스마트폰 포렌식을 위한 증거수집 및 분석절차 연구

이재현* · 박대우*

*호서대학교 벤처전문대학원

A Study evidence collection and analysis procedures for smartphone forensic

Jae-Hyun Lee* · Dea-Woo Park*

**Hoseo Graduate School of Venture

E-mail : leejh9708@gmail.com · prof_pdw@naver.com

요 약

스마트폰(Smartphone)의 발전과 함께 스마트폰을 이용한 범죄도 증거하고 있다. 스마트폰의 내부 저장매체에는 사건에 증거자료로 활용될 수 있는 이미지, 동영상, 통화내역, GPS정보, 인터넷 사용기록 등의 데이터들이 존재한다. 따라서 이러한 데이터들을 수집하기 위한 체계적인 증거수집 및 증거분석에 대한 절차가 필요하다. 본 논문에서는 스마트폰을 대상으로 모바일 포렌식의 포렌식 증거수집, 증거분석, 결과보고서 작성까지의 절차 및 방법에 대해서 도출한다. 본 논문을 통해 스마트폰 포렌식 조사 및 수사에 대한 기초자료로 활용될 것이다.

ABSTRACT

Smartphones along with the development of crime evidence has been using smartphones. Phone's internal storage medium can be used as evidence in the case of images, video, phone, GPS information, there are Internet access and other data records. Therefore, these data to collect evidence of a systematic procedure for collecting and analyzing evidence is needed. In this paper, the target mobile phone forensics forensic evidence collection, evidence analysis, and reporting results to the procedures and how to draw. Through this paper, phone forensics and will serve as a basis for the investigation.

키워드

Smartphone Forensic, Evidence Collection, Mobile Forensic, Analysis Procedures

Ⅰ. 서 론

디지털 포렌식기술이 전문화되고 있으며 수사·조사 기관에서는 디지털 범죄 및 침해사고에 대응하기 위한 기술력을 확보가 필요하다[1].

범죄증거에 있어 스마트폰이 사건의 중요한 증거자료로 채택되는 사례가 증가하고 있다. 스마트폰 포렌식에 대한 연구가 국내·외에서 이루어지고 있으며 도구 역시 개발되고 있다.

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

따라서 본 논문에서는 스마트폰 포렌식 과정에서 범죄에 대한 증거자료를 확보하기 위해 증거수집, 증거분석, 결과보고서 작성까지의 절차 및 방법에 대해서 도출하고자 한다.

Ⅱ. 관련연구

2.1 모바일 포렌식

모바일 포렌식은 휴대폰, PDA, Laptop, 전자수첩, 디지털 카메라, USB메모리 카드 등 휴대용 기기에서 필요한 정보를 입수하여 분석하는 포렌식 분야를 말한다[3].

모바일 포렌식 기법은 저장된 데이터를 추출하는 방법에 따라 3가지로 분류할 수 있다. 전원의 동작이 정상적으로 이루어지면서 현장에서 긴급하게 데이터의 존재 유무와 삭제되지 않은 데이터를 추출하는 방법인 SYN 통신 방식을 이용한

분석 기법과 전원의 불량, 삭제되거나 데이터의 정밀분석을 위하여 사용하는 JTAG 통신방식을 이용한 분석 기법, 휴대폰이 완전히 고장 나거나 임의로 훼손하였으나 디지털 증거의 추출이 매우 중요한 사안일 때 휴대폰의 메모리를 분리하여 데이터를 추출하는 리볼링 방식이 있다[4].

2.2 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 증거로 활용될 수 있는 정보를 문서화하여 법정에 제출하는 행위를 말한다.

스마트폰 포렌식은 모바일 포렌식의 절차에서를 기반으로 진행되며 일부 스마트폰의 특성을 바탕으로 일부 절차들을 주의하며 증거데이터 수집을 진행하도록 해야 한다. 기본적인 스마트폰 포렌식 절차는 크게 사전준비, 증거수집, 증거분석, 결과보고서 작성으로 그림 1과 같이 분류할 수 있다[5][6].

