Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.1, Feb. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.1.109

스마트 기기에 설치된 내비게이션 어플리케이션의 위치 정보 흔적 연구*

연 규 철,† 김 문 호, 김 도 현, 이 상 진‡
고려대학교 정보보호대학원

A Study on Geodata Trace of Navigation Application in Smart Devices*

KyuChul Yeon,† Moon-Ho Kim, Dohyun Kim, Sang-jin Lee‡
Graduate School of Information Security, Korea University

요 약

근래에는 디지털 포렌식 수사에서 다양한 스마트 기기들이 수사 대상에 속하고 있다. 스마트 기기 중에서 지속적인 전원의 공급과 데이터 통신을 하는 스마트 폰에서는 다양한 정보가 획득할 수 있다. 이 논문은 안드로이드 스마트 폰으로부터 획득 가능한 많은 정보 중에서 GPS 기능을 사용하는 내비게이션 어플리케이션을 사용할 때 기기에 남는 흔적에 대한 연구 결과이다. 해외에서 사용되는 어플리케이션과 국내에서 사용되는 어플리케이션 중에서 마켓에서 다운로드 수가 높은 어플리케이션을 선정하여 실험을 하고 분석을 하였으며, 분석 결과가 디지털 포렌식 수사에서 어떠한 의미를 가질 수 있는지 기술하고 있다.

ABSTRACT

Nowadays, smart devices are the target of the digital forensic investigation. Among various smart devices, we can obtain much information from smart phone which is provided with continuous power and used for data communication. This paper deals with the traces to be left in Android smart phones after using the navigation applications with the GPS function. We selected navigation applications(domestic and overseas) which have a high number of download times, anaylzed them and discussed the meaning of the analysis result in digital forensic investigation.

Keywords: Navigation Application, Android, Geodata, Digital Forensic.

I. 서 론

위치 정보는 조사 대상자의 행적을 조사하는데 매우 중요한 정보이다. 위치 정보는 조사 대상자가 주장하는 자신의 알리바이를 입증하거나, 그 주장이 거짓임을 입증하기 위한 중요한 증거 자료로 사용될 수 있다.

이동 경로, 목적지의 위치 등을 알 수 있는 위치 정보를 과거에는 차량에 장착하여 사용하는 PND(Personal Navigation Device)를 통하여 수집 가능하였다. 근래에는 스마트 기기에 GPS Chip이 장착되어 있으며 내비게이션 어플리케이션을 사용자가 다운받아 설치하여 사용하는 형태가 크게 늘어나고 있다. 다양한 스마트 기기 중에서 특히 상시 휴대하고, 지속적인 전원의 공급 및 데이터 통신이 가능한 스마트 폰의 보급으로 별도로 구매해야 하는 PND보다 스마트 폰에서 내비게이션 어플리케이션을 이용하는 사용자가 많아지고 있다[1]. 따라서, 스마트 폰에서 위치 정보 흔적을 확인할 수 있는

Received(09. 17. 2015), Modified(12. 10. 2015), Accepted(12. 11. 2015)
* 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 한국연구재단-공공복지안전사업의 지원을 받아 수행된 연구임(2012M3A2A1051106)
† 주저자, kyuf3@korea.ac.kr
‡ 교신저자, sangjjn@korea.ac.kr(Corresponding author)

내비게이션 어플리케이션의 분석이 중요하다.

본 논문에서는 안드로이드 환경의 스마트 폰에서 GPS 기능을 요구하는 내비게이션 어플리케이션을 사용하였을 경우에 기기에 남게 되는 흔적이 어떠한 것들이 있으며, 어플리케이션에 따른 흔적의 차이에 대하여 소개한다.

II. 관련 연구

2.1 PND(Personal Navigation Device) 동향

과거의 PND는 GPS 기능과 더불어 사용하는 지역의 지도 정보가 들어있는 기기로 자동차에 장착된 형태로 대부분 사용하였다. 때문에 기기내의 지도 정보나 기타 기기에서 사용하는 정보를 업데이트하기 위해서는 대부분 기기 혹은 기기에 장착하는 메모리 카드를 PC에 직접 연결해야만 하였다.

