하며, 심비안 운영체제에 중점을 맞추었으며, 윈도우 모바일과 RIM 운영체제도 지원한다[12]. [그림 2]는 Oxygen Forensic Suite 2 메인화면이다.

3.3 CellDEK

CellDEK은 휴대폰 포렌식 도구가 하나의 하드웨어로 구성되어 있다. LCD화면을 지원하여 수집하는 정보를 바로 볼 수 있으며, 데이터 수집, 디스플레이, 분석을 할 수 있고, 현장에서 직접 휴대폰을 수집, 분석 할 수 있다. SIM 리더기가 내장 되어있고, 네트워크 차단 카드가 지원된다. [그림 3]은 CellDEK 데이터 수집도구이다[13].



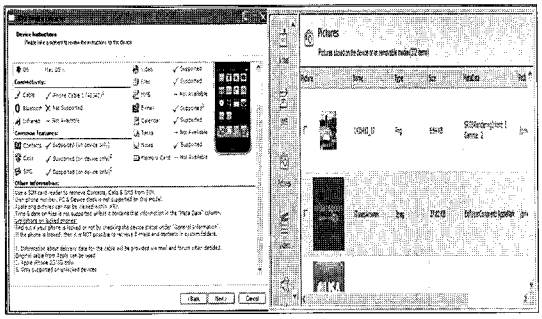
〔그림 2〕 Oxygen Forensic Suite 2 메인화면



〔그림 3〕 CellDEK 데이터 수집도구

3.4 .XRY - MICRO SYSTEMATION

.XRY는 논리적인 수집을 한다. 시스템 이용하는 나라의 언어로 리포트 출력이 가능하며, 심비안 운영체제에 대한 지원, 노키아 휴대폰에 기록된 파일에 대한 파일 시그니처 디코딩이 가능하다. 윈도우 모바일 이용기기에 대한 메모리 덤프와 파일 시스템 디코딩이 가능하다[14]. [그림 4]는 .XRY의 분석 화면이다.



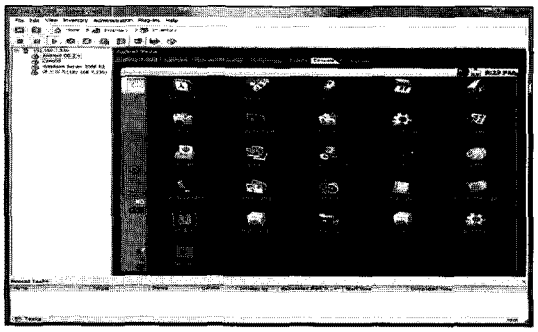
〔그림 4〕 .XRY의 분석 화면

Ⅳ. 스마트폰 포렌식 수사 절차 모델

기존의 휴대폰에서 SMS, 전화번호부, 통화목록, 메모, 스케줄, 사진, 동영상 등의 자료는 이동단말기 플래시 메모리에 저장되어 컴퓨터 등 디지털 기기로 전송하는 방식은 유·무선 방식으로 구분 한다. 스마트폰 내에 저장된 데이터는 범죄 수사 과정에서 분석을 위해 중요한 정보로 제공될 수 있다[15][16]. 스마트폰은 다양한 OS를 가지는 것만큼 저장매체와 형태, 방식이 다양하며 범죄와 관련된 정보를 수집하기 위해서 스마트폰의 표준화된 포렌식 절차가 필요하다. 스마트폰도 휴대폰을 모태로 발달한 이동단말기기로 휴대폰에 대한 모바일 포렌식 방법을 준용하여 디지털 포렌식 수사에서의 범죄와 관련된 스마트폰의 취급 방안을 제시하여 표준 절차를 마련한다.

