情 報 保 護 學 會 誌
第 18 券 第 1 號, 2008. 2

# 국내 휴대폰 포렌식 기술 동향

성 진 원*, 김 권 엽*, 이 상 진*

요 약

디지털 기기의 기능이 발달하고, 디지털 기기의 보급이 활발해 지면서 PDA, 디지털 카메라, 휴대폰 등의 디지털 장비들이 생활필수품이 되었다. 특히 휴대폰은 국내의 약 86%에 달하는 사람들이 사용하고 있는 디지털 장비로 전화통화 뿐만 아니라 문자메시지, 사진기능, 동영상 기능 등과 같은 많은 기능을 제공한다. 이러한 휴대폰은 여러 기능을 제공함에 따라 사용자와 관련된 많은 정보를 담고 있어 사건 발생 시 분석되어야 할 중요한 물품 중에 하나가 되었다. 그러나 국내 휴대폰의 경우 제조사나 모델의 종류에 따라 휴대폰 메모리 사용방식이 달라 휴대폰 분석에 많은 어려움이 있다. 이에 본 논문에서는 휴대폰 포렌식 절차와 기술, 그리고 현재 국내에서 사용되고 있는 도구들에 대해 간략이 설명하고 이와 함께 국내 휴대폰 포렌식 분야에서의 문제점이 무엇인지 알아보고 대안을 제시하고자 한다.

## Ⅰ. 서 론

디지털 기술의 발전으로 인해 PDA, 카메라, GPS, 휴대폰 등 많은 디지털 장치들이 우리 생활의 많은 부분을 차지하게 되었다. 특히 국내에서 휴대폰을 사용하는 사람이 정보통신부 통계에 따르면 2007년 12월말 약 4천만 명에 이를 정도로 휴대폰은 거의 모든 사람들이 사용하고 있다고 해도 과언이 아니다[1].

이러한 휴대폰은 전화통화 뿐만 아니라 문자메시지, 사진촬영, 스케줄관리, 전화번호부관리, 동영상촬영 등 많은 기능을 포함하는 장치로 발전하여 사용자와 관련된 많은 정보를 담고 있다. 이에 따라 휴대폰은 사건 발생 시 사건과 관련된 직접적인 증거 또는 사건과 연관된 간접적인 증거들이 보관 되어 있을 가능성이 높아짐에 따라 분석되어야 할 중요한 압수 물품 중에 하나가 되었다.

| 구 분 | 2007.11월말 | 12월 가입현황 | | 2007.12월말 | 점유율 (12월말 기준) |
|---|---|---|---|---|---|
| | | 증 감 | 증감율 | | |
| 시내전화 | 23,113,075 | 17,178 | 0.1% | 23,130,253 | 34.5% |
| 이동전화 | 43,196,617 | 300,924 | 0.7% | 43,497,541 | 64.8% |
| 무선호출 | 39,554 | -226 | -0.6% | 39,328 | 0.1% |
| TRS | 334,569 | -1,822 | -0.5% | 332,747 | 0.5% |
| 무선데이타통신 | 97,769 | 2,585 | 2.6% | 100,354 | 0.1% |
| GM-PCS | 4,436 | -24 | -0.5% | 4,412 | 0.0% |
| 합 계 | 66,786,020 | 318,615 | 0.5% | 67,104,635 | 100.0% |

〔그림 1〕 유·무선통신서비스 가입자 (단위 : 명)

하지만 국내에서 사용되는 휴대폰을 분석할 수 있는 포렌식 도구가 거의 없고, 사용되고 있는 제품들은 상용 소프트웨어이여서 비싸다는 단점이 있다. 몇몇 외국에서 개발되어 사용되고 있는 휴대폰 포렌식 도구의 경우 대부분 GSM 방식의 휴대폰을 지원하기 때문에 국내에서 사용되는 CDMA 방식의 휴대폰에 적용하는데 한계가 있다. 또한 국내 휴대폰의 경우 플래쉬 메모리 사용방식이 제조사나 각 모델별마다 모두 다르기 때문에 CDMA방식의 휴대폰 분석을 지원하는 몇몇 도구들도 국내의 모든 휴대폰 분석을 하기에는 어려움이 있다[2].

## Ⅱ. 휴대폰 관련사건 및 휴대폰 중요데이터

### 2.1. 휴대폰 관련사건

사건 발생 시 휴대폰 분석을 통해 사건과 관련된 직접적인 증거 또는 간접적인 증거들을 획득할 수 있다.

본 연구는 과학재단 디지털 정보 획득 기반기술 연구(M10740030004-07N4003-00410)의 지원으로 수행되었습니다.

* 고려대학교 정보경영공학전문대학원 ({jinwonsung,kkyoup,sangjin}@korea.ac.kr)

이 장에서는 휴대폰 분석을 통해 해결된 사건 사례를 알아보고 이를 바탕으로 휴대폰에서 어떠한 정보들이 분석되어야 하는지 알아보고자 한다.

