ISSN(Print) : 1976-5304, ISSN(Online) : 2713-931X
https://kdfs.jams.or.kr, DOI : 10.22798/kdfs.2022.16.2.163

안드로이드 환경에서의 지도 애플리케이션 아티팩트 분석 및 복호화 방안 연구

박 귀 은*, 강 수 진*, 김 종 성**,***
국민대학교 금융정보보안학과 (대학원생)*, (교수)**,
국민대학교 정보보안암호수학과(교수)***

A Study on Decryption Method and Artifacts Analysis of Map Applications in Android

Gwuieun Park*, Soojin Kang*, Jongsung Kim,*****
Dept. of Financial Information Security, Kookmin University (Graduate Student)*, (Professor)**
Dept. of Information Security, Cryptology and Mathematics, Kookmin University (Professor)***

요 약

지도 애플리케이션은 내비게이션, 경로 검색, 대중교통 길찾기 및 교통 상황 서비스 등 다양한 위치 기반 서비스 제공으로 스마트폰 사용자들에게 필수 애플리케이션으로 자리 잡고 있다. 이때 생성되는 사용자의 이동 경로와 목적지의 위치 정보는 시간 정보와 결합하여 디지털 포렌식 관점에서 중요한 데이터로 사용될 수 있다. 따라서 사전에 지도 애플리케이션 데이터를 선별하여 증거로써 활용할 수 있도록 수집하고 분석하는 연구가 필요하다. 본 논문에서는 지도 및 내비게이션에 해당하는 애플리케이션 중 사용량이 가장 많은 네이버 지도, TMAP과 카카오맵을 분석하였다. 안드로이드 환경에서 각 애플리케이션 사용으로 생성되는 아티팩트를 사용자 행위 기반으로 식별하고 디지털 포렌식 관점에서 주요한 데이터를 획득하였다. TMAP과 카카오맵은 모든 데이터가 평문 형태로 저장되어 있으며, 사용자 행위 중심의 아티팩트를 분석하였다. 네이버 지도는 주요 데이터베이스 파일을 암호화하여 저장하며, Android Keystore를 사용하여 암호화에 사용되는 암호키인 passphrase를 보관한다. 따라서 API Hooking을 통해 복호화된 passphrase를 추출하여 암호화된 데이터베이스 파일을 복호화하였다. 이를 통해 네이버 지도에 존재하는 위치 정보와 관련된 아티팩트를 분석하였다.

주제어 : 지도 애플리케이션, 네이버 지도, TMAP, 카카오맵, 아티팩트, 복호화, 디지털 포렌식

ABSTRACT

Map applications are becoming an essential application for smartphone users by providing various location-based services such as navigation, route search, public transportation directions, and traffic information. At this time, The location information of user travel paths and destinations generated by the use of the application can be combined with time to be used as important data from a digital forensics perspective. Therefore, it is necessary to collocet and analyze map application data in advance so that it can be used as evidence. In this paper, we analyzed Naver Map, TMAP and Kakao Map which are used the most among maps and navigation applications. We identified the artifacts generated by the use of each application in the Android environment based on user behavior and obtained important data from a digital forensic perspective. We found that TMAP and Kakao Map store all data in plaintext, and we analyzed user artifacts in the data. However, Naver Maps encrypts and stores main database files, and uses Android Keystore to archive the passphrase, the encryption key used for encryption. We decrypted the encrypted database by hooking the API to extract the decrypted passphrase. Through this, we analyzed artifacts related to location information on Naver Map.

Key Words : Map application, Naver map, TMAP, Kakao map, Artifact, Decryption, Digital Forensics

※ 이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2021-0-00540, GPU/ASIC 기반 암호알고리즘 고속화 설계 및 구현 기술개발)
- Received 19 April 2022, Revised 06 May 2022, Accepted 27 June 2022
- 제1저자(First Author) : Gwuieun Park (Email : dhnr16@kookmin.ac.kr)
- 교신저자(Corresponding Author) : Jongsung Kim (Email : jskim@kookmin.ac.kr)

Ⅰ. 서 론

지도 애플리케이션은 위치 기반 서비스를 제공하는 대표적인 애플리케이션이다. 이와 같은 애플리케이션은 사용자가 설치 후 삭제하지 않고 사용하는 비율이 높으며, 점차 스마트폰에 필수적인 요소로 자리하고 있다. 지도 애플리케이션은 사용자의 실시간 위치를 기반으로 서비스를 제공하므로 애플리케이션 사용에 따라 검색 기록, 이동 경로, 목적지 위치나 사용자의 마지막 위치 데이터 등이 저장된다. 이는 특정 시간과 결합하여 디지털 포렌식 수사 관점에서 사용자 위치 추정에 활용될 수 있다. 그러나 애플리케이션마다 저장되는 형태와 데이터 타입이 다르므로 데이터 수집 방안 및 주요 데이터를 식별하는 연구가 선행되어야 한다.

본 논문에서는 2021년 12월 사용자 수를 기준으로 지도 및 내비게이션에 해당하는 상위 3개 애플리케이션인 네이버 지도, TMAP 및 카카오맵의 분석을 진행하였다[2]. 특히 네이버 지도와 카카오맵은 코로나19와 관련된 잔여 백신 확인 및 예약, 검사기관 혼잡도 정보[3] 등을 제공하여 사용자와 실행 횟수가 증가하였다. 따라서 위의 3가지 애플리케이션을 분석하여 사용자 행위를 중심으로 생성되는 사용자 위치 데이터를 선별하고, 증거로써 활용 가능한 데이터를 분류하였다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 기술하며, 3장에서는 분석 환경과 주요 연구 결과를 요약한다. 4장에서는 네이버 지도를 분석하여 암호화된 데이터에 대한 복호화 방안을 제시하고, 복호화한 데이터를 중심으로 사용자 아티팩트를 분류한다. 5장과 6장에서는 각각 TMAP과 카카오맵을 분석하여 주요 아티팩트를 식별한다. 마지막 7장에서는 결론으로 마무리한다.

Ⅱ. 관련 연구

지도 애플리케이션 사용으로 생성되는 위치 정보, 검색 기록 관련 데이터, 시간 정보와 사용자 정보 등은 디지털 포렌식 수사관점에서 중요한 증거로 활용될 수 있다. 이에 따라 애플리케이션 사용으로 생성되는 데이터 내 존재하는 주요 위치 정보를 파악하고 의미 있는 데이터 획득을 위한 지속적인 연구가 진행되고 있다. Seungwon Jung 등은 안드로이드 스마트폰에 선탑재된 애플리케이션 중 Google Map을 포함한 5가지 애플리케이션을 대상으로 위치 정보와 시간 정보를 결합하여 획득할 수 있는 데이터를 통해 이동 경로 추적 방안 및 경로를 추적할 수 있는 자동화 도구를 개발하였다[4]. Jason Moore 등은 모바일 GPS 지도 애플리케이션인 Google Map, Apple Map, Waze, MapQuest, Bing Map과 Scout GPS 6종을 대상으로 각각 안드로이드와 iOS 환경에서 주소, 위도, 경도 지점 등 사용자의 검색 기록과 관련된 많은 데이터가 스마트폰에 저장되어 있음을 밝혀냈다[5]. Yongseok Choi 등은 국내 내비게이션인 맵피, 아이나비, 지니 및 아틀란의 사용 흔적 정보 파일을 분석함으로써 사용자의 행위 추적과 차량 이동 정보 등의 데이터를 획득하였다[6]. 국외에서는 Beverley Nutter이 TomTom 내비게이션을 대상으로 위치 정보, 목적지 검색 기록과 삭제된 데이터 획득 방법 등 증거 가치가 있는 데이터를 식별하였고[7], Xenia Semenova 등은 안드로이드 환경에서 2GIS 내비게이션 애플리케이션을 대상으로 디지털 포렌식 관점에서 사용자 중심의 주요 아티팩트 분석 결과를 정리하였다[8].

본 논문에서 분석한 네이버 지도, TMAP 및 카카오맵에 관한 연구는 다수 존재한다. Dohyun Kim 등은 2012년 기준 Google Map, Naver Map 및 Daum Map을 대상으로 안드로이드와 iOS 환경에서 검색 기록 관련 타임스탬프, GPS 정보와 같은 위치 정보와 사용자 흔적 등을 분석하였다[9]. Youngjun Son 등은 Naver Map(2014년 기준 버전 4.0.1), Daum Map(2014년 기준 버전 3.7.0) 및 Google Map과 내비게이션 애플리케이션 2종을 대상으로 안드로이드 스마트폰에 저장되는 위치 정보 데이터의 종류와 각 애플리케이션에 따라 생성되는 경로, 검색 기록에 대하여 주요 데이터를 선별하였다[10]. KyuChul Yeon 등은 안드로이드 환경에서 T map(2016년 기준 버전 4.4.5) 외 3종의 지도 및 내비게이션 애플리케이션과 2종의 택시 애플리케이션을 대상으로 목적지의 위치 정보와 이동 경로 정보를 각각 분류하여 아티팩트 분석 결과를 제시하였다[11]. 본 논문에서 분석한 네이버 지도, TMAP 및 카카오맵은 2021년 12월 기준 최신 버전으로 업데이트가 진행되며 기존 연구와 비교하여 다양한 기능이 추가되었다. 따라서 기존에 연구된 정보 외에도 디지털 포렌식 관점에서 유용하게 활용될 수 있는 새로운 아티팩트가 존재하며, 업데이트에 따라 데이터 저장 형태가 변경될 수 있으므로 최신 버전에서의 분석을 수행한다. 또한, 각 애플리케이션에서 획득할 수 있는 아티팩트를 사용자 행위 중심으로 분석하고 정리한다.

Ⅲ. 분석 환경 및 연구 결과

본 논문에서는 안드로이드 환경에서 2021년 12월 기준 최신 버전인 네이버 지도, TMAP 및 카카오맵을 분석하였다. 애플리케이션 다운로드 수는 모두 오천만 이상으로 다수의 사용자가 사용하고 있다. 스마트폰에서 각 애플리케이션을 사용한 후 안드로이드에서 제공하는 ADB (Android Debug Bridge)[12]를 활용하여 사용자 행위에 따라 생성되는 내부 데이터를 추출하였다. 이후 추출한 데이터 형태에 따라 DB Browser, MongoDB Realm Studio, HxD, DCode와 JEB Decompiler 분석 도구를 적합하게 활용하였다. 다음 [표 1]은 분석 환경과 사용 도구를 정리한 표이다.

