情報保護學會論文誌
第 21 卷 第 1 號, 2011. 2

Android & iOS 기반 스마트폰의 디지털 증거 수집 및 분석*

구 본 민,[1†] 김 주 영[1], 이 태 림[1], 신 상 욱[2‡]
[1]부경대학교 대학원 정보보호협동과정, [2]부경대학교 IT융합응용공학과

Collection and Analysis of the Digital Evidence for Android and iOS Smart Phones*

Bon-Min Goo,[1†] Ju-Young Kim[1], Tae-Rim Lee[1], Sang Uk Shin[2‡]
[1]Dept. of Information Security Graduate School, Pukyoung National University,
[2]Dept. of IT Convergence and Application Eng, Pukyoung National University

요 약

최근 스마트폰의 등장으로 모바일 서비스가 다양한 형태로 성장하고 있다. 각 회사들은 Window Mobile, Android, iOS 등 다양한 운영체제를 탑재하여 출시하고 있지만, 현재 가장 보급이 원활하게 이루어지는 스마트폰은 Android와 iOS를 탑재한 스마트폰이 활발히 보급되고 있다. 이에 따라 스마트폰의 다양한 기능을 이용하여 각종 범죄로 연결될 수 있으며, 다양한 증거들이 남아 있을 수 있다. 본 논문에서는 디지털 포렌식(Forensic)의 관점에 따라 스마트폰에서 수집될 수 있는 증거 데이터의 위치를 파악하고, 도구를 설계해 수집된 데이터를 분석하였다. 이로 인해, 범죄사용으로 인한 스마트폰의 증거들을 수집할 때 시간을 단축시킬 수 있는 기대효과를 가져본다.

ABSTRACT

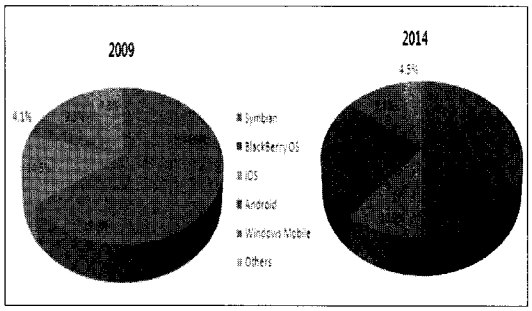
As recent emergence of smart phones, mobile services are growing in various forms. Many companies released smart phones of various operating systems such as Window Mobile, Android and iOS. Currently, most popular smart phone operating systems are Android and iOS. Due to the various features of these smart phone, they can be employed to various crimes. From the point of view of digital forensics, this paper analyzes the evidence data which needs to be collected in the smart phone, and implements the evidence analysis tool. By using this tool, it can reduce the time and effort for collecting and analyzing the evidence of the smart phone.

Keywords: digital forensics, digital evidence, android, iOS, smart phone

I. 서 론

현재 국내 보급이 원활하게 이루어지고 있는 스마트폰의 OS는 대표적으로 Android와 iOS로 나눌 수 있다. 판매 초기에는 iOS를 탑재한 스마트폰의 판매량이 급격히 늘었으나, 시간이 지남에 따라 Android를 탑재한 스마트폰의 생산이 다양하게 이루어졌고, 그 결과 Android를 탑재한 스마트폰의 판매량이

접수일(2010년 12월 3일) 게재확정일(2011년 1월 4일)
* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(No. 20100003222), 그리고 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업[10035157, 실시간 분석을 위한 디지털 포렌식 기술 개발]의 일환으로 수행된 연구임
† 주저자, takara00@pknu.ac.kr,
‡ 교신저자, shinsu@pknu.ac.kr



〔그림 1〕. 전세계 스마트폰 운영체제 점유율, 2009/2014

iOS를 탑재한 스마트폰과 더불어 판매수요가 더욱 높아지고 있다. 〔그림 1〕〔1〕과 같이 IDC에서는 전체 휴대폰에서 스마트폰이 차지하는 비중이 2009년 15%에서 2010년 20%를 넘어설 전망으로 예측했고, 판매량 순위는 Apple이 2위 Samsung, HTC가 4, 5위를 기록하였다〔2〕. 또한 스마트폰은 기능도 다양해져서 기본 전화나 문자 기능뿐만 아니라 엔터테인먼트 기능, 모바일 오피스 기능 등 거의 모든 PC 기능을 보유하고 있다.

이처럼 일상에서 스마트폰의 특성에 의해 사용 범위가 다양하게 확장됨에 따라 스마트폰이 범죄에 이용되거나, 관련 증거가 스마트폰에 보관되어 있을 가능성이 높아졌다. 따라서 스마트폰에 저장된 데이터가 디지털 증거가 될 수 있는 것을 보여주는 것이며, 이는 수사와 법정의 증거자료로 활용된다. 이에 따라 본 논문에서는 디지털 포렌식의 관점에서 각 OS별로 스마트폰의 디지털 증거가 되는 데이터의 위치를 미리 파악하고, 분석하는 방법을 제시하고자 한다.