#### 2.1.1. 삭제된 핸드폰 문자 메시지를 복구하여 공범관계를 밝힌 사례

고소인은, 사실은 피고소인과 사기 범행의 공범관계임에도 불구하고 다른 피해자들로부터 고소를 당할 것이 우려되어 피고소인을 상대로 자신도 피해자라고 주장하며 고소를 하였으나, 고소인과 피고소인 사이의 삭제된 핸드폰 문자 메시지를 복구하여 공범관계를 밝힌 사례이다. 수사기관은 피고소인과 고소인 사이에 오고간 핸드폰 문자 메시지를 입수하기 위해 피고소인의 핸드폰을 압수하였으나 이미 문자 메시지는 삭제되어 있었다. 이에 수사기관은 압수한 핸드폰의 삭제된 문자 메시지를 복구하고, 이를 근거로 고소인에 대해 무고와 사기를 인지하여 공범인 피고소인과 병합 기소하였다[3].

#### 2.1.2. 보복폭행 사건

2007년 3월에 모그룹에서 일어난 보복폭행 사건을 수사 중 휴대폰 통화내역 분석결과 비서실장인 김 모씨와 감사인 김 모씨, 그리고 오 모씨간의 통화가 사건발생 직후부터 빈번하게 오갔으며 거액의 자금이 흘러간 단서가 포착됐다. 이에 따라 수사기관은 비서실장인 김 모씨와 폭력배를 동원한 것으로 알려진 감사 김 모씨가 사건발생 직후 통화를 집중적으로 하게 된 배경에 주목하고 조사한 사건이다.

#### 2.1.3. 사기대출 사건

2003년 사기대출 사건을 저지르고 잠적한 용의자 김 모씨를 추적하던 검찰은 그가 애인과 수시로 휴대폰으로 통화해온 사실을 포착, 애인의 휴대폰 통화내역과 발신자 위치추적을 통해 경기도 안산시로 포위망을 좁혔고, 잠복근무 끝에 용의자를 체포하는데 성공했다.

#### 2.1.4. 날치기 사건

2002년 12월 서울 강남의 한 은행 앞에서 현금 1000만원이 든 가방을 날치기한 2인조 오토바이 날치기 범들은 지난해 10월 또다시 같은 오토바이를 타고 날치기를 시도하던 중 경찰에게 덜미를 잡히고 말았다. 오리발을 내밀며 혐의를 부인하던 이들에게, 경찰은 몇 달 전 이들이 범행 장소를 물색할 당시 이를 수상히 여겨 카메라 휴대폰으로 찍어둔 사진들을 눈앞에 들이밀어 범죄 사실을 자백 받았다.

### 2.2. 휴대폰에서 획득할 수 있는 중요 데이터

앞서 알아본 휴대폰 관련 사건들과 같이 휴대폰은 사건에 있어 사건과 관련된 직접적인 증거 또는 사건의 실마리를 제공하는 간접적인 증거들을 포함하고 있어 사건 조사 시 휴대폰에서 사용자와 관련된 모든 데이터들이 분석되어야 한다. 휴대폰 데이터에서 획득할 수 있는 중요 정보들은 아래와 같다.

- 문자메시지(SMS)
- 보낸 문자메시지(Send SMS)
- 임시저장 문자메시지(Temporary SMS)
- 전화번호부(Phone Book)
- 통화목록(Call History)
- 메모(Memo)
- 스케줄(Schedules)
- 사진(Picture)
- 동영상, 녹음, 인터넷 사용정보 등

이러한 정보들은 사건에 있어 중요한 정보를 제공한다. 문자메시지의 사용이 일반화됨에 따라 문자메시지를 통한 정보 전송이 빈번해져 문자메시지에서 사건과 관련된 정보를 획득할 수 있다. 또한 전화번호부에서는 용의자와 관련된 주변 인물들의 연락처를 획득할 수 있고, 통화목록을 통해 용의자가 최근에 통화한 기록들을 획득할 수 있으며 메모와 스케줄을 통해서 용의자의 일정과 같은 정보를 확인할 수 있다.

또한, 휴대폰 사용자들은 휴대폰에 저장된 내용을 인위적으로 삭제하면 해당 정보를 복구할 수 없을 것이라고 생각하고 있는 경우가 많다. 그러나 실제로 삭제된 정보가 다른 데이터에 의해 덮어 쓰이지 않는다면 삭제된 데이터를 복구할 수 있는 가능성이 있다[4].

## Ⅲ. 휴대폰 증거 수집 절차

디지털 포렌식에서 일반적인 증거 수집 절차는 크게 "초기대응-증거수집-조사 및 분석-리포팅"으로 나눌 수 있다. 휴대폰도 디지털 기기에 속하므로 증거 수집에 있어 이 절차에서 크게 벗어나지는 않고 세부적인 단계에서 차이가 있다[5].

