

# 압수 수색된 안드로이드와 윈도우모바일 스마트폰의 포렌식 증거 자료

윤경배\* · 천우성\*\* · 박대우\*\*\*

Forensic Evidence of Search and Seized Android and Windows Mobile Smart Phone

Kyung-Bae Yoon\* · Woo-Sung Chun\*\* · Dea-Woo Park\*\*\*

본 논문은 2012년도 김포대학교의 연구비 지원에 의거하여 연구되었습니다.

## 요 약

휴대폰에서 포렌식 증거 자료를 추출하는 방법은 SYN, JTAG, Revolving 3가지 방법이 있다. 하지만 휴대폰과 스마트폰의 기술과 사용방법의 차이로 인하여, 포렌식 증거 자료를 추출하는 방법도 달라야 한다. 따라서 본 논문에서는 압수 수색된 스마트폰에서의 포렌식 증거 자료의 추출 방법을 연구하고자 한다. 압수 수색된 스마트폰에서 많이 사용되는 구글 안드로이드와 윈도우모바일 스마트폰의 분석을 위하여 스마트폰의 사양과 운영체제, 백업 분석, 증거 자료를 분석 한다. 또한 구글 안드로이드와 윈도우모바일 스마트폰의 전화번호부, SMS, 사진, 동영상에 관한 포렌식 증거 자료를 추출하여 법적인 증거자료와 포렌식 보고서를 생성한다. 본 논문에서 실험된 스마트폰 포렌식 기술 연구는 모바일 포렌식 기술 발전에 기여할 것이다.

## ABSTRACT

There are three ways how to extract forensic evidence from mobile phone, such as SYN, JTAG, Revolving. However, it should be a different way to extract forensic evidence due to the differences of their usage and technology between them(mobile phone and smart phone). Therefore, in this paper, I will come up with extraction method that forensics evidence by search and seizure of a smart phone. This study aims to analyze specifications and O.S., backup analysis, evidence in smart to analyze for search and seizure of a smart phone commonly used google android and windows mobile smart phone. This study also aim to extract forensics evidence related to google android and phone book, SMS, photos, video of window mobile smart phone to make legal evidence and forensics report. It is expected that this study on smart phone forensics technology will contribute to developing mobile forensics technology.

## 키워드

모바일 포렌식, 증거, 스마트폰, 윈도우 모바일, 안드로이드

## Key word

Mobile Forensic, Evidence, Smart Phone, Windows Mobile, Android

\* 정회원 : 김포대학교 경영정보과(주저자)  
\*\* 정회원 : 호서대학교 벤처전문대학원(공동저자)  
\*\*\* 종신회원 : 호서대학교 벤처전문대학원(교신저자, prof\_pdw@naver.com)

접수일자 : 2012. 12. 31  
심사완료일자 : 2013. 01. 17

## I. 서 론

2010년 이후의 정보기술(IT)과 정보통신의 주요 이슈 중 하나는 스마트폰이다. 이동 중에도 정보 검색과 정보 전송이 가능한 스마트폰은 기존 휴대폰 시장을 대체하고 있다. 삼성전자와 LG전자 등 국내 기업을 비롯해 애플, 노키아, 소니, HP까지 스마트폰을 통해 세계에서 경쟁하고 있다.

세계 3G(세대) 이동통신 표준 정착과 기술 발전은 음성통신 및 데이터통신을 모두 빠른 속도로 할 수 있게 해주었다. PDA폰도 기본적으로 스마트폰이 할 수 있는 기능을 모두 제공했지만, 3G에서 빨라진 데이터통신은 외부에서 인터넷 웹서핑과 이메일 확인을 더 유용하게 해주고 있다.

IDC(International Data Corporation)의 보고서에 의하면, 2012년 3분기에는 1.8억대의 스마트폰이 판매되었다. 판매된 스마트폰의 75.1%가 안드로이드를 탑재하고 있다. iOS는 14.85% 점유율이며, 블랙베리의 점유율은 4.25%로 전년 동기(9.5%)에 비해 빠르게 감소하고 있으며, MS계열은 아직 시장의 판도를 뒤집기에는 미비하다[1].

또한 2012년부터 4G로 이동통신 서비스가 전개되면서 LTE(Long Term Evolution) 기술과 함께, 5기가 주파수 대역의 초고속 Wi-Fi 기술을 사용한 이동통신 서비스가 확대되고 있다.

스마트폰 시장이 확산됨에 따라, 스마트폰에 대한 범죄관련 위협도 확산되고 있다. 특히, 개방형 운영체제인 구글 안드로이드는 운영체제의 취약점을 통해 우회 공격하는 행위가 발생할 가능성이 높다. 그리고 윈도우 모바일의 경우에도 PC Windows의 취약점들을 그대로 가지고 스마트폰으로 옮겨지면서, 기존의 Windows가 가지고 있는 취약점을 그대로 가지게 되었다[2].