II. 관련연구

2.1. 모바일 포렌식

모바일 장비는 디지털 장비 중에 이동성을 부여한 것으로, 대표적인 것은 휴대폰, PDA, 디지털 녹음기, 디지털 카메라와 이동기기 등이 포함된다. 특히 휴대폰은 세계적으로 가장 많이 사용하는 모바일 장비이다. 다양해진 성능에 의해 모바일 장비들이 범죄에 이용되고 있으며, 각 모바일 장비들은 디지털 증거 데이터를 갖고 있다. 모바일 포렌식을 적용하기 위해 확보해야할 디지털 증거 데이터의 분류는 다음과 같다.

- 휴대폰의 음성 및 SMS 데이터
- 음성 녹음 데이터
- 디지털 카메라나 휴대폰의 사진 및 동영상 데이터
- 차량, 선박, 비행기, 기차 등 이동기기들의 전자기록 데이터
- 이동저장장치에 부가된 전자자료

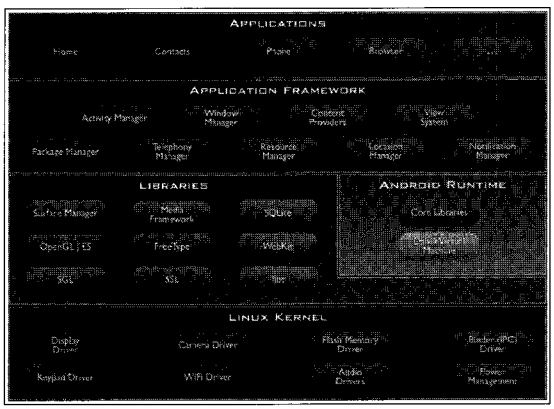
위의 증거 데이터들 중 휴대폰의 디지털 증거자료 수집 및 분석기법은 3가지가 있는데 첫 번째는 휴대폰 제작사에서 제공하고 있는 PC 동기화 기능을 이용하여 데이터를 수집하는 방법, 두 번째는 JTAG 포트를 이용하여 휴대폰에 접속한 다음 모든 영역의 데이터를 덤프하는 방법, 세 번째는 휴대폰에 장착된 플래시 메모리를 분리하여 데이터를 수집하는 기법 등이 있다〔3〕.

2.2. 스마트폰의 OS 특징

이전 모바일 포렌식에서는 휴대폰 제조업체에서 제공하는 PC 동기화 기능이나 JTAG 포트를 이용하는 등 특정 준비가 필요했지만, 스마트폰은 전용 OS의 분석만 잘 이루어진다면, 다른 준비가 필요 없이 디지털 증거들을 수집할 수 있다.

2.2.1. Android

Android는 〔그림 2〕〔4〕에서 보는 것과 같이 크게 5가지 계층으로 구분된다. 리눅스 커널을 기반으로 동작하며 최상위 계층의 APPLICATIONS에는 기본 프로그램인 전화, SMS, 달력, 지도, 웹 브라우저 등 기본 프로그램이 위치해 있고, 아래 계층인 APPLICATION FRAMEWORK에는 각 기본 프로그램들의 API와 더불어 향후 탑재될 프로그램의 프레임워크와 라이브러리 등이 있고, LIBRARIES에는 Android 운용을 위한 DB나 매체에 대한 라이브러리들을



〔그림 2〕 Android 시스템 구조

포함하고 있으며, ANDROID RUNTIME에는 리눅스 커널 위에서 Android가 동작할 수 있게 도와주는 Dalvik 가상머신이 위치하고 있다.

2.2.2. iOS

iOS는 OS X 10.5(Leopard)를 바탕으로 구성되어 있으며, Core OS, Core Services API, Media layer, Cocoa Tough layer 등 4가지 계층으로 나뉜다[5].

OS 버전으로는 초기 3.1번대 버전으로 시작하여 현재 4.2버전까지 업데이트가 완료되었다. iOS를 사용하는 iPhone은 iTunes라는 PC 동기화 프로그램을 사용하는데 이는 App Store와 연동이 되어있어 iPhone에 다양한 어플리케이션을 다운받을 수 있도록 도와주고 iPhone과 연결하면 스마트폰 내부에 있는 데이터들이 iTunes와 동기화가 되는데 이는 어플리케이션 뿐만 아니라 내부 폴더에 있는 데이터들까지 전부 백업이 되어 디지털 증거로써 활용 가능한 데이터가 존재한다.

