스마트폰 모바일 포렌식 증거 수집 분석을 위한 준비사항 및 절차 연구

이재현* · 박대우*

*호서대학교 벤처전문대학원

A study of the preparation And procedures by Smartphone Mobile Forensic evidence collection and analysis

Jae-Hyun Lee* · Dea-Woo Park*

*Hoseo Graduate School of Venture

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

요 약

스마트폰에 대한 소송이 이루어지고 있고, 최근, 법정에서의 스마트폰 증거데이터에 대한 증거자료 채택이 많아지고 있다. 따라서 불법적인 스마트폰 사용에 대한 증거데이터 추출을 위한 포렌식 절차와 증거물 수집에 대한 연구가 필요하다. 본 논문에서는 스마트폰의 증거데이터 주출에 대한 포렌식 절차를 제시하고, 스마트폰 포렌식 증거를 수집함으로써 디지털 증거의 무결성을 확보하고 사건을 진실을 발견하기 위한 방법에 대해 연구하였다. 본 연구를 통해 스마트폰 포렌식의 발전에 기여할 수 있을 것이다.

ABSTRACT

The lawsuit is being made on the smart phone. And recent is getting a lot of evidence for the smart phone data in a court of law. Thus, the evidence of illegal use smartphone for the extraction of data and evidence collection, forensic procedure is a need for research. In this paper, evidence of phone forensic procedure for the extraction of the data suggests. And, by collecting forensic evidence from smartphones ensure the integrity of digital evidence and how to solve the case investigated. With this study, smartphone forensic will be able to contribute to the development.

키워드

Smart Phone Forensic, Evidence, Forensic Preparation, Forensic Procedures

Ⅰ. 서 론

2011년 7월 방송통신위원회와 한국인터넷진흥원의 상반기 스마트폰이용실태조사 결과 발표의 따르면 스마트폰의 이용자가 20, 30대에서 전 연령층 및 전 계층으로 확대되고 있고, 스마트폰 이용자의 87.1%가 스마트폰을 통해 SNS(Social Network Service)를 이용한 경험이 있다고 밝혔다[1]. 이처럼 정보를 주고받는 전송형태가 무선으로 확장되면서 시간과 장소에 구애받지 않고 이메일, 금융 등 다양한 업무를 처리하는 편리함을 제공하고 있어 무선 이동전화의 가입자가 그림 2와 같이 증가하고 있다.

그러나 악의적 사용자의 의해서 저작권 위반, 불법거래 등 스마트폰을 이용한 범죄가 발생하고 있어 보안대책이 필요한 실정이다[2].

따라서 법죄의 책임 소재에 대한 법의 판단을 위해서 스마트폰 포렌식을 위한 체계적인 준비사항 및 증거수집 절차에 대한 연구가 필요하다.

본 논문에서는 스마트폰의 준비사항 및 증거수집 절차에 포렌식 기술을 적용하여 스마트폰 범죄에 대한 분석을 실시한다.

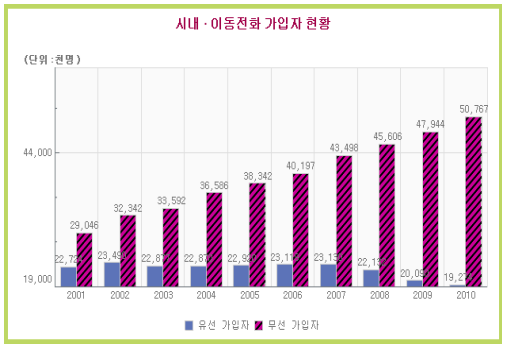


그림 1. 이동전화 가입자 현황

Ⅱ. 관련연구

2.1 스마트폰

스마트폰은 기존의 피처폰(Feature Phone) 기능에 운영체제를 포함하고 있는 형태로 WiFi, 3G, 4G를 이용해 다양한 어플리케이션을 설치 및 삭제 할 수 있기 때문에 금융거래, 이메일, SNS 등 PC에서 수행할 수 있는 다양한 기능을 제공한다. 따라서 이동성과 PC의 효율성이 결합되어 데이터의 송수신이 원활하고 정보의 접근이 가능하다.