〈Table 1〉 Analysis environment

Category	Name	Version
Application (Package name)	Naver map (com.nhn.android.nmap)	5.15.2.7
	TMAP (com.skt.tmap.ku)	9.3.0
	Kakao map (net.daum.android.map)	5.0.5
Smartphone	Pixel 4a	Android 11
PC	Windows 11 Pro	-
Analysis Tool	DB Browser for SQLite (SQLite Viewer)	3.12.2
	MongoDB Realm Editor	11.1.1
	HxD (Hex Viewer)	2.5
	DCode (Time Decoder)	5.5
	JEB Decompiler Pro (Android Application Decompiler)	4.11.0

3가지 지도 애플리케이션을 분석한 결과 사용자 행위에 따라 생성되는 데이터는 검색 기록 정보, 사용자 및 위치 정보, 즐겨찾기 및 집, 회사 정보, 이미지 정보로 나눌 수 있다. 애플리케이션마다 저장되는 데이터뿐 아니라 암호화 유무에 따라 획득 가능한 아티팩트도 차이가 존재한다. 분석 결과를 정리하면 [표 2]와 같다.

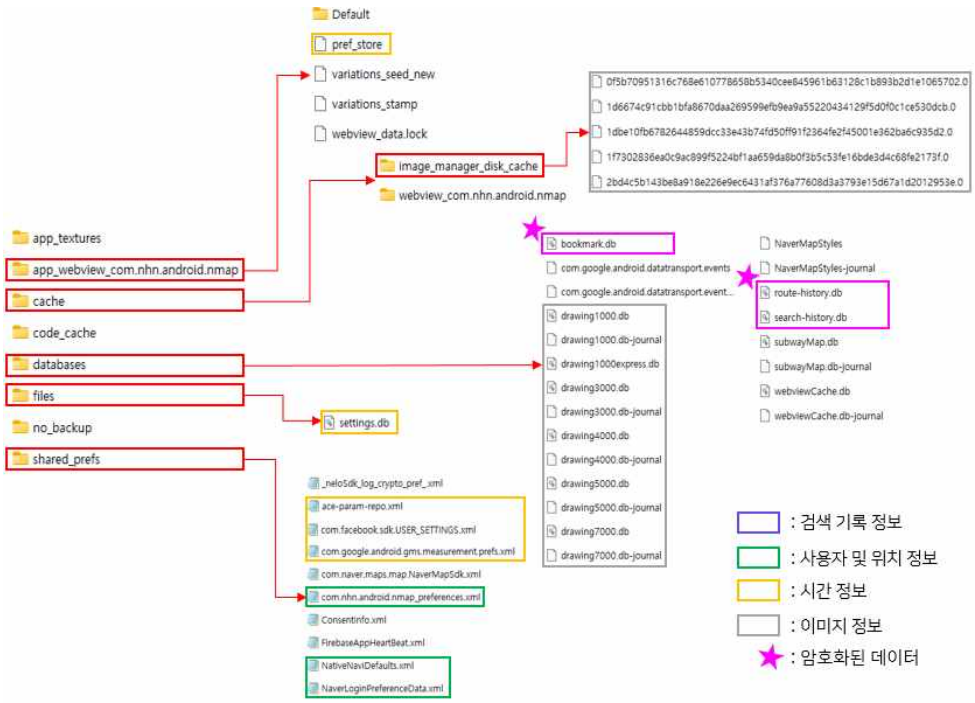
〈Table 2〉 Analysis result

Data type		Naver map	TMAP	Kakao map
Data encryption		O	X	X
Search history		*	O	O
Uesr information		O	O	O
Location	User's location	O	O	X
	Map location	O	X	O
Bookmark information		*	O	O
Home/Office information		X	O	O
Image	User confirmation	O	X	O
	User's subway screen	X	X	O

O : Plain data
X : Not exist
*: Encrypted data

Ⅳ. 네이버 지도 아티팩트 분석

네이버 지도는 2002년 서비스가 시작되어, 2021년 8월 기준 한국인이 가장 많이 사용하는 지도 애플리케이션으로 선정되었다[13]. 네이버 지도는 사용자 계정 등록 없이 사용 가능하지만, 즐겨찾기 및 집, 회사 설정과 네이버 블로그와 연관된 MY 플레이스 기능 등 일부 기능에 대해 사용이 제한된다. 주요 데이터 경로는 (그림 1)과 같으며, 검색 기록, 사용자 및 위치, 즐겨찾기와 시간 정보 등을 저장한다. databases 디렉터리의 bookmark.db, search-history.db 및 route-history.db 파일 모두 데이터베이스 암호화되어 있으며, 그 외의 데이터는 평문 형태로 저장된다. 로그아웃 후 재로그인하는 경우와 애플리케이션 삭제 후 재설치하는 경우 기존 데이터를 모두 획득할 수 있다.



〈Figure 1〉 Data structure of Naver map

4.1 암호화 프로세스 분석

네이버 지도는 주요 사용자 데이터가 저장된 bookmark.db, search-history.db와 route-history.db 파일의 전체를 SQLCipher4 알고리즘으로 암호화하여 저장한다. SQLCipher4의 default 파라미터를 사용하며, 상세 파라미터는 다음과 같다.

HMAC/KDF Algorithm = SHA512
Pagesize = 4,096 bytes
Key Derivation Function Iteration = 256,000

네이버 지도는 암호화에 사용하는 암호키인 passphrase를 안전하게 보관하기 위해 Android Keystore를 사용한다. Android Keystore는 안드로이드의 컨테이너 속에 암호키를 저장하며 암/복호화 작업 시 시스템 프로세스로부터 키를 사용할 수 있다. 이를 통해 키 사용 시기와 방법을 제한하여 기기 외부에서 키를 추출할 수 없도록 한다. 데이터베이스 암호화에 사용된 passphrase는 Android Keystore에 저장된 키를 사용하여 RSA/ECB/PKCS1Padding으로 암호화한다. 해당 알고리즘은 Java의 Cipher instance 중 하나로 PKCS1에 정의된 OAEP 패딩을 활용한 RSA 암호화 기법이다[14]. 이후 암호화된 passphrase를 base64로 인코딩하여 (그림 2)와 같이 shared_prefs/com.nhn.android.nmap_preferences.xml 파일 내 저장한다. 따라서 데이터베이스 복호화를 위해 Android Keystore로 복호화된 passphrase를 획득하는 과정이 필요하다.

com.nhn.android.nmap_preferences.xml

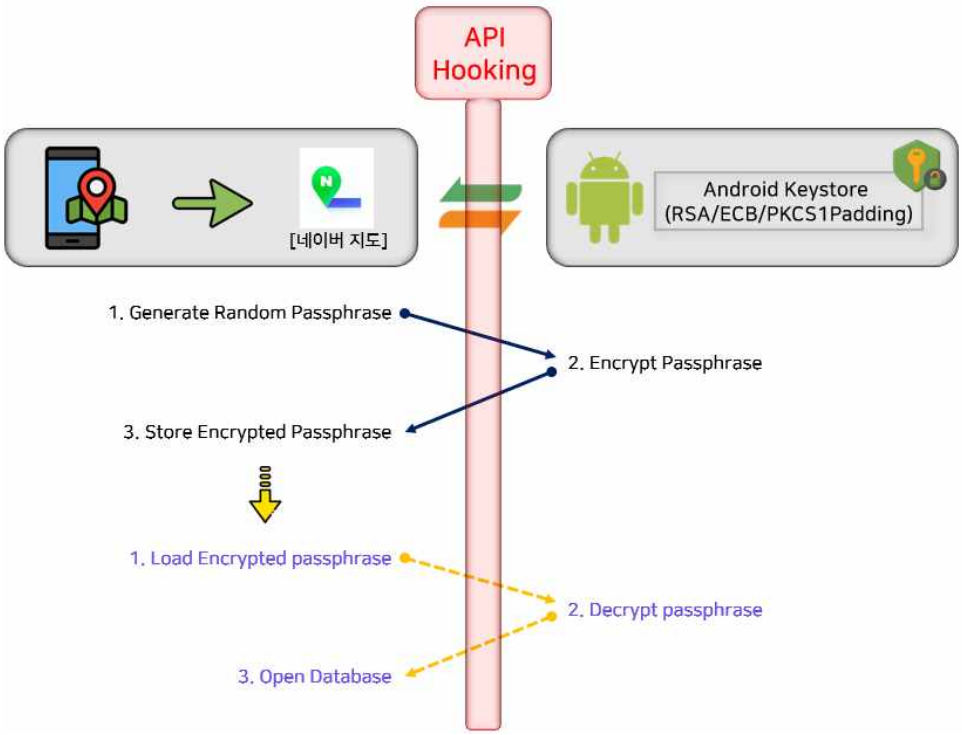
<string name="BOOKMARK_CACHE_PASSPHRASE">dfaz7B3vFzlil+4vJkMJ95g+zj1tRl4gJNgbNMPDEu4yOFkgQ5A1kZkXkXJytdPxSt1f8FwnFqzP
PWhh+vgA3hyc7s0sglouuc2876AeGoUWHU6hfunQaPXVKlAdQPnCY/WCNQ1FPDx6SrA5d/z73T2T sUpEAZi3GwP2jPDtFLNq3Qxs5oReGzSqYMCkpeb+2/m//ixLOHyU2CcgxUm+LoXTIIC9tFeb2G9+
Fz5DZ9ltmjqrRxkabTa3my0DNIh7zFXIj3GiSCQb9ldXG7c0wwolfOCzAzuZk6356IG709ctWoYL aOjt+jMnHijhMFLOOSTwp4/6+z06vXiu/RK/jA== </string>