4.1 스마트폰 포렌식 사전조사

모바일 웹은 PC에서 접근이 불가능한 경우가 많아 범죄열람표는 PC에 모바일 환경을 구축(Vmware 안드로이드 가상 OS, Eclipse 등)하여 작성한다. [그림 5]는 Vmware 안드로이드 환경 구축하여 Mobile Web 페이

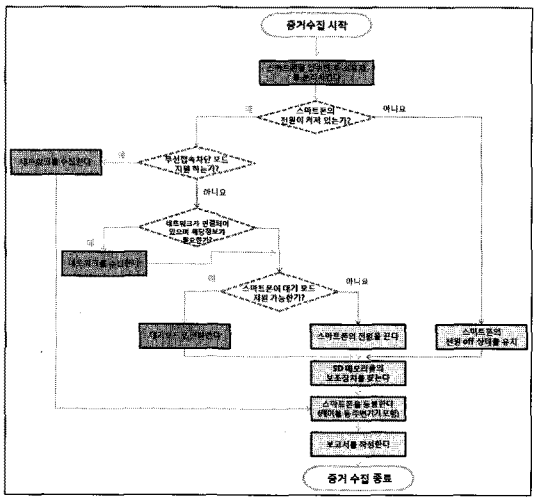


〔그림 5〕 Vmware 안드로이드 환경 구축하여 Mobile Web 페이지 접속

지 접속화면이다.

4.2 스마트폰 포렌식 증거수집 모델

스마트폰에서 증거 자료를 수집하기 위해서 [그림 6]과 같은 절차를 통해 실시한다.



〔그림 6〕 스마트폰 디지털 증거수집 절차

4.2.1 증거물 수집

현장에서 수집대상을 식별하고, 수집의 필요성을 결정한다. 수집대상을 압수한 후 사진을 촬영하고 스마트폰 사용자를 대상으로 운영체제, 응용프로그램, 패스워드 등의 정보를 수집한다.

4.2.2 전원 확인

스마트폰의 사용자 또는 소유자를 심문 할 때에는 스마트폰의 보안코드나 패스워드를 요구해야 하며, 스마트폰의 초기화 기능을 사용하지 못하도록 하고, 스마트폰 등은 배터리를 제거하면 내용이 지워질 수도 있으므로 함부로 배터리를 제거해서는 안 된다. 압수 당시 전원이 켜진 상태라면 무선접속차단 모드를 지원하는 기기의 경우 무선접속차단모드로 전환하고, 무선접속차단 모드를 지원하지 않을 시 전원을 차단하여 외부접속 및 무선접속으로 인한 무결성의 훼손을 방지한다.

4.2.3 증거물 포장

전파 차단용 봉투와 전파 차단용 장치를 이용하여 대상기기를 포장하고 또한, 데이터케이블, 컴퓨터설치드라이버, 충전기, 외장형 메모리 등도 같이 동봉하고 봉인지를 이용해 봉인한다. 봉인 후 증거물 라벨에 해당 장치의 압수일자, 집행기관, 인적사항, 대상정보(모델명, 시리얼 넘버 등) 등을 기록한다.

4.2.4 증거 수집 완료 및 이송

수집된 증거와 증거물 목록이 맞는지 최종 확인한 후 증거 수집자와 증거 이송자가 인수인계서에 서명한 후 이송을 실시한다. 이송 시 증거물들은 제전용 보호필름, 충격완화제, 충격보호박스 등 안전하게 포장한다.

4.2.5 증거 수집 결과보고서 작성

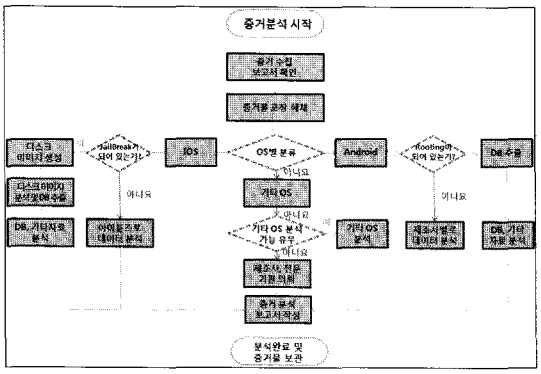
증거 수집이 완료된 후 집행기관, 사건개요, 수집일시, 수집장소, 인적사항, 증거물 목록, 수집절차 등이 포함된 증거 수집 결과보고서를 작성한다.

4.3 스마트폰 포렌식 증거분석 절차 모델

스마트폰에서 증거 자료를 수집 한 후 증거분석을 하기 위해서 [그림 7]과 같은 절차를 통해 실시한다.