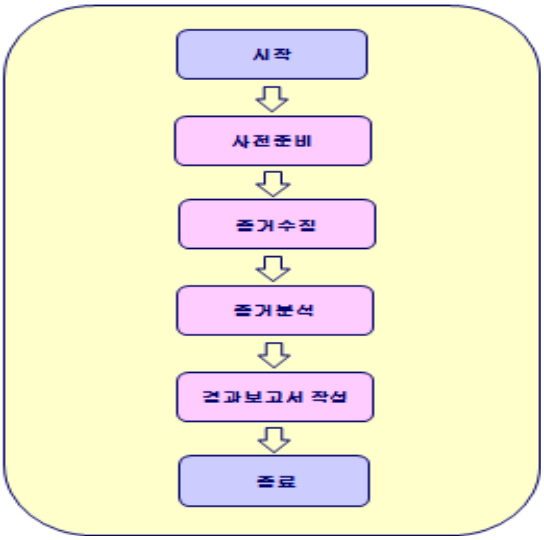

그림 1. 스마트폰 포렌식 절차

Ⅲ. 스마트폰 포렌식 사전 준비 절차

스마트폰 포렌식 사전 준비 단계는 스마트폰 데이터의 원활한 수집 및 분석을 위한 제반 사항에 대한 준비이다. 최초 증거수집 및 분석에 필요한 사항을 준비하는 사전준비, 사건에 증거자료를 수집하는 증거수집, 수집한 증거를 분석하는 증거분석, 분석한 절차에 따른 결과를 작성하는 결과보고서 작성으로 분류할 수 있다[7].

포렌식 수사 시 준비해야 할 사항에는 포렌식 전문가 구성, 수사를 위한 행정절차, 대상 및 범위 선정사건의 환경, 사건의 비중, 포렌식 구성원의 훈련경험, 수사에 대한 계획 수립 등의 사항들을 어떻게 준비하느냐에 따라 다양한 결과를 나타낼 수 있다[8].

3.1 포렌식 전문가 구성

스마트폰 포렌식 전문가는 스마트폰의 운영체제의 파일시스템, 중요 데이터의 디렉토리 구조 및 형태 등에 대해 알고 있어야 하며, 스마트폰 포렌식 툴 사용능력, 모바일 포렌식 분야의 전문지식을 갖춘 사람으로 구성되어야 한다.

3.2 수사를 위한 행정절차

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

3.3 대상 및 범위 선정

범죄현장 방문 시 스마트폰의 증거수집이 신속하고 정확하게 수행될 수 있도록 증거수집의 대상과 범위를 선정하여 리스트를 작성하도록 한다.

각 스마트폰 대상 OS의에 따른 수집방법과 범위를

3.4 증거 수집계획 수립

스마트폰 대상에 따라 증거를 수집하는 방법이 다르게 진행되는 점을 고려해 증거 수집계획을 정의한다. 즉 수집 계획을 세울 시 각 조사자들이 각각 어떠한 기술과 능력에 맞춰 증거수집을 할 것인지에 대해 선정하고 역할을 수행해야 한다.

여기서 고려해야할 점은 스마트폰의 운영체제, 내장메모리의 유무 등이 포함되며 포렌식 툴을 이용해 시스템 시간 정보, 사용자 계정 정보, 프로세스 정보, 네트워크 정보, 문서정보 등 증거수집 시 증거수집 대상 스마트폰을 지원하고 있는지 확인하는 것이 중요하다. 따라서 스마트폰 포렌식 도구가 포함하고 있는 구성품을 확인하여 증거 수집 시 착오가 발생하지 않도록 한다.

3.5 증거 분석계획 수립

증거 데이터의 분석을 위해 계획을 정의한다. 분석 시 원본 이미지가 변조되지 않도록 사본을 이용해서 분석을 하며 증거수집한 데이터의 사건과 관련하여 증거가 포함되어 있을만한 파일 포맷의 우선순위를 선정하여 증거데이터를 분석한다. 또한 데이터가 위조되거나 변조된 흔적 발견 시 파일시스템에 맞는 데이터 복구를 통해 안티포렌식 흔적을 분석하도록 한다.

Ⅳ. 스마트폰 포렌식 증거수집 및 분석 절차

4.1 사진촬영 및 현장 스케치

수사 시 현장의 당시 주변 상황을 촬영 및 스케치하고 사건과 관련된 증거자료에 대해서는 상

세하게 기재하여 놓는다. 따라서 의뢰받은 증거분석 담당자가 현장 촬영내용 및 상세정보를 확인하고 분석에 도움이 될 수 있도록 한다.

4.2 증거수집

현장에서 무결성을 보증하기 위하여, 카메라, 캠코더 등을 이용하여 증거확보 과정을 녹화하고 쓰기방지 장비 및 포렌식 복제장비를 사용하여 원본과 사본의 동일성을 확보한다. 디지털 증거의 획득시 사본을 2개 이상 생성하여 원본은 봉인하고, 나머지 2개의 사본 중 1개는 증거분석용으로 사용하며, 나머지 1개는 업무의 연장을 위해서 해당 컴퓨터의 사용자에게 제공된다. 최종적으로 획득된 증거의 해쉬값 검증을 통해서 무결성이 유지되었다는 것을 원 소유주에게 확인하고 서명을 받는다. 또한 이러한 일련의 과정을 서면 기록한다. 이와 같은 디지털 증거의 확보단계를 모두 수행하였으면, 관련 증거물을 안전한 보관장치를 통해서 디지털 포렌식 센터로 이송한다. 스마트폰 증거수집 절차는 그림 2와 같으며, 그림 3과 같이 스마트폰 증거를 수집할 수 있다.

