# 동기화 스마트폰 백업 데이터 포렌식 분석 기술

이재현* · 박대우*

*호서대학교 벤처전문대학원

# Forensic Analysis Technology of Smart phone backup data via synchronization

Jae-Hyun Lee* · Dea-Woo Park*

*Hoseo Graduate School of Venture

E-mail : leejh9708@paran.com · prof1@paran.com

## 요 약

스마트폰에서 동기화 기능은 디폴트(default)값으로 설정되어 있다. 동기화가 설정된 스마트폰은 스마트폰 전용 케이블을 이용해 PC에 연결되면 자동적으로 스마트폰 데이터가 백업되어 저장된다. 이 백업 데이터는 일반적인 기술로는 내용을 분석하기가 어려워서 포렌식 기술을 적용하여야 범죄 용의자의 정보를 알아낼 수 있다. 따라서 본 논문에서는 동기화 스마트폰의 백업 데이터에 대한 포렌식 분석을 통한 포렌식 증거자료에 대한 연구를 한다. 실험실 환경에서 스마트폰에 개인 금융정보를 보내고, 스마트폰을 훼손하였다고 가정하에 실험을 한다. 스마트폰의 백업 데이터를 포렌식 툴을 사용하여 개인 금융정보 및 범죄 연관 데이터를 분석하고, 포렌식 기술을 적용하여 법정 증거자료로 채택되도록 연구한다. 본 논문을 통해 스마트폰 포렌식 분석에 대한 기초자료로 활용 할 수 있을 것이다.

## ABSTRACT

The synchronization feature on the smartphone by default (default) value is set. Smartphone synchronization has been set is stored that smartphone data is automatically backed up is stored When connected to a PC with a smartphone dedicated cable. The backup data is a common technique to analyze the content to be difficult to apply forensic techniques can find out information on criminal suspects. In this paper, the backup data is synchronized to the smartphone through forensic analysis is the study of forensic evidence. In a lab environment to send personal financial information on smartphone, smartphone is assumed that the experiment is compromised. Smartphone's backup data by using the forensic tools in crime associated with personal financial information and analyze data. And, to be adopted by the court will study the evidence leveraging forensic technology. Through this paper as a basis for smartphone forensic analysis will be utilized.

키워드

Smart Phone Forensic, Smart Phone Back Up Data, Forensic Evidence, Forensic Analysis

## Ⅰ. 서 론

모바일 이동통신 기술이 발전됨에 따라 스마트폰의 비중이 그림 1과 같이 증가하고 있고, 스마트폰 범죄 및 범죄 기술에 지능적으로 사용되는 문제점도 발생하고 있다.

범죄현장에서 용의자가 압수 수색을 실시하기 전에 휴대용 스마트폰을 고의로 파괴하거나, 데이터를 삭제하여 훼손하는 경우가 많아 범죄 증거 수집의 어려움이 있다. 따라서 모바일 이동매체관련 범죄의 대응 기술을 통한 모바일 포렌식의 증거 확보방안은 마련되어야 한다[1].

스마트폰에는 동기화 기능이 있다. 이 동기화 기능은 디폴트(default)값으로 설정되어 있는데 동기화가 설정된 스마트폰은 스마트폰 전용 케이블을 이용해 PC에 연결되면 자동적으로 데이터가 백업되어 저장된다. 이 백업 데이터에 포렌식을 적용하고 용의자의 정보를 알아낼 수 있다.

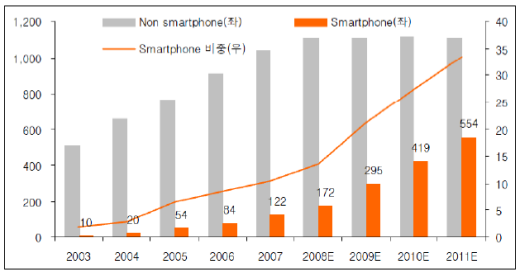


그림 1. 스마트폰의 비중 추이

하지만 스마트폰에서 일반적인 기술로 백업 데이터를 분석하여도, 분석 자료를 생성하기가 어렵다. 따라서 스마트폰 백업 데이터에 대한 포렌식 기술 연구가 필요하다.