4.3.1 증거 수집 결과서 확인

이송된 증거와 증거물 목록이 맞는지 최종 확인한 후



〔그림 7〕 스마트폰 디지털 증거분석 절차

증거 이송자와 증거 분석자가 인수인계서에 서명한다. 이송된 증거물들은 전파 차단장치가 있는 증거분석실에서 포장을 해체한다.

4.3.2 증거물 분류

제조사 및 운영체제에 따라 분류하고 해킹(Jailbreak, Rooting 등) 여부를 확인하여 분석을 실시한다. 스마트폰은 각 운영체제별, 제조사별로 지원되는 범위와 파일시스템 포맷이 상이하기 때문에 주의하여 분류한다. 일반적으로 많이 사용되는 파일시스템 포맷으로는 iPhone HFSX, 안드로이드 LFS 등이 있다.

4.3.3 증거 분석

물리적인 데이터 추출 시 각 운영체제별로 서로 다른 파일 포맷을 사용하기 때문에 주의해야 한다. 각 제조사마다 파일시스템을 변경하여 사용하고 있어 이에 따라 스마트폰 제조사, 기기종류에 따른 파일 포맷을 지원할 수 있는 분석도구가 필요하다. 논리적으로 데이터를 추출 시 휴대폰과 PC를 연결하여 각 제조사에서 제공하는 백업 프로그램, 백업 응용프로그램을 활용할 수 있으며 기기에 따라서 해킹된 폰의 경우 콘솔로 접근하여 복사하는 방법도 존재한다.

스마트폰 데이터에서 사용할 수 있는 기본적으로 분석 대상이 되는 데이터는 연락처, 최근통화기록, SMS, MMS, 응용프로그램정보, 일정, 메모, 사진, 멀티미디어 등의 정보를 추출할 수 있으며 새로운 운영체제나 특이사항의 경우 제조사나 전문기관에 의뢰하여 분석을 실시한다.

4.3.4 증거 분석 결과서 작성

증거 분석 결과서는 분석자가 각 단계별로 법적이 절차에 맞게 작성하고 조사자가 쉽게 이해할 수 있는 용어를 사용해 객관적인 사실에 기반 하여 논리정연하게 작성한다. 작성된 결과서는 수집자, 분석자, 검토자, 법률전문가가 이상이 없음을 확인하고 사인한고 수사기관에 정식 공문으로 발송한다.

4.3.5 증거물 보관 및 이송

데이터 추출이 완료된 후에는 다시 증거수집 절차에 맞춰 전파 차단용 봉투와 전파 차단용 장치에 넣고 봉인하여 봉인일시, 봉인자, 분석개요, 인적사항 등을 기재하고 충격완충제, 충격보호 박스에 넣어 수사기관으로의 이송을 실시한다.

V. 스마트폰 포렌식 증거 수집 · 분석

5.1 iPhone 증거 수집 · 분석

5.1.1 증거 수집

iPhone에서의 증거수집 방법은 탈옥여부에 따라서 그 방법이 다르다. 탈옥을 했을 경우에는 시스템의 root 권한을 획득하여 dd 명령어를 이용해서 디스크 이미지를 생성하고 그렇지 않을 경우에는 iPhone Backup 파일등을 이용해서 증거를 수집한다.

5.1.1.1 With Jailbreaking(iPhone dd 이미지 생성)

■ Unencrypted Recovery : Mac OS X / Widnows

$ nc -l 7000 | dd of=./rdisk0s2 bs=4096 or $ nc -l -p 7000 | dd of=./rdisk0s2 bs=4096	
nc	Calls netcat
-l	Tells netcat to listen for incoming connections
7000	Tells netcat to use port 7000
| dd	Pipes(relays) the information received by netcat to the dd disk copy utility
of=./rdisk0s2	Stores the disk image locally(of stands for "output file") with the filename rdisk0s2.
bs=4096	Uses a disk block size of 4K