2.2 모바일 포렌식

모바일 포렌식은 피처폰 스마트폰 외의 범죄와 관련있을 만한 이동형기기를 증거 데이터를 대상으로 하는 포렌식으로 PDA, 디지털 카메라, USB 메모리 카드 등 휴대가 편한 데이터 저장 기기들이 모바일 포렌식에 속하며 범죄나 수사에서 디지털 증거를 수집, 분석, 보존, 문서화하여 법정에 제출하는 일련의 행위를 나타낸다[3][4].

2.3 스마트폰 포렌식

스마트폰 포렌식은 스마트폰을 대상으로 하는 포렌식으로 피처폰에 저장되어 있는 연락처, 사진, 동영상, 통화기록 외의 이메일, 인터넷사용, SNS, 금융거래 등 다양한 서비스에 대한 데이터를 수집하여 법정에 제출하는 행위를 말한다. 스마트폰의 경우 소형저장장치의 효율성을 높이기 위하여 각 회사별로 별도의 메모리 저장 공간을 이용한다. 스마트폰에서 증거데이터 수집을 진행하기 전에 전원이 꺼져 있는 상태라면 스마트폰의 입회인에게 현재 상태를 확인한 후 전원을 켜고 무선 네트워크가 차단되도록 설정한 뒤 스마트폰 포렌식 S/W를 이용해 증거 데이터를 수집한다[5][6].

Ⅲ. 스마트폰 포렌식 증거 수집 준비사항

3.1 스마트폰 포렌식 증거 수집 계획 수립

스마트폰 데이터를 추출하기 위한 체계적인 포렌식 계획을 수립함으로써 조사관 및 수사관이 범죄에 대한 증거 수집을 신속하고 정확하게 할 수 있도록 해야 한다. 그림 2는 스마트폰 포렌식 계획 수립 절차이다.

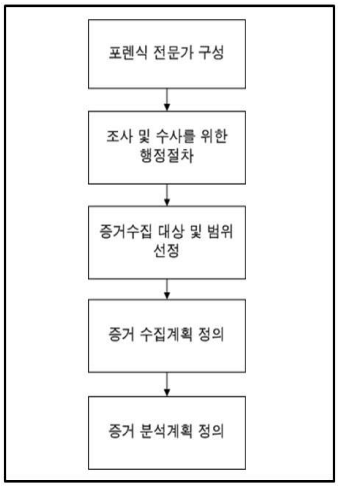


그림 2. 증거 수집 계획수립 절차

3.1.1 포렌식 전문가 구성

스마트폰 포렌식 전문가는 스마트폰의 운영체제 및 파일시스템, 데이터 저장 위치 등에 대해 알고 있어야 하며, 스마트폰 포렌식 툴을 원활하게 사용할 수 있고, 포렌식 분야의 전문지식을 갖춘 사람으로 구성되어야 한다.

3.1.2 조사 및 수사를 위한 행정절차

스마트폰 포렌식에 앞서 조사 및 수사에 필요한 행정서류 및 절차에 대해 숙지하고 법규를 준수하며 진행될 수 있도록 해야 한다.

3.1.3 증거수집 대상 및 범위 선정

범죄현장 방문 시 스마트폰의 증거수집이 신속하고 정확하게 수행될 수 있도록 증거수집의 대상과 범위를 선정하도록 한다.

3.1.4 증거 수집계획 정의

스마트폰 대상에 따라 증거를 수집하는 방법이 다르게 진행되는 점을 고려해 증거 수집계획을 정의한다. 즉 여기서 고려해야할 점은 스마트폰의 운영체제, 내장메모리의 유무 등이 포함되며 포렌식 툴을 이용해 증거수집 시 증거수집 대상 스마트폰을 지원하고 있는지 확인하는 것이 중요하다.

3.1.5 증거 분석계획 정의

증거 데이터의 분석을 위해 계획을 정의한다. 분석 시 사건과 관련하여 증거가 포함되어 있을 만한 파일 포맷의 우선순위를 선정하여 증거데이

터를 분석하도록 한다.

3.2 스마트폰 포렌식 S/W, H/W 툴 준비

스마트폰 데이터를 추출하기 위해 그림과 같이 스마트폰 포렌식 S/W, H/W를 준비한다. 그리고 증거 수집을 위한 H/W 구성품 중에 포함되지 않은 것은 없는지 확인하고 S/W는 정상적으로 설치되는지를 확인함으로써 증거 수집 시 착오가 발생하지 않도록 한다.