<string name="SEARCH_HISTORY_CACHE_PASSPHRASE">a16lrhrCl2oB8Ht4cjwk7fYhVi5tu/rqfKvzB5ATDP+EWTBmpyzVcVR1cdl9mXeQTTnhsT1dBqUp
xcEqsEtGnbHFlltC1c56udZGeCdzzrtWpNqFRjPLAuYxpB/qT3/hnlRRFxmtl1yjStOVivPQyi/n TEbsmSHcH92U/xyZvRuzxV7lfHnXPSiDel1tx0aoHzpcM3bt2B1LY98o2YRpONjOlyWhFl1lRonc
1qAE49lfTg37vVzXuzvwILNoCAadLphe/bp+N8ep3n06WhnspUuX1vlrtUTE56J5V9w1i8Yw5p/n 7kKlGMOPUR/UxX9gMgvE02/EC7Ao62Gwc2ZFWg== </string>

<string name="ROUTE_HISTORY_CACHE_PASSPHRASE">DkxKAVUx0o9of2LmBaxNa7CCfQ0uKinNA31bzHcuAaldljCGYy9MkybynflXZ8fj6l3BFazGJMtk
zsGasmB2HN+GZvNMuA4/DSu8h0Cph4+Ks6K05FTpBrsfbINNL00halzL3u3HsNRkyUVi2fUShuUq fi8c14xs0kun1Yk64w5RkpIO6ma7eVuRimWnS3Jey2FpMiHtZZTbiEeZSon1EYnbjwFVXcl/N4Jo
+bl2lFPrLFamtzZKHISnPPD5ZZ08WAsOHiOK/j2TjS8qLp7qrimJewyVqWXssnuXWm2zM5uhV307 1RUWFMQM2CFbiCI23WIL6RZtvqq4Frwj8GL7LQ== </string>

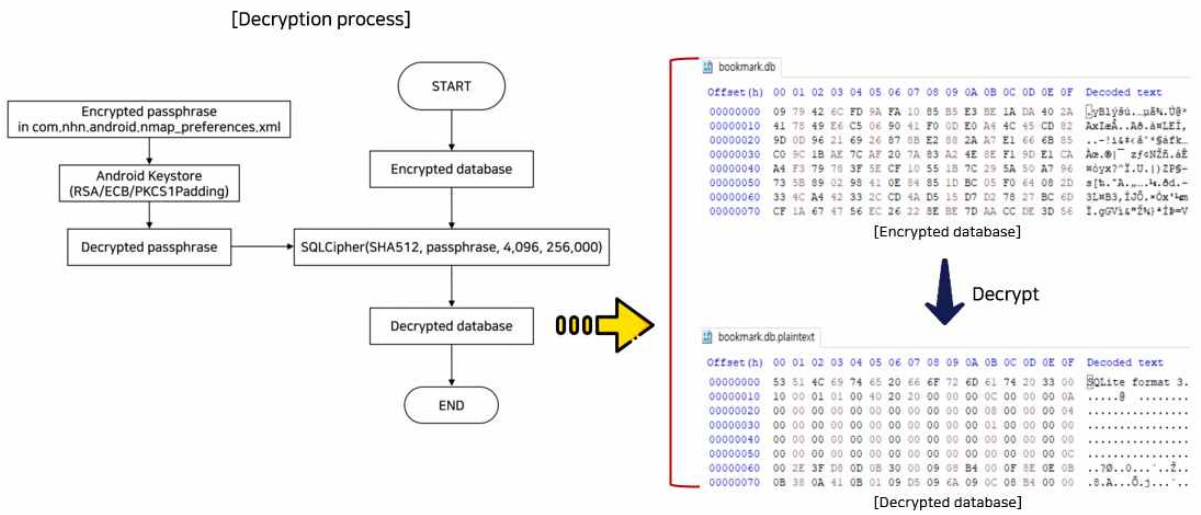
〈Figure 2〉 Encrypted passphrase stored in com.nhn.android.nmap_preferences.xml

본 논문에서는 네이버 지도에 사용되는 API (Application Programming Interface)를 Hooking하여 분석을 진행하였다(그림 3). 네이버 지도에서는 passphrase 암/복호화를 위해 Android Keystore를 사용한다. 애플리케이션 사용 시 매회 Android Keystore를 통해 com.nhn.android.nmap_preferences.xml 파일 내 저장된 passphrase를 복호화한다. 복호화된 passphrase와 SQLCipher4를 이용해 데이터베이스를 open한다. 해당 과정에 사용되는 API를 Hooking하여 복호화된 passphrase와 데이터베이스를 획득한다.



〈Figure 3〉 API Hooking process

분석 결과를 기반으로 구성한 전체 복호화 과정과 실제 복호화된 결과는 다음 (그림 4)와 같다. 주요 사용자 데이터가 저장되는 데이터베이스 파일의 복호화를 통해 주요 아티팩트를 식별하였다.



〈Figure 4〉 Decryption process for encrypted database and decrypted results

4.2 검색 기록 정보

사용자의 검색 기록은 장소 및 대중교통에 대한 검색 기록과 길찾기 경로 기록으로 나눌 수 있다. 검색 기록 관련 데이터는 databases 디렉터리 내 search-history.db, route-history.db와 subwayMap.db 파일 및 shared_prefs 디렉터리 내 pubtrans_cache.xml 파일에 저장된다. databases 디렉터리 내 3가지 파일은 장소 및 대중교통에 대한 검색 기록, 길찾기 경로 기록과 지하철역 검색 기록을 저장하며, 각 파일에 따라 획득 가능한 주요 데이터를 정리하면 〔표 3〕과 같다.

〈Table 3〉 Artifacts of search history in databases directory

Path	Column	Value	Remark
search-history.db (history table)	key	Type of search history content	PLACE_POI, SEARCH_WORD, ADDRESS_POI, BUS, SUBWAY_STATION etc
	value	Search history name, address, latitude, longitude	
	updateTime	Search history time	Unix Milliseconds
route-history.db (history table)	key	Type of route history content	ROUTE_TRANSIT, CAR, BICYCLE, WALK
	value	Start place name, latitude, longitude End place name, latitude, longitude	
	updateTime	Route history time	Unix Milliseconds
subwayMap.db (RecentWord table)	time	Search time related subway station	Unix Milliseconds
	departureName	Subway station departure name	
	departureLine	Start subway line	
	arrivalName	Subway station destination name	
	arrivalLine	End subway line	
	waypointName	Subway station intermediate stop	

search-history.db 파일에는 사용자가 검색한 단어, 장소, 주소, 버스 및 지하철 기록이 유형별로 저장되며, 이를 통해 각 검색 기록에 대한 명칭과 주소를 획득할 수 있다. 검색 기록에는 장소에 대한 위도, 경도 값이 저장되며, 검색한 시간이 Unix Milliseconds 형태로 저장된다. route-history.db 파일에는 사용자가 검색한 경로 기록이 대중교통, 자동차, 자전거 및 도보 유형으로 나뉘어 저장되며, 각 경로 유형에 대한 출발지와 도착지의 명칭과 위도, 경도 값을 획득할 수 있다. subwayMap.db 파일에는 사용자가 검색한 지하철역 검색 기록과 경로가 저장되며, 각 경로에 대한 출발지, 경유지 및 도착지의 지하철역 명칭과 호선을 확인할 수 있다.

shared_prefs 디렉터리 내에 pubtrans_cache.xml 파일에는 대중교통 길찾기 경로 기록에 해당하는 사용자 마지막 행위 정보가 저장되며 획득 가능한 주요 데이터는 〔표 4〕와 같다.

〈Table 4〉 Artifacts of search history in pubtrans_cache.xml

File	Column	Value	Remark
pubtrans_cache.xml	latitude, longitude	Latitude and longitude of Start and End place	
	name	Start and End place name	
	address	Start and End place address	
	departureTime, arrivalTime	Departure and arrival time	YYYY-MM-DD hh:mm:ss

사용자가 마지막으로 검색한 대중교통 길찾기 경로의 출발지와 도착지 명칭과 주소, 위도, 경도 값이 저장된다. 또한, 경로 검색한 시간과 중간 경유지 및 도착지의 시간 정보가 YYYY-MM-DD hh:mm:ss 형태로 저장된다.

4.3 사용자 및 위치 정보

사용자 정보 관련 데이터는 shared_prefs 디렉터리에 저장되며, 각 경로에 따라 획득 가능한 주요 데이터를 정리하면 〔표 5〕와 같다. 사용자 로그인 ID 정보와 사용자가 입력한 생년월일 정보가 YYYY-MM-DD 형태로 저장된다.

〈Table 5〉 Artifacts of user information in shared_prefs directory

Path		Column	Value	Remark
shared_prefs	NaverLogin PreferenceData.xml	LAST_LOGIN_SUCCESS_ID	User ID	
		TRY_LOGIN_ID		
		WITHOUT_GSON_ACCOUNT_INFO	User ID and User's birth date	YYYY-MM-DD
	com.nhn.android.nmap_ preferences.xml	HISTORY_MIGRATED_ID	User ID	
	NativeNaviDefaults.xml	NaviUserIdKey		

네이버 지도의 경우 shared_prefs 디렉터리에 사용자의 마지막 위치 정보가 실제 해당 위치의 위도, 경도로 저장된다. com.nhn.android.nmap_preferences.xml 파일을 통해 사용자가 마지막으로 검색한 지도 위치의 위도, 경도 값 혹은 마지막으로 확인한 지도 화면의 중앙 위치에 해당하는 위도, 경도 값을 획득할 수 있다. 또한, NativeNaviDefaults.xml 파일을 통해 (그림 5)와 같이 사용자가 마지막으로 내비게이션 길 안내 기능을 실행시킨 장소의 위도, 경도 값을 획득할 수 있다.

[NativeNaviDefaults.xml 파일 내 저장된 위도, 경도 값]

[마지막으로 사용자가 내비게이션 실행시킨 위치]

〈Figure 5〉 The location (latitude, longitude) where the user last ran the navigation

4.4 즐겨찾기 정보

네이버 지도의 경우 특정 장소에 대한 즐겨찾기가 가능하며, 즐겨찾기 관련 데이터는 databases 디렉터리 내 bookmark.db 파일에 저장된다. 각 테이블에 따라 획득 가능한 주요 데이터를 정리하면 〔표 6〕과 같다.