〔그림 8〕 Unencrypted Recovery 명령어

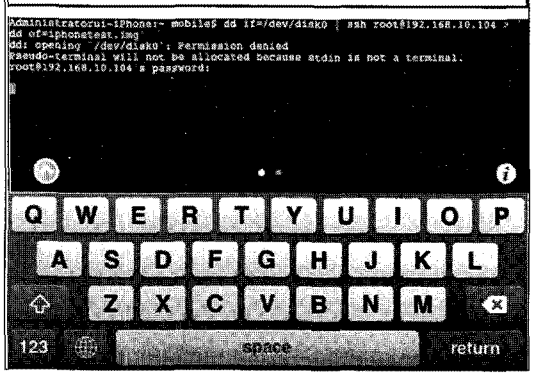
■ Sending the data

$ ssh -l root xxxx # /bin/dd if=/dev/rdisk0s2 bs=4096 | nc y.y.y.y 7000	
/bin/dd	Calls the disk copy utility on the iPhone
if=/dev/rdisk0s 2	Instructs disk copy to read the second partition of the raw disk as input
bs=4096	Uses a disk block size of 4K
| nc	Pipes(relays) the information received by the disk copy utility ot netcat
y.y.y.y	Since -l wasn't specified, instructs netcat to send the data to(not receive from) the specified address
7000	Instructs netcat to use port 7000

〔그림 9〕 Sending the data 명령어

■ Making dd image & Sending the data

```
$ dd if=/dev/disk0 | ssh <username>@<computer-ip> 'dd of=iphone-dump.img'
$ dd if=/dev/disk0s1 bs=4096 | nc <ip> <port>
$ dd if=/dev/disk0s2 conv=sync, noerror bs-4k | -w1  <ip> > <port>
```



〔그림 10〕 iPhone에서 dd이미지 생성 화면

5.1.1.2 Without Jailbreaking

■ iTunes를 이용하여 Backup 파일을 수집

OS	Backup 파일 경로
Mac	/사용자/사용자 이름/라이브러리/Application Support/MobileSync/Backup/
Win XP	\Documents and Settings\사용자 이름\Application Data\Apple Computer\MobileSync\Backup\
Win 7	\사용자\사용자 이름\AppData\Roaming\Apple Computer\MobileSync\Backup\

〔그림 11〕 iPhone Backup 파일 경로

탈옥을 하지 않은 iPhone의 경우에는 컴퓨터에서 iTunes를 이용하여 Backup파일을 수집한다. 상용 포렌식 도구를 사용해서 iPhone의 Backup 파일로부터 얻을 수 있는 정보(최신 통화기록, 메시지, 이미지 등)를 수집할 수 있다.

5.1.2 증거 분석

5.1.2.1 With Jailbreaking(iPhone dd 이미지 분석)

■ iPhone에서는 HFSX 파일시스템 사용
■ Header Signature : 48 58(H X)
■ Encase 지원 파일시스템은 HFS, HFS+이므로 Signature를 "H+"로 수정

5.1.2.2 Without Jailbreaking

■ iTunes 또는 그 밖의 동기화 프로그램을 사용하여 백업 폴더의 파일들을 복사, 속도는 빠르지만 삭제, 변경, 은닉한 파일들에 대해서는 복구 어려움
■ Disassembling : 물리적으로 iPhone의 Flash Rom Chip을 분리하여 데이터를 추출하는 방법으로 롬이 물리적으로 손상될 경우 데이터 추출에 문제가 발생하므로, 전문적인 장비와 하드웨어를 다루는 엔지니어 수준의 기술이 필요
■ Sim(Subscriber identity Module) Card : 사용자 정보 및 식별번호, Service Key(MSI) 등을 저장하고 있으며, 이 외에 PhoneBook, SMS, Call History등이 저장되어 있다 iPhone을 업무용으로 사용 시 조직의 정보 및 민감한 정보가 Sim Card에 남게 되어 증거 자료가 될 수 있음.

5.2 안드로이드폰 증거 수집 · 분석

5.2.1 증거 수집

안드로이드에서는 사용정보(연락처, 메시지, 미디어 등)를 저장한 데이터베이스인 SQlite에 직접 접근이 불가능하다. 따라서 사용정보를 추출하기 위해서는 전문 포렌식 도구를 사용하거나 콘텐트 프로바이더(Content Provider), 또는 루팅(Rooting)을 이용해 접근하여야 한다.