본 논문에서는 스마트폰에서 취약점을 이용하거나, 스마트폰에서의 해킹 공격이나 범죄에 사용되었을 때, 압수 수색한 스마트폰에 대한 모바일 포렌식(Mobile Forensic) 증거 자료를 생성하는 연구를 한다.

휴대폰에서 포렌식 증거 자료를 추출하는 방법은 상태에 따라서 SYN, JTAG, Revolving 3가지 방법이 있다. 하지만 휴대폰과 스마트폰의 제조 기술과 운영체제, 애플리케이션의 사용방법의 차이로 인하여 포렌식 증거 자료를 추출하는 방법도 달라야 한다.

본 논문에서는 안드로이드와 윈도우모바일이 탑재되어 있는 스마트폰을 분석하고, 전화번호부, SMS, 사진, 동영상에 대한 모바일 포렌식 증거 자료를 추출하여, 법적인 증거 자료로서 사용하는 연구를 한다.

본 논문의 구성은 I 장 서론에서는 논문의 필요성과 II 장 관련연구에서는 윈도우모바일, 구글 안드로이드, 모바일 포렌식에 대해 연구하고, III 장 압수 수색된 안드로이드와 윈도우 스마트폰의 증거 자료 분석에서는 범죄 사례와 연관된 Wi-Fi 존에서의 무료 인터넷과 취약성 분석을 하고, 윈도우모바일 증거 자료의 백업, 구글 안드로이드 증거 자료의 백업, 스마트폰 동기화 백업 연구, IV 장 윈도우모바일과 구글 안드로이드 스마트폰의 전화번호부, SMS, 사진, 동영상에 대한 포렌식 증거 자료를 생성하고, 삭제된 증거자료의 복구를 하고, 원본성과 무결성을 검증한 스마트폰 포렌식 보고서 작성을 하고, V 장 결론과 향후 연구를 한다.

## II. 관련연구

### 2.1. 구글 안드로이드

구글에서 개발한 리눅스 운영체제 기반의 개방형 휴대폰용 플랫폼으로 OHA(Open Handset Alliance)를 구성하여 구글 서비스에 최적화된 스마트폰이다. UI, Application Layer 개발을 구글이 주도하고, 그 밖의 Kernel 개발은 GPL 진영의 소스를 이용하여 개발하였다. 단말기를 위한 소프트웨어 스택으로 운영체제, 미들웨어, 주요 애플리케이션으로 구성되고 애플리케이션은 Java VM으로 실행되고, 가상 머신은 리눅스 커널 위에서 돌아가는 Dalvik(재사용과 교체가 가능한 App framework으로 모바일 디바이스에 최적화된 Dalvic virtual machine)을 사용하였고 오픈소스의 Webkit 엔진 기반의 통합된 브라우저와 2D 그래픽 및 OpenGL ES 1.0 스펙 기반의 3D를 지원하는 최적화된 그래픽 지원한다[3].

그림 1은 안드로이드 플랫폼의 구조이다.

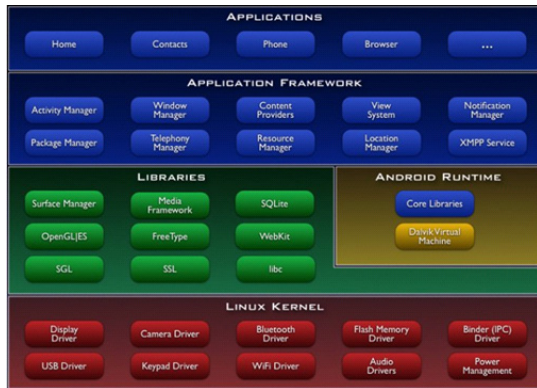


그림 1. 안드로이드 플랫폼의 구조  
Fig. 1 The structure of the Android platform

## 2.2. 윈도우모바일

Windows CE 위에 .NET Compact Version을 올린 것으로 비주얼 스튜디오 통합개발환경과 연동하여 개발이 용이하며 Native Head File 및 다양한 Library File 제공하고 커널, 미들웨어, AEE, Application Suite 사이에 완벽한 소프트웨어 스택 지원한다[4].

PDA 및 스마트폰에 사용하는 운영체제로 포켓 PC라고 불렸다. 이 운영체제는 마이크로소프트사에서 내놓은 모바일 운영체제로 임베디드 운영 체제인 Windows CE 위에 .NET Compact Version을 올린 것으로 비주얼 스튜디오 통합개발환경과 연동하여 개발이 용이하며, 모바일 환경에 적합한 새로운 터치식 사용자 인터페이스를 추가하여 개발하였다. Windows CE의 기본적인 기능에 휴대폰 기능이 추가되어 있고 Native Head File 및 다양한 Library File 제공하고 커널, 미들웨어, AEE (Application Execution Engine), Application Suite 사이에 완벽한 소프트웨어 스택을 지원한다[5].