근래에는 자동차에 장착하여 사용하는 기존 기기보다 개인이 일상생활에서 사용하는 스마트 기기에 내비게이션 어플리케이션을 설치하여 내비게이션 기능을 사용하는 사용자가 크게 늘고 있다[1].

PND 사용자의 스마트 기기를 통한 내비게이션 서비스 사용 비중이 지속적으로 늘어나고 있는 이유는 어플리케이션을 마켓에서 다운받아 설치하면 내비게이션 기능을 사용 가능한 GPS가 탑재된 스마트 폰의 보급이 크게 늘고 있기 때문이다. 운전자가 추가적으로 장비를 구입하지 않고 기존에 소유하고 있는 스마트 폰을 이용하여 내비게이션 기능을 사용할 수 있으며, 또한 기존 PND와 달리 실시간 네트워크 통신이 가능하기 때문에 최신 지도의 갱신과 교통사고, 정체와 같은 도로교통상황을 실시간으로 안내하는 것과 같은 편리성 또한 운전자가 자신의 스마트 폰을 PND로써 사용하는 이유가 될 수 있다[2].

스마트 폰을 이용한 내비게이션 어플리케이션을 사용하는 사용자가 늘어나고 있으므로, 이러한 어플리케이션을 사용하였을 경우 기기에 어떤 흔적이 남으며, 흔적으로부터 어떤 정보를 획득 가능한지에 대한 연구가 필요하다.

2.2 안드로이드 기기의 Geodata

전 세계적으로 가장 널리 사용되는 안드로이드 운영체제 기반의 스마트 폰에는 GPS Chip이 내장되어 있다. GPS Chip를 통하여 얻어지는 위도와 경도를 기반으로 한 Geodata는 단순히 지리학적 정보를 떠나 디지털 포렌식 분석에서 큰 의미가 있다[3][4].

대부분의 사람이 항상 소지하고 있는 스마트 폰으로부터[5] 얻어지는 Geodata는 스마트 폰의 소유주가 언제, 어디에 위치하였는지, 이동경로의 출발지와 목적지는 어떻게 되는지 확인할 수 있는 법적 증거로써 매우 중요하다[3][4].

따라서 디지털 포렌식 분석가는 스마트 폰에 존재하는 Geodata가 위조나 변조되어 있는지, 해당 데이터가 어떠한 의미를 갖는 데이터인지 정확하게 분석 가능해야 한다.

스마트 폰에 존재하는 Geodata는 다양한 어플리케이션 사용으로 인하여 남게 된다. 해외 및 국내 지도 어플리케이션[6]과 해외 내비게이션 어플리케이션[7]이 남기는 흔적에 대한 연구 결과는 있으나 국내 내비게이션 어플리케이션 흔적에 대한 연구 결과는 발표된 것이 없다.

지도 어플리케이션을 사용할 때 남게 되는 Geodata는 검색기능으로 인하여 남는 흔적이므로 사용자의 이동경로에 대해서 Geodata를 분석하기 위해서는 내비게이션 어플리케이션에서 남기는 정보에 대한 연구가 필요하다.

III. 실험 방법

안드로이드 스마트 기기에서 동작하며 Google Play에서 다운로드를 제공하는 내비게이션 어플리케이션과 특정 통신사의 스마트 폰에 기본으로 설치되어 있는 내비게이션 어플리케이션을 SHW-M440S (SAMSUNG Galaxy S3 3G) 기기의 Android

Table 1. Install application information in Android smart device

Service Area	Application Name	Developer	Version
Global	Waze	Waze	3.9.4.0
Republic Of Korea	T Map	SK Planet	4.4.5
	KimGiSa	Loc&All	2.6.3
	Olleh Navi	KT Corporation	3.6.7
	Kakao Taxi	Daum Kakao	1.1.7
	T Map Taxi	SK Planet	1.0.4

4.3(JellyBean) 운영체제에 설치를 하여 실험을 진행하였다.

