스마트폰 환경에서 디지털 포렌식 분석 사례 연구

이기욱, 최옥경, 홍만표
아주대학교 지식정보보안학과
e-mail : ohgani27@ajou.ac.kr, okchoi@ajou.ac.kr, mphong@ajou.ac.kr

Digital Forensic Analysis Case study on Smartphone

Ki-Wook Lee, Ok-kyung Choi, Manphyo Hong
Dept. of Knowldege Information Security, Graduate School of Ajou University

요 약

IT 와 비즈니스가 융합화 되고 정보가 디지털화 됨에 따라 그에 대한 저장매체도 점점 더 다양해지고 있다. 그 중 이동성이 편리하고 휴대하기 간편한 스마트폰을 활용하여 개인 정보를 주고 받고 이를 이용한 비즈니스가 현재 활발히 진행되고 있다. 이러한 소셜 네트워크 서비스 이용이 급격히 증가함에 따라 개인 정보 보안에 대한 중요성은 점점 더 강조 되고 있는 실정이다.

본 연구에서 제안하는 디지털 포렌식 분석 방법을 이용하면 스마트폰에서 지원하는 서비스 형태에 따라 텍스트, 이미지, 동영상 등의 개인 정보를 수집 및 분석이 가능하다. 또한 디지털 포렌식의 관점에 따라 스마트폰 에서 사용되고 있는 애플리케이션의 로그 정보를 수집 및 분석함으로써 스마트폰의 저장 장치에 남겨진 기록들을 훼손 없이 그대로 보존시키고 디지털 증거 자료로 활용이 가능해 사이버 범죄에 대한 신속한 해결이 가능하다.

1. 서론

스마트폰 포렌식은 디지털 포렌식에 포함되는 개념으로도 표현 할 수 있다. 모바일 분야에서 새로운 영역이며 그 애플리케이션의 다양성으로 인하여 스마트폰을 PC 와 연동하여 사용하거나 단독으로 업무를 수행 할 수 있다. 현재 사이버 범죄가 확장되고 있는 추세처럼 스마트폰을 이용하여 개인 PC 및 각종 디지털 기기와 연동한 악의적인 상황이 발견 되고 있다. 따라서 디바이스에 내장된 디지털 자료를 근거로 스마트폰의 매개체로 어떤 행위에 대한 관계를 규명하고 증명하는 기법이 필요하다.

스마트폰 포렌식은 3G, WIFI 상의 감시 카메라처럼 사용자가 어떤 웹 사이트에 접속해 어떤 데이터를 주고 받았는지를 확인 할 수 있는 기술이며 디지털 증거 수집뿐만 아니라 개인에 대한 보안 수준을 높이는데 활용성이 높다. 하지만 스마트폰 기기 사용이 급증하면서 스마트폰 기기에 남겨진 디지털 증거를 정확히 분석해줄 포렌식 기술이 부족하다.

본 연구에서는 스마트폰 환경에서 디지털 포렌식 기술을 이용하여 데이터의 정보 및 소셜 네트워크 서비스 어플리케이션을 분석하여 원하는 데이터 정보에 대한 수집 및 분석을 수행하고 스마트폰에 남아있는 기록에 대한 보안의 위험성 체크를 가능하게 함으로써 중요한 개인 정보에 대한 효율적인 정보 분석 및 보안이 가능하다.

2. 관련연구

2.1 스마트폰 포렌식이란 ?

포렌식 이란 전자 증거물 등을 사법기관에 제출하기 위해 데이터를 수집, 분석, 보고서를 작성하는 일련의 작업을 말한다. 그 분야에서 스마트폰 포렌식은 모바일 디바이스에 내장된 디지털 자료를 근거로 스마트폰의 매개체로 어떤 행위에 대한 관계를 규명하고 증명하는 기법이다. 통화 목록, 연락처, SMS, 음성 메시지, 사파리 웹브라우저 사용 정보 등이 수사에 많은 도움이 된다. 특히 메일이 증거 관점에서 큰 이점으로 작용하며 카카오톡등 채팅 내역 또한 보관이 되기 때문에 증거로 활용할 수 있다

2.2 스마트폰 증거 수집 방법

스마트폰 기기의 특성과 휘발성 및 비 휘발성에 관하여 절차 단계마다 검증이 필요하다. 차폐장치, 이미징, 해쉬함수를 적용하며 중점적으로 덤프메모리 분석, 레지스트리 분석, Timeline 분석, 삭제된 파일 기록, 비정상적인 파일 기록, 슬랙 공간분석, 로그 분석 등

이 필요하다.
복원 단계에서 일반 영역과 삭제 영역을 구분하여 각각의 해쉬 함수 알고리즘을 적용한다, 적용하는 주요 쟁점은 해외 및 국내에서 표준화된 방식을 이용하여 과정을 진행 한다.[4]
현재 국내 보급이 원활하게 이루어지고 있는 스마트폰의 OS 는 대표적으로 Android 와 IOS 로 나눌 수 있다.