III. Android, iOS 기반 스마트폰의 디지털 증거 수집 및 분석방법

이전 모바일 포렌식을 위한 디지털 증거 데이터로의 분류는 5가지가 있었다. 특히 휴대폰 포렌식을 위한 디지털 증거 데이터는 음성 및 SMS 데이터, 음성 녹음 데이터, 이미지 파일 등의 데이터가 존재하였으나, 스마트폰에서 디지털 증거가 될 수 있는 데이터는 음성 및 SMS 데이터 이미지 파일등은 물론이고, 웹 브라우저, 일정, 통화목록, 주소록, GPS 데이터, SNS 데이터 등 수집해야 할 데이터가 더 많이 존재한다. 따라서 스마트폰의 순정상태에서 수집할 수 있는 데이터와 수집할 수 없는 데이터를 나누어 수집방법을 설명한다. 이 때, 순정상태란 스마트폰 자체적인 기능만 갖고 수행하는 상태로 정의하며, Android와 iOS의 경우엔 각각 루팅, 탈옥이라는 방법을 이용하여 순정상태에서 벗어나 스마트폰의 유저가 직접 OS를 수정하고, 변경할 수 있다. 하지만 루팅, 탈옥은 사용자가 임의로 조작하는 행위로 이를 통한 기기의 고장시 A/S 등 법적 보호를 받지 못한다. 현재 Android와 iOS의 최신버전까지 루팅, 탈옥이 가능한 상황이지만, Android는 리눅스의 Bootloader를 Unlock하는 루팅 방법을 사용하면, 기기의 부팅시 자물쇠가 풀린 이미지가 출력되고, iOS의 경우 최신 버전(4.1이상) 탈옥시 워터마크가 생성이 되며, 탈옥이 이루어진 스마트폰으로 구분된다. 본 논문에서는 국내에 유통되는 스마트폰 중 점유율이 높은 Android와 iOS기반 스마트폰으로 디지털 증거가 되는 데이터를 수집, 분석하는 기기로 Android 스마트폰은 Nexus One, iOS 스마트폰은 iPhone 3GS를 사용하였다.

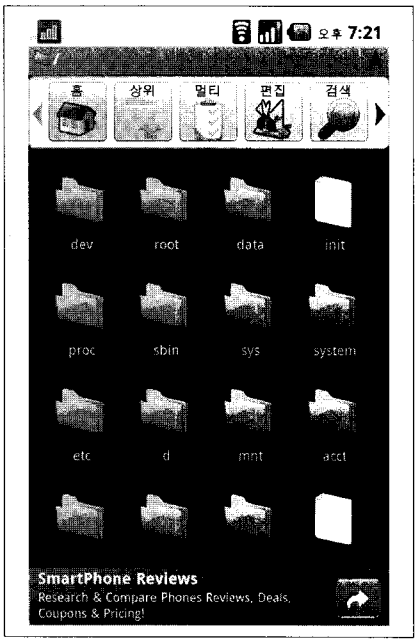
3.1. Android상의 디지털 포렌식 적용법

Nexus One에는 제공하는 PC 동기화 프로그램은 존재하지 않으나, 기본 기능인 동기화[6]를 이용하여 주소록, Gmail, 캘린더 데이터 저장이 가능하다. Nexus One을 처음 켰을 때 Google 아이디와 동기화 하는 과정이 나오는데 이 때 등록한 Google 아이디로 데이터가 저장이 되며, 동기화 후 등록된 아이디로 Google에 접속하면 주소록과 Gmail, 캘린더가 동기화 되어 있는 것을 볼 수 있다. 하지만 Android는 리눅스 커널 기반으로 동작함에 따라 권한 문제로 인해 다른 데이터 수집이 제한되어 있다. 순정 상태에서 Android 내부 폴더로 접근할 수 있는 방법은 2가지가 있다. 첫 번째는 안드로이드 마켓에 있는 어플리케이션을 이용하는 것이고, 두 번째는 Android SDK인 ADB(Android Debug Bridge)[7]를 사용하면 내부 폴더에 접근이 가능하다[8].

안드로이드 마켓에는 많은 어플리케이션이 존재한다. 그 중에서도 25만회 이상 다운로드 된 ASTRO[9]는 탐색기와 비슷한 기능을 제공하며 SD카드와 내부 폴더로 접근이 가능하다. SD카드에서는 ASTRO의 기본 기능을 이용하여 파일의 삭제, 복사, APK파일의 설치 등이 가능하나, 내부 폴더에서는 그 기능이 자유롭지 못하다.