### 3.1. 증거 수집 준비(초기 대응)

증거 수집 준비 단계에서는 사건의 초기 대응 단계로 사건 현장을 보존하고 기록한 후 압수해야 할 휴대폰에 대해 확인을 하는 단계라고 할 수 있다. 초기 대응 단계에서는 현장에 있던 모든 상황을 기록하고 문서로 남겨두어 차후에 있을 재현에 대비해야 한다. 또한 이 때 압수 대상 휴대폰을 확인한다면 조사 및 분석에 있어서 어떤 포렌식 툴을 사용하여야 할지에 빠르게 대응할 수 있다.

### 3.2. 이송 및 증거 수집

증거 수집 단계에서는 휴대폰을 수거하는 과정을 말한다. 증거 수집 단계에서 수사관이 주의해야 할 점이 있다. 첫 번째로 확인해야 할 것은 휴대폰의 전원이다. 전원이 켜진 상태라면 전원을 차단하고 네트워크를 차단해야 한다. 휴대폰을 포렌식 랩으로 이송하는 도중 전화나 SMS의 수신으로 인해 휴대폰의 상태가 압수 당시의 상태와 달라질 수 있기 때문이다. 전원을 차단하기 전에 휴대폰을 열고 휴대폰 액정에 나타나는 정보를 기록해야 한다. 볼륨 버튼과 같은 무의미한 버튼을 눌러 액정을 켜진 상태로 유지하면서 휴대폰 액정에 나타난 시간이나 여러 다른 정보(액정에 나타난 이름 등)를 기록하도록 한다. 전원과 네트워크를 차단한 휴대폰은 증거 운반용 가방에 넣어 외부 충격이나 전자파로부터 안전하게 보호된 상태에서 포렌식 랩까지 이송되어야 한다.

포렌식 랩으로 이송된 휴대폰은 전원을 켠 상태에서 증거를 수집하는데 통합 데이터 수집 프로그램이 있다면 그 프로그램을 이용하고 그렇지 않으면 해당 휴대폰에 맞은 포렌식 툴을 사용하여 "주소록, SMS, 메모, 통화 목록, 스케줄" 등을 추출한다. 이 때 추출되는 데이터들은 정상 데이터는 물론 사용자에 의해 삭제된 데이터까지 포함하여야 할 것이다.

### 3.3. 조사 및 분석

조사 및 분석 단계는 과학적인 방법으로 디지털 증거를 면밀히 살펴 법정에 제출할 수 있는 상태로 만들어 주는 단계로 수집한 증거를 복사하는 것으로부터 시작된다[6]. 수집한 증거들을 토대로 사건과 직접적으로 관련이 있는 증거를 추출하게 되는데 예를 들어, 피해자가 살해당하기 전에 찍힌 사진을 용의자의 휴대폰에서 복구할 수 있었다거나 협박 문자를 복구할 수 있었다면 이것은 명백히 유죄를 판가름할 수 있는 증거가 될 수 있는 것이다. 조사 및 분석 단계에서는 눈에 보이는 증거이든 감춰져있는 증거이든 그 증거를 찾아내어 유·무죄를 증명할 수 있는 기반을 마련하는 단계이다. 조사 및 분석 단계에서 포렌식 전문가가 살펴보아야 할 휴대폰 내 정보는 앞서 설명한 휴대폰에서 획득할 수 있는 중요 정보와 같다.

### 3.4. 리포팅

리포팅 단계는 사건이 결론에 도달하고 각 단계 별로 결과를 낼 때마다의 기록을 모아 상세한 결과물을 도출하는 절차이다. 리포팅은 모든 행동과 관찰, 기록이 정확히 유지되어야 각 단계의 결과와 완벽히 일치해야 그 결과를 증거로 인정할 수 있게 된다. 간결하고 정확한 문장을 사용하여 읽는 사람으로 하여금 혼란을 야기시켜서는 안된다[6]. 리포트에 포함되어야 하는 정보는 아래와 같다.

- 케이스 번호
- 수사관 정보
- 리포팅 날짜(보고일)
- 조사 및 분석관의 신분과 사인(sign)
- 조사 및 분석에 있어서의 환경
- 사진, 인쇄물 등과 같은 첨부 증거

## Ⅳ. 휴대폰 포렌식 기술

휴대폰은 주파수 사용방식에 따라 크게 CDMA (Code Division Multiple Access) 방식과 GSM (Global System for Mobile Communications)방식으로 나뉜다.

GSM 방식은 유럽 표준으로 유럽 및 기타 지역에서 광범위하게 사용되고 있다. GSM 기반의 휴대폰은 전화번호부, SMS, 개인정보 등을 (U)SIM 카드에 저장한다. 따라서 GSM 휴대폰에 대한 포렌식에서 중요 기술은 SIM 카드에서 정보를 추출하는 것이다. CDMA는 한국, 일본, 동남아 일부, 미국 일부 등에서 사용되고 있는 방식으로 미국의 Qualcomm사에서 디자인한 기술로 무선링크에 대한 대역확산(spread spectrum) 기술 통신을 이용한다. CDMA 방식의 휴대폰은 SMS, 전화번호부, 개인정보 등을 플래쉬 메모리에 저장한다. 따라서 CDMA 휴대폰에 대한 포렌식에서 중요 기술은 플래쉬 메모리에 저장된 데이터를 추출하는 것이다[7].