## 2.3. 모바일 포렌식

모바일 포렌식이란 이동통신 장비 등 모바일 기기가 범죄에 관련되었을 때, 범죄 사실의 증거 자료로서 모바일 포렌식을 적용한다.

모바일 포렌식은 기존의 휴대폰 포렌식과 새로운 스마트폰 포렌식, 그리고 이동기기에 대한 자동차 포렌식, 기차 포렌식, 선박 포렌식, 비행기 포렌식 등으로 구분할 수 있다[6].

하지만 기존의 포렌식 현장의 경험과 포렌식 실무에

적용하기 위한 임의의 분류는 1) 휴대폰(Mobile Phone)의 전화번호부, 음성 및 SMS 기록 증거 자료, 2) PDA(Personal Digital Assistant)의 증거 자료, 3) Digital Voice Record의 증거 자료, 4) 디지털카메라와 휴대폰의 사진 및 동영상 증거 자료, 5) 차량, 선박, 기차, 비행기 등 이동기기들의 전자기록 증거 자료, 6) 이동저장장치에 부가된 전자증거 자료를 등을 말한다.

모바일 포렌식의 특징은 디지털 장비 중에서 이동성을 부여한 것이고, 대표적인 것으로는 휴대폰, PDA, 디지털 녹음기, 디지털 카메라와 이동기기 등에 임베디드 시스템이 활용되는 분야라고 할 수 있다.

특히 휴대폰은 전 세계적으로 가장 많이 사용하는 모바일 장비이고, 무선 네트워크가 구성되어 있으므로, 모바일 포렌식에서 압수수색 등 절차 상 가장 유의하여야 하는 분야이다[7].

## 2.4. 스마트폰 포렌식 기술

스마트폰 포렌식에서 증거 자료를 추출하는 방법에는 SYN, JTAG, Revolving 3가지 방법이 있다.

전원동작이 정상적으로 이루어지고 현장에서 긴급하게 데이터의 존재 유무와 삭제되지 않은 데이터를 추출하는 방법인 SYN 통신 방식을 이용한 분석 방법, 전원의 불량, 데이터가 삭제되거나 데이터의 정밀 분석을 위한 JTAG 통신 방식을 이용한 분석 방법과 스마트폰이나 휴대폰이 완전히 고장 나거나 임의로 훼손하였으나 디지털 증거의 추출이 매우 중요한 사안일 때 메모리를 분리하여 데이터를 추출하는 Revolving 통신 방식을 이용한 분석방법이 있다.

그러나 스마트폰의 전화기의 기능이 있어서 하드웨어적으로 이상이 있는 경우는 특수한 경우에 해당한다.

기존 휴대폰과 달리 스마트폰은 운영체제와 구조, 사용방식과 기술의 차이로 인한 포렌식 연구 방법도 달라야 한다.

## III. 압수 수색된 안드로이드와 Windows 스마트폰의 분석 및 증거 자료 백업

안드로이드 운영체제와 윈도우모바일 운영체제가 탑재된 스마트폰이 불법 범죄와 관련된 사례와 취약성을 분석하고, 압수 수색된 스마트폰의 증거 자료 백업에

대한 연구를 한다.

### 3.1. 스마트폰의 범죄 관련 사례

지디넷코리아에 2012년 3월 21일에 보도에 따르면, 카카오톡을 통해 피싱을 당했다는 피해 사례가 접수돼 경찰이 수사에 나섰다고 한다. 피해자 장모씨는 친구로부터 카카오톡 메시지를 받고 600만원을 송금했지만 몇 시간 뒤 확인해보니 대화명과 사진이 바뀌어 있어 경찰에 신고를 했다. 이미 범인은 현금을 인출해 달아난 뒤였다.

그동안 다른 사람의 메신저 아이디를 도용해 지인들에게 금전을 요구하던 사례는 많았지만 스마트폰의 카카오톡을 통한 피해 사례가 경찰에 접수된 것은 이례적이다.

또한, 2012년 3월 7일에 한 트위터러안은 “지인이 스마트폰을 분실했는데 카카오톡 피싱으로 가족에게 송금을 요구해 200만원을 사기 당했다”며 이용자들의 주의를 당부했다. 3월 9일에도 인터넷 커뮤니티 등을 통해 카카오톡 친구로 위장해 급전이 필요하다는 송금을 요구한 사건이 알려졌다. 이 이용자는 150만원을 송금했다가 은행에서 보이스피싱 계좌를 의심해 지급을 중지시키면서 피해를 막았다[8].

### 3.2. Wi-Fi 존에서의 인터넷과 취약성 분석

스마트폰의 Wi-Fi 기능을 사용하면, 통신사마다 무료로 제공해주는 Wi-Fi 존에서 무료로 데이터 서비스를 이용할 수 있다.

Wi-Fi 존은 특성상 무선으로 서비스가 이루어지기 때문에 이를 악용해 가짜 무선랜을 만들어 해킹 공격을 시도할 수 있다.