Android Developer에서 소개되는 ADB는 SDK를 설치해야 하며 Android 기기 내부로 접속 가능하게 하는 도구이다. 먼저 PC와 Android 기기를 연결하고, PC 상에서 Android 기기 고유번호를 확인하여 접속한다. Android 기기는 스마트폰뿐만 아니라 임베디드 보드, 개발 도구, 에뮬레이터 등 모두 다른 고유번호를 갖고 있다. Command상에서 ADB 명령어를 사용하여 접속 시 내부 폴더의 접근이 가능하나, 어플리케이션을 사용했을 경우와 마찬가지로 복사, 삭제 등이 불가능하다.

위에서 제시한 내부 폴더 접근법 중 ASTRO를 이

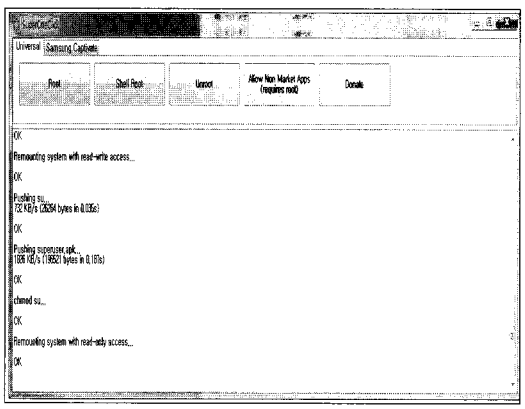


〔그림 3〕 Android 내부 폴더 목록

용하여 Android OS의 내부 폴더 목록들을 나타낸 것이 다음 〔그림 3〕이다.

3.1.1. Android의 디지털 증거 수집 방법

기본 Android의 권한으론 내부 폴더에 접근이 불가능 하였다. 리눅스 커널의 일반권한으로 동작하기 때문인데, 이를 Root 권한으로 바꿔서 동작하게 만드는 행동을 루팅이라고 한다. 실제 기기에 대해 다음 〔그림 4〕의 루팅 프로그램을 이용하여 현재 Nexus One의 Android 버전인 2.2.1 루팅을 시도하고,



〔그림 4〕 SuperOneClick 루팅 프로그램

〔표 1〕 Android 주요 증거 데이터 파일 위치

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		

Root 권한을 가진 Android 스마트폰 내부 폴더를 검색하여 증거 데이터를 수집한다.

그림 3에서 보았던 순정 상태의 내부 폴더 목록 중 data의 내부 데이터들은 순정상태일 때 빈 폴더로 나왔으나, 루팅 후에는 숨겨진 폴더가 나타난다. Android 내부 폴더 중 중요 폴더는 〔표 1〕로 정리해 보았다.

3.1.2. 수집 데이터 분석

기본 기능인 동기화로 인해 수집 가능한 데이터를 제외하면 SMS, 통화목록, 브라우저, SNS 데이터가 디지털 증거로써 수집되어야 할 데이터이며, 데이터는 SQLite로 저장되어 있다. 위 〔표 1〕의 데이터 파일 내용을 확인해보면 주요 데이터의 테이블 내용은 아래의 표들과 같다. 〔표 2〕는 mmssms DB 파일의 sms 테이블이며 address에 수신 전화번호, body 부분에 수신 전화번호로부터 받은 문자 메시지가 저장되어 있고, 〔표 3〕은 contact2 DB 파일의 calls 테

이블로 number에 통화목록에 남겨진 전화번호 데이터가 존재하며 type에는 저장되어 있는 데이터에 1은 수신, 2는 발신으로 저장되어 있다. [표 4]는 같은 contact2 DB 파일의 data 테이블로 주소록이 저장되어 있다. data1에는 이름과 성을 합친 이름과, 전화번호가 저장되어 있고, data2에는 이름, data3에는 성 정보가 저장된다. [표 5]는 browser DB 파일의 bookmarks 테이블로 각 url에 맞는 title이 저장되어 있으며, [표 6]은 twitter DB 파일의 statuses 테이블로써 Nexus One에 기본 저장되어 있는 트윗을 사용하였을 때 트윗 데이터가 content에 저장되는 것을 볼 수 있다. [표 7]은 search_history DB 파일의 suggestions 테이블로 구글 맵을 사용하여 장소를 검색했을 때 검색한 데이터가 data1에 저장이 되는 것을 볼 수 있다.