실험은 총 4개의 내비게이션 어플리케이션과 내비게이션 어플리케이션과 연동이 되는 2개의 택시 호출 어플리케이션을 설치하여 실제 사용 후 스마트 폰을 이미징하여 기기에 남는 흔적을 분석하였다.

설치한 내비게이션 어플리케이션은 해외에서 많이 사용되고 있는 Waze와 한국에서 많이 사용되고 있는 T Map, 김기사, 올레 내비이며, 택시 호출 어플리케이션은 카카오택시, T Map 택시이다. 해당 어플리케이션에 대한 상세 정보는 Table 1.과 같다.

IV. 실험 결과

실험 대상 어플리케이션을 사용하였을 때 사용한 기기에 남는 흔적을 분석한 결과 크게 두 가지 형태로 나눌 수 있으며, 이는 목적지의 위치 정보를 저장하는 어플리케이션과 이동 경로만 저장하는 어플리케이션으로 구분된다.

실험 대상 어플리케이션 중 한 개를 제외한 어플리케이션들이 목적지의 위치 정보를 저장하고 있으며, 실험 결과를 정리한 Table 2.를 통하여 확인할 수 있다.

목적지의 위치 정보 흔적이 남는 어플리케이션들은 어플리케이션에 따라 마지막 어플리케이션 종료 위치, 출발 지점 위치, 목적지 실제 도착 여부에 대한 정보를 가지고 있다.

스마트 기기에 남는 흔적은 기본적으로 SqlLite 형태의 DB 파일에 존재하며, 텍스트 혹은 XML 파일에 추가적인 흔적이 남는다. 이 파일들을 분석하여 Fig. 1.과 같이 스마트 기기 사용자의 목적지를 파악 가능하다.

각각의 실험 대상 어플리케이션을 사용하였을 때 스마트 기기에 남는 흔적에 대한 자세한 정보는 다음

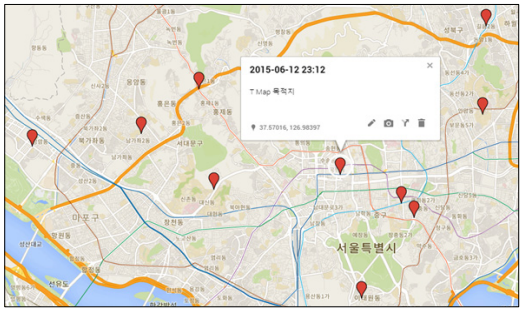

Fig. 1. Application analysis result

소단원에 포함되어 있다.

4.1 Waze 어플리케이션

Waze 어플리케이션은 내비게이션 기능을 사용하였을 때 Table 3.과 같은 파일에 사용 흔적이 남는다.

user.db 파일에는 "PLACES" 테이블에 목적지의 주소와 위치(위도, 경도), 길 안내 기능을 시작한 시점의 시간이 저장된다. 이때 저장되는 시간은 UNIX TIME 포맷으로 저장된다.

session 파일에는 마지막으로 어플리케이션을 종료한 위치(위도, 경도), 가장 최근에 안내한 목적지의 위치(위도, 경도), 목적지 명에 대한 정보가 남는다.

```
14  HoldLock.Position: 34794810, 32106010
15  HoldLock.Direction: 0
16  Location.Position: 127126149,37389002
17  ORIG_GPS.Position: 34794810, 32106010
```

Fig. 2. GEO data of last application termination in session file

Table 3. Artifact file list of Waze Application

Directory	File Name	File Type
/data/data/com.waze	user.db	SQLite
	session	TEXT

Table 2. Application analysis result

Artifact Information	Waze	T Map	KimGisa	Olleh Navi	KakaoTaxi	T Map Taxi
Driving path	X	X	O	X	X	X
Application terminate	O	O	X	X	X	O
Starting point	X	X	X	X	O	X
Destination point	O	O	X	O	O	O
Destination arrival status	X	O	X	X	X	X
Artifact file type	SQLite, Text	SQLite, XML	SQLite	SQLite	SQLite	SQLite, XML

```
Push Notifications.Request shown: yes
Navigation.Last position: 127125793,37388698
Navigation.Last dest name: 이매한신아파트
Navigation.Is navigating: 0
```