〈Table 6〉 Artifacts of bookmark data in bookmark.db

Table	Column	Value	Remark
bookmark	type	Bookmark content type	place
	name	Bookmark place name	
	displayName	Bookmark place nickname	User setting
	lat, lng	Bookmark place latitude, longitude	
	useTime lastUpdateTime creationTime	Bookmark setting time	Unix Milliseconds
	memo	Bookmark memo content	User setting
	address	Bookmark place address	

folder	name	Bookmark folder name	
	lastUseTime creationTime	Bookmark folder create time	Unix Milliseconds
	isDefaultFolder	Confirm default folder	Defaultfolder : 1 Other folders : 0
	memo	Bookmark memo content	User setting
	shouldOverlay	Bookmark folder view on the map	View on the map : 1 View off the map : 0
	bookmarkCount	Bookmark folder view count	

bookmark 테이블에는 즐겨찾기한 장소에 대한 이름, 위도, 경도 값과 실제 주소가 저장된다. 또한, 사용자가 직접 입력한 메모 내용 및 장소 닉네임이 저장되며, 장소를 즐겨찾기에 추가한 시간이 Unix Milliseconds 형태로 저장된다. folder 테이블에는 사용자가 설정한 즐겨찾기 폴더 관련 데이터가 저장되고, 즐겨찾기 폴더명, 메모 내용과 조회수에 대한 정보를 획득할 수 있다. 또한, 해당 즐겨찾기 폴더의 지도 표시 유무와 기본 즐겨찾기 폴더를 확인할 수 있고, 즐겨찾기 폴더 생성 시간은 Unix Milliseconds 형태로 저장된다.

4.5 시간 정보

네이버 지도 사용과 관련하여 생성되는 다양한 시간 정보는 files, app_webview 및 shared_prefs 디렉터리에 저장된다. 각 경로에 따라 획득 가능한 주요 데이터를 정리하면 〔표 7〕과 같다.

〈Table 7〉 Paths and artifacts in time related data

Path		Column	Value	Remark
files\settings.db		last_position	The last recent connection time	Unix Milliseconds
app_webview_com.nhn.android.nmap\pref_store		installation_date2	App installation time	Unix Seconds
shared_prefs	com.google.android.gms.measurement.prefs.xml	first_open_time	After installation first time to access the app	Unix Milliseconds
		previous_os_version	Android version	
		last_puase_time	Time to end the app	
	ace-param-repo.xml	time		
	com.facebook.sdk.USER_SETTINGS.xml	last_timestamp	Naver map application start time	
	NaverLoginPreferenceData.xml	LAST_LOGOUT_TIMESTAMP	Logout time	Unix Seconds
		LAST_LOGIN_SUCCESS_TIMESTAMP	Login time	

files 디렉터리 내 settings.db 파일에는 사용자가 가장 최근에 접속한 시간이 Unix Milliseconds 형태로 저장되고, shared_prefs 디렉터리 내 ace-param-repo.xml 파일과 com.facebooksdk.USER_SETTINGS.xml 파일에는 애플리케이션 실행 시간과 종료 시간이 Unix Milliseconds 형태로 저장된다. NaverLoginPreferenceData.xml 파일에는 로그인과 로그아웃한 시간이 Unix Seconds 형태로 저장된다. 이를 통해 사용자의 애플리케이션 사용으로 생성되는 시간 정보를 활용할 수 있다.

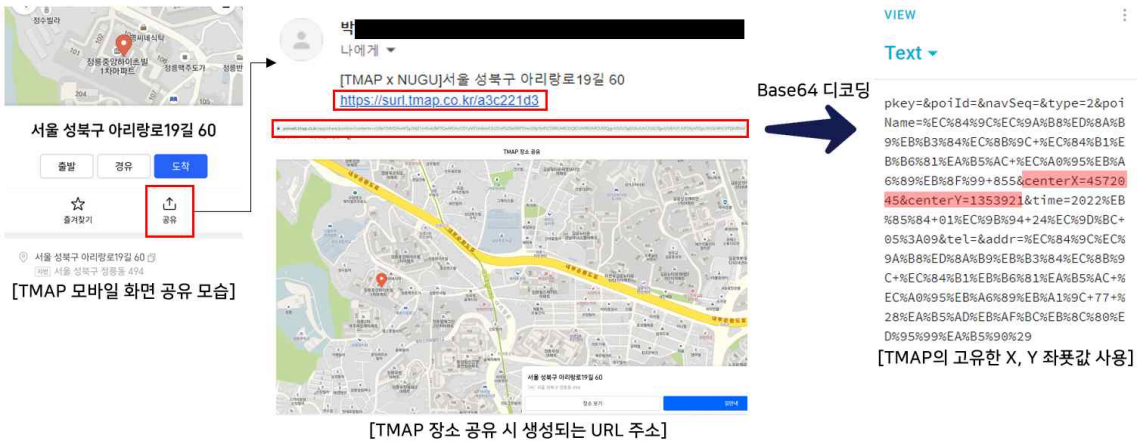
4.6 이미지 정보

사용자 행위에 따라 생성되는 이미지 정보는 cache 디렉터리와 databases 디렉터리 내에 저장된다. 애플리케이션 내에 저장된 이미지 중 사용자가 확인한 이미지는 image_manager_disk_cache 디렉터리에 〔random value〕.0 파일 형태로 저장되며, (그림 6)과 같이 JPG, PNG 등의 이미지 확장자 추가 후 원본 파일을 확인할 수 있다.

〈Figure 6〉 Images viewed by users that are stored in an application

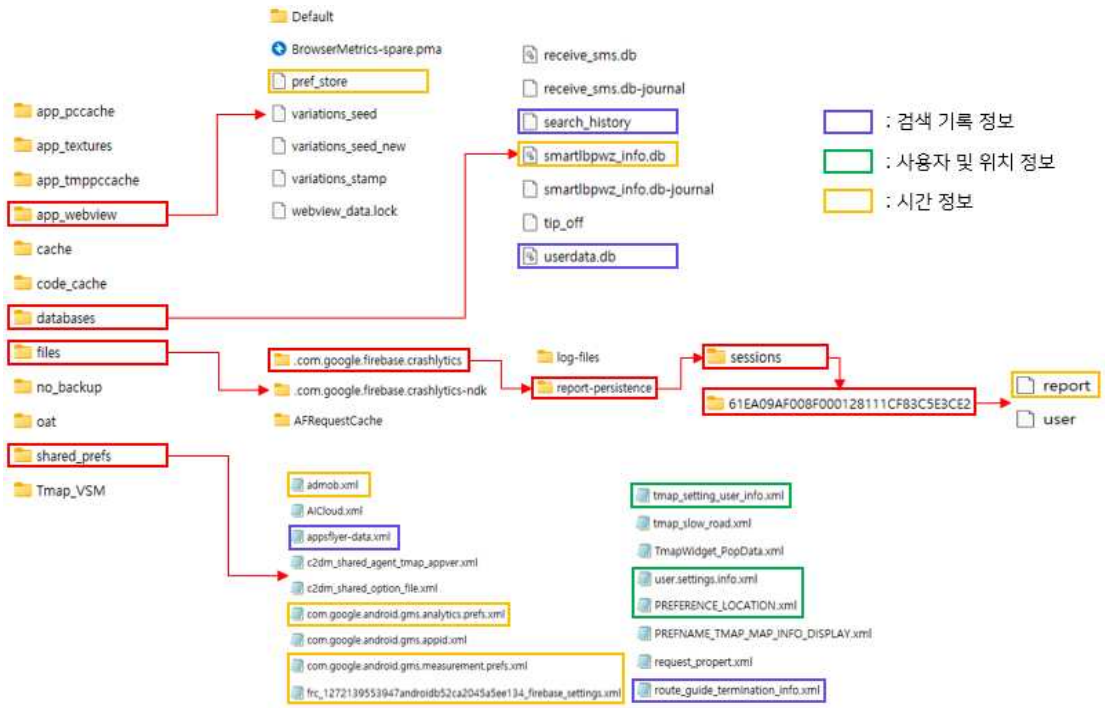
Ⅴ. TMAP 아티팩트 분석

TMAP은 2021년 6월 기준으로 서비스 출시 이후 3,000만 명 이상의 사용자가 이용 중이다[15]. TMAP은 사용자 계정 등록 혹은 휴대폰 번호 인증 후 사용이 가능하다. TMAP은 장소에 대한 고유한 X, Y 좌표값을 생성하며, 이는 TMAP으로 장소 공유 시 생성되는 URL 주소의 contents 값에 Base64 인코딩되어 저장된다(그림 7).



〈Figure 7〉 Unique X, Y coordinates of TMAP

주요 데이터 경로는 (그림 8)과 같으며, 검색 기록, 사용자 및 위치, 즐겨찾기, 집, 회사와 시간 정보 등을 평문 형태로 저장한다. 로그아웃 후 재로그인하는 경우와 애플리케이션 삭제 후 재설치하는 경우 기존 데이터를 모두 획득할 수 있다.



〈Figure 8〉 Data structure of TMAP

5.1 검색 기록 정보

사용자의 검색 기록은 홈 화면에 존재하는 최근 목적지 기록과 검색창에 실제로 검색한 단어에 대한 기록으로 나눌 수 있다. 검색 기록 관련 데이터는 databases 디렉터리 내 search_history와 userdata.db 파일 및 shared_prefs 디렉터리 내 route_guide_termination_info.xml과 appsflyer-data.xml 파일에 저장된다. databases 디렉터리 내 2가지 파일은 사용자가 검색한 단어 기록과 최근 목적지 기록이 저장되며, 각 파일에 따라 획득 가능한 주요 데이터를 정리하면 〔표 8〕과 같다.