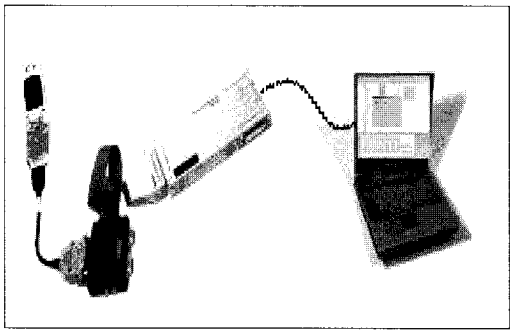
### 4.1. 휴대폰 데이터 추출 방법

휴대폰 포렌식 도구(tool)는 PC용 포렌식 도구와는 상황이 다르다. PC는 많은 일들을 수행할 수 있도록 설계된 범용적 시스템(General Purpose System)인 반면, 휴대폰은 특정 업무를 수행하기 위한 용도로 설계되었다. 휴대폰은 그 생명주기가 매우 짧기 때문에 휴대폰 포렌식 도구 제조업자들은 새로운 휴대폰을 지원하기 위해 지속적으로 그들의 도구를 업그레이드 해야 한다. 포렌식 도구를 사용하여 디바이스에서 데이터를 획득하는 방법은 다음과 같다.

- 물리적 방법 : 플래쉬 메모리에 bit단위로 접근하여 메모리에 대한 전체 이미지를 획득하는 방법(전체 물리 디스크)
- 논리적 방법 : 플래쉬 메모리에 저장되어 있는 데이터를 프로토콜을 이용하여 획득하는 방법(논리 디스크)

포렌식 도구가 저장장치에서 데이터를 추출하는 방법은 크게 물리적인 방법(Physical)과 논리적인 방법(Logical)으로 나뉜다.

물리적인 방법은 메모리와 같은 물리적 저장장치에서 bit-by-bit로 전체 데이터를 복사하는 것을 의미하며, 논리적인 방법은 논리적인 저장 공간에 저장되어 있는 파일이나 디렉토리 같은 데이터를 복사하는 것을 의미한다. 물리적인 방법의 장점은 지워진 파일이나 보이지 않는 데이터도 나타난다는 것이다. 그러나 논리적인 방법은 좀 더 이해하기에 적합한 구조를 제공하여 조사/분석 시 편리하다[8].



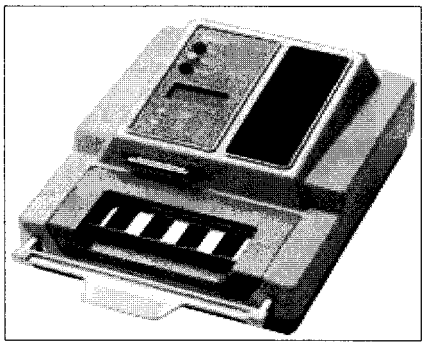
〔그림 2〕 JTAG을 이용한 데이터의 물리적 획득[8]

#### 4.1.1. 물리적 방법으로 데이터 추출

휴대폰에서 물리적인 방법으로 데이터를 추출하기 위해서는 [그림 2]와 같이 JTAG 에뮬레이터와 같은 장비를 이용한다[8].

즉, 휴대폰 PCB(Printed Circuit Board)에 숨겨져 있는 JTAG 핀을 찾아 JTAG 에뮬레이터와 연결하여 전체 물리 메모리를 bit 단위로 접근하여 모든 영역의 메모리 덤프를 한다. 따라서 플래쉬 메모리에 저장되어 있는 삭제된 데이터들도 복구가 가능하다. 그러나 제조사마다 JTAG 핀맵이 모두 달라 모든 휴대폰의 데이터를 획득하기에는 어려움이 따른다[8,12].

또한 플래쉬 메모리를 PCB로부터 물리적으로 분리하여 플래쉬 메모리 리더기를 이용하여 데이터를 획득하는 방법이 있다. [그림 3]은 플래쉬팩이라는 제품으로 플래쉬메모리 디바이스들을 프로그램할 수 있도록 설계



〔그림 3〕 플래쉬팩을 이용한 물리적 획득[10]

된 제품이다. 이러한 장비를 이용하여 플래쉬메모리의 전체 물리 데이터를 획득할 수 있다[10].