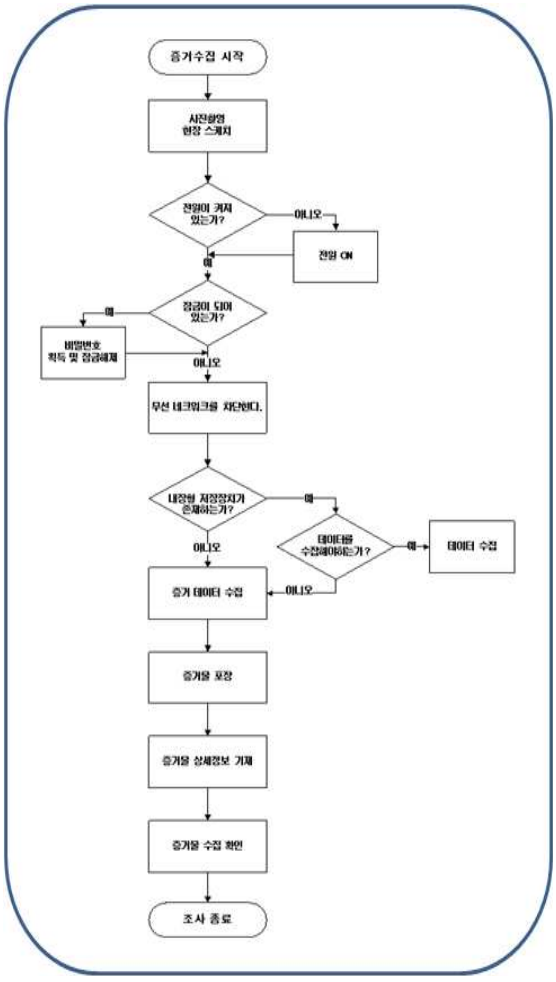

그림 2. 스마트폰 증거수집 절차

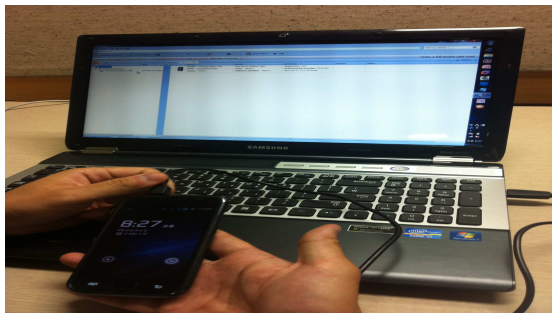

그림 3. 스마트폰 증거수집

4.3 증거분석

디지털포렌식 센터로 이송된 분석대상 스마트폰 증거물은 분석 전에 다양한 디지털포렌식 분석도구에서 인식할 수 있는 압축된 이미지 형태로 변경시킨다. 이러한 변형된 디지털 증거물은 기존의 획득 당시의 해쉬값과 동일한 해쉬값을 유지하며, 압축되어 대용량 저장매체에 보관된다. 변경되어 저장된 디지털 증거물은 디지털포렌식 전문 분석도구를 이용하여 분석하게 된다. 일반적으로 운영체제 설치 일시, 메모리 등 인터넷 사용기록, 삭제된 파일 복구, 키워드 검색 등 다양한 정밀 분석을 수행한다. 스마트폰 증거분석 절차는 그림 4와 같으며, 그림 5와 같이 스마트폰 전용 S/W를 통해 분석할 수 있다.