Wi-Fi 신호 중에 해킹을 위한 바이럴 SSIA(무선인터넷 식별번호) 형태의 애드혹(Ad-hoc) 네트워크를 설정하고 무선 해킹을 할 수 있다. 확장 안테나가 부착된 노트북을 Wi-Fi 존의 이름으로 위장한 네트워크 피싱 AP 모드로 전환 후, 강제 연결 해제를 주기적으로 하면, 사용자가 스마트폰으로 웹 페이지 인증을 시도할 때, 웹 피싱 페이지에서 개인정보를 입력받을 수 있다.

무선 네트워크(IEEE 802.11) 자체 연결 과정에서 결합 및 인증 절차 취약점과 사회공학학을 이용한 Wi-Fi 피싱 공격으로 사용자 ID와 패스워드, 그리고 신용카드 정보 등 다양한 개인 정보를 취합하고, 악성코드의 전파가

가능하다.

### 3.3. 압수 수색된 스마트폰 조사

#### ■ 갤럭시 S 제품사양

- 모델명 : SHW-M110S
- CPU : S5PC111 1GHz
- 메모리 : 512MB RAM, 16GB Storage
- 운영체제 : Android Platform ver 2.3 (Gingerbread)
- 통신규격 : WCDMA HSPDA 7.2Mbps, HSUPA 5.76Mbps

#### ■ 옴니아 제품사양

- 모델명 : SCH-M490
- CPU : Marvell Monahans PXA312 806MHzLV
- 메모리 : Internal 160MB
- 운영체제 : Microsoft Windows Mobile 6.1
- 통신규격 : DMA HSDPA

#### ■ Desktop 제품사양

- CPU : Inter(R)Core(TM)2Quad Q9400 @ 2.66GHz
- 메모리 : 3.0GB RAM
- 운영체제 : Windows 7 Home Premium K SP 1 32bit

### 3.4. 구글 안드로이드 스마트폰의 증거 백업

안드로이드 운영체제를 탑재한 갤럭시 S는 삼성전자에서 제공하는 프로그램인 Kies 프로그램은 멀티미디어가 강화된 소프트웨어로 콘텐츠 매니저, 콘텐츠 스토어, 아웃룩 동기화 등 다양한 기능을 지원한다.

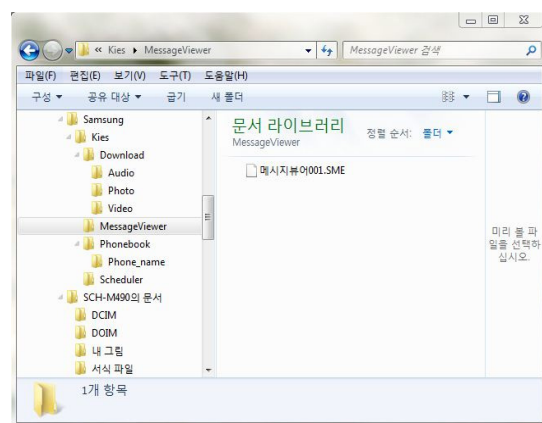


그림 2. 갤럭시 S 백업 파일  
Fig. 2 Galaxy S backup file

별도의 USB 인식 유틸리티를 받을 필요 없이 Kies 프로그램만 설치하면 PC에서 스마트폰의 증거 자료를 백업 할 수 있다. 그림 2는 Kies 프로그램을 사용하여 갤럭시 S에서 SMS 증거자료를 백업받아 PC의 폴더에서 저장된 파일을 확인한 것이다.

백업된 증거 자료를 살펴보면, SMS의 경우 .SME 파일로 압축되어 저장이 되고, 전화번호부인 폰북에 경우에는 .SPB 파일로 압축되어 저장 되고, 일정의 경우 .SSC로 압축되어 저장이 되어 진다. 그리고 멀티미디어 증거 자료들은 원형 그대로 저장되는 것을 볼 수 있다.

### 3.4. 윈도우모바일 스마트폰의 증거 백업

윈도우모바일 운영체제가 탑재된 옴니아 스마트폰의 경우, 운영체제가 윈도우모바일 6.1이어서 Windows XP에서는 ActiveSync 4.5, Windows VISTA나 Windows 7의 경우에는 윈도우모바일 Device Center로 스마트폰과 USB로 연결을 하면 인식을 하고 프로그램이 작동을 한다.

업체에서 제공하는 USB 통합 드라이버를 설치하고 삼성모바일에서 제공하는 MITs Store Installer에 PC 유틸리티에 있는 MITs Wizard 3.0을 PC에 설치하여 스마트폰과 동기화 하여 이메일, 전화번호부나 문자 등의 증거 자료를 PC에 백업 받을 수 있다.

그림 3에서와 같이, 옴니아 스마트폰에서 백업받은 SMS를 PC에서 파일로 저장된 것을 확인 할 수 있다.

