Analysis of Smartphone-Based Location Information

Dohyun Kim, Jewan Bang and Sangjin Lee

Abstract Location information is an important factor for figuring out user's behavior in digital forensic investigations. Smartphone-based map applications keep record user's data about location information such as timestamp, GPS information for searched locations. In this paper, we will analyze data generated by famous map applications–Google map, Daum map, Naver map and extract necessary information to assist digital forensic investigations.

Keywords Digital forensics · Location information · Smartphone · Map application

1 Introduction

Recently, Smartphone users steadily keep on growing and its rate is expected to be increased by almost 30% in 2011 in worldwide mobile phone market. Furthermore, its shipments will soon overtake those of PCs shipped (both desktops and notebooks) in 2012. These rapid growth comes from various smartphone applications such as games or useful applications in daily life.

D. Kim (✉) · J. Bang · S. Lee
Center for Information Security Technologies, Korea University, Seoul, South Korea
e-mail: exdus84@korea.ac.kr

J. Bang
e-mail: jwbang@korea.ac.kr

S. Lee
e-mail: sangjin@korea.ac.kr

James J. (Jong Hyuk) Park et al. (eds.), *Computer Science and Convergence*, Lecture Notes in Electrical Engineering 114, DOI: 10.1007/978-94-007-2792-2_5,

Table 1 Application-related data storage path of genaeral, galaxy S smartphone

	Default application	User application	Additional file storage path
General Android Phone	/data/data/package name	/data/data/package name	/mnt/sdcard/package name
Galaxy S	/dbdata/databases/package name	/data/data/package name	/mnt/sdcard/package name

In numerous smartphone-based map applications are most commonly used among users, and it offers users location search, route search, transportation search, destination viewing, bookmark. Whenever a user access this application, user-searched information (starting point, destination, latitude, longitude and so on) and timestamp are automatically recorded in particular files in application. In a view of digital forensic investigations, this information is key evidences to figure out a user's behavior and intention as well as to find a critical clue to a case. Thus, it is necessary for us to research this famous map applications connected to digital forensic investigations.

In this paper, it will be discussed how to extract inside information recorded in particular files through famous map application—Google map, Daum map and Naver map and how to analyze internal data, related to digital forensic investigations. And we suggested digital forensic tool (MapAn) utilizing smartphone-based map application for the investigation.

This paper consists of five parts, not including introduction–related work, the analysis of smartphone-based map applications, tool for analyzing smartphone-based map application, conclusion and future work.

2 Related Work

In this chapter, it will be discussed about a technique to extract files which contain history using an application. In case of Android phone, these data are mainly recorded to SQLite Database files while iPhone recorded to SQLite Database files or plist files according to an application.

2.1 The File Path in Android Phone

Android phone has a different file path to store applications related to Galaxy S and other Android smart phones. In case of general Android phone, default application—SMS/MMS, address book, e-mail and call history as well as user application are installed in the same file path. On the contrary, Galaxy S installs both default and user application in different file path. However, after installation, a file path for both Android phone and Galaxy S become same on account of file download function. These paths presented in Table 1.

Table 2 Map application's function and description

Function	Description
Location Search	Finding destination
Route Search	Looking for the way from current location to destination location
Transportation Search	Finding public transportation to destination
View (Street & Air)	Providing view on the street and air
Bookmark	Storing searched result

Rooting is necessary for extracting files from a path. General rooting is performed, integrity may get damaged, whereas Temporary rooting does not affect any damage to an internal data. Therefore, by performing Temporary rooting, we use ADB (Android Debugger Bridge), type "adb pull [The path for extracting a file from Android Phone] [The path for storing an extracted file]" instruction, and extract the files asked for [1].

2.2 The File Path in iPhone

In case of iPhone, all internal data are encoded; selecting files for extraction is not available. For extracting files without damaging integrity, we use not Jail Breaking but iTunes's Backup function, the software which is able to sync with iPhone, so as to get all Backup files in iPhone.

The path for creating Backup files is "%APPDATA%/Roaming/Apple Computer/MobileSync/Backup/*[Device ID]*". The backup files substitute for the hash value toward the name of the file and are generated in the path. In the process of extracting a file from the path, the real names and path of files need to be figure out among the files named as hash value. With open tool named "mbdbump.exe", not only the files real name, but also file's path to extract [2].