본 논문에서는 스마트폰 포렌식 수사에서 용의자가 스마트폰의 데이터를 훼손했을 경우 PC의 백업 데이터를 확보한다. 확보된 백업 데이터에 포렌식 툴을 적용해 증거수집를 실시한다. 증거수집을 통해 포렌식 보고서를 작성하여 법정의 증거로 채택될 수 있도록 한다.

본 논문 연구는 최신 스마트폰 포렌식 증거수집 환경에서 새로운 기술적 모바일 포렌식 모델을 적용함으로서 스마트폰 포렌식 분석에 대한 기초자료로 활용 할 수 있을 것이다.

## Ⅱ. 관련연구

### 2.1 스마트폰 동기화

모바일 기기에서의 동기화는 개발회사에서 지원하는 S/W를 이용하여 모바일 기기의 데이터를 기기의 전용 케이블을 이용해 PC와 연결되면 데이터가 일치하도록 하는 작업을 말한다. 따라서 스마트폰을 사용하는 사용자가 기기를 PC와 연결시켰을 때 스마트폰에 저장된 데이터가 PC로 백업된다. 스마트폰을 이용한 범죄나 개인정보 등의 데이터도 PC와 연결하여 동기화가 진행되었다면 스마트폰을 압수하지 않고도 PC의 데이터를 이용해 포렌식을 적용시킬 수 있다[3].

### 2.2 스마트폰 포렌식 툴

기존의 데이터를 수집하는 모바일 포렌식 툴과 다르게 운영체제가 탑재되어 있는 스마트폰의 데이터를 수집하기 위해서는 스마트폰 전용 포렌식 툴을 사용해야 한다. 현재 국내에서 사용되고 있는 스마트폰 툴은 국산 제품인 EC 플랫폼의 MD Extractor를 제외하고 외국 제품인 UFED, Oxygen Forensic Suite, XRY 등이 스마트폰 포렌식이 가능한 대표적 소프트웨어이다. 이러한 포렌식 툴은 스마트폰에 저장되어 있는 데이터와 PC에 백업되어 있는 데이터의 분석도 가능하다. 따라서 이러한 포렌식 툴을 이용해서 스마트폰 범죄에 대한 포렌식을 적용할 수 있다[4].

### 2.3 스마트폰

스마트폰의 휴대폰에 컴퓨터 OS 기능을 추가한 지능형 휴대폰으로, 휴대폰 기능에 충실하면서 인터넷, 이메일, 메신저, 모바일뱅킹 등 사용에 편리한 인터페이스를 갖추고 있다. 또한 Wi-fi, 3G, WiBro의 무선인터넷 기능의 지원으로 다양한 기능의 제공한다[5][6].

## Ⅲ. 동기화 스마트폰 백업 데이터 수집 및 분석

### 3.1 동기화 스마트폰 백업 데이터 수집

동기화 스마트폰 백업파일은 그림 2와 같이 사용자 경로를 통해 확인할 수 있다.

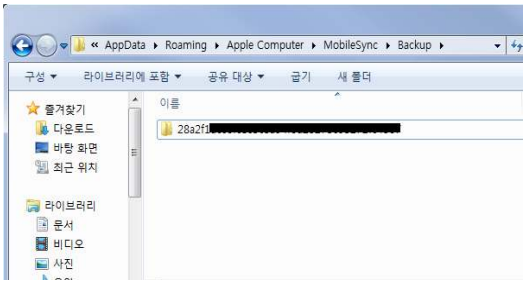


그림 2. 백업폴더

백업 파일은 각 동기화를 제공하는 소프트웨어마다 백업 경로와 데이터를 암호화 하는 경우도 있고 그렇지 않은 경우도 있다. 따라서 데이터를 수집하는 기기의 대한 기존적인 정보를 숙지하고 있어야 데이터를 신속하게 수집할 수 있다.

### 3.2 동기화 스마트폰 백업 데이터 분석

3.1에서 동기화를 통한 백업파일은 Meta data로 구성되어 있어 분석을 위해서는 파일 확장자 즉 Signature값을 확인해야 한다. 하지만 스마트폰 포렌식 툴을 적용시켜 백업 데이터의 내용을 확인할 수 있다. 그림 2는 백업폴더에 백업파일을 나타낸 것이다.