〈Table 8〉 Artifacts related to search history in databases directory

Path	Column	Value	Remark
search_history	id	Search word order	
	searchWord	Search for words	
	searchDate	Search time for words	Unix Milliseconds
	seq	Total number of searches in search history	
userdata.db (userdata_recent Table)	id	Destination search order	
	navSeq	Using navigation	Use : 1, Not use : 0
	custName	Destination search name	
	noorX, centerX	X coordinate	
	noorY, centerY	Y coordinate	
	(l/m/s/d)cdName	-do/-si, -gu, -gun/-eup, -dong, -myeon/-ri	administrative district name
	(primary/secondary)Bun	Land number	
	roadName	road name	
	bldNo1/2	Building number	
	cls(A/B/C/D)Name	Place classification name	
	telNo	Location phone number	
	totalCnt	Destination search count	
	svcDate	Destination search date	YYYYMMDDhhmmss
	fixedIndex	Fixed function	Fixed : 1, Setting home : 2

search_history 파일에는 사용자가 검색한 단어가 저장되며, 검색한 시간이 Unix Milliseconds 형태로 저장된다. 해당 검색 기록 삭제 시 데이터는 사라지고 검색 순서와 총 검색 횟수를 통해 삭제한 데이터의 삭제 여부만을 확인할 수 있다. userdata.db 파일에는 사용자가 검색한 장소나 길찾기 실행한 장소의 최근 기록이 순서대로 저장된다. 내비게이션의 사용 유무는 navSeq 컬럼에 따라 길찾기 실행 시 1, 아닐 시 0의 값으로 저장된다. id 컬럼 값에는 최초 검색 기록이 1부터 저장되며, 이후 최근에 검색한 기록일수록 1씩 증가한 값으로 저장된다. 검색 및 길찾기 장소명과 이에 해당하는 행정 구역과 도로명 주소를 획득할 수 있다. 또한, 목적지에 해당하는 X, Y 좌푯값, 장소에 따른 다양한 분류 명칭과 해당 장소에 등록된 실제 전화번호 정보가 저장된다. 사용자가 검색한 날짜와 시간 정보는 YYYYMMDDhhmmss 형태로 저장되고, 각 주소를 검색한 횟수도 저장된다. 사용자가 집으로 설정한 검색명과 주소는 fixedIndex 컬럼에 2로 저장되며, 고정핀을 설정한 검색명과 주소는 1로 저장된다.

shared_prefs 디렉터리 내 2가지 파일은 사용자의 마지막 행위를 기반으로 생성된 검색 기록 관련 데이터가 저장되며, 각 파일에 따라 획득 가능한 주요 데이터를 정리하면 〔표 9〕와 같다.

〈Table 9〉 Artifacts of search history in shared_prefs directory

Path	Column	Value	Remark
route_guide_ termination_info.xml	route_guide_destination_name	Search name	
appsflyer-data.xml	prev_event_name	Recent user's activity name	Function_trial, login, logout, click, place_banner_view etc
	prev_event_timestamp	Activity time	Unix Milliseconds
	prev_event_value	Activity value	Search, driving etc

route_guide.termination_info.xml 파일을 통해 사용자가 마지막으로 검색한 기록명을 획득할 수 있다. appsflyer-data.xml 파일에는 주소 검색, 기능 실행과 장소 클릭 등 사용자가 마지막으로 했던 행위에 따라 활동명, 활동 시간과 활동명에 대한 구체적인 활동 내용이 저장된다.

5.2 사용자 및 위치 정보

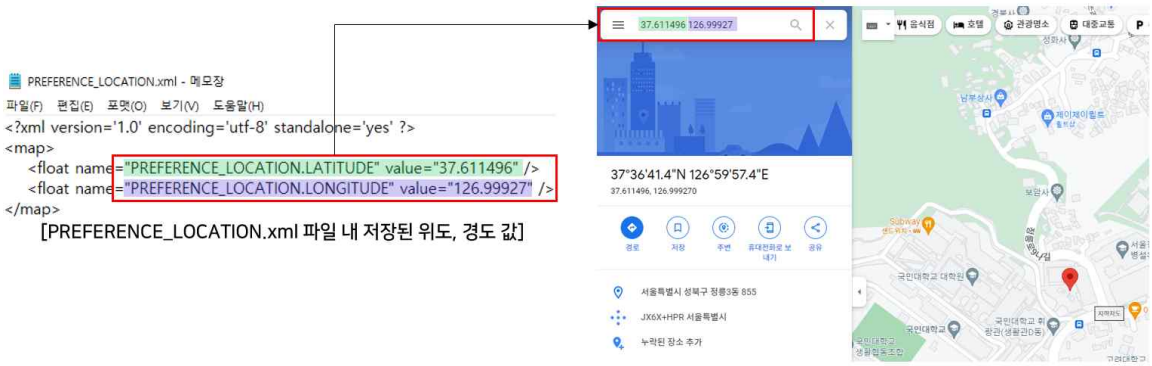
사용자 기기 및 개인 정보 등 사용자 관련 데이터는 files 디렉터리와 shared_prefs 디렉터리에 저장된다. 각 경로에 따라 획득 가능한 주요 데이터를 정리하면 〔표 10〕과 같다.

〈Table 10〉 Paths and artifacts of user information

Path	Column	Value	Remark
files/ .com.google.firebase.crashlytics/ report-persistence/ sessions/ 〔random value〕/ report	model	User device model	
	manufacturer	User device manufacturer	
shared_prefs/ usersettings.info.xml	user.birth	User's birth date	YYYYMMDD
	user.name	User name	User registered
	car.number	User's car number	
shared_prefs/ tmap_setting_user_info.xml	set_gnb_user_info_mode	User name and phone number	

files 디렉터리 내 report 파일을 통해 사용자 기기의 모델명 및 제조사 정보를 획득할 수 있다. shared_prefs 디렉터리 내 usersettings.info.xml 파일에는 사용자가 입력한 생년월일 정보, 자동차 번호와 사용자가 설정한 이름이 저장된다. 또한, tmap_setting_user.info.xml 파일을 통해 사용자가 설정한 이름과 휴대폰 번호를 획득할 수 있다.

shared_prefs 디렉터리 내 PREFERENCE_LOCATION.xml 파일을 통해 (그림 9)와 같이 사용자가 마지막으로 내비게이션 길 안내 기능을 실행시킨 장소의 위도, 경도 값을 획득할 수 있다.



〈Figure 9〉 The location (latitude, longitude) where the user last ran the navigation

5.3 즐겨찾기 및 집/회사 설정 정보

TMAP의 경우 사용자 편의를 위해 자주 가는 장소 혹은 집이나 회사를 직접 등록하여 한 번의 클릭으로 해당 주소로 길 안내를 받을 수 있다. 즐겨찾기 관련 데이터는 databases 디렉터리 내 userdata.db 파일의 userdata_favorite 테이블에 저장되고, 집이나 회사 설정 관련 데이터는 databases 디렉터리 내 userdata.db 파일의 userdata_home_office 테이블에 저장된다. userdata_favorite 테이블의 경우 검색 기록 관련 데이터인 userdata_recent 테이블과 동일하지만 추가로 즐겨찾기한 장소에 해당하는 실제 주소를 획득할 수 있다. userdata_home_office 테이블의 획득 가능한 주요 데이터를 정리하면 〔표 11〕과 같다.

〈Table 11〉 Artifacts of home/office information in userdata_home_office Table

Table	Column	Value	Remark
userdata_ home_office	homeCustName	Setting home place	
	homeNoorX, Y	X, Y coordinate	
	homeAddInfo	Detail home address	
	homeInsDatetime	Setting home time	YYYYMMDDhhmmss
	officeCustName	Setting office place	
	officeNoorX, Y	X, Y coordinate	
	officeAddInfo	Detail office address	
	officeInsDatetime	Setting office time	YYYYMMDDhhmmss

집으로 설정한 데이터는 컬럼이 home으로 시작하고 회사로 설정한 데이터는 컬럼이 office로 시작한다. 집 혹은 회사로 설정한 장소명과 해당 장소의 실제 주소가 저장되고, 등록한 장소의 X, Y 좌푯값과 등록한 시간 정보가 YYYYMMDDhhmmss 형태로 저장된다.

5.4 시간 정보

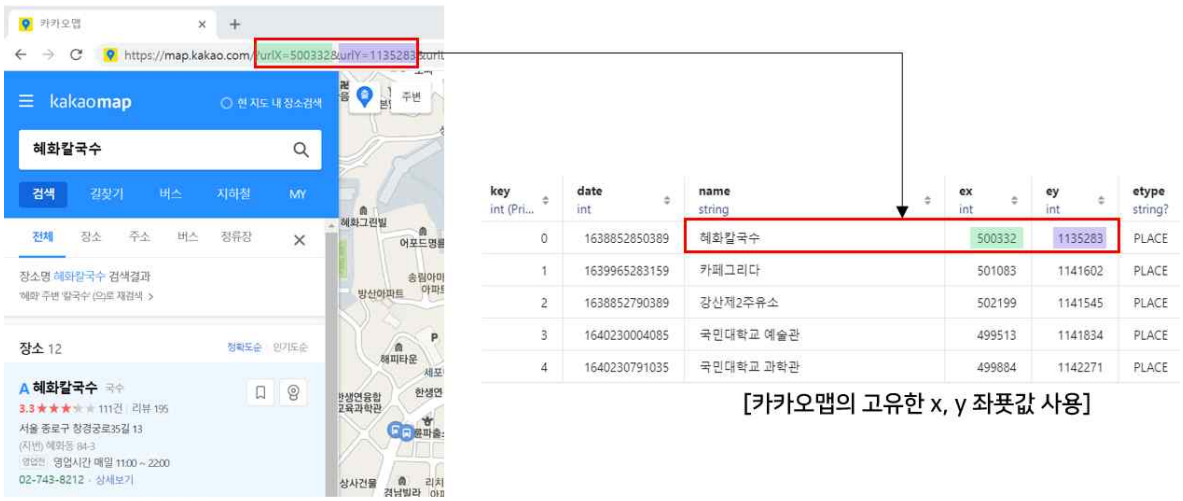
TMAP 사용과 관련하여 생성되는 다양한 시간 정보는 files, app_webview, databases 및 shared_prefs 디렉터리에 저장된다. 각 경로에 따라 획득 가능한 주요 데이터를 정리하면 〔표 12〕와 같다. 애플리케이션 실행 시간, 애플리케이션 종료 시간, 애플리케이션 설치 시간과 내비게이션 길 안내 기능 사용 시간으로 나눌 수 있고, 시간에 따라 Unix Seconds와 Unix Milliseconds 형태로 저장된다.