그림 3. 스마트폰 포렌식 S/W, H/W

3.3 스마트폰 포렌식 S/W, H/W 툴 적용

스마트폰 대상 기기의 따라 S/W, H/W 중 데이터를 추출 가능한 방식을 선택하여 신속하게 데이터를 추출하도록 한다.

그림 4. 스마트폰 포렌식 S/W 적용

그림 4는 스마트폰 포렌식 S/W를 적용하여 데이터를 추출하는 그림이다.

그림 5. 스마트폰 포렌식 H/W 적용

그림 5는 스마트폰 포렌식 H/W를 적용하여 데이터를 추출하는 그림이다.

Ⅳ. 스마트폰 포렌식 증거 수집 분석 절차

그림 6은 스마트폰 포렌식 증거 수집 분석 절차를 나타낸 그림이다.

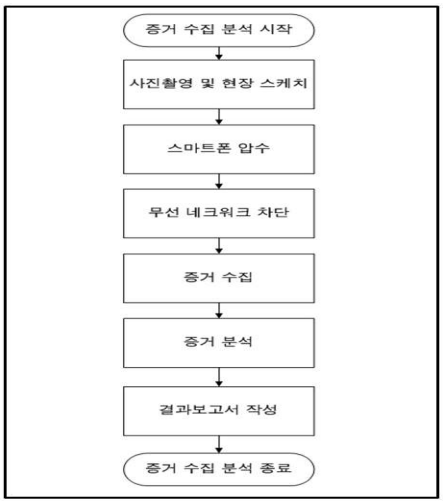


그림 6. 스마트폰 포렌식 증거 수집 분석 절차

4.1 사진촬영 및 현장 스케치

수사 시 현장의 당시 주변 상황을 촬영 및 스케치하고 사건과 관련된 증거자료에 대해서는 상세하게 기재하여 놓는다. 따라서 의뢰받은 증거분석 담당자가 현장 촬영내용 및 상세정보를 확인하고 분석에 도움이 될 수 있도록 한다.

4.2 스마트폰 압수

스마트폰을 압수하기 위해 동의서에 입회인의 서명과 받도록 하고 압수한 스마트폰의 이상이나 특이사항이 없는지 즉각 확인하도록 한다. 또한 잠금이 설정되어 있는 경우 입회자에게 비밀번호 등을 알아내서 증거수집 및 분석 진행에 어려움이 없도록 한다.

4.3 스마트폰 전파 차단

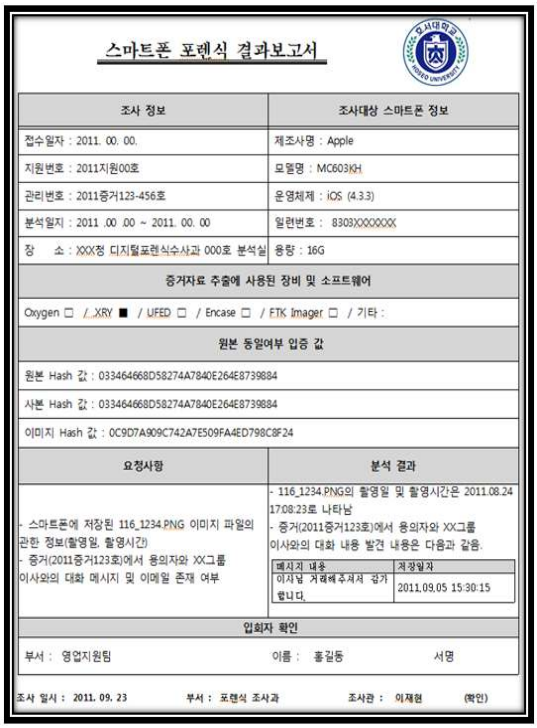
모바일 기기의 무결성을 입증하기 위해 기존의 전파 차단 봉투를 이용해 외부에서의 모바일 기기로의 접근을 막는 방법이 스마트폰으로 변경되면서 Airplain 모드를 이용한 무선 네트워크 차단이 가능해졌다. 따라서 Airplain 모드를 활성화하여 셀룰러 데이터 및 Wifi를 동시에 차단함으로써 기존의 전파차단봉투의 역할을 할 수 있다.