2.3 Android

기본 Android 의 권한으로는 내부 폴더에 접근이 불가능 하다. 리눅스 커널의 권한을 일반권한에서 Root 권한으로 바꾼다. Root 권한을 가진 Android 스마트폰 내부 폴더를 검색하여 증거 데이터를 수집한다. [1][2]

설명	위치		
기본 어플리케이션 파일 위치	/system/app		
다운 어플리케이션 파일 위치	/data/app		
어플리케이션의 DB, 라이브러리 데이터 위치	/data/data	SMS	/data/data/com.android.providers.telephony /databases/mmssms.db
		통화목록 주소록	/data/data/com.android.providers.contacts/databases/contacts2.db
		브라우저	/data/data/com.android.browser/databases/browser.db
		트위터	/data/data/com.twitter.android/databases/twitter.db
		구글맵 history	/data/data/com.google.android.apps.maps/search_history.db
카메라 파일위치	/sdcard/DCIM		

<그림 1. Android 구조> [2]

2.4 iOS

iOS 는 내부 폴더에 대한 접근이 불가능 하다. 하지만 iTunes 라는 PC 동기화 프로그램을 사용하여 내부 중요 데이터들을 수집한다. iPhone 과 동기화한 데이터들이 mddata 형태로 저장되며 파일들은 SQLite Expert 로 데이터 확인이 가능하다.[1][6]

폴더명	파일명	설명
C:\사용자\〈계정명〉\App Data\Roaming\Apple Computer\MobileSync	31bb7ba8914766d4ba40d6dfb6113c8b614be442.mddata	주소록
	3d0d7e5fb2ce288813306e4d4636395e047a3d28.mddata	SMS
	ff1324e6b949111b2fb449ecddb50c89c3699a78.mddata	통화 목록

<그림 2. ios 구조> [3]

3. 어플리케이션 포렌식 분석

루팅 된 스마트폰에서 이미지를 추출하여 어플의 개별적인 데이터를 분석하며 또한 전체적인 이미지뿐만 아니라 유심(Usim)카드를 따로 각출하여 리더기를 통한 이미지를 추출해 데이터를 분석 한다. 각 어플들의 아이디 및 비밀번호는 스마트폰의 사용자가 입력한 값을 데이터가 백업 되어 있는 상태에서 추출하며 그에 대한 값을 출력한다.

다음과 같이 mobilesyncbrowser tool 을 이용하여 스마트폰 기본 정보와 정보가 저장된 백업된 위치를 찾아내고 다음과 같이 나타낼 수 있다.

Basic Informaion	- Info.plist	- 장치명 - UDID - 전화번호 등
Voice Communication	- Callhistory.db - Voicemail.db	- 통화기록 - 음성 메세지
Network Related	- wifi.plist	- 접속 wifi 흔적
Text communication	- sms.db	- 문자메세지
Audio-visual	- DCIM folder	- 사진,동영상
Location Related	- maps.plist	- 위치정보,지도
Online Activity	- bookmarks.plist - history.plist	- 즐겨찾기 - 웹 서핑
User Activity	- AddressBook. Sqlitedb - Calendar. Sqlitedb	- 주소록 - 일정

<표 1. Mobilesyncbrowser 이용한 smartphone framework>

위와 같이 해당 필드에 대한 데이터(값)을 추출하여 위치정보, 프로필정보, WIFI 정보 등 본인이 이용한 정보에 대해 기록을 추출해 낼 것 이다.

Facebook App	- Com.facbook. facebook.plist	- 페이스북정보
Nateon App	-Com.nateon. nateon.plist	- 네이트온정보

<표 2. AccessData FTK 이용한 SNS App 분석>

위와 같이 어플리케이션 분석을 통해 스마트폰의 다양한 애플리케이션을 분석 각 OS 별로 증거 데이터가 저장되어 있는 폴더들을 나열하고 위치를 파악하여 스마트폰을 수집했을 때 재빠른 증거 데이터 확보가 가능 할 것이다.[7] 또한 애플리케이션의 로그를 토대로 스마트폰의 남아있는 사용했던 기록에 대한 보안의 위험성을 체크 할 수 있을 것이다.

4. 결론

본 논문에서는 스마트폰의 디지털 증거 수집 방법에 관해 다루었다. 다음과 같이 스마트폰에 대한 포렌식을 수행하면 효과적인 데이터 분석이 가능하다. 애플리케이션 정보를 취득함으로써 개개인의 취향이나 관심사를 파악하고 그에 대한 인적관계 분석이 가능 할 것이다.[5] 아직 표준이 확립되어 있지 않기 때문에 법에 위배 되지 않는 한도 내에서 개인의 스마트폰에

대한 정보를 취득 함으로써 불법적으로 사용되고 있는 프로세스나 해킹으로 인해 피해를 입을 시 대책을 마련 할 수 있을 것이다. 향후 Android 와 IOS 기반 스마트폰의 증거 수집과 분석 시 무결성을 어떻게 확보할 것인지에 대한 연구가 필요하며, 사용자의 요구사항을 충분히 충족시키고 확장성과 유용성이 뛰어난 분석 도구의 개발이 요구된다.

참고문헌

[1] “Android & Ios 기반 스마트폰의 디지털 증거 수집 및 분석” 부경대학교 대학원 정보보호 협동과정 구본민, 김주영, 이태림, 신상욱. 2011 년 02 월

[2] “Android 기반 스마트폰 디지털증거수집” 한국멀티미디어 학회, 추계학술발표대회논문집. 구본민, 김주영, 이태림, 신상욱. 2010 년 11 월

[3]”아이튠즈를 이용한 아이폰 디지털 증거수집” 한국정보보호학회 영남지부, 학술발표논문집 p55-60 김주영, 구본민, 이태림, 신상욱. 2010 년 04 월

[4]”논리적 분석 기반의 안드로이드 스마트폰 포렌식 도구 구현” 숭실대학교 컴퓨터학부. 김익수, 안영건, 이정현, 양승제, 김명호. 2011 년 04 월

[5]”소셜 네트워크 서비스를 위한 프라이버시 보호 정책언어 및 프라이버시 보호 모듈 구현” 정보과학연구소. 김지혜, 이형효. 2011 년 02 월

[6]”Apple- iTunes, http://www.apple.com/kr/itu nes/what-is

[7]”Facebook Forensics” www.vxrl.org. Kelvin wong