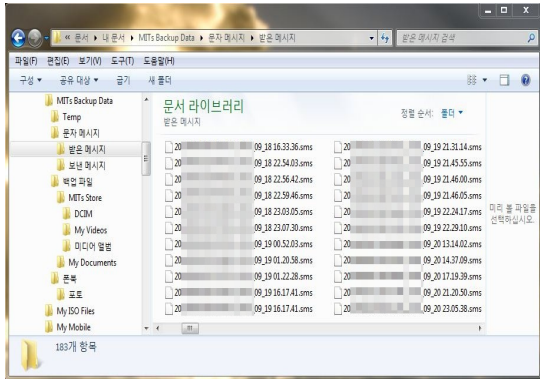


그림 3. 옴니아 백업 파일  
Fig. 3 Omnia backup file

### 3.5. 스마트폰의 PC와 동기화 백업

스마트폰의 경우, PC와 동기화하여 스마트폰의 내용을 PC로 전송하고 스마트폰의 데이터와 PC의 데이터가 똑같이 만드는 동기화를 한다.

이 동기화 과정은 스마트폰이 켜져 있고 PC와 스마트폰을 연결하였을 때 이루어지는 것으로, 동기화의 특성을 사용하여 백업을 하게 된다. 동기화로 백업을 정확하게 하기 위해서는 설정이 필요한데, 그 설정에 따라 스마트폰 위주의 백업을 할 것인지, PC위주의 백업을 할 것인지 결정을 하고 백업을 하게 된다. 백업 과정에서는 스마트폰이 켜져 있어야하고, 스마트폰의 증거 자료가 그대로 PC로 전달되기 때문에 동기화 과정 중에 스마트폰이나 PC중 한군데에서도 틀린 부분이 나오게 되면 오류 메시지가 뜨게 되어 동기화 분석을 할 수 없다.

### 3.6. 스마트폰 증거 백업 자료 분석

스마트폰과 PC와의 동기화를 통해 스마트폰에서 증거자료를 백업받은 PC에 저장된 자료에 대한 분석을 표 1과 같이 하였다.

표 1. 스마트폰 증거 백업 자료 분석  
Table. 1 Evidence backup data analysis of smart  
phone

|           | 안드로이드                        | 분석가능<br>프로그램                           | 윈도우<br>모바일 | 분석가능<br>프로그램                           |
|-----------|------------------------------|--|------------|--|
| 전화<br>번호부 | .spb                         | kies                                   | .vcf       | MITs                                   |
| 문자<br>메시지 | .sme                         | kies                                   | .sms       | MITs,<br>메모장                           |
| 일정        | .ssc                         | kies                                   | .csv       | MITs, Excel                            |
| 멀티<br>미디어 | .mp3, .avi 등<br>(원본파일<br>형식) | windows<br>media player,<br>곰플레이어<br>등 | .skm       | windows<br>media player.<br>곰플레이어<br>등 |

PC의 저장된 증거 파일을 다른 PC에서 확인이 가능  
한지 확인한 결과, 옴니아의 백업 파일에 경우에는  
MITs 프로그램과 PC의 윈도우 계열 프로그램인 메모  
장이나 Excel 등에서 확인이 가능하였고, 갤럭시 S의  
백업 파일에 경우에는 Kies 프로그램을 통해 확인이 가  
능하였다.



#### IV. 안드로이드와 윈도우모바일 스마트폰의 포렌식 증거 자료 추출 및 보고서 작성

안드로이드 운영체제인 갤럭시 S와 윈도우모바일 운영체제인 옴니아에서 포렌식 증거 자료를 추출하였는데, 스마트폰과 PC와 동기화를 통해 PC로의 백업을 하는 자체가 포렌식 증거 자료를 추출하는 방법이 된다.

그림 4와 같이 스마트폰을 PC와 동기화 하는 과정에서 법적 증거 자료로 인정되기 위해 과정을 사진자료로 날짜가 나오도록 하고 백업된 증거 자료의 무결성을 입증하기위해 이미징 작업을 해야 한다.



그림 4. 스마트폰 포렌식 증거 자료 추출  
Fig. 4 Smart Phone forensic data extraction

##### 4.1. 구글 안드로이드 스마트폰의 포렌식 증거 자료 추출

갤럭시 S를 PC와 연결하여 Kies 프로그램을 사용하여 백업하는 과정에서 볼 수 있듯이 갤럭시 S가 활성화되어 있어, 그림 5와 같이 Kies 프로그램과 동기화를 하면서 스마트폰의 증거 자료와 PC에 백업 증거 자료가 같은 것을 증명하여 포렌식 증거 자료를 추출한다.

갤럭시 S의 경우, SMS나 전화번호부인 폰북에 정보는 압축된 파일로 백업이 되어 Kies 프로그램이 아닌 다른 프로그램으로는 파일의 내용을 확인 할 수가 없다.