Fig. 3. GEO data of recent destination in session file

4.2 T Map 어플리케이션

T Map 어플리케이션은 내비게이션 기능을 사용하였을 때 Table 4.와 같은 파일에 사용 흔적이 남는다.

recent.db 파일에는 "Recent" 테이블에 목적지명과 목적지의 주소, 위치(위도, 경도), 길 안내 기능을 시작한 시점의 시간이 저장된다. 이때 저장되는 시간은 UNIX TIME 포맷으로 저장된다. 저장되는 목적지의 주소는 어플리케이션의 안내를 받아 목적지까지 도착한 경우에만 저장되고, 목적지에 도착하기 전 내비게이션 기능 종료 시 "null"로 저장된다. 이를 통하여 어플리케이션의 안내를 받아 목적지에 도착하였는지에 대한 여부를 판단할 수 있다.

분석 대상 XML 형식의 파일은 2개이며, 각각의 XML 파일에는 서로 다른 정보가 남는다.

가장 최근에 지정한 목적지의 이름, 도착 여부에 대한 정보는 route_guide_termination_info.xml (Fig. 4.) 파일에 저장된다.

마지막으로 어플리케이션을 종료한 위치(위도, 경도)에 대한 정보는 tmap_setting_display.xml(Fig. 5) 파일에 저장된다.

Table 4. Artifact file list of T Map Application

Directory	File Name	File Type
/data/data/com.skt.skaf.l001mtm091/databases	recent.db	SQLite
/data/data/com.skt.skaf.l001mtm091/shared_prefs	route_guide_termination_info.xml	XML
	tmap_setting_display.xml	XML

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <int name="route_guide_route_option" value="1" />
    <string name="route_guide_destination_name">이매촌동부코오롱아파트</string>
    <string name="route_guide_destination_weather_condition">SKY_O01</string>
    <string name="route_guide_destination_weather_rainfall">0.00</string>
    <string name="route_guide_destination_weather_temperature">10.00</string>
    <boolean name="route_guide_termination" value="false" />
</map>
```

Fig. 4. XML of route_guide_termination_info.xml file

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="set_prev_position_lat">37.58474979503574</string>
    <string name="set_prev_position_lon">127.02784876533433</string>
    <int name="set_tbt_position_x" value="220" />
    <int name="set_tbt_position_y" value="226" />
</map>
```

Fig. 5. XML of tmap_setting_display.xml file

4.3 김기사 어플리케이션

김기사 어플리케이션은 내비게이션 기능을 사용하였을 때 Table 5.와 같은 파일에 사용 흔적이 남는다.

KimGisa 파일의 "KimGisa_dirSnd" 테이블을 분석하여 사용자가 이동하는 동안 지나간 장소명과 시간 정보를 획득 가능하다. 시간 정보는 "YYMMDDHHmmSS"의 형태로 저장된다.

해당 어플리케이션은 다른 실험 대상 어플리케이션과는 다르게 사용 후 남게 되는 정보들을 분석하여 Fig. 6.과 같이 특정 시간에 어느 위치를 지나갔는지 이동경로를 분석할 수 있다.

Table 5. Artifact file list of KimGisa Application

Directory	File Name	File Type
/data/data/com.locnall.Kim.GiSa/databases	KimGisa	SQLite

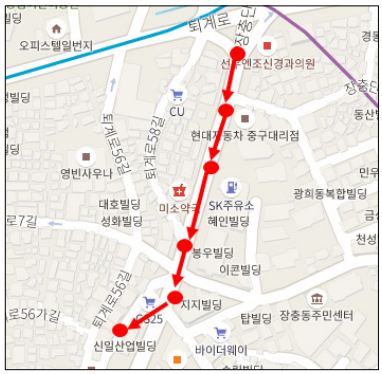

Fig. 6. Drive path analysis with KimGisa Artifact

4.4 올레 내비 어플리케이션

올레 내비 어플리케이션은 내비게이션 기능을 사용하였을 때 Table 6.과 같은 파일에 사용 흔적이 남는다.