[표 2] mmssms DB sms 테이블

필드명	설명
address	모든 수신, 발신된 전화번호
type	값이 1이면 수신, 2이면 발신
body	SMS 내용 데이터

[표 3] contact2 DB Calls 테이블

필드명	설명
number	수신, 발신에 사용된 전화번호
type	값이 1이면 수신, 2이면 발신
name	저장된 number에 따른 이름값

[표 4] contact2 DB data 테이블

필드명	설명
data1	성과 이름을 합친 전체 이름과 전화번호
data2	이름란에 해당되는 데이터
data3	성란에 해당되는 데이터

[표 5] browser DB BookMark 테이블

필드명	설명
title	해당url의 타이틀
url	스마트폰 사용자가 접속한 url
visits	해당 url에 방문한 횟수

[표 6] twitter DB statuses 테이블

필드명	설명
content	twitt 데이터
source	twitter 사용 프로그램
souce_url	프로그램에 대한 url 정보

[표 7] search_history DB suggestions 테이블

필드명	설명
data1	map search 데이터

3.2. iOS의 디지털 포렌식 적용법 및 수집

iPhone은 내부 폴더 접근 자체가 금지되어 있다. 폐쇄적 OS 운영방침에 어플리케이션도 내부 탐색이 가능한 어플리케이션은 존재하지 않는다. 하지만 iPhone은 iTunes라는 PC 동기화 프로그램을 사용하며 이 때 iTunes는 Apple사에서 제작한 멀티미디어 플레이어 및 iPod, iPhone 동기화로 인해 PC 백업까지 도와주는 프로그램이다[10]. 윈도우즈용과 맥 OS용 두 가지 버전이 제공되어 iPod 및 iPhone의 각종 어플리케이션을 구매하고 설치하는데 사용된다. 또한 동기화 기능을 기용하여 내부 중요 데이터들이 백업되므로 디지털 증거가 될 수 있는 내용을 수집할 수 있다[11]. 실험에 사용된 iOS는 4.0버전이다.

기본적으로 iTunes를 설치하면 백업 폴더가 하드에 생성되는데 이곳에 iPhone과 동기화한 데이터들이 mddata형태로 저장된다. 파일들은 SQLite Expert로 데이터 확인이 가능하며, 일부 파일은 XML로 되어 있다. 폴더에서 수집해낸 주요 데이터의 폴더명, 파일명은 [표 8]로 정리해 보았다.

[표 8] iOS 주요 증거 데이터 파일

폴더명	파일명	설명
C:\사용자\<계정명>\App Data\Roaming\Apple Computer\MobileSync	31bb7ba8914766d4ba40d6dfb6113c8b614be442.mddata	주소록
	3d0d7e5fb2ce288813306e4d4636395e047a3d28.mddata	SMS
	ff1324e6b949111b2fb449ecddb50c89c3699a78.mddata	통화목록

3.2.1. 수집 데이터 분석

위 [표 8]을 참고로 증거 데이터 폴더 안에 있는 mddata파일을 열었을 때, 주요 데이터의 테이블 내용은 아래 표들과 같다. [표 9]의 주소록 ABPerson 테이블의 경우 사용자 이름을 저장하여 ROWID라는 Key를 이용해 다른 테이블과 관계를 형성하고 있다. 전화번호를 저장하고 있는 [표 10]의 ABMulti-

Value 테이블 record_id가 같은 Key 값으로 적용되는데 두 테이블을 합치면 주소록 데이터 내용을 확인 할 수 있다. [표 11]의 SMS message 테이블의 경우 addres s에 수신번호, text에 메시지 내역이 저장되어 있으며, flags를 이용해 저장된 SMS 데이터가 수신된 데이터인지, 발신된 데이터인지 구분하고 있다. [표 12]의 통화목록 call 테이블은 address에 전화번호가 저장되어 있고, flags에 수신, 발신정보가 4와 5로 나뉘어 저장되어 있는 것을 확인 할 수 있다 [12].

[표 9] 주소록 DB파일의 ABPerson 테이블

필드명	설명
ROWID	다른 테이블과의 식별 Key값
first	이름란에 해당하는 데이터
Last	성란에 해당하는 데이터
Organization	회사란에 해당하는 데이터
Department	부서란에 해당하는 데이터
Note	메모란에 해당하는 데이터

[표 10] 주소록 DB파일의 ABMultiValue 테이블

필드명	설명
record_id	ROWID와 동일한 데이터
value	전화번호

[표 11] SMS DB파일의 message 테이블

필드명	설명
ROWID	다른 테이블과의 식별 Key 값
address	수신번호
text	SMS 내역
flag	값이 2이면 수신, 3이면 발신

[표 12] 통화목록 DB파일의 call 테이블

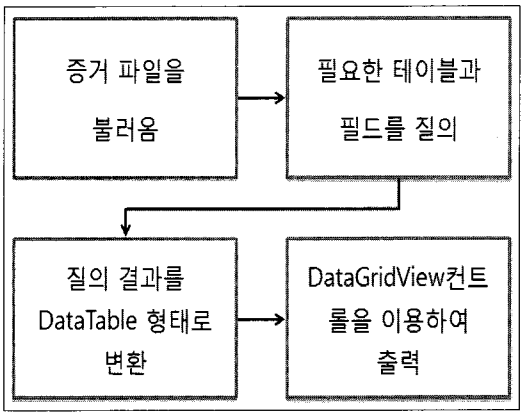
필드명	설명
ROWID	다른 테이블과의 식별 Key 값
address	전화번호
flag	값이 2이면 수신, 3이면 발신