3 Analysis of Smartphone-Based Map Applications

In this chapter, we are going to discuss about the famous smartphone-based map applications and those functions and then analyze files that recorded users history according to an application.

3.1 The Type and Functional Analysis of Map Applications

Google map, Daum map, and Naver map are mainly used as the famous map applications. These map applications offer useful functions such as location search, route search, transportation search, view support and bookmark. The description for each function is presented in Tables 2 and 3.

Table 3 Offered functions by each map application

	Location Search	Route Search	Transportation Search	View (Street & Air)	Bookmark
Google map	O	O	O	X	X
Daum map	O	O	O	O	O
Naver map	O	O	O	O	O

Table 4 Target file of Google Map in Android Phone

File Name	Search_history.db	
Path	General Android Phone	/data/data/com.google.android.apps.maps
	Galaxy S	/dbdata/com.google.android.apps.maps
File Type	SQLite Database	

3.2 Analysis of User History about Map Applications

To analyze the user history of using map applications, the path to files that recorded user history data and its format should be identified. Here are the steps for analyzing the path and the format of files.

First of all, due to the fact that third Party applications record data into files in its own format, files should be analyzed individually according to the applications. Secondly, meaningful data selection and extraction from a lot of data should be conducted to help digital forensic investigations.

In map applications, the file name, path and format that recorded in the user data are given in Table 4, 5, 6, 7, 8, and 9.

Google Map

Android Phone. In Android phone, search "history.db" file record the user history data of Google Map. In viewpoint of digital forensic, meaningful data is data 1 field in suggestions table. When location search is performed, the contents are recorded in order, but the timestamp is not recorded in the field. More recent data is located at the bottom of contents. The meaning of each field is given in Table 10.

iPhone. Unlike Android phone, files recorded user history in iPhone of Google Maps are "b60c382887dfa562166f099f24797e55c12a94e4 (History.plist)" and "a30335a2c 0f0316c9610d868a527b2ade1911542 (com.apple.map.plist)". Both files are formed as plist file. In a view of digital forensic, meaningful data from "b60c382887dfa56216 6f099f24797e55c12a94e4 (History.plist)" file are keyword for location search, latitude and longitude. This file does not contain time information, located at the top of the more recent data is the data retrieved. "a30335a2c0f0316c9610d868a527b2ade 1911542 (com.apple.map.plist)" file located in the most recently conducted searches and searches where the location information(latitude, longitude) and time to have the information [4]. The meaning of each element is in Table 11.

Table 5 Target file of Google Map in iPhone

File Name	b60c382887dfa562166f099f24797e55c12a94e4(History.plist)
Path	%APPDATA%/Roaming/Apple Computer/MobileSync/Backup/*[Device ID]*
File Type	plist
File Name	a30335a2c0f0316c9610d868a527b2ade1911542(com.apple.map.plist)
Path	%APPDATA%/Roaming/Apple Computer/MobileSync/Backup/*[Device ID]*
File Type	plist

Table 6 Target file of Daum Map in Android Phone

File Name	history.db
Path	/data/data/net.daum.android.map/map/data
File Type	SQLite database
File Name	favorite.db
Path	/data/data/net.daum.android.map/map/data/*[Daum Account ID]*
File Type	SQLite database

Table 7 Target file of Daum Map in iPhone

File Name	ae6522d1ef6dd52694d53cc015c04749603ac95a(history.db)
Path	%APPDATA%/Roaming/Apple Computer/MobileSync/Backup/*[Device ID]*
File Type	SQLite database
File Name	59ea2d577b192bcce21149ce2a8385180d72313e(favorite.db)
Path	%APPDATA%/Roaming/Apple Computer/MobileSync/Backup/*[Device ID]*
File Type	SQLite database

Table 8 Target file of Daum Map in iPhone

File Name	mapHistory.db
Path	/data/data/com.nhn.android.nmap/databases
File Type	SQLite database

Table 9 Target file of Daum Map in iPhone

File Name	6be48053cd29804a3a30e78846c30d828c75eb8a(History.db)
Path	%APPDATA%/Roaming/Apple Computer/MobileSync/Backup/*[Device ID]*
File Type	SQLite database
File Name	d5c541e19cdfec4cdbb833719ced812564dd43ba(NMap.db)
Path	%APPDATA%/Roaming/Apple Computer/MobileSync/Backup/*[Device ID]*
File Type	SQLite database

Daum Map

Android Phone. History files of Daum Map in Android phone are shown as "history.db" and "favorite.db". In "history.db" file, there are "route_history" table which contains "startPoint, endPoint, hitcount, and updatetime" fields as well as "word_history" table which takes "key, address, hitcount, updatetime" fields. On the other hand, in "favorite.db" file, "name, and attime" fields exists. Both files contain very much important data in digital forensic investigations and the meaning of each field is displayed in Table 12.