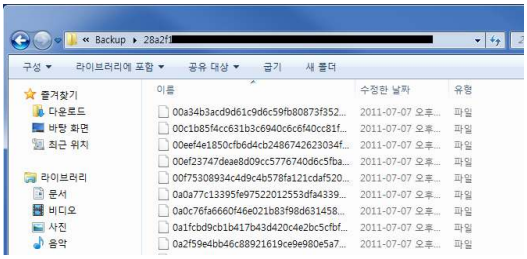


그림 3. 백업폴더의 파일

## Ⅳ. 동기화 스마트폰 백업 데이터 포렌식 분석

### 4.1 동기화 스마트폰 백업 데이터 포렌식

현재 디스크 포렌식 과정에서 확보한 하드디스크에서 동기화 스마트폰 백업데이터 포렌식을 적용함으로서 범죄에 대한 접근이 용이해질 수 있다. 하지만 스마트폰에서의 동기화는 사용자의 설정에 따라 달리지는 부분이기 때문에 제한적일 수 있다. 그러나 동기화 스마트폰을 통해 PC나 워크스테이션의 사용자의 스마트폰 기종과 연락처, 메시지, 녹음파일, 일정, 인터넷 사용기록, 통화기록 등을 조사할 수 있어 조사 대상자의 최근 현황에 대해서 파악할 수 있다. 또한 용의자가 알리바이를 만들어 스마트폰 조사에 방해하는 경우나 스마트폰 데이터를 삭제하고 훼손하는 경우 동기화 스마트폰 포렌식을 적용시킬 수 있다.

### 4.2 실험환경 및 포렌식 툴 적용

다음 스마트폰 포렌식 실험환경 및 포렌식 툴 적용은 다음과 같다.

■ 동기화 스마트폰 시스템
- iPhone 4G(v4.3)

■ 동기화 소프트에어
- itunes(v10.1)

■ 데이터 수집 및 분석 Forensic Tool
- Device Seizure

■ 실험내용
- 금융거래를 통해 민감한 정보의 메시지를 전송시켜 후 동기화 스마트폰의 백업 데이터 생성하여 스마트폰 포렌식 툴을 적용시켜 데이터를 수집한다. 수집한 데이터를 분석하여 금융거래내역을 확인한다.

그림 4와 같이 인터넷을 통해 금융거래 내역을 스마트폰에 전송시킨다.

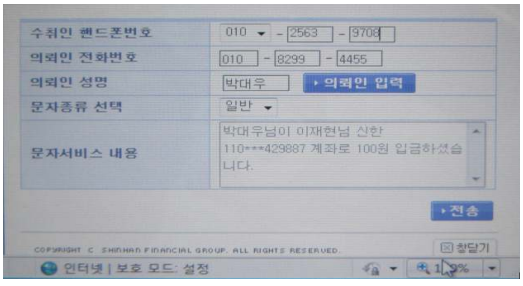


그림 4. 금융거래 내역 전송 프로그램

그림 5와 같이 금융거래 내역이 전송된 것을 확인한다.

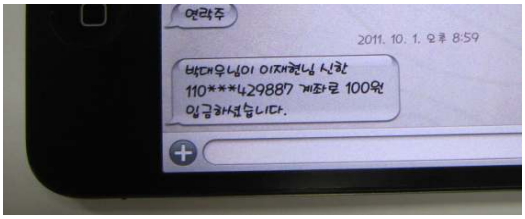


그림 5. 금융거래 내역 전송 확인

그림 6와 같이 동기화를 진행하여 백업 데이터가 생성되도록 한다.


그림 6. 동기화를 통한 백업 데이터 생성

그림 7과 같이 백업 데이터가 생성되었다.