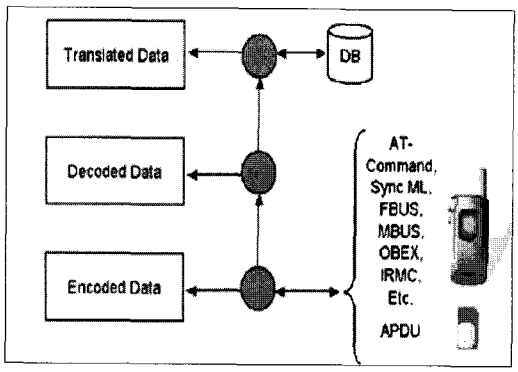
하지만 휴대폰 플래쉬 메모리를 물리적으로 분리를 해야 한다는 문제점과 포렌식 도구로써 제작된 제품이 아니고 플래쉬 메모리 디바이스들을 프로그램 하기 위해 제작된 제품이기 때문에 법정에서 무결성 문제가 대두될 수 있는 문제점이 있다.

#### 4.1.2. 논리적 방법으로 데이터 추출

휴대폰과 (U)SIM 카드에서 논리적인 방법으로 데이터를 추출하기 위한 대부분의 포렌식 도구들은 [그림 4]처럼 동기화하여 통신하고 디버깅하기 위하여 일반적인 디바이스 프로토콜을 사용한다[7].

휴대폰용 소프트웨어는 상용 포렌식 도구, 휴대폰 관리 도구, 오픈 소스 도구, 자체 개발 도구, 진단 도구, 해킹 도구가 있다. 휴대폰 포렌식 도구는 전형적으로 단말기 내부 메모리 그리고 GSM에서 쓰는 (U)SIM 카드와 같은 장치들에서 데이터를 수집한다. 휴대폰 포렌식 도구와 비 휴대폰 포렌식 도구는 종종 디바이스와 통신하기 위해 같은 프로토콜을 사용한다. 하지만 비 휴대폰 포렌식 도구는 누군가의 휴대폰을 최적화/강화하기 위해 정보의 양방향 흐름을 허용하는 반면 휴대폰 포렌식 도구는 특별히 휴대폰 내 내용을 변화시키지 않고 데이터를 수집하도록 설계되었다. 이것은 나중에 데이터의 무결성 검사를 위한 해쉬값을 계산하는데 의미를 부여한다[5].

NIST는 "Guidelines on Cell Phone Forensics"과 "Cell Phone Forensic Tools: An Overview and Analysis"에서 논리적 접근 방법을 이용하는 휴대폰포렌식 도구에 대한 분석 결과를 [표 1]과 같이 제공한다[7,8,11].




[그림 4] 휴대폰 포렌식 도구의 데이터 처리절차[7]

[표 1] 논리적 접근 방법을 이용한 휴대폰 포렌식 도구

| 도구 | 기능 | 분석 대상 장비 |
|---|---|---|
| Forensic Card Reader | 수집, 리포팅 | SIMs |
| ForesnsicSIM | 수집, 분석, 리포팅 | SIMs, USIMs |
| SIMCon | 수집, 분석, 리포팅 | SIMs, USIMs |
| SIMIS | 수집, 분석, 리포팅 | SIMs, USIMs |
| BitPIM | 수집, 분석, | 퀄컴 칩셋 사용 Certain CDMA phone |
| Oxygen PM (Forensic Ver) | 수집, 분석, 리포팅 | Nokia Phone |
| Oxygen PM for Symbian | 수집, 분석, 리포팅 | Symbian Phone |
| PDA Seiaure | 수집, 분석, 리포팅 | Palm OS, Windows Moblie |
| Polot-Link | 수집 | Palm OS |
| Secure View | 수집, 분석, 리포팅 | TDMA, CDMA, GSM 폰, SIMs |
| Cell Seizure | 수집, 분석, 리포팅 | TDMA, CDMA, GSM, SIMs, USIMs |
| GSM .XRY | 수집, 분석, 리포팅 | GSM, CDMA 폰 SIMs, USIMs |
| Phonebase | 수집, 분석, 리포팅 | GSM 폰, SIMs, USIMs |
| MobilEdit! | 수집, 분석, 리포팅 | GSM 폰, SIMs |
| TULP2G | 수집, 리포팅 | GSM 폰, SIMs |

하지만 이러한 도구들은 대부분 GSM 방식의 휴대폰 분석을 지원하고 국내에서 사용하는 CDMA 방식의 휴대폰 분석은 거의 지원이 되지 않는다. 몇몇 도구들이 CDMA 방식의 휴대폰 분석을 지원하지만 국내에서 사용되고 있는 다양한 모델들을 모두 분석하기에는 많은 어려움이 있다.