IV. 증거 분석 도구

모바일 포렌식 증거 데이터의 분류와 수집 및 분석 방법과 더불어 현재 국내 스마트폰들 중 보급률이 가장 높은 두 가지 스마트폰의 OS들을 분석하여 각 OS의 소개 및 접근 방법에 대해서 기술하였다. Android 스마트폰으로 실험한 Nexus One에는 PC 동기화 프로그램이 존재하지 않아 기본 기능을 통한 동기화와 더불어 루팅을 통한 디지털 증거의 수집 방법을 다루었고, iOS를 탑재한 iPhone은 Apple의 폐쇄적 정책에 내부 폴더 접근 자체가 제한되어 있었다. 하지만 iTunes라는 PC 동기화 프로그램을 사용하여 iPhone의 내용을 동기화, PC 폴더에 백업함으로써 디지털 증거를 쉽게 수집할 수 있는 방법을 다루었다. 이러한 방법들로 수집한 데이터들을 분석 할 필요가 있으며, 이를 위한 도구를 설계하여 본다.

4.1. 도구 설계

본 도구는 분석한 데이터베이스 파일을 기반으로 앞서 언급한 증거 데이터 테이블의 내용을 보여준다. iOS와 Android는 모두 SQLite를 이용하여 연락처와 SMS 내역 등 주요 증거 데이터를 관리함으로 www.sqlite.org에서 제공하는 C#용 라이브러리를 이용하여 프로그램을 구현하였다. 증거 분석 도구는 증거 데이터베이스 파일을 불러와 필요한 테이블과 필드들을 DataTable 형태로 변환한다. 이 때 iOS와 Android를 구분하여 동작하도록 만들었으며 좌측 박스를 통해 iOS, Android를 구분할 수 있다. 수집하는 데이터는 [표 1], [표 8]에서 나열한 주요 데이터 폴더들의 DB 파일을 수집하였으며, 증거 데이터를 불러왔을 때 메인 필드 상단에 Device Information, Address, SMS, Call History, Twitter GPS, 브라우저로 나누어 각 데이터 들이 보기 쉽게 나열 되도록 하였다. DataTable로 변환한 뒤 출력 결과를 DataGridView 컨트롤을 이용하여 출력하며, 아래 [그림 5]는 도구의 흐름을 도식화하여 나타낸 것이다.

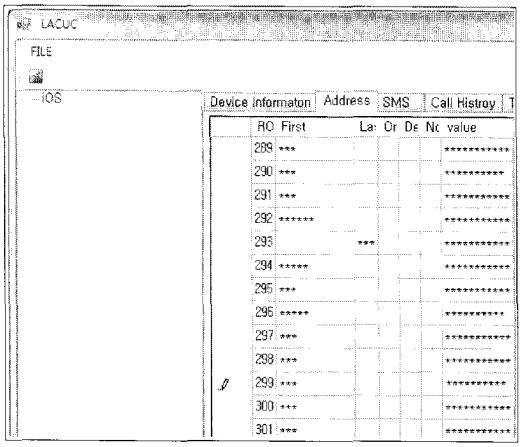


[그림 5] 증거 분석도구 흐름도

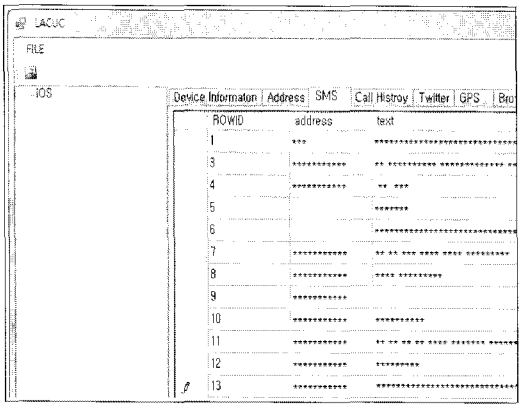
4.2. iOS 데이터 분석

본 도구를 이용하여 iOS의 데이터를 분석하였다. iOS에서 추출한 데이터는 주소록, 통화목록, SMS데이터 내역이며, 주소록의 데이터베이스 파일의 경우 주소록에 등록된 이름과 전화번호가 서로 다른 필드에 존재함으로 이를 연결하는 작업이 필요하다. 주소록의 데이터베이스 파일에 있는 ABPerson 테이블에 등록된 이름 필드와 ABMultiValue에 있는 전화번호 필드를 ROWID Key 값 비교를 통하여 추출 한다. 도구를 이용한 결과는 [그림 6], [그림 7]과 같다.