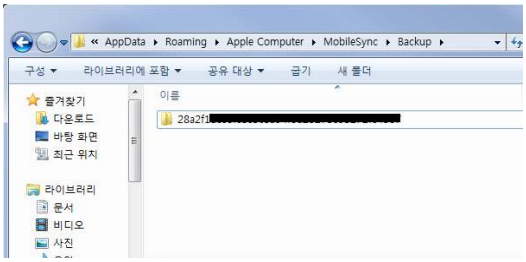


그림 7. 백업데이터 생성

그림 8과 동기화 스마트폰 백업 데이터를 분석하기 위해 스마트폰 포렌식 툴을 적용시켜 분석을 실시하였다.

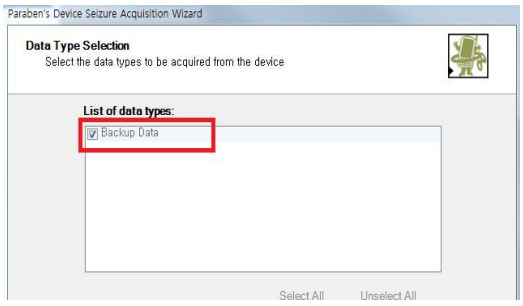


그림 8. 포렌식툴에서 백업파일 확인

### 4.3 동기화 스마트폰 백업 데이터 포렌식 분석

실험 결과 그림 9와 같이 전송한 금융거래 메시지 내용의 “박대우님이 이재현님 신한 110***4298877 계좌로 100원 입금하였습니다.” 개인정보가 백업 데이터를 통해 추출된 것을 확

인할 수 있다.

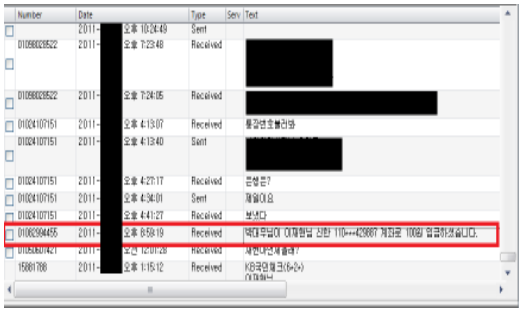

그림 9. 백업 데이터 포렌식 분석

## V. 결 론

스마트폰 사용자가 이메일, SNS 등을 이용하여 스마트폰에서 거래를 위반하거나 침해 사건이 발생하였지만, 스마트폰에서 증거를 발견하지 못하거나, 스마트폰이 훼손 되었을 때, 동기화된 스마트폰의 PC를 압수수색 한 후에 모바일 포렌식 기술을 적용할 수 있다.

본 논문은 동기화 스마트폰 거래에 대한 포렌식 적용 방안을 제시하고, 동기화 스마트폰 포렌식 절차를 제시 하였다. 본 논문을 통하여 IT 강국으로서 국가 경쟁력 향상과 첨단 범죄 수사를 통한 안전한 사회건설에 이바지 하고, 모바일 포렌식을 위한 과학수사의 기술을 한 단계 발전시키고자 한다.

향후 연구로는 스마트폰 파일포맷의 표준화 추출과 분석에 관한 기법을 지속적으로 연구하여 포렌식 자료 추출과 삭제된 자료의 분석 및 여러 기종의 스마트폰으로부터 포렌식 자료를 추출하고 분석 할 수 있도록 하여야 한다.

## 참고문헌

[1] 김동국, 장성용, 이원영, 김용호, 박창현, "모바일 포렌식의 무결성 보장을 위한 효과적인 통제방법", 정보보호학회, 2009.

[2] 이규안, 박대우, 신용태, "휴대폰 압수수색 표준절차와 포렌식 무결성 입증", 한국통신학회, 2008.

[3] 이광열, 최윤성, 최해랑, 김승주, 원동호, "현행 증거법에 적합한 디지털 포렌식 절차", 정보보호학회, 2008.

[4] 장성균, 조인휘, "모바일 포렌식의 디지털 증거 획득을 위한 표준 모듈 개발", 대한전자공학회, 2008.

[5] 김주영, 구본민, 이태림, 신상욱, "아이폰을 위한 디지털 증거 분석 도구 설계", 한국멀티미디어학회, 2010.

[6] 이정훈, 박대우, "Smart Phone 저작권 위반과 포렌식 적용 방안", 한국해양정보통신학회, 2010.