### 4.2. 국내 휴대폰 포렌식 도구 사용 현황

현재 국내에서 휴대폰 분석을 위해 사용하고 있는 도구로는 QPST, EasyCDMA, BitPim, Final Mobile Forensics, 등이 있다. QPST, EasyCDMA는 프로토콜을 이용하여 논리적 접근 방법으로 데이터를 획득하는 도구로, QPST는 퀄컴사에서 휴대폰 제조업체에 무료로 제공하는 휴대폰 개발 툴로 휴대폰 내장 메모리의 파일

시스템 뷰어, 휴대폰 데이터의 추출 및 삽입 기능, 휴대폰 비밀번호 알아내기, 그 외의 휴대폰 개발 및 테스트를 위한 기능이 있다. EasyCDMA는 Plinksoft사에서 만든 휴대폰을 PC에 연결하는 툴로 휴대폰 내장 메모리의 파일시스템 뷰어, 휴대폰 데이터의 추출 및 삽입 기능이 있다. Bitpim은 GNU 일반 공중 사용 허가서에 적용받는 Open Source 프로그램으로 휴대폰의 포렌식 분석을 위한 툴로 휴대폰 내장 메모리의 파일시스템 뷰어, 휴대폰 데이터의 추출 및 삽입기능, 휴대폰 포렌식 분석기능이 있다.

그러나 QPST, EasyCDMA, BitPim은 국내에서 사용되고 있는 모든 휴대폰에 적용하기에는 한계가 있다.

Final Mobile Forensics는 국내 업체인 Final Data사에서 개발한 제품으로 논리적 접근 방법으로 데이터를 획득하여 데이터 분석 및 리포트 기능까지 있는 휴대폰 포렌식 도구이다.

## V. 국내 휴대폰 포렌식 기술의 문제점

앞서 알아본 바와 같이 국내 휴대폰은 퀄컴사에서 개발한 CDMA방식을 사용한다. 이에 따라 휴대폰 데이터들이 플래쉬 메모리에 저장되는데 이에 따른 다양한 문제점들이 존재한다.

휴대폰 포렌식에 대한 연구는 영국과 미국을 중심으로 활발히 이뤄지고 있다. 영국은 GSM 방식을, 미국은 GSM 방식과 CDMA 방식을 모두 사용하고 있다.

영국은 휴대폰의 도난사건과 도난당한 휴대폰을 사용한 범죄가 급증하면서 경찰과 정부 그리고 이동통신 업체가 협조해 'Immobilise'라는 캠페인을 벌이기 시작했다. 또한, 'Central Equipment Identity Register (CEIR)'이라는 영국에서 도난 또는 분실 신고된 모든 휴대폰에 대한 데이터베이스 시스템을 구축했다. 다음으로 National Mobile Phone Crime Unit(NMPCU)은 산업체와 경찰 그리고 그 외 수사기관을 서로 연계해 활동하는 조직으로 휴대폰을 훔쳐서 다시 프로그래밍해 수출하는 조직이나 개인에 대한 정보를 수집해 National Intelligence Model(NIM)에 정의된 모든 레벨의 범죄를 지원한다.

미국은 주로 CDMA 방식을 사용하고 있다. 미국은 영국처럼 모바일 포렌식에 대해 많은 연구가 체계적으로 이뤄지지 않았으나 최근 몇 년 전부터 모바일 포렌식에 대한 중요성을 인식해, 미국상무부 기술관리국 산하의 미국 국립기술표준원인 NIST에서 모바일 포렌식에 대한 연구가 이뤄지고 있다. 2006년에는 'Guide lines on Cell phone Forensics'와 'Guide lines on PDA Forensics'를 발행해 모바일 포렌식의 가이드 라인을 제공했다[6,7].

국내는 퀄컴 칩을 사용하는 CDMA 방식의 휴대폰을 사용하고 있다. 국내는 휴대폰 제조업체마다 휴대폰 모델마다 표준화된 운영체제 및 메모리 사용방식이 없는 휴대폰의 특성상 CDMA 폰이 지원되는 외국산 모바일 포렌식 분석 툴도 사용할 수 없어 휴대폰을 분석하는데 휴대폰 제조업체에서 제공하는 소프트웨어만 의존하고 있는 실정이다.

휴대폰 포렌식의 문제는 휴대폰은 내장 메모리의 구조가 표준화되어 있지 않아서 휴대폰에 저장되는 데이터가 모델마다 메모리의 다른 위치에 저장되어 휴대폰의 내장 메모리에서 데이터를 추출하는 것이 어렵고, 모바일 포렌식 툴이 지원하는 휴대폰의 종류가 그리 다양하지 않으며, 휴대폰의 생명주기가 매우 짧다는 것이다.

### 5.1. 휴대폰 데이터 획득에서의 문제점

휴대폰에서 데이터를 획득하는 방법에는 논리적 접근 방법으로 획득과 물리적 접근 방법으로 획득이 존재한다는 것을 앞서 알아보았다.