〈Table 12〉 Paths and artifacts of time data generated by using TMAP

Path		Column	Value	Remark
files/ .com.google.firebase.crashlytics/ report-persistence/ sessions/ 〔random value〕/ report		startedAt	TMAP application start time	Unix Seconds
app_webview/ pref_store		installation_date2	App installation time	
databases/ smartlbpwz_info.db (new_pref_info Table)		service_start_time	TMAP application start time	Unix Milliseconds
		driving_job_last_work_time	Recent navigation usage time	
shared_prefs/	admob.xml	app_last_background_time_ms	Time to end the app	
	com.google.android.gms.analytics.prefs.xml	monitoring:start	TMAP application start time	
		first_run		
	com.google.android.gms.measurement.prefs.xml	first_open_time	After installation first time to access the app	
		last_pause_time	Time to end the app	
	frc_〔gmpAppId〕_firebase_settings.xml	last_fetch_time_in_millis	App installation time	

Ⅵ. 카카오맵 아티팩트 분석

카카오맵은 2003년경 콩나물맵을 시작으로 2011년 다음 지도로 개편되고, 안드로이드 환경은 2016년 9월에 카카오맵으로 새롭게 개편되었다〔16〕. 카카오맵은 사용자 계정 등록 없이 사용 가능하지만, 즐겨찾기 및 집, 회사 설정 등 일부 기능에 대해 사용이 제한된다. 카카오맵은 장소에 대한 고유한 x, y 좌푯값을 생성하며, 이는 카카오맵 웹 사이트의 urlX, urlY 값과 동일하다(그림 10).

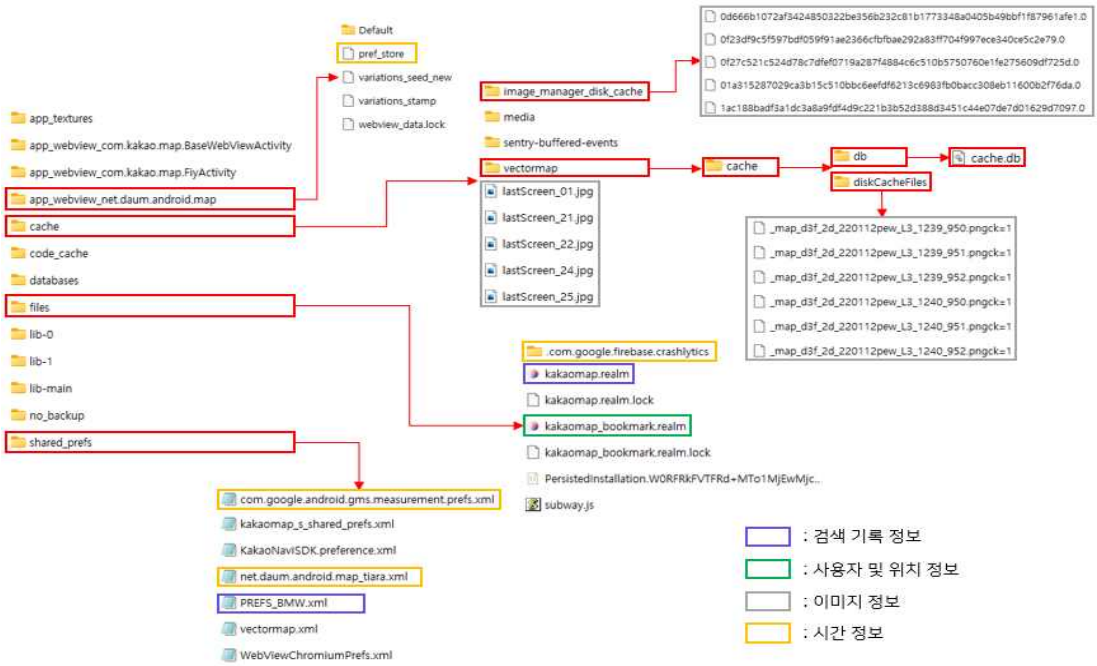


[카카오맵 웹 사이트의 URL 주소]

[카카오맵의 고유한 x, y 좌푯값 사용]

〈Figure 10〉 Unique x, y coordinates of Kakao map

주요 데이터 경로는 (그림 11)과 같으며, 검색 기록, 사용자 및 위치, 즐겨찾기, 집, 회사 정보, 다양한 기능 관련 데이터와 시간 정보 등을 평문 형태로 저장한다. 로그아웃 후 재로그인하는 경우 해당 데이터들은 모두 존재하지만, 애플리케이션 삭제 이후 재설치하는 경우 집, 회사 등록 정보와 일부 즐겨찾기 정보를 제외한 나머지 데이터는 모두 삭제된다.



〈Figure 11〉 Data structure of Kakao map

6.1 검색 기록 정보

사용자가 검색한 기록은 3가지 종류로 내비게이션 항목에 존재하는 최근 목적지 기록, 검색창에 남는 최근 검색 기록과 길찾기 항목에 존재하는 경로 기록으로 나눌 수 있다. 최근 목적지 기록은 사용자가 내비게이션 안내 시작할 경우와 최근 목적지 목록에서 직접 추가할 때 데이터가 생성된다. 최근 검색 기록은 검색창에서 확인할 수 있고, 목적지 및 경로 등 사용자가 검색한 모든 기록이 남는다. 길찾기 경로 기록은 자동차, 대중교통, 도보 및 자전거 경로로 나뉘어 사용자가 경로를 설정할 때마다 데이터가 생성된다. 검색 기록 관련 데이터는 files 디렉터리 내 kakaomap.realm 파일과 shared_prefs 디렉터리 내 PREFS_BMW.xml 파일에 저장된다. kakaomap.realm 파일은 MongoDB Realm Studio를 통해 내부 데이터를 확인하였으며, 각 CLASSES에 따라 획득 가능한 주요 데이터를 정리하면 〔표 13〕과 같다.

〈Table 13〉 Search history artifacts related to CLASSES in kakaomap.realm

CLASSES	Column	Value	Remark
Navigation DestinationModel	key	Recent destination order	
	date	Navigation destination start time	Unix Milliseconds
	name	Destination name	
	ex, ey	Destination x, y coordinate	
	stype	Destination type	Only PLACE
RouteLogModel	date	Public transportation route search time	Unix Milliseconds
	routeKey	Start place name | End place name	
	sx, sy	Start place x, y coordinate	
	ex, ey	End place x, y coordinate	
	steps	Detailed route	Click then go to RouteStepLogModel
RouteStep LogModel	#	Detailed route order	
	date	Public transportation route search time	Unix Milliseconds
	nodeName	Middle place name in the public transport route	
	nodeX, Y	Middle place's x, y coordinate	
	transports	Transportation information	Click then go to RouteStepTransportLogModel

RouteStep TransportLogModel	transportId	Transportation ID	
	transportName	Transportation name	Bus : bus number Subway : line
History	timestamp	Search/Destination/Route time	Unix Milliseconds
	count	Search/Destination/Route count	
	category	Category	r : routeway s : search place
	type	Type of search history content	QUERY(search), ADDRESS, PLACE or ROUTE_CAR, PUBTRANS, BICYCLE, WALK
	bookmark	Bookmark content in search history	Click then go to bookmark
	ko_inital_ consonant	Place name's Korean initial value	
	roadviewX, Y	Place x, y coordinate	
	display 1, 2	Place name and address	
	routeForm	Start and End place information (name and x, y coordinate)	
	routeKey	Start place name | End place name	

NavigationDestinationModel CLASSES에는 최근 목적지 기록이 저장된다. key 컬럼 값은 0부터 시작하며, 이는 최초 검색 기록임을 알 수 있다. 이후 최근에 검색한 기록일수록 1씩 증가한 값으로 저장된다. 유형은 항상 PLACE 값이 저장되며, 검색한 목적지 장소에 대한 명칭과 x, y 좌표값이 저장된다. 내비게이션 실행 시간은 Unix Milliseconds 형태로 저장된다. RouteLogModel, RouteStepLogModel 및 RouteStepTransportLogModel CLASSES에는 사용자가 4가지 길찾기 유형 중 대중교통 경로 설정 시 상세 경로 정보가 저장된다. RouteLogModel CLASSES에는 출발지와 도착지에 대한 명칭과 x, y 좌표값을 획득할 수 있고, 해당 경로를 선택한 시간이 Unix Milliseconds 형태로 저장된다. steps 컬럼 클릭 시 RouteStepLogModel CLASSES로 연결되며, 도착지까지의 중간 지점 장소명과 x, y 좌표값을 획득할 수 있다. transports 컬럼 클릭 시 RouteStepTransportLogModel CLASSES로 연결되며, 각 경로 지점에 해당하는 교통수단 정보를 획득할 수 있다. History CLASSES에는 최근 목적지, 최근 검색 및 경로 기록이 저장된다. 각 검색 기록은 사용자 행위에 따라 생성되는 시간 정보와 횟수가 저장되고, Category 컬럼을 통해 길찾기 경로 기록은 r, 나머지 기록은 s로 구분할 수 있다. r은 4가지의 길찾기 유형이 있고, 출발지와 도착지에 대한 명칭과 x, y 좌표값이 저장된다. s는 명칭, 주소와 장소 유형이 있고, 단일 장소에 대한 명칭, 주소와 x, y 좌표값이 저장된다.

shared_prefs 디렉터리 내에 PREFS_BMW.xml 파일에는 경로 기록과 검색 기록에 해당하는 사용자 마지막 행위 정보가 저장되며 획득 가능한 주요 데이터는 〔표 14〕와 같다.