콘텐트 프로바이더는 공유할 수 있는 데이터의 저장소인데 애플리케이션 데이터베이스를 관리하고 공유하는데 사용되어지며, 그 외의 기기에 있는 각종 데이터에 대한 추상적인 인터페이스 제공 및 여러 애플리케이션을 사용할 수 있다. 콘텐트 프로바이더를 구성하면 데이터에 대한 통제권을 충분히 확보한 상태에서 이와 같이 개발 중인 애플리케이션뿐만 아니라 다른 애플리케이션

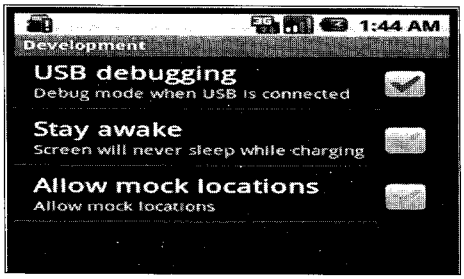
에서도 접근 가능하도록 기능을 제공 할 수 있다. 기본적으로 설치되는 애플리케이션들은 자신들의 Native Content Provider를 가지고 있으며 이들 Native Content Provider가 공개하는 URI를 통해 SQlite 데이터베이스에 접근할 수 있다.

루팅은 안드로이드 스마트폰의 운영체제를 해킹해 관리자의 권한을 얻는 행위를 말하며, 리눅스에서 관리자 권한을 얻는 행위를 지칭하는 용어에서 파생됐다. 안드로이드는 리눅스를 운영체제로 사용하는데, 리눅스에서 최고 권한을 가진 계정이 '루트(root)'다. 즉, 루팅으로 안드로이드 운영체제의 사용자 권한을 '슈퍼 유저'로 바꿔 안드로이드 운영체제가 지원하지 않는 기능을 추가하거나 지원하는 기능을 삭제할 수 있다.

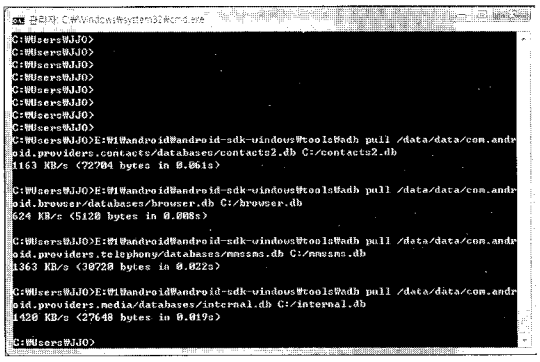
5.2.1.1 증거수집 - 루팅 활용 가능

■ 명령어 기반의 데이터 추출

루팅이 되어 있는 상태에서 안드로이드 스마트폰으로 접근하기 위해서는 Android SDK, 안드로이드 스마트폰 Driver가 필요하다. Android SDK는 개발자를 위한 개발도구인데 http://developer.android.com/sdk/index.html에서 다운로드가 가능하며 안드로이드 스마트폰 Driver는 각 제조사의 홈페이지에서 구할 수 있다. [그림 12]는 USB Debugging 설정 한 화면이고, [그림 13]은 명령어 프롬프트 창에서 Android SDK의 adb로 DB 백업을 한 화면이다.