Table 10 Structure of target file for Google Map in Android Phone

File Name	seach_history.db		
Table Name	Suggestions (Location Search)	**Field Name**	**Contents**
		_id	Number
		data1	Keyword

Table 11 Structure of target file for Google Map in iPhone

File Name	b60c382887dfa562166f099f24797e55c12a94e4(History.plist)
Contents	• Result of Location Search • Location of Performed Location Search (Latitude, Longitude)
File Name	a30335a2c0f0316c9610d868a527b2ade1911542(com.apple.map.plist)
Contents	• Last Time of Performed Location Search • Last Location of Performed Location Search (Latitude, Longitude) • Contents of Last Performed Location Search

iPhone. In iPhone, history of Daum map is stored as "ae6522d1ef6dd52694d53cc015 c04749603ac95a (history.db)" and "59ea2d577b192bcce21149ce2a8385180d72313e (favorite. db)" and internal structure is as same as "history.db and favorite.db" in Android phone.

Naver Map

Android Phone. It is "mapHistory.db" file that is stored as history of Naver map in Android phone. Key data as evidence in digital forensics are inside of "Bookmark" table as "title, time, tel, and addr" fields. "uid, and time" fields in "RecentPub" table, "start, end, and time" fields in "RecentRoute" table as well as "uid, and time" fields in "RecentWord" table are meaningful data for digital forensic investigations. (See below Table 13 for each meaning in field.)

iPhone. In iPhone, "6be48053cd29804a3a30e78846c30d828c75eb8a (History.db)" and "d5c5 41e19cdfec4cdbb833719ced812564dd43ba (NMap.db)" are history file of Naver map. In "6be48053cd29804a3 a30e78846c30d828c75eb8a (History.db)" file, not only "uid, and time" fields in "LocHistory" table, "uid, and time" fields in "PubHistory" table, but also "start, destination, and time" fields "RouteHistory" table is essential key in digital forensic perspective. And, in "d5c541e19cdfec4cdbb833719 ced812564dd43ba (NMap.db)" file, in viewpoint of digital forensics, we put emphasis on "title, time, tel, and addr" fields in "Bookmark" table, "uid, and title" fields in "OfflineMapList" table and "uid, start, and destination" fields in "OfflineRouteList". The meaning of each field is shown in Table 14.

4 Tool for Analyzing Smartphone-Based Map Application

When using map application, a user puts the destination where they are looking for into the search bar. Then, he searches for the route, transportation from the present location to the destination and follows the direction to reach the place. When

Table 12 Structure of target file for Daum Map in Android Phone

File Name		seach_history.db	
Table Name	route_history (Route Search)	**Field Name**	**Contents**
		idx	Number
		startPoint	Starting Point for Route Search
		startX	Latitude of Starting Point for Route Search
		startY	Longitude of Starting Point for Route Search
		endpoint	Destination for Route Search
		endX	Latitude of Destination for Route Search
		endY	Longitude of Destination for Route Search
		hitcount	Count of performed Search
		updatetime	Time of performed Search (Unix Time)
	word_history (Location Search)	**Field Name**	**Contents**
		idx	Number
		key	Keyword for Location Search
		chosungKey	Initial Consonant of Keyword
		address	Address of Location for Location Search
		posX	Latitude of Location for Location Search
		posY	Longitude of Location for Location Search
		hitcount	Count of performing search
		updatetime	Time of performed Search (Unix Time)
File Name		seach_history.db	
Table Name	favorite (Bookmark)	**Field Name**	**Contents**
		id	Number
		name	Contents of Bookmark
		type	Location: 100, Route: 200
		cords	Lattitude and Longitude, registered in Bookmark
		attime	Time to Register Bookmark
		mtime	Time of Modified Bookmark
		route_start_name	Starting Point for Route Search
		route_end_name	Destination for Route Search

coming closer to the destination, a user tries to search for the destination again so that they could get more precise information from where they are to where they want to be. In this process, all information is recorded inside of application files whenever he accesses the application. Furthermore, the place where a user was looking for might have been visited. Thus, this recorded information is very much useful in digital forensic investigations.