〈Table 14〉 Artifacts of search history in PREFS_BMW.xml

File	Column	Value	Remark
PREFS_BMW.xml	PREFS_LAST_ROUTE_PARAM	Start, End place information (name, x, y coordinate)	Last route information
	PREFS_LAST_SEARCH_RESULT	Last search name	
		Search time	Unix Milliseconds

PREFS_LAST_ROUTE_PARAM 컬럼에는 마지막 길찾기 경로 기록이 저장되며, 출발지와 도착지에 대한 명칭과 x, y 좌표값을 획득할 수 있다. PREFS_LAST_SEARCH_RESULT 컬럼에는 마지막 검색 기록이 저장되며, 검색명과 검색 시간이 Unix Milliseconds 형태로 저장된다.

6.2 사용자 및 위치 정보

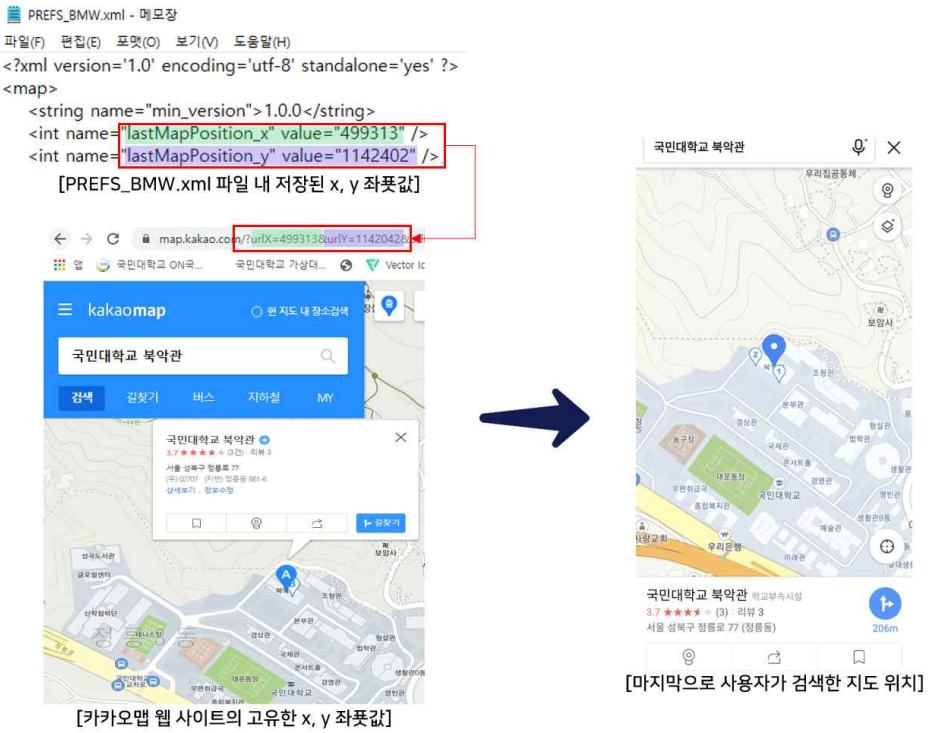
사용자 기기 및 개인 정보 등 사용자 관련 데이터는 files 디렉터리에 저장되며 각 경로에 따라 획득 가능한 주요 데이터를 정리하면 〔표 15〕와 같다.

〈Table 15〉 Paths and artifacts of user information

Path	Column	Value	Remark
files/ .com.google.firebase.crashlytics/ report-persistence/ sessions/ 〔random value〕/ report	model	User device model	
	manufacturer	User device manufacturer	
files/ kakaomap_bookmark.realm/ BookmarkFolder	nickname	User name	User registered
	profile_image	User profile image	URL

files 디렉터리 내 report 파일에는 사용자 기기의 모델명 및 제조사 정보가 저장되며, kakaomap_bookmark.realm 파일의 BookmarkFolder CLASSES에 사용자가 등록한 이름과 사용자 프로필 이미지가 URL 형태로 저장된다.

shared_prefs 디렉터리 내 PREFS_BMW.xml 파일을 통해 (그림 12)와 같이 사용자가 마지막으로 검색한 지도 위치의 x, y 좌푯값 혹은 마지막으로 확인한 지도 화면의 중앙 위치에 해당하는 x, y 좌푯값을 획득할 수 있다.



〈Figure 12〉 The location (x, y) where the user last searched the map

6.3 즐겨찾기 및 집/회사 설정 정보

카카오맵의 경우 길찾기 경로와 장소에 대한 즐겨찾기가 가능하며, 즐겨찾기 관련 데이터는 files 디렉터리 내 kakaomap.realm 파일과 kakaomap_bookmark.realm 파일에 저장된다. 각 경로에 따라 획득 가능한 주요 데이터를 정리하면 〔표 16〕과 같다.

〈Table 16〉 Paths and artifacts of Bookmark data

Path	Column	Value	Remark
kakaomap.realm/ Bookmark CLASSES and kakaomap_bookmark.realm/ Bookmark CLASSES	folderid	Bookmark folder id	
	category	Category	r : routeway s : search place
	type	Bookmark content type	ROUTE_CAR ROUTE_PUBTRANS BUSSTOP PLACE etc
	ko_initial_consonant	Bookmark place initial	
	routForm	Bookmark route (start, end place information)	
	x, y	Bookmark place x, y coordinate	
	display1	Bookmark place name	
	display2	Bookmark place address	
	updatedTime/createdTime	Bookmark setting time	YYYY-MM-DD hh:mm:ss
	timestamp		Unix Milliseconds
	memo	Bookmark memo content	User setting
kakaomap_bookmark.realm/ Bookmark Folder CLASSES	title	Bookmark folder name	
	memo	Bookmark folder memo content	
	status	Bookmark folder status	O : open P : private
	view_cnt	Bookmark folder view count	
	created/updatedTime	Bookmark folder create time	YYYY-MM-DD hh:mm:ss
	timestamp		Unix Milliseconds
	itemUpdatedTime	Last bookmark item added time	YYYY-MM-DD hh:mm:ss
	viewon	Bookmark folder view on the map	View on the map : true View off the map : false

kakaomap.realm 파일의 Bookmark CLASSES와 kakaomap_bookmark.realm 파일의 Bookmark CLASSES는 History CLASSES와 동일한 내용을 저장하며, 즐겨찾기한 길찾기 경로와 장소에 대한 정보를 획득할 수 있다. 또한, 사용자가 직접 입력한 메모 내용도 확인할 수 있다. 카카오맵은 사용자가 등록한 폴더에 따라 즐겨찾기 설정한 길찾기 경로와 장소를 분류할 수 있다. 사용자가 설정한 즐겨찾기 폴더 관련 데이터는 kakaomap_bookmark.realm 파일의 Bookmark Folder CLASSES에 저장되고, 즐겨찾기 폴더명, 메모 내용과 조회수에 대한 정보를 획득할 수 있다. 또한, 즐겨찾기 폴더의 공개, 비공개 유무와 지도에 표시 여부를 확인할 수 있으며, 즐겨찾기 폴더 생성 시간은 YYYY-MM-DD hh:mm:ss와 Unix Milliseconds 형태로 저장된다.

집이나 회사 설정 관련 데이터는 files 디렉터리 내 kakaomap.realm 파일의 MyPlace CLASSES에 저장되며 획득 가능한 주요 데이터는 〔표 17〕과 같다.

〈Table 17〉 Artifacts of home/office information in MyPlace CLASSES

CLASSES	Column	Value	Remark
MyPlace	type	Place type	Home or COMPANY
	disp1	Setting place name	
	priority	HOME : 1, COMPANY : 2	
	updateTime	Setting home or company time	YYYY-MM-DD hh:mm:ss

설정한 집과 회사에 따라 각각 type은 HOME과 COMPANY로 저장되며, priority는 1과 2로 구분된다. 집 혹은 회사로 설정한 장소명을 획득할 수 있고, 설정한 시간은 YYYY-MM-DD hh:mm:ss 형태로 저장된다.

6.4 시간 정보

카카오맵 사용과 관련하여 생성되는 다양한 시간 정보는 files, app_webview 및 shared_prefs 디렉터리에 저장된다. 각 경로에 따라 획득 가능한 주요 데이터를 정리하면 〔표 18〕과 같다.

〈Table 18〉 Paths and artifacts of time data generated by using Kakao map

Path		Column	Value	Remark
files/ .com.google.firebase.crashlytics/ report-persistence/ sessions/ 〔random value〕/ report		startedAt	Kakao map application start time	Unix Seconds
app_webview_ net.daum.android.map/ pref_store		installation_date2	App installation time	
shared_prefs	com.google.android.gms.measurement.prefs.xml	first_open_time	After installation first time to access the app	Unix Milliseconds
		last_puase_time	Time to end the app	
	net.daum.android.map_tiara.xml	install_begin_time	App installation time	Unix Seconds
		install_date	App installation date	YYYY-MM-DD
		install_first_launch_time	After installation first time to access the app	Unix Seconds

애플리케이션 실행 시간과 종료 시간, 애플리케이션 설치 후 처음으로 접속한 시간이 Unix Seconds와 Unix Milliseconds 형태로 저장된다. 또한, shared_prefs 디렉터리 내 net.daum.android.map_tiara.xml 파일에는 애플리케이션 설치 시간과 애플리케이션 설치 후 처음 접속 시간이 Unix Seconds 형태로 저장된다.

6.5 이미지 정보

사용자 행위에 따라 생성되는 이미지 정보는 cache 디렉터리 내에 저장된다. 애플리케이션 내에 저장된 이미지 중 사용자가 확인한 이미지는 image_manager_disk_cache 디렉터리에 〔random value〕.0 파일 형태로 저장되며 JPG, PNG 등의 이미지 확장자 추가 후 원본 파일을 확인할 수 있다. 카카오맵은 지역별 5개의 지하철 노선도를 제공하며, (그림 13)과 같이 사용자가 애플리케이션을 통해 마지막으로 확인한 지하철 노선도 화면 모습이 lastScreen_##.jpg 파일 형태로 저장된다. 1은 수도권, 21은 부산, 22는 대구, 24는 광주, 25는 대전 지역에 해당한다.

〈Figure 13〉 The last subway screen that user checked

6.6 기능 관련 정보

카카오맵은 승하차 알람 설정 기능, 사용자 추천 도착 정보 기능과 고정핀 기능을 통해 데이터 획득이 가능하며 모두 files 디렉터리 내 kakaomap.realm 파일에 저장된다.