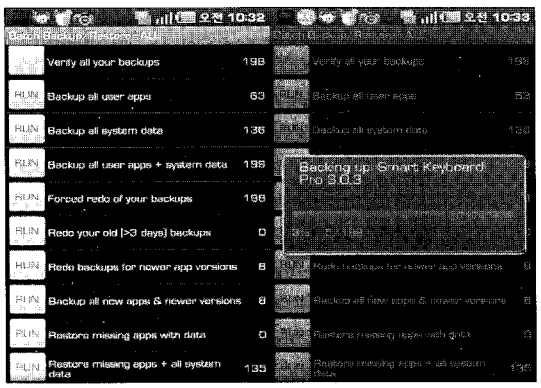


〔그림 12〕 USB Debugging 설정 화면



〔그림 13〕 adb 백업 화면

〔그림 14〕 Titanium Backup 구동화면 및 백업화면

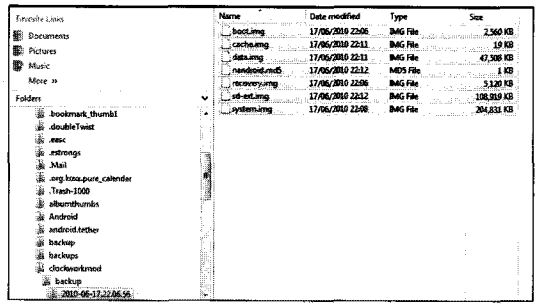


〔그림 15〕 Titanium Backup 실행 화면

■ APP 기반의 데이터 추출

[그림 14]와 [그림 15]처럼 Titanium Backup 루팅 후 애플리케이션을 설치하여 안드로이드의 간단한 백업 기능(애플리케이션 파일, SD Card 파일, 연락처, 즐겨찾기 등)과 파일 리스트 및 애플리케이션 리스트 등을 Content Provider URI를 통해 SQlite 데이터베이스에 쿼리를 전송하고 그 결과로 사용정보를 받아오는 형식으로 구현되어 있다.

백업된 자료들은 /mnt/sdcard/clockworkmod/backup/<해당일자> 디렉터리에 [그림 16]과 같이 .img 형식으로



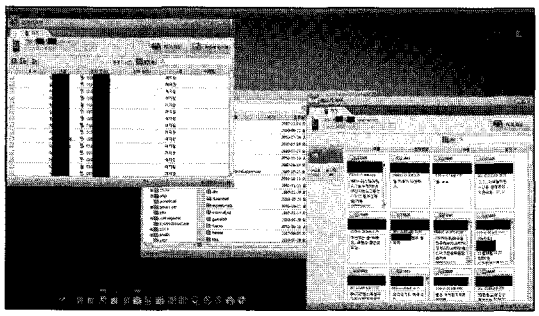
〔그림 16〕 Titanium Backup 백업파일 위치

저장된다.

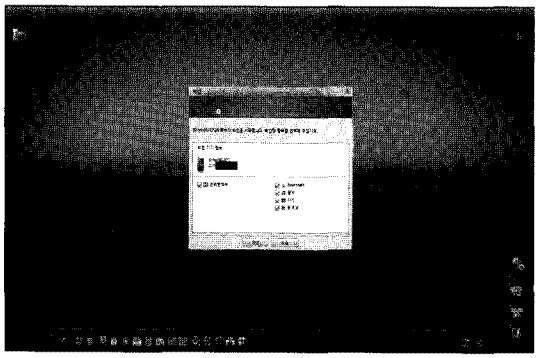
5.2.1.2 증거수집 - 루팅 활용 불가능

■ 제조사 프로그램 기반의 데이터 추출

안드로이드 스마트폰의 경우 OS의 정보가 공개되어 있는 관계로 OS에 대한 수정이 가능하여 제조사별로 Driver, UI, 관리프로그램이 다르기 때문에 각 제조사에서 제공하는 관리프로그램을 이용하여 데이터 추출에 이용한다. [그림 17]은 삼성 KIES 프로그램을 이용하여



〔그림 17〕 삼성 KIES 프로그램 - 갤럭시S 사용정보 확인

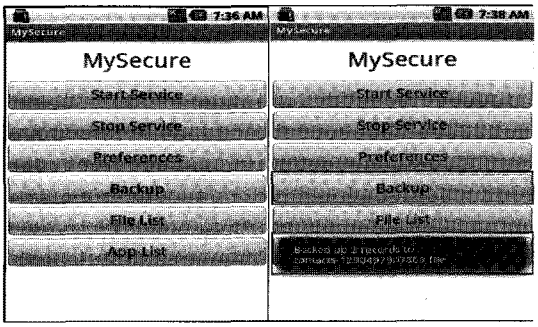


〔그림 18〕 삼성 KIES 프로그램 - 갤럭시S 백업

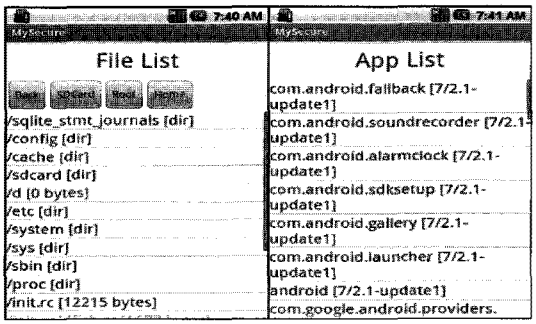
사용정보를 확인 한 것이고, [그림 18]과 같이 백업이 가능 하다.