4.4 스마트폰 포렌식 증거 수집 분석

스마트폰 증거를 수집하고 분석할 때에는 분석을 위한 사본을 생성하여 작업 하도록 한다. 이는 원본성을 유지하고 사본을 생성함으로서 증거데이터의 추출에 대해 다수의 분석을 할 수 있는 장점이 있다. 따라서 사본 생성 시에는 원본의 무결성이 유지되도록 주의하며 분석하도록 하며 각 분석 과정마다 분석내용을 기재하도록 한다.

4.5 스마트폰 포렌식 결과보고서 작성

포렌식 보고서는 법정에 제출된 증거자료로서 포렌식 분석 보고서를 프린트하고, 포렌식 문서로 제출하기 위해 포렌식 보고서를 작성한다. 따라서 각 단계별 내용이 상세하게 포함되어 있어야 하며 스마트폰 운영체제, 모델명, 일련번호, 특이사항 등에 대해서도 자세하게 작성한다. 또한 스마트폰 포렌식 툴 사용에 따른 데이터 추출 과정과 증거항목 분석과정에 대해 그림 7과 같이 서술되어야 한다.



스마트폰 포렌식 결과보고서

조사 정보	조사대상 스마트폰 정보
접수일자 : 2011. 00. 00.	제조사명 : Apple
지원번호 : 2011지원00호	모델명 : MC603KH
관리번호 : 2011증거123-456호	운영체제 : iOS (4.3.3)
분석일자 : 2011 .00 .00 ~ 2011. 00. 00	일련번호 : 8303XXXXXXX
장 소 : XXX정 디지털포렌식수사과 000호 분석실	용량 : 16G

증거자료 추출에 사용된 장비 및 소프트웨어

Oxygen ☐ / XRY ■ / UFED ☐ / Encase ☐ / FTK Imager ☐ / 기타 :

원본 동일여부 입증 값

원본 Hash 값 : 033464668D58274A7840E264E8739884

사본 Hash 값 : 033464668D58274A7840E264E8739884

이미지 Hash 값 : 0C9D7A909C742A7E509FA4ED798C8F24

요청사항	분석 결과
- 스마트폰에 저장된 116_1234.PNG 이미지 파일의 관한 정보(촬영일, 촬영시간) - 증거(2011증거123호)에서 용의자와 XX그룹 이사와의 대화 메시지 및 이메일 존재 여부	- 116_1234.PNG의 촬영일 및 촬영시간은 2011.08.24 17:08:23로 나타남 - 증거(2011증거123호)에서 용의자와 XX그룹 이사와의 대화 내용 발견 내용은 다음과 같음. 메시지 내용 : 이자님 계획해주셔서 감사합니다. / 저장일자 : 2011.09.05 15:30:15

입회자 확인

부서 : 영업지원팀 이름 : 홍길동 서명

조사 일시 : 2011. 09. 23 부서 : 포렌식 조사과 조사관 : 이재원 (확인)

그림 7. 스마트폰 포렌식 결과보고서

Ⅴ. 결 론

스마트폰은 기존의 피처폰 서비스 방식에서 PC에서 사용할 수 있는 무선인터넷 환경을 이용함으로써 송신자와 수신자의 교류가 실시간으로 전달된다는 것이다. 이러한 이점을 이용해 악의적인 목적으로 불법거래에 대한 내용을 전달하거나 저작권 및 공정거래에 위배되는 행위가 발생하고 있다. 따라서 스마트폰 증거 데이터의 추출하기 위한 준비사항부터 증거수집, 증거분석, 결과보고서 작성 및 제출의 단계까지 체계적인 절차가 마련되어 조사 및 수사가 신속하고 정확하게 진행되어야 한다.

향후 연구에서는 스마트폰 증거분석 및 절차에 대한 포렌식 방법론에 대해 연구할 것이다.

참고문헌

[1] 방송통신위원회, 한국인터넷진흥원, "2011년 상반기 스마트폰이용실태조사", 2011.

[2] 이규안, 박대우, 신용태, "포렌식 자료의 무결성 확보를 위한 수사현장의 연계관리 방법 연구" , 한국컴퓨터정보학회, 2006.

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

[4] 이정훈, 박대우, "휴대폰과 스마트폰의 모바일 포렌식 추출방법 연구", 디지털산업정보학회, 2010.

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

[6] 구본민, 김주영, 이태림, 신상욱, "Android & iOS 기반 스마트폰의 디지털 증거 수집 및 분석" 한국정보보호학회, 2011.