6.6.1 승하차 알람 설정 기능

승하차 알람 설정 기능은 대중교통 길찾기에서 사용할 수 있는 기능으로 사용자가 원하는 경로에 대하여 승하차 알람을 설정할 수 있다. 승하차 알람 설정 관련 데이터는 AlarmLogModel CLASSES에 저장되며 획득 가능한 주요 데이터는 〔표 19〕와 같다.

〈Table 19〉 Artifacts of the alarm for getting on and off in AlarmLogModel CLASSES

CLASSES	Column	Value	Remark
AlarmLogModel	pk	Alarm setting order	
	routeType	Public transportation type	1 : Only bus 2 : Only subway 0 : Both of them
	routeKey	Alarm setting route (start, end place name)	Start place | End place
	date	Alarm setting time	Unix Milliseconds

승하차 알람 설정은 동시에 2개 이상 할 수 없고, 설정한 알람 순서대로 pk 컬럼 값이 0부터 1씩 증가한다. 알람 설정한 경로가 버스로만 구성 시 type은 1, 지하철로만 구성 시 2, 버스와 지하철 모두 구성 시 0의 값으로 저장된다. 또한, 출발지와 도착지에 대한 명칭을 획득할 수 있고, 알람 설정한 시간은 Unix Milliseconds 형태로 저장된다.

6.6.2 사용자 추천 도착 정보 기능

사용자 추천 도착 정보 기능은 사용자 위치를 기반으로 주변 정류장, 주변 지하철역을 추천해주는 기능이다. 사용자가 원하는 버스 정류장이나 지하철역을 클릭 시 추천 도착 정보 항목에 각 정류장, 역까지의 거리, 도착 시간과 전체 노선 등을 확인할 수 있다. 또한, 지하철 노선도를 통해 출발지와 도착지 경로를 검색하면 모든 역에 대한 데이터가 생성된다. 사용자 추천 도착 정보 관련 데이터는 ArrivalInfoNodeLogModel CLASSES에 저장되며 획득 가능한 주요 데이터는 〔표 20〕과 같다.

〈Table 20〉 Artifacts of recommended arrival information in ArrivalInfoNodeLogModel CLASSES

CLASSES	Column	Value	Remark
ArrivalInfo NodeLogModel	date	Recommended arrival information click time	Unix Milliseconds
	nodeType	Public transportation type	1 : bus, 2 : subway
	nodeId	Bus stop or Subway station place ID	
	nodeName	Bus stop or Subway station place name	
	nodeSubName	Bus stop place sub name	sub number
	nodeDirection	Bus stop next direction name	
	nodeX, Y	Bus stop or Subway station place's X, Y coordinate	
	transportId	Subway station ID	
	transportName	Bus number or Subway station line	

사용자가 주변 정류장 및 지하철역을 클릭한 시간이 Unix Milliseconds 형태로 저장되고, 클릭할 때마다 데이터가 생성된다. 그 외에도 버스 정류장 및 지하철역의 명칭과 다음 방향, X, Y 좌푯값, 버스 번호와 지하철 호선 등의 정보를 획득할 수 있다. 사용자 현재 위치 기반으로 생성되는 주변 지역의 정보를 통해 사용자의 경로 위치를 추정할 수 있다.

6.6.3 고정핀 기능

고정핀 관련 데이터는 History CLASSES와 QuickTabPin CLASSES에 저장되며 각 CLASSES에 따라 획득 가능한 주요 데이터를 정리하면 〔표 21〕과 같다.

〈Table 21〉 Paths and artifacts in fixed pin data

CLASSES	Column	Value	Remark
History	isPinned	Pinned state	true : pinned false : not pinned
	pinData	Pinned time	Unix Milliseconds
QuickTabPin	type	Tab pin type	TYPE_DESTINATION TYPE_ARRIVAL
	date	Tab pin time	Unix Milliseconds

History CLASSES에는 검색창에 있는 최근 검색 기록 중 상단 핀 고정 시 데이터가 생성되고 고정된 시간은 Unix Milliseconds 형태로 저장된다. QuickTabPin에는 최근 목적지 기록과 추천 도착 정보에서 사용되는 고정핀 기능이 각각 TYPE_DESTINATION과 TYPE_ARRIVAL 형태로 저장된다. 고정된 시간은 Unix Milliseconds 형태로 저장된다.

Ⅷ. 결론

스마트폰의 위치 기반으로 내비게이션 기능을 제공하는 지도 애플리케이션은 지속적으로 사용률이 증가하고 있다. 지도 애플리케이션 사용 시, 사용자의 실시간 위치를 기반으로 생성되는 위치, 시간, 길찾기 경로 및 목적지 관련 데이터는 디지털 포렌식 관점에서 활용 가치가 높다. 이에 비해 기존 지도 애플리케이션에 분석된 결과의 범위는 한정적이고, 업데이트에 따라 생성되는 아티팩트가 변경되거나 애플리케이션마다 저장되는 데이터 형태가 다양하다. 따라서 지도 애플리케이션에 저장되는 데이터를 활용하기 위해 최신 버전에서의 데이터 수집 방안 및 식별하는 연구가 필요하다.

본 논문에서는 지도 애플리케이션 중 사용량이 많은 네이버 지도, TMAP과 카카오맵을 대상으로 사용자 이동 경로와 위치 및 목적지 정보를 특정 시간 정보와 결합하여 분석하였다. TMAP과 카카오맵의 경우 모든 데이터가 평문으로 저장되어 있으며, 사용자의 행위 중심으로 주요 아티팩트를 식별하고 유의미한 데이터를 정리하였다. 반면 네이버 지도의 경우 사용자 행위와 관련된 주요 데이터베이스 파일 전체를 SQLCipher4 알고리즘으로 암호화하여 저장하며, 암호화에 사용된 passphrase는 Android Keystore에 저장된 키로 암호화한다. 이에 대한 복호화 방안으로 네이버 지도에 사용되는 API를 Hooking하여 복호화된 passphrase와 데이터베이스를 획득하였다. 이를 바탕으로 전체적인 복호화 과정을 정리하고, 실제 복호화된 데이터베이스 파일을 분석하여 주요 아티팩트를 식별하였다. 본 논문의 분석 결과를 바탕으로 디지털 포렌식 수사에 지도 애플리케이션의 데이터를 활용할 수 있을 것으로 기대한다.

참 고 문 헌 (References)

[1] "Kstartupvalley", https://www.ksvalley.com/news/article.html?no=3818

[2] "MOBILEINDEX", https://hd.mobileindex.com/report/?s=179&p=1

[3] "Seouldaily", https://www.sedaily.com/NewsVIew/22OZYVWJNY

[4] Seungwon Jung, Jaegeon Bae, Seonghyeon Gong, Jinseong Park, Gihoon Nam and Chang hoon Lee, "A Study on Collection and Utilization Methods of Location Information in Android Pre-installed Applications for Digital Forensics Analysis", Journal of Digital Forensics 14(1), pp. 59-74, Mar. 2020

[5] Jason Moore, Ibrahim Baggili and Frank Breitinger, "Find Me If You Can: Mobile GPS Mapping Applications Forensic Analysis & SNAVP the Open Source, Modular, Extensible Parser", Journal of Digital Forensics, Security and Law Volume 12, Article 7, March. 2017

[6] YongSeok Choi, "Analysis of car navigation using information", Master Thesis, Dept. of Information Management & Security, Korea Univ. 2010

[7] Beverley Nutter, "Pinpointing TomTom location records: A forensic Analysis," Digital Investigation, Vol. 5, pp. 10-18, 2008

[8] Xenia Semenova and Natalia Knyazeva, "Forensic Analysis of 2GIS Navigation App Installed on an Android-Based Smartphone", IEEE, June. 2021

[9] Dohyun Kim, Jewan Bang, and Sangjin Lee. "Analysis of smartphone-based location information", Computer Science and Convergence. Springer, Dordrecht, pp. 43-53, December. 2012

[10] Youngjun Son and Mokdong Chung, "Digital Forensics for Android Location Information using Hierarchical Clustering", Journal of the Institute of electronics and Information Engineers 51(6), pp. 143-151, June. 2014

[11] Kyuchul Yeon, Moonho Kim, Dohyun Kim and Sang-jin Lee, "A Study on Geodata Trace of Navigation Application in Smart Devices", Journal of The Korea Institute of Information Security and Cryptology 26(1), pp. 109-115, Feb. 2016

[12] "Android developers", https://developer.android.com/studio/command-line/adb ?hl=ko

[13] "Dailian", https://m.dailian.co.kr/news/view/1033380

[14] "Java Platform Standard Ed. 7", https://docs.oracle.com/javase/7/docs/api/javax/crypto/Cipher.html

[15] "TMAP MOBILITY", https://www.tmapmobility.com/pc/html/news/news-view.html?article_id=4402954474137

[16] "Kakao", https://www.kakaocorp.com/page/service/service/KakaoMap

저 자 소 개

박 귀 은 (Gwuieun Park)
정회원

2022년 2월 : 국민대학교 정보보안암호수학과 졸업
2022년 3월 ~ 현재 : 국민대학교 금융정보보안학과 석사과정
관심분야 : 디지털 포렌식, 정보보호

강 수 진 (Soojin Kang)
정회원

2018년 2월 : 국민대학교 정보보안암호수학과 졸업
2022년 2월 : 국민대학교 금융정보보안학과 석사
2022년 3월 ~ 현재 : 국민대학교 금융정보보안학과 박사과정
관심분야 : 디지털 포렌식, 정보보호

김 종 성 (Jongsung Kim)
평생회원

2006년 11월 : K.U.Leuven, ESAT/SCD-COSIC 정보보호 공학박사
2007년 2월 : 고려대학교 정보보호대학원 공학박사
2009년 9월 ~ 2013년 2월 : 경남대학교 e-비즈니수학과 교수
2013년 9월 ~ 2017년 2월 : 국민대학교 수학과 교수
2017년 3월 ~ 현재 : 국민대학교 정보보안암호수학과/금융정보보안학과 교수
관심분야 : 정보보호, 암호 알고리즘, 디지털 포렌식