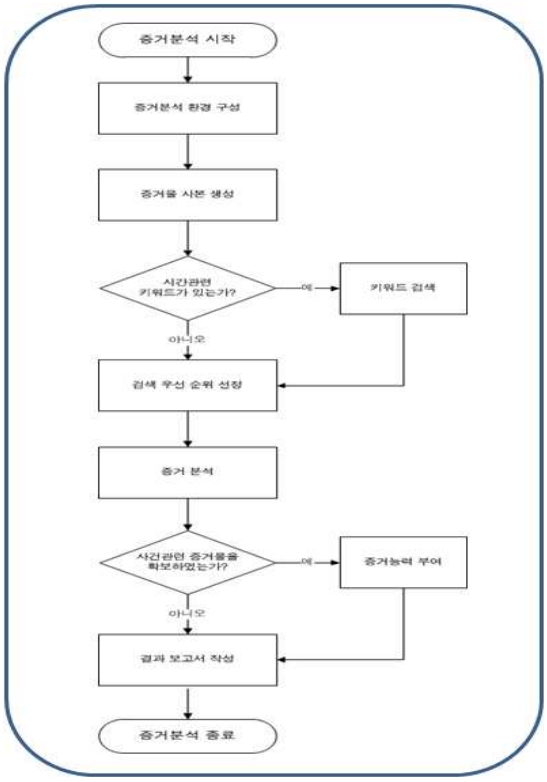

그림 4. 스마트폰 증거분석 절차

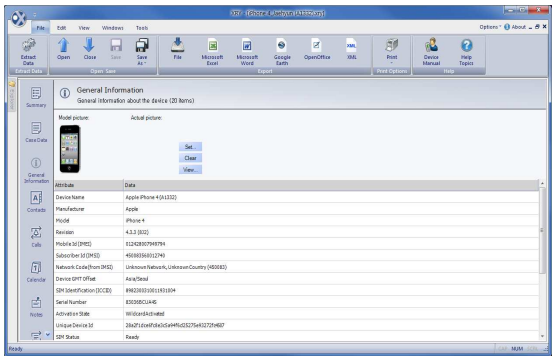

그림 5 스마트폰 증거분석

4.4 포렌식 결과보고서 작성

디지털 증거자료 중 법정에서 간접증거로 적용될 수 있는 의미있고 객관적인 데이터를 추출하여 디지털포렌식 전문 분석도구에서 제공되는 형태로 1차 보고서가 완성된다. 1차 보고서를 기반으로 각 수사기관에서 정해진 분석 결과 보고서 형태로 수작업을 통한 2차 보고서가 완성된다. 2차 보고서는 육하원칙에 따라 기술된 보고서이며, 관련 디지털 증거를 법률적인 시각 및 정책적인 시각으로 판단할 수 있도록 기술된다.

포렌식 결과보고서는 법정에 제출된 증거자료로서 포렌식 문서로 제출하기 위해 포렌식 보고서를 작성한다. 작성된 포렌식 기법을 적용시킨 스마트폰이 불법저작물이 메모리에 저장되어 있는지, 최근에 불법저작물을 사용했는지 확인한다. 확인 결과 불법 저작물을 사용하지 않았을 경우 그동안 포렌식 기법을 적용한 내용을 그림 6과 같이 보고서 형태로 작성한다.

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)
분석일지 : 2011 .00 .00 ~ 2011. 00. 00	일련번호 : 8308XXXXXXX
장 소 : XXX청 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 / 저장일자 이지입 거래해주셔서 감사합니다. / 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 6. 스마트폰 결과보고서

V. 결 론

스마트폰 사용자가 침해 사건이 발생하였을 때, 스마트폰을 압수수색 한 후에 스마트폰 포렌식 절차에 준수하여 기술을 적용하는 것이 증거자료 수집에서 분석까지 증거의 위·변조를 방지하는 방안이다.

본 논문은 스마트폰 포렌식 수사 과정에서 포렌식 준비과정부터 증거수집, 증거분석, 결과보고서 작성까지의 절차를 제시 하였다. 본 논문을 스마트폰 범죄 수사를 통한 모바일 포렌식을 위한 기술을 한 단계 발전시키고자 한다.

향후 연구로는 스마트폰 파일시스템에 따른 스마트폰 표준화 추출과정과 분석에 관한 기법을 지속적으로 연구하여 스마트폰 포렌식 자료 추출과 삭제된 자료의 분석 스마트폰으로부터 포렌식 자료를 추출하고 분석 할 수 있도록 하여야 한다.

참고문헌

[1] 이정훈, 박대우, “휴대폰과 스마트폰의 모바일 포렌식 추출방법 연구,” 디지털산업정보학회, 제6권, 제3호, pp.79-89, 2010.

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

[3] S.Y. Willassen, “Forensic analysis of mobile phone internal memory,” IFIP, vol. 194, pp.191-204, 2005.

[4] 박대우, “스마트폰 저작권과 포렌식 적용방안,” 2010년 불법복제물 단속 유관기관 합동 워크숍, 한국저작권위원회, 2010.

[5] Venansius Baryamureeba and Florence Tushabe, “The Enhanced Digital Investigation Process Model,”

[6] 경찰청, 디지털 증거처리 표준 가이드라인, 경찰청 2006. 12

[7] 이광열, 최윤성, 최해랑, 김승주, 원동호, "현행 증거법에 적합한 디지털 포렌식 절차" 정보보호학회지 제18권 제3호, pp.81-91, 2008.6.

[8] 이규안, 박대우, 신용태, "휴대폰 압수수색 표준절차와 포렌식 무결성 입증", 한국통신학회, 제33권, 제6호, pp.423-530, 2008.