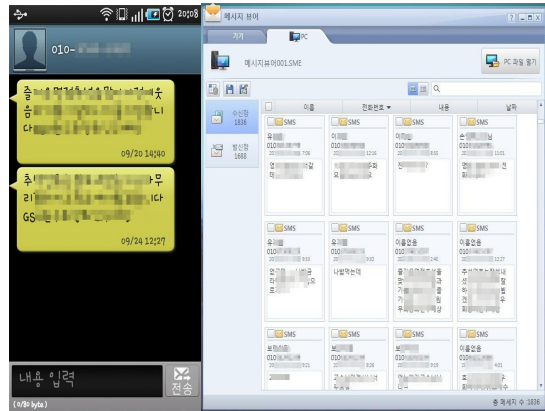


그림 5. 갤럭시 S 포렌식 증거 자료 추출  
Fig. 5 Galaxy S forensic data extraction

##### 4.2. 윈도우모바일 스마트폰의 포렌식 증거 자료 추출

옴니아 스마트폰도 포렌식 증거 자료 추출과정을 거치게 되는데, 그림 6에서와 같이 동기화되어 스마트폰과 PC와의 백업되어 저장되는 데이터와 같은 내용의 증거 자료가 추출된 것을 볼 수 있다.

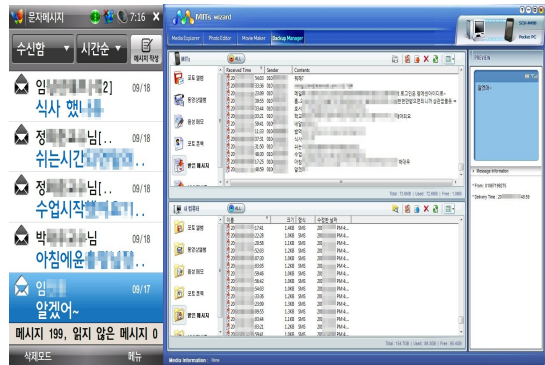


그림 6. 옴니아 포렌식 증거 자료 추출  
Fig. 6 Omnia forensic data extraction

옴니아 스마트폰에서는 .EDB파일로 SMS의 내용이 저장되는데 MITs Wizard 3.0을 사용하여 동기화하여 백업을 하게 되면 .SMS라는 확장자로 PC에 저장되어진다.

이 파일을 메모장으로 열어보면, 그림 7과 같은 압수 수색된 스마트폰의 증거 자료가 그대로 나오는 것을 볼 수 있다.

```
[SMS_INFO]
<MSG_ID>[REDACTED] </MSG_ID>
<bReadFlag>1</bReadFlag>
<bTempFlag>0</bTempFlag>
<nPriority>0</nPriority>
<szPhoneNumber>010[REDACTED] </szPhoneNumber>
<MSG_SENDER>010[REDACTED] </MSG_SENDER>
<MSG_RECEIVER>010[REDACTED] </MSG_RECEIVER>
<szData>알겠어~</szData>
<MSG_TITLE>알겠어~</MSG_TITLE>
<MSG_BODY>알겠어~</MSG_BODY>
<MSG_TIME_SEND>30103226,2215903104</MSG_TIME_SEND>
<MSG_TIME_RECEIVE>30103226,2215903104</MSG_TIME_RECEIVE>
<nTID>130</nTID>
<nSmsType>0</nSmsType>
<ITEM_COUNT>14</ITEM_COUNT>
[/SMS_INFO]
```

그림 7. SMS 포렌식 증거 소스  
Fig. 7 SMS forensic data source

#### 4.3. 스마트폰 포렌식 증거 자료 추출

갤럭시 S 스마트폰과 옴니아 스마트폰에서 포렌식 증거 자료를 추출할 때, 각 단말기 업체에서 제공해주는 백업 프로그램을 사용하여 포렌식 증거 자료를 추출하였다. 이 증거 자료들은 동기화라는 개념에서 현재 있는 증거 자료를 포렌식 증거 자료화한 것이다.

하지만 압수 수색된 스마트폰에서 삭제된 데이터에 대한 포렌식 자료를 추출하기 위해서는 그림 8과 같이 포렌식 툴을 사용하여 삭제된 그림이나 동영상, 문서 파일들을 복원하여 포렌식 증거 자료로 사용할 수 있다.

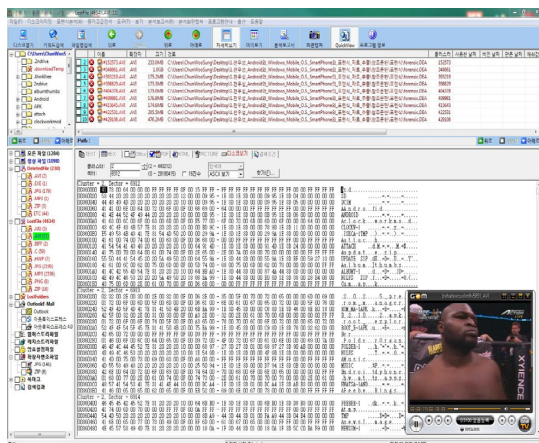


그림 8. 삭제된 포렌식 증거 자료 복구  
Fig. 8 Deleted forensic data recovery

스마트폰의 백업 프로그램을 사용하지 않고 USB로 연결시켰을 때는, 이동디스크 장치로만 스마트폰을 인식하게 하고, 메모리로 인식하여, 저장되어있는 증거 자료와 삭제된 증거 자료를 확인한다.