Db_RecentDestination 파일의 "Tbl_Recent Destination" 테이블을 분석하여 사용자가 목적지

Table 6. Artifact file list of Olleh Navi Application

Directory	File Name	File Type
/data/data/kt.navi/databases	Db_RecentDestination	SQLite

로 지정한 위치 명, 목적지 주소, 위치(위도, 경도)에 대한 정보를 획득할 수 있다.

4.5 카카오택시 어플리케이션

카카오택시 어플리케이션은 택시 호출 기능을 사용하였을 때 Table 7.과 같은 파일에 사용 흔적이 남는다.

data.db 파일의 "location_item" 테이블을 분석하여 사용자가 지정한 출발지와 도착지의 위치(위도, 경도), 위치 명, 주소, 택시 호출 기능을 사용한 시점의 시간정보를 획득할 수 있다. 이때 저장되는 시간은 UNIX TIME 포맷으로 저장된다.

Table 7. Artifact file list of KakaoTaxi Application

Directory	File Name	File Type
/data/data/com.kakao.taxi/databases	data.db	SQLite

4.6 T Map 택시 어플리케이션

T Map 어플리케이션은 택시 호출 기능을 사용하였을 때 Table 8.과 같은 파일에 사용 흔적이 남는다.

TMapPassenger 파일의 "ADDRESS" 테이블을 분석하여 사용자가 택시 호출 기능을 사용할 때 목적지로 지정한 위치의 목적지 명, 주소, 위치(위도, 경도)에 대한 정보를 획득할 수 있다.

com.skplanet.tmaptaxi.android.passenger.xml 파일은 분석 시 해당 어플리케이션을 마지막으로 종료한 위치의 위도, 경도 정보와 마지막으로 실행한 시점의 시간 정보를 획득할 수 있다.

Table 8. Artifact file list of T Map Taxi Application

Directory	File Name	File Type
/data/data/com.skplanet.tmaptaxi.android.passenger/databases	TMapPassenger	SQLite
/data/data/com.skplanet.tmaptaxi.android.passenger/shared_prefs	com.skplanet.tmaptaxi.android.passenger.xml	XML

V. 결론 및 향후 연구

안드로이드 기반의 스마트 기기에서 사용되는 내비게이션 어플리케이션은 어플리케이션 사용 시 기기에 남는 정보의 차이가 있어 분석 시 획득한 정보가 다르다.

분석 결과 어플리케이션의 종류에 따라 기기에 남은 정보가 디지털 포렌식 수사 시 웹 브라우저의 기록과 같은 정황 증거로써 활용되거나, 분석 대상의 스마트 기기가 특정 시간대에 특정 위치에 존재하였다는 것을 입증하는데 중요한 증거로써 활용할 수도 있다.

SQLite DB파일에는 과거부터 현재까지 기록들이 시간 정보와 함께 저장되고, XML이나 텍스트 파일에는 가장 최근에 어플리케이션을 사용한 데이터가 남게 되므로 이를 분석하면 목적지에 실제로 도착하였는지, 마지막으로 어플리케이션을 종료한 위치가 어디였는지, 특정 시간에 어디를 지나고 있었는지에 대한 정보를 획득할 수 있다. 이러한 정보들은 포렌식 수사 시 매우 중요한 증거가 될 수 있을 것이다.