Table 13 Structure of target file for Naver Map in Android Phone

File Name		mapHistory.db	
Table Name	Bookmark (Bookmark)	**Field Name**	**Contents**
		title	Location of Registered Bookmark
		x	Latitude of Location Registered Bookmark
		y	Longitude of Location Registered Bookmark
		time	Time of Registered Bookmark (Unix Time)
		tel	Telephone Number of Location
		addr	Address of Location of Registered Bookmark
	Bookmark (Transportation Search)	**Field Name**	**Contents**
		uid	Contents for Transportation Search
		time	Time of Transportation Search (Unix Time)
File Name		favorite.db	
Table Name	RecentRoute (Route Search)	**Field Name**	**Contents**
		start	Starting Point for Route Search
		startx	Latitude of Starting Point for Route Search
		starty	Longitude of Starting Point for Route Search
		end	Destination for Route Search
		endx	Latitude of Destination for Route Search
		endy	Longitude of Destination for Route Search
		time	Time of performed Search (Unix Time)
	RecentWord (Location Search)	**Field Name**	**Contents**
		uid	Contents of Location Search
		time	Time of Performed Search (Unix Time)

If a criminal intends to commit a crime, normally he sets the place to do and then visits the scene in advance. Instead of going to the place by himself, he is able to check the place through map application. Not only looking around the place by using street view or air view through location search, but also he can take a picture from many angles, capturing every inch of the scene. Those pictures can be sent to e-mail or sent as MMS message. However, the history data from street and air view function are not recorded individually. Accordingly, making a thorough investigation into photo book, e-mail, MMS records is needed in digital forensic investigations.

History data gives us the information of the user's behavior and his route by the hour and is going to be much helpful factor in digital forensic investigations.

Table 14 Structure of target file for Naver Map in iPhone

File Name		6be48053cd29804a3a30e78846c30d828c75eb8a (History.db)	
Table Name	LocHistory (Location Search)	**Field Name**	**Contents**
		uid	Contents of Location Search
		time	Time of performed Search (Unix Time)
	PubHistory (Transportation Search)	**Field Name**	**Contents**
		uid	Contents of Location Search
		time	Time of Transportation Search (Unix Time)
	RouteHistory (Route Search)	**Field Name**	**Contents**
		start	Starting Point for Route Search
		startx	Latitude of Starting Point for Route Search
		starty	Longitude of Starting Point for Route Search
		destination	Destination for Route Search
		endx	Latitude of Destination for Route Search
		endy	Longitude of Destination for Route Search
		time	Time of performed Search (Unix Time)
File Name		d5c541e19cdfec4cdbb833719ced812564dd43ba (NMap.db)	
Table Name	Bookmark (Bookmark)	**Field Name**	**Contents**
		title	Location of Registered Bookmark
		x	Latitude of Location Registered Bookmark
		y	Longitude of Location Registered Bookmark
		time	Time of Registered Bookmark (Unix Time)
		tel	Telephone Number of Location
		addr	Address of Location of Registered Bookmark
	OfflineMapList (SaveLocation Picture)	**Field Name**	**Contents**
		uid	Time of Saved Location Picture (Unix Time)
		title	Location of Saved Picture
		x	Latitude of the place you saved the picture
		y	Longitude of the place you saved the picture
		radius	The radius of where you saved the picture
	OfflineRouteList (SaveRoute Picture)	**Field Name**	**Contents**
		uid	Time of Saved Route Picture (Unix Time)
		start	Starting Point
		sposx	Latitude of Starting Point
		sposy	Longitude of Stating Point
		destination	Destination
		destposx	Latitude of Destination
		destposy	Longitude of Destination
		xml	Driving directorition from Starting Point to Destination