■ APP 기반의 데이터 추출

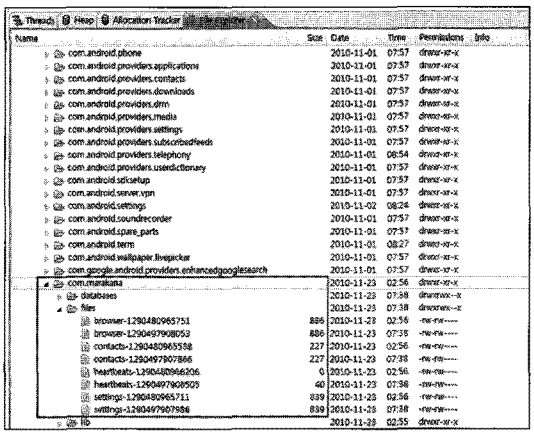
[그림 19]처럼 MySecure은 안드로이드의 간단한 백업 기능(애플리케이션 파일, SD Card 파일, 연락처, 즐겨찾기 등)과 [그림 20]과 같이 파일 리스트 및 애플리



〔그림 19〕 MySecure 구동화면 및 백업화면



〔그림 20〕 MySecure File List View 및 App List View



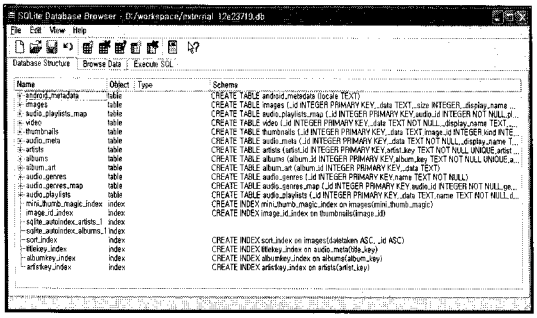
〔그림 21〕 MySecure 백업파일 위치

케이션 리스트 등을 Content Provider URI를 통해 SQlite 데이터베이스에 쿼리를 전송하고 그 결과로 사용정보를 받아오는 형식으로 구현되어 있다.

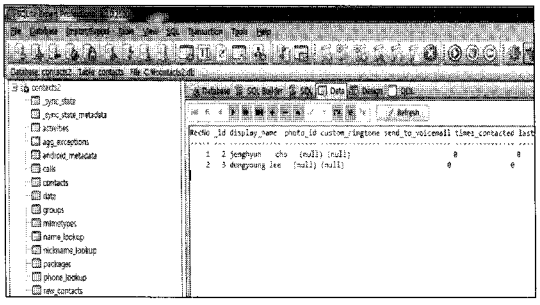
백업된 자료들은 [그림 21]과 같이 /data/data/com.marakana/files 디렉터리에 텍스트 형식으로 저장된다.

5.2.2 증거 분석

증거수집에서 데이터 추출 시 텍스트나 관리프로그램이 있는 경우 특별한 분석도구가 필요하지 않지만 SQlite DB 형태로 데이터가 추출되었을 경우 분석도구가 필요하게 된다. 분석은 [그림 22]와 [그림 23]과 같이 SQlite DB 관리 도구를 이용하여 수행할 수 있다.



〔그림 22〕 SQLite Database Browser를 이용한 DB 테이블 확인



〔그림 23〕 SQLite Expert Professional을 이용한 DB 데이터 확인

Ⅵ. 결 론

인터넷통신과 모바일통신 기술의 발달로 인하여 통신정보의 생활화와 일반화로 인한 사이버 범죄도 증가하고 있다. 모바일 IT응용기기에서 최근에 급속도로 활성화된 스마트폰을 이용한 범죄가 발생 할 때, 범죄에 대한 증거로서 디지털 데이터를 추출하고 분석하는 연구가 필요하다. 특히 스마트폰에서의 멀티미디어 서비스의 활용이 다양해지고, 스마트폰 사용자들의 해킹과 루팅을 통한 멀티미디어 콘텐츠를 불법으로 이용하고 있다. 또한 실생활과 연결된 범죄에 관련성이 있는 스마트폰의 자료는 법정의 책임을 묻는 근거로서 범죄수사와 증거의 활용에 필요한 기술인 모바일 포렌식을 연구할 필요가 있다.