삭제된 증거 자료에 대한 포렌식 자료를 추출하기 위한 포렌식 툴 중에서 DEAS(Digital Evidence Analysis System)를 이용한다. DEAS 포렌식 툴은 스마트폰의 데이터 중 삭제된 데이터나 유실된 데이터를 복원하여 포렌식 자료로 생성해 주는 포렌식 툴이다. 또한, 스마트폰의 데이터와 포렌식 자료의 원본성과 무결성을 입증하기 위해 Hash 함수값을 적용하여 포렌식 자료를 생성해 주는 포렌식 툴이다.

SYN 방식의 분석 방법을 통해 자료를 추출하는 과정은 스마트폰을 메모리로 인식하여 자료를 추출하므로 데이터의 손상이 없고 메모리 영역에서 데이터를 추출하기 때문에 지워진 파일의 메모리 영역을 분석하여 복원할 수 있는 장점이 있다.

그러나 스마트폰의 메모리는 플래시 메모리이기 때문에 압수 수색 과정 중에 전파의 영향을 받아 데이터의 손상을 줄 수 있고 스마트폰의 전원을 키거나 끄거나 애플리케이션을 실행 하는 등 스마트폰을 사용하게 되면 데이터가 변형되거나 기존의 자료에 덮어쓰기 등의 단점이 있다. 그래서 압수 수색할 때에는 필히 전파차단 봉투를 사용하여야 한다.

#### 4.4. 스마트폰의 모바일 포렌식 보고서 작성

스마트폰에서 포렌식 증거 자료를 확인하였을 경우, 증거를 수집하여 포렌식 보고서 형태로 작성한 다음, 수사에 착수하여 증거기록으로 사용한다.

스마트폰에서 포렌식 증거 자료는 법정에서 인정하는 수사관이 인증된 포렌식 툴과 포렌식 기술과 공공의 장소나, 현장에서, 포렌식 증거 자료를 생성하고, 백업 프로그램을 통해 추출할 수 있는 증거 자료의 원본성과 무결성을 입증하기 위해 Hash 함수 값을 비교하여, 무결성을 입증한 자료를 보고서에 같이 제출한다.

확인 결과를 포렌식 분석 보고서에 맞춰 그림 9와 같이 작성한다.

<명세서의 제 5호>
스마트폰 포렌식

## 스마트폰 포렌식 결과보고서

● 조사 일시 : 2012. 12. 12
● 부서 : 포렌식 조사과
● 조사관 : 윤경배 (국인)

1. 조사정보

| 연수일과         | 지문번호      | 광진번호         | 분석일시                     | 분석장소                       |
|--------------|-----------|--------------|--------------------------|----------------------------|
| 2012. 12. 12 | 2012지문12호 | 2012광진12-34호 | 2012.12.01. ~ 2012.12.12 | X.XX 디지털포렌식수사과<br>XXX호 분석실 |

2. 조사대상 정보

| 제조사 | 모델명       | 운영체제        | 일련번호       | 저장용량 | 기타   |
|-----|-----------|-------------|------------|------|------|
| 삼성  | SHW-M110B | Android 2.3 | R95Z923121 | 16G  | 루틴 X |

3. 조사대상 자료 추출 방식 및 데이터 상태

|           |  |
|-----------|--|
| 데이터 추출 방식 | <input checked="" type="checkbox"/> SYN 방식 <input type="checkbox"/> JTAG 방식 <input type="checkbox"/> Revolving 방식                        |
| 데이터 상태    | <input type="checkbox"/> 정상 <input checked="" type="checkbox"/> 부분(일부) 삭제 <input type="checkbox"/> 초기화 <input type="checkbox"/> Micro SD |

4. 조사대상 포렌식 도구

|          |  |
|----------|--|
| 포렌식 도구   | <input checked="" type="checkbox"/> Oxygen / <input type="checkbox"/> XRY / <input type="checkbox"/> UFED / <input checked="" type="checkbox"/> Encase / <input type="checkbox"/> FTK Imager |
| 기타 분석 도구 | Samsung Mobile Kies v.1.0, Digital Evidence Analysis System 2  |
| 해커수단 분석  | 송수신의 스마트폰용 특화형은 송수신에게 필요정보를 획득하였다. 이후 스마트폰의 연립을 차단하였고, 스마트폰 포렌식 도구인 Oxygen Forensic Suite Encase를 이용하여 미정격악업을 수행하였다. DEAS 2 프로그램 등을 이용하여 삭제된 데이터를 복원하였다.                                     |

5. 원본상 일괄 확인

|           |                                  |
|-----------|----------------------------------|
| 원본 Hash 값 | a04443349a692e221de00dba3a12612e |
| 사본 Hash 값 | a04443349a692e221de00dba3a12612e |

그림 9. 포렌식 분석 보고서  
Fig. 9 The forensic analysis report

포렌식 보고서는 법정에서 증거 자료로 사용하기 위한, 포렌식 분석 보고서를 프린트하여, 포렌식 문서로 작성하여 제출한다.