RecNo	time	type_id	action_id	app_id	content	detail	hitcount	contact_id	deleted_flag
					Click here to define a filter				
1	<null>	지도프로그램	위치 검색	Google 지도	서울특별시 강남구 압구정동		<null>	<null>	<null>
2	<null>	지도프로그램	위치 검색	Google 지도	생명과학관 139호		<null>	<null>	<null>
3	<null>	지도프로그램	위치 검색	Google 지도	고려대학교 생명과학관		<null>	<null>	<null>
4	2010-11-07 14:56:59	지도프로그램	위치 검색	Daum 지도	신막침례교회	<null>	1	<null>	<null>
5	2010-11-07 14:57:00	지도프로그램	경로 검색	Daum 지도	경기도 오산시 대원동	신막침례교회	1	<null>	<null>
6	2011-03-04 17:15:55	지도프로그램	버스노선 검색	Daum 지도	성북20	<null>	2	<null>	<null>
7	2011-03-04 17:22:00	지도프로그램	버스노선 검색	Daum 지도	143	<null>	6	<null>	<null>
8	2011-03-04 17:22:10	지도프로그램	즐겨 찾기	Daum 지도	고려대학교 안암캠퍼스 - 고속터미널역 7호선	<null>	<null>	<null>	<null>
9	2011-03-04 17:23:13	지도프로그램	즐겨 찾기	Naver 지도	서울고속버스터미널	서울특별시 서초구 반포4동 19-4	<null>	1688-4700	<null>
10	2011-03-04 17:24:10	지도프로그램	즐겨 찾기	Naver 지도	고려대학교 안암캠퍼스 - 고속터미널역 7호선	<null>	<null>	<null>	<null>
11	2011-03-04 18:57:30	지도프로그램	위치 검색	Naver 지도	고려대학교	<null>	<null>	<null>	<null>

Fig. 1 Contents of "MapAn.db"

Table 15 Structure of "MapAN.db"

Field Name	Contents
time	Time (Google Maps does not provide)
type_id	Type of Application
action_id	Function of Application
app_id	Application Name
content	Searched Result (Starting Point for Route Search)
detail	Searched Result2 (Destination for Route Search)
hitcount	The Number of Searches Performed (Only provide Daum map)
contact_id	Phone Number for Search Results (Only provide Naver map)
deleted_flag	Display Deleted Records

Despite of these helpful evidences, in investigation process, too much time is consuming in data opening, analyzing, and selecting for needs. Since all different file formats and paths are generated in Google map, Daum map, and N aver map, data in Android phone do not match with those in iPhone. Thus, we need analysis tool for selecting essential data from extracted file and integrating them into singular format.

"MapAn" application is the useful tool for digital forensics by extracting valuable data generated from the files that contain the user data at various angles. Once a user input files that contain user history data, a single database file which called "MapAn.db" comes out and there are information about connect and using hour, the name of application, the searched contents and so forth. By analyzing "MapAn.db" file, we can figure out which map-based application a user use, when he access to the application, what he does with application and where he goes. Coming-out data is appeared in Fig. 1, and Table 15.

5 Conclusion and Future Work

Smartphone-based map application such as Google map, Daum map, and Naver map leaves various information in smartphone. Such information like connect hour or searched information is much valuable in a criminal investigation because it

becomes such a good evidence to find out a criminal. Even though these application is preferred to be analyzed, the numerous applications are out there and have great many approaches to extract data from user's files depending on various smartphones.

In this paper, we suggest "MapAn" that helps us to analyze a file produced from smartphone-based mapping application in a view of digital forensic investigations. Besides "MapAn" application, more effective analysis would be possible if other applications like "Call history and SMS/MMS" can be integrated as well as recovered data changes the shape, combined with a real image map. These application becomes much useful tools for accurate analysis in the future and additional researches should be carried out for future study.

References

1. Lessard J, Kessler GC (2010) Android forensics: simplifying cell phone examinations. Small Scale Disgital Forensics J 4(1):1–12 Sep
2. iPhone Backup Browser, http://code.google.com/p/iphonebackupbrowser/wiki/MbdbMbdx Format
3. Husain MI et al (2011) A simple cost-effective framework for iPhone forensic analysis. Digital Forensics and Cyber Crime. Lecture notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 53. pp 27–37
4. Google Map, http://maps.google.co.kr/maps
5. DaumDNA: openApi mapAPI coordinate system, http://dna.daum.net/apis/maps/coordinate