스마트폰 또한 컴퓨터이기 때문에 모바일 웹, 웹하드 애플리케이션의 사전조사는 위에서 제시한 가상머신(Vmware, Eclipse등)을 이용하여 범죄열람표를 작성하고 데이터베이스에 대한 증거 수집·분석은 기존의 OSP 수사와 동일하게 한다.

그리고 스마트폰에 대응하기 위해 포렌식 기술을 확보하여야 하며, 스마트폰 압수 시에는 위에서 제시한 스마트폰 포렌식 증거 수집·분석 모델을 적용하여 법정 증거가 될 수 있도록 하여야하며, 스마트폰 사용자들에게 스마트폰 보안의식을 높이기 위한 교육 자료와 정책적인 연구가 필요하다.

참고문헌

[1] 이정훈, 박대우, "휴대폰과 스마트폰의 모바일 포렌식 추출방법 연구," 디지털산업정보학회논문지, 6(3), pp.79-89, 2010년 9월.

[2] 이성환, "스마트폰 보급에 따른 저작권 침해와 대응방안," 제4회 저작권 포럼, pp.37-40, 2010년 6월.

[3] 김동국, 장성용, 이원영, 김용호, 박창현, "모바일 포렌식의 무결성 보장을 위한 효과적인 통제방법," 정보보호학회논문지, 19(5), pp.151-166, 2009년 10월.

[4] 이규안, 박대우, 신용태, "포렌식자료의 무결성 확보를 위한 수사현장의 연계관리 방법 연구," 한국컴퓨터정보학회논문지, 11(6), pp.175-184, 2006년 12월.

[5] 신성원, "휴대폰 범죄의 실태 및 효율적 대응방안에 관한 연구," 한국콘텐츠학회논문지, 6(9), pp.75-84, 2006년 9월.

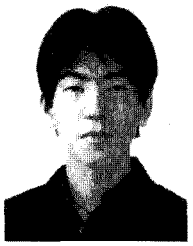
[6] 대검찰청, 2007년 검찰 올해의 사건 3, 과학수사사례.hwp, 2007.

[7] 김지선, "스마트폰 범죄 증거분석 고도화," 디지털타임스, http://www.dt.co.kr, 2010.11.29.

[8] 김기영, 강동호, "개방형 모바일 환경에서 스마트폰 보안기술," 정보보호학회논문지, 19(5), pp.21-28, 2009년 10월.
[9] 오병민, "포르노 재생기 위장 안드로이드 악성코드, 인터넷 유포!," 보안뉴스, http://www.boannews.com, 2010.09.10.
[10] 디지털뉴스팀, "스마트폰으로 여성 치마속 몰카 찍은 정수기 기사 입건," 동아닷컴, http://www.donga.com, 2011.09.23.
[11] http://www.paraben-forensics.com/
[12] http://www.oxygen-forensics.com/
[13] http://www.logicubeforensics.com/
[14] http://www.msab.com/
[15] A.D. Schmidit and S. Albayrak, "Malicious Software for Smartphones," Technical Report, DAI-Labor der Technischen University Berlin, pp.1-53, Feb 2008.
[16] H. Jahankhani and A. Azam, "Review of Forensic Tools for Smartphones," EC2ND 2006, Section II, pp.69-84, 2007.

〈著者紹介〉

이 정 훈 (Jeong-Hoon Lee)
정회원
2009년 2월 : 호서대학교 정보통신공학과 졸업
2011년 2월 : 호서대학교 벤처전문대학원 IT응용기술학과(정보통신보안전공) 석사
2011년 5월~ 현재 : 한국저작권위원회 디지털정보보호팀
<관심분야> 디지털포렌식, 정보보호, IT Convergence



천 우 성 (Woo-Sung Chun)
정회원
2006년 2월 : 숭실대학교 전산원 졸업
2006년 8월 : 한국교육개발원 멀티미디어학 전공
2009년 2월 : 호서대학교 벤처전문대학원 IT응용기술학과(정보보호전공) 석사
2010년 3월~현재 : 호서대학교 벤처전문대학원 IT응용기술학과 박사과정
<관심분야> 정보보호, 추적기법, Hacking, Forensic