## V. 결 론

스마트폰의 장점인 휴대성과 편리성이 해킹 공격과 범죄에 활용되면서 스마트폰에서의 범죄 증거 자료 추출을 위한 스마트폰 포렌식 연구가 필요하다.

스마트폰의 포렌식 증거 자료를 추출하기 위해 압수  
수색된 구글 안드로이드의 갤럭시 S와 원도우모바일의  
옵니아를 백업프로그램을 사용하여 스마트폰의 증거  
자료를 백업받아 전화번호부, SMS, 사진, 동영상의 포렌  
식 증거 자료 추출하는 연구를 하였다. 또한 삭제된 증거  
자료의 경우에는 포렌식 툴을 사용하여 데이터를 복구  
하고 Hash값을 적용하여 무경성과 원본성을 입증하고  
포렌식 보고서를 작성하였다.

본 연구를 통하여 실험된 기술 연구는 모바일 스마트 폰 포렌식 기술 발전에 기여할 것이다.

향후 연구로는 초기화 되어진 아이폰에 대한 삭제된 증거 자료의 복원에 대한 증거 자료 추출 연구가 되어져야 한다.

## 참고문헌

- [1] International Data Corporation, "Worldwide Smart Phone OS Market Share, 2012Q3," [idc.com](http://www.idc.com), 2012.
- [2] Jin-whan Kim, Hyuk-gyo Cho, Chang-Ji n, Seo, Eui-young Cha, "Mobile Implementation of Enhanced Dynamic Signature Verification for the Smart-phone," KIICE, v.11, no.9, pp.1781-1785, 2007.
- [3] S. P. Oh, I. H. Choi, "A Study on Comparison and Analysis for Smart Phone's OS and feature," IEEEK, v.33, no.1, pp. 2002-2007, 2010.
- [4] Kim dong-min, Lee chil-woo, "Technology Trends of Smartphone User Interface," KIISE, v.28, no.5, pp.15-26, 2010.
- [5] Eun Young Choi, Mi joo Kim, and Hyun Cheol Jung, "A study for enhancing smartphone security," KSII, pp.781-785, 2010.
- [6] Dea-Woo Park, "Smartphone Copyright and Forensic Application Method," 2010's Illegal Copies Enforcement Related Agencies joint Workshops, Korea Copyright Commission, 2010. 5.
- [7] Gyu-an Lee, Dea-Woo Park, Cheong-Sim Go, "Digital Forensics for Forensic Science," GSInterVision, 2011. 2.
- [8] Chung Hyun Jung, Kim Hee Yeon, "Kaka o Talk, Phishing Safety Zone? "Not Phishing," ZDnet korea, [http://www.zdnet.co.kr/news/news\\_view.asp?article\\_id=20120322114832](http://www.zdnet.co.kr/news/news_view.asp?article_id=20120322114832), 2012. 3.



## 저자소개



**윤경배(Kyung-Bae Yoon)**

1994: 인하대학교 정보공학  
(공학석사)

1998: 서강대학교 정보기술경제학  
(경제학석사)

2003: 인하대학교 컴퓨터공학 (공학박사)

1986 ~ 1987: 대우자동차(주) MIS

1988 ~ 1991: LG-EDS(주)기술연구소

1992 ~ 1997: 동부정보기술(주)연구소

1998 ~ 현재 김포대학교 경영정보과 부교수

※ 관심분야: 웹공학, 데이터마이닝, 정보보호 및 보안,

CRM, 지문 및 음성 인식, ERP, 생산정보화



**천우성(Woo-Sung Chun)**

2006년 숭실대학교  
전산원 졸업

2006년 한국교육개발원  
멀티미디어학 전공(공학사)

2009년 호서대학교 벤처전문대학원 IT응용기술학과  
(공학석사(정보보호전공))

2010년 호서대학교 벤처전문대학원 IT응용기술학과  
(박사과정)

※ 관심분야: 정보보호, 네트워크 보안, WiBro 보안,  
추적기법, 포렌식



**박대우(Dea-Woo Park)**

1998년 숭실대학교  
컴퓨터학과(공학석사)

2004년 숭실대학교  
컴퓨터학과(공학박사)

2006년 정보보호진흥원(KISA) 선임연구원

2007년~현재 호서대학교 벤처전문대학원 부교수

※ 관심분야: Hacking, Forensic, e-Discovery, CERT/CC,

VoIP 보안, 이동통신 및 WiBro 보안, 국가 사이버  
보안, 금융 네트워크 및 보안 및 시스템,

IT-Convergence, 정보보호 등