도구를 이용하여 열람한 결과 주소록의 연락처 SMS 송수신 내역과 메시지 내용, 전화통화 데이터와 송수신 내역 등을 추출할 수 있었다.



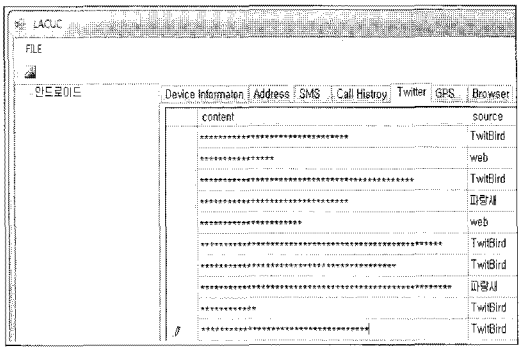
[그림 6] 주소록 데이터



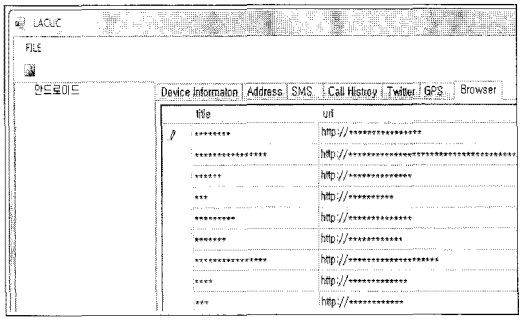
[그림 7] SMS 데이터

4.3. Android 데이터 분석

Android에서 추출한 증거 데이터는 SMS 데이터, twitter 데이터, Map 검색 데이터, 브라우저 사용 데이터로 도구를 통해 분석해 보았다. iOS와 Android는 테이블 구조가 다르므로 별도의 Android 모드를 구현하여 동작하게 하였다.



[그림 8] twitter 데이터

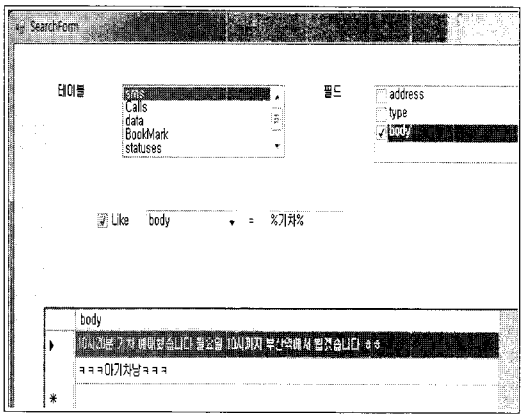


[그림 9] 브라우저 데이터

도구를 사용한 결과 iOS와 마찬가지로 주소록, SMS, 통화목록을 확인 할 수 있었으며, 추가로 twitter와 Map 검색 결과, 브라우저 사용 내역도 추출 할 수 있었다. Android와 iOS의 데이터 분석은 실제 사용하는 스마트폰의 데이터를 추출해 낸 것이므로 개인의 프라이버시를 위해 주요 데이터는 *로 출력시켰다.

4.4. 분석 도구의 활용 방안

분석 도구를 통해 iOS와 Android의 증거 데이터를 열람해 보면 기본적으로 연락처와 SMS, 통화목록은 모두 분석 할 수 있었다. SMS 내용과 통화목록,



〔그림 10〕 도구의 데이터 검색 기능

통화 시간 등을 한눈에 알아 볼 수 있으므로 증거나 단서를 찾을 때 유용하게 사용 할 수 있다. iOS는 별도의 동작을 취하지 않더라도 iTunes의 백업 폴더에서 쉽게 데이터 들을 수집하여 분석 할 수 있었으며, Android의 경우 twitter의 사용 내역과 브라우저의 visit 필드를 이용하여 즐겨 찾는 사이트의 목록 등을 분석 할 수 있고, Map 검색 내역도 확인 할 수 있어 스마트폰 사용자의 행동 패턴을 한 눈에 알아볼 수 있다. 〔그림 10〕과 같이 도구에 있는 검색 기능을 이용하여 스마트폰에서 추출한 데이터들에서 중요 데이터를 한눈에 보기도 가능하며 이러한 기능을 토대로 범죄에 연루된 스마트폰을 포렌식 할 때 많은 도움이 될 것이다.