먼저 논리적 접근 방법으로 데이터를 획득하는 방법은 프로토콜을 이용하여 데이터를 수집하는데 국내에서 사용되고 있는 모든 휴대폰들을 똑같은 프로토콜을 사용하여 데이터를 수집할 수 없다는 문제점이 있다. 각 제조사는 고유한 자체 하드웨어 특성이나 여러 다른 이유로, 독자적인 Know-How 에 따라 휴대폰 외부에서 내부 메모리에 접근하는 통신 Interface 기술을 개발하여 적용한다. 따라서 플래쉬 메모리 데이터에 대한 획득과 분석을 위해서는 각 제조사의 각 휴대폰 모델별로 별도의 Interface를 개발해야 한다는 어려움이 있다.

또한 논리적 접근 방법으로 데이터를 획득할 경우 플래쉬 메모리에 대한 전체 이미지를 획득하지 않고 저장되어 있는 데이터만을 획득하게 되어 삭제된 사진이나 동영상과 같은 정보들을 복구하지 못할 확률이 커지게 되고 증거 데이터에 대한 무결성 문제가 대두될 수 있다.

물리적 접근 방법으로 데이터를 획득하는 방법에서도 많은 문제점들이 있다. 먼저 JTAG을 이용하여 휴대

폰의 플래쉬 메모리에서 이미지를 획득하기 위해서는 플래쉬 메모리에서의 JTAG 핀맵을 알아야만 한다. 하지만 휴대폰 제조사의 모델별로 JTAG 핀맵을 알아내기에는 많은 어려움이 있다. 또한 플래쉬팩과 같은 장비를 이용하여 플래쉬 메모리에서 이미지를 획득하기 위해서는 데이터를 획득하고자 하는 플래쉬 메모리에 맞는 소켓이 있어야만 한다. 그리고 플래쉬 메모리를 휴대폰 PCB에서 물리적으로 분리 시켜야 하므로 증거 데이터가 손상될 수 있는 문제점이 존재한다.

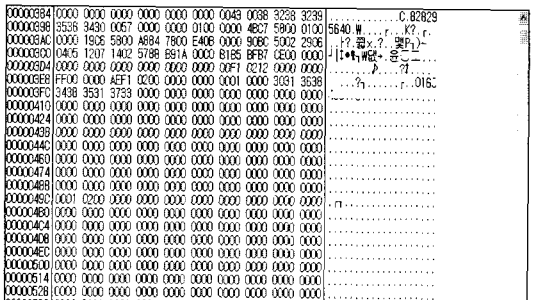
이외에도 물리적 접근 방법으로 데이터를 획득하는 도구들이 포렌식 도구로써 개발 된 장비들이 아니 여서 원본 데이터에 대한 무결성을 검증할 수 없다는 문제점도 존재한다.

### 5.2. 획득한 데이터 분석에서의 문제점

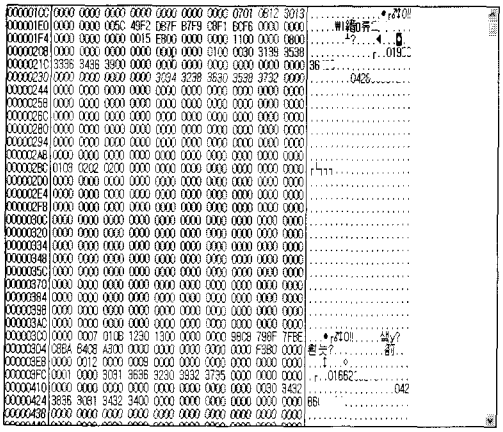
논리적 접근 방법 또는 물리적 접근 방법으로 데이터를 획득한 후 획득한 데이터를 분석할 때에도 많은 문제점이 존재한다.

논리적 접근 방법으로 획득한 데이터에서 문자, 전화번호부, 통화기록 등과 같은 정보를 알아내기 위해서는 제조사 모델 마다의 데이터 스트럭쳐를 분석해야 하는 문제점이 존재한다.

[그림 5]와 [그림 6]은 LG 전자의 SV420과 SV590 모델에서 논리적인 방법을 이용하여 전화번호부 정보를 획득한 것이다. 같은 제조사임에도 불구하고 저장되어 있는 데이터 포맷이 다른 것을 확인할 수 있다[13].



〔그림 5〕 논리적 방식으로 획득한 LG-sv590의 전화번호부



〔그림 6〕 논리적 방식으로 획득한 LG-sv420의 전화번호부

물리적 접근 방법으로 획득한 데이터는 플래쉬 메모리의 처음부터 마지막까지의 데이터이다. 이 데이터를 분석하기 위해서는 플래쉬 메모리에서 사용한 파일시스템을 알아야 한다. 현재 플래쉬 메모리에서 사용하는 파일시스템으로는 EFS, EFS2, TFS 등이 있는데 이러한 파일시스템에 대한 정보는 공개 되어 있지 않아 파일시스템을 분석하는데 어려움이 따른다. 또한 각 제조사마다 파일시스템을 각 제조사의 Know-How에 따라 변형하여 사용하고 있어 파일시스템 또한 휴대폰 모델마다 분석되어야 한다.