실험 대상으로 선정한 어플리케이션 외에도 구글 공식 마켓이나 각 이동통신사의 마켓에는 직접적으로 내비게이션의 역할을 하는 어플리케이션이나 이러한 어플리케이션과 연동 혹은 지도 어플리케이션과 연동되어 사용가능한 많은 어플리케이션이 존재하며, Table 2.와 같이 사용 시 기기에 남아 포렌식 수사에 증거로써 활용 가능한 정보들도 어플리케이션에 따라 차이가 존재한다. 실험에 포함된 어플리케이션 외에도 국내 및 해외에서 사용되는 내비게이션 역할을 하는 어플리케이션에 대하여 분석 시 수사에 증거로 활용 가능한 정보들을 파악하여 분석 가이드 라인을 작성한다면, 수사에서 조사 대상자의 행적을 파악하기 위한 스마트 기기 분석에 많은 도움이 될 수 있을 것이다.

향후에는 앞서 말한 스마트 기기에 대한 분석 가이드 라인을 작성하기 위한 추가적인 어플리케이션 사용 흔적 분석에 대한 연구와 더불어, 기존에 알려진 스마트 기기에 남게 되는 정보 외에 디지털 포렌식 수사에서 증거로 활용 가능한 정보들에 대하여 연구를 진행할 예정이다.

References

〔1〕 M2M.World.News, "Global PND shipments declined to 33 million units in 2011 as competition from navigation apps intensified," http://m2mworldnews.com/2012/01/17/66889-global-pnd-shipments-declined-to-33-million-units-in-2011-as-competition-from-navigation-apps-intensified/, Jan 17, 2012.

〔2〕 ZDNET, "Smartphone for GPS Navigation is better than a dedicated device," http://www.zdnet.com/article/smartphone-for-gps-navigation-is-better-than-a-dedicated-device/, Jun 28, 2011.

〔3〕 Stefan Maus, Hans Höfken and Marko Schuba, "Forensic Analysis of Geodata in Android Smartphones," International Conference on Cybercrime, Security and Digital Forensics, Jun. 2011.

〔4〕 Yi-Hua Weng, Fu-Shing Sun and Jeffry D. Grigsby, "GeoTools: An android phone application in geology," Computer & Geosciences 44, pp. 24-30, 2012.

〔5〕 L. Barkhuus and V. Polichar, "Empowerment through seamfulness: Smartphones in everyday life," Personal and Ubiquitous Computing, vol. 15(6), pp. 629 - 639, 2011.

〔6〕 Dohyun Kim, Jewan Bang, and Sangjin Lee, "Analysis of Smartphone-Based Location Information," Computer Science and Convergence. LNEE, Vol. 114, pp. 43-53, 2012.

〔7〕 Nhien-An Le-Khac, Mark Roeloffs and Tahar Kechadi, "FORENSIC ANALYSIS OF THE TOMTOM NAVIGATION APPLICATION," International Federation for Information Processing, IFIP AICT 433, pp. 267 - 276, 2014.

〔8〕 Namheun Son, Yunho Lee, Dohyun Kim, Joshua I. James and Sangjin Lee, "A study of user data integrity during acquisition of Android devices," Digital Investigation 10, pp. S3-S11, 2013.

〈저자소개〉

연 규 철 (KyuChul Yeon) 학생회원
2014년 2월: 홍익대학교 컴퓨터정보통신공학과 공학사
2014년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 디지털 포렌식, 모바일 포렌식, 사이버 범죄 수사

김 문 호 (Moon-Ho Kim) 학생회원
2004년 3월: 육군사관학교 일본어과 졸업
2014년 3월~2016년 2월: 고려대학교 정보보호대학원 석사
〈관심분야〉 디지털 포렌식, 정보보호

김 도 현 (Dohyun Kim) 학생회원
2011년 2월: 서울과학기술대학교 정보통신대학 컴퓨터공학 공학사
2011년 3월~2013년 8월: 고려대학교 정보보호대학원 석사
2013년 9월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 디지털 포렌식, 모바일 포렌식, 파일 시스템

이 상 진 (Sang-jin Lee) 종신회원
1987년 2월: 고려대학교 수학과 학사
1989년 2월: 고려대학교 수학과 석사
1994년 8월: 고려대학교 수학과 박사
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
2015년 1월~현재: 고려대학교 정보보호대학원 부원장
〈관심분야〉 디지털 포렌식, 심층 암호, 해쉬 함수