V. 결 론

본 논문에서는 국내 보급이 원활하게 이루어지는 두 가지 스마트폰의 디지털 증거 수집 방법과 분석에 관해 다루었다. Android에서는 순정상태일 때 수집할 수 있는 데이터와 루팅을 하여야만 수집 할 수 있는 데이터를 분별하여 분석하였고, iOS에서는 I-Tunes 프로그램의 동기화 기능을 이용하여 PC에 저장되어 있는 증거 데이터들을 수집, 분석하였다. 각 OS 별로 증거 데이터가 저장되어 있는 폴더들을 나열하고, 위치를 파악하여 스마트폰을 수집했을 때 재빠른 증거 데이터 확보가 가능하게 되었다. 하지만 현재까지 국내에는 스마트폰에 대한 증거 수집 도구가 미흡한 상황이며, 이에 대해 스마트폰 포렌식의 무결성을 확보하는 것과 동시에 증거 데이터가 수집, 분석되어야할 도구 개발이 시급한 상황이다. 향후 연구로 도구를 이용하여 두 OS의 증거 수집과 분석시 무결성을 어떻게 확보할 것인지에 대해서는 지속적인 연구가 필요하며, 증거 수집 도구의 검색 기능 및 필드의 가독성을 높이고, 수집 및 분석 이후 이를 보고할 수 있는 보고서의 작성, 수집한 데이터의 백업이나 이미징의 연구 등이 필요하다. 앞으로 분석 도구가 갖추어야 할 요구사항을 꾸준히 도출하여 이를 구현 할 수 있는 연구가 필요하다.

참고문헌

〔1〕 한국IDC, "내년부터 안드로이드가 세계 2위 스마트폰 운영체제(OS)가 될 것으로 전망," IDC, 2010년 9월

〔2〕 "3분기 세계 스마트폰 시장 8110만대 출하, 89.5% 성장," IDC 2010년 11월

〔3〕 이규안, 박대우, 신용태, "휴대폰 압수수색 표준절차와 포렌식 무결성 입증," 한국통신학회논문지, Vol3(6), 2009년 6월.

〔4〕 Android Developer, http://developer.android.com/guide/basics/what-is-android.html

〔5〕 Andrew Hoog, "iPhone Forensics," Annual Report on iPhone Forensic Industry - March 2, 2009

〔6〕 Bud Smith, How to do Everything Nexus One, July. 2010.

〔7〕 Android Debug Bridge, http://developer.android.com/guIde/developing/tools/adb.html

〔8〕 구본민, 김주영, 이태림, 신상욱, "Android 기반 스마트폰 디지털 증거 수집," 한국멀티미디어 학회, 추계학술발표대회논문집, 13(2), p15. 2010년 11월

〔9〕 ASTRO File Manager, http://www.metago.net/astro/fm

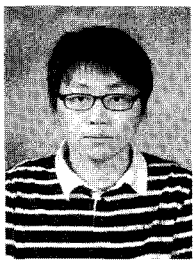
〔10〕 Apple - iTunes, http://www.apple.com/kr/itu nes/what-is/

〔11〕 김주영, 구본민, 이태림, 신상욱, "아이튠즈를 이용한 아이폰 디지털 증거 수집," 한국정보보호학회 영남지부, 학술발표논문집, p55-60, 2010년 4월

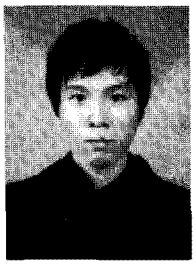
〔12〕 김주영, 구본민, 이태림, 신상욱, "아이폰을 위한 디지털 증거 분석 도구 설계," 한국 멀티미디어학회, 춘계학술발표눈문집, 13(1), p.138 2010년 5월

〈著者紹介〉

구 본 민 (Bon-Min Goo) 정회원
2010년 2월: 동의대학교 컴퓨터공학과 학사
2010년 3월~현재: 부경대학교 정보보호협동과정 석사과정
〈관심분야〉 정보보호, 디지털 포렌식, Android, e-Discovery



김 주 영 (Ju-Young Kim) 정회원
2010년 2월: 부경대학교 컴퓨터멀티미디어학과 학사
2010년 3월~현재: 부경대학교 정보보호협동과정 석사과정
〈관심분야〉 정보보호, 디지털 포렌식, e-Discovery, Cloud Computing



이 태 림 (Tae-Rim Lee) 정회원
2008년 3월: 부경대학교 컴퓨터멀티미디어학과 학사
2010년 2월: 부경대학교 정보보호협동과정 석사
2010년 3월~현재: 부경대학교 정보보호협동과정 박사과정
〈관심분야〉 정보보호, 디지털 포렌식, e-Discovery

신 상 욱 (Sang Uk Shin) 정회원
1995년 2월 : 부경대학교 전자계산학과(학사)
1997년 2월 : 부경대학교 전자계산학과(석사)
2000년 2월 : 부경대학교 전자계산학과(박사)
2000년 4월~2003년 8월 : 한국전자통신연구원 선임연구원
2003년 9월~현재 : 부경대학교 IT융합응용공학과 부교수
〈관심분야〉 디지털 포렌식, 모바일네트워크보안, 암호프로토콜, 멀티미디어콘텐츠보호