그리고 논리적 접근 방법으로 획득한 데이터 분석과 마찬가지로 물리적 접근 방법으로 획득한 이미지에서 파일시스템 분석을 통하여 데이터를 획득한 후 문자, 전화번호부, 통화기록 등과 같은 의미 있는 정보를 알아내기 위해서는 각각의 제조사 모델마다의 데이터 스트럭쳐를 분석해야만 한다.

## Ⅵ. 결 론

국내 휴대폰 포렌식 분야는 그 중요성이 커짐에도 불구하고 아직까지 증거 수집/분석 기술의 발전이 미흡한 현실이다. 그이유중에 하나로 국내에서 사용하고 있는 휴대폰은 제조사 마다 CDMA기반의 플래쉬 메모리 사용 방식이 모두 틀려 휴대폰 내에서의 데이터 획득이 어렵고 획득한 데이터를 분석하는 데에도 많은 어려움이 있다. 또한 기술 발달로 인해 새로운 휴대폰이 빠르게 출시되어, 새롭게 개발된 휴대폰을 분석하여 휴대폰 분석 도구에 빠르게 적용해야 하는 어려움도 존재한다.

따라서 국내 휴대폰 환경에 적합한 휴대폰 포렌식 도

구를 개발하기 위해서 수사기관 및 국가 연구기관들이 휴대폰 포렌식 연구에 많은 노력을 기울어야 하며 더불어 휴대폰 포렌식 기술을 연구하는 학교 또는 기업들과 함께 휴대폰 포렌식에 대한 연구를 활발히 진행해야 할 것이다.

## 참고문헌


[1] 정보통신부 통신전파방송정책본부, "유무선통계(2007.12월.xls)", Jan 2008.

[2] 경찰청 사이버테러대응센터, (사)한국디지털포렌식학회, "제2회 디지털 포렌식 세미나 발표자료", 발표자료, 2007

[3] 대검찰청, 2007년 검찰 올해의 사건 3, "과학수사 사례.hwp", Jan 2008.

[4] Wayne Jansen and Rick Ayers, "Guidelines on Cell Phone Forensics", NIST, Draft Special Publication 800-101, 2006..

[5] 백은주, 성진원, 이상진, "휴대폰 증거 수집 방안", 제1회 안티포렌식 대응기술워크샵, 7-11, 2007.

[6] Wayne Jansen and Rick Ayers, "Guidelines on Cell Phone Forensics", NIST, Aug 2006.

[7] Wayne Jansen and Rick Ayers, "Guidelines on Cell Phone Forensics", NIST, Draft Special Publication 800-101, 2006..

[8] 김건우, "휴패폰 플래쉬 메모리 데이터 수집",제1회 안티포렌식워크샵, 2007

[9] Wayne Jansen and Rick Ayers, "Guidelines on Cell Phone Forensics", NIST, Aug 2006.

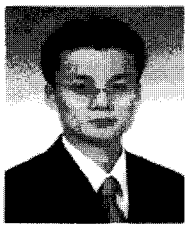
[10] (주)디텍프론티어, http://www.di-tek.co.kr/

[11] "Cell Phone Forensic Tools: An Overview and Analysis", NIST, 2005.

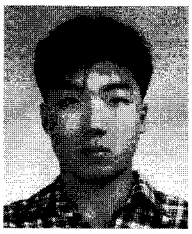
[12] M. Breeuwsma, "Forensic imaging of embedded systems using JTAG (boundary-scan)", Digital Investigation, vol. 3, ed. 1, March 2006.

[13] LG 싸이언, http://www.cyon.co.kr.

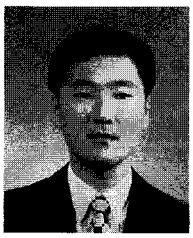

## 〈著者紹介〉

**성 진 원 (Sung Jinwon)**
**학생회원**
2006년 2월 : 세종사이버대학교 정보보호시스템 학사
2006년 3월~현재 : 고려대학교 정보경영공학전문대학원 석사과정
관심분야 : 모바일 포렌식, 컴퓨터 포렌식, 역공학



**김 권 엽 (Kim Kwonyoup)**
**학생회원**
2003년 2월 : 강남대학교 전자계산학과 학사
2007년 2월 : 고려대학교 정보보호대학원 석사
2007년 3월~현재 : 고려대학교 정보경영공학전문대학원 박사과정
관심분야 : 컴퓨터 포렌식, 모바일 포렌식, 소프트웨어/하드웨어 역공학



**이 상 진 (Lee Sangjin)**
**정회원**
1987년 2월 : 고려대학교 수학과 학사
1989년 2월 : 고려대학교 수학과 석사
1994년 2월 : 고려대학교 수학과 박사
1999년 2월~2001년 8월 : 고려대학교 자연과학대학 조교수
2001년 2월~현재 : 고려대학교 정보경영공학전문대학원 정교수
관심분야 : 포렌식 어카운팅, 컴퓨터 포렌식, 암호 이론, 스테가노그래피