공 학 석 사 학 위 논 문

계층적 군집화를 이용한 스마트폰 위치정보 포렌식 분석 모델

2014년 8월

부 경 대 학 교 대 학 원

컴 퓨 터 공 학 과

손 영 준

공 학 석 사 학 위 논 문

계층적 군집화를 이용한 스마트폰 위치정보 포렌식 분석 모델

지도교수 정 목 동

이 논문을 공학석사 학위논문으로 제출함.

2014년 8월

부 경 대 학 교 대 학 원

컴 퓨 터 공 학 과

손 영 준

손영준의 공학석사 학위논문을 인준함

2014년 8월 22일

위 원 장 공학박사 서 경 룡 인

위 원 이학박사 신 상 욱 인

위 원 공학박사 정 목 동 인

목 차

그 림 목 차

표 목 차

A Digital Forensic Model for Smartphone Location Information using Hierarchical Clustering

Young Jun Son

Department of Computer Engineering, Graduate School,

Pukyong National University

Abstract

Today, as digital devices are widespread, a variety of user's private information is created and managed in digital form. Especially the location information in a smartphone can show the user's position at a specific time and the user's area of interest, which could be very useful during criminal investigation. Although the location information plays an important role in solving the crimes such as serial murder, rape, arson cases, etc, there is a lack of research on location information for digital forensics. In this paper, we analyze the artifact and the location information from android logs, images, and applications on android devices, and we suggest the integrated model for analyzing location information using hierarchical clustering algorithm. The proposed model may be useful in criminal investigation by improving the efficiency of data analysis and providing information about a criminal case.

Ⅰ. 서론

최근 전화기능뿐 아니라 인터넷과 다양한 애플리케이션을 이용할 수 있는 스마트폰이 널리 보급되고 있다. 한국인터넷진흥원의 자료에 따르면, 국내 스마트폰 평균 이용기간은 19.5개월이고 일평균 이용시간은 3.4시간으로 나타난다[1]. 이는 스마트폰이 이미 사람들의 생활의 일부로 자리매김하고 있음을 알 수 있다. 또한 스마트폰은 이용자가 항상 소지하고 있고 다양한 기능을 활용할 수 있으므로 이용자와 관련된 다양한 정보가 저장된다. 그러므로 스마트폰에는 이용자의 사용 흔적과 생활 패턴 등이 담겨 있을 확률이 높고, 이는 범죄 수사 시 유용한 자료로 활용될 수 있다.

특히 스마트폰은 GPS 등 각종 센서와 통신기능을 탑재하고 있어 그 위치정보를 측정할 수 있다. 이러한 위치정보는 보통 시간정보와 함께 저장되므로 스마트폰 이용자가 특정 시점에 어디에 있었는지를 나타낼 수 있는 매우 중요한 정보이다. 또한 지역 검색, 경로 탐색, 대중교통 등의 위치정보를 통해 이용자의 관심 지역이나 이동 패턴, 동선 등을 파악할 수 있다. 이러한 위치정보는 디지털 포렌식 측면에서 범죄를 해결하는데 중요한 단서 또는 증거로 활용될 수 있다.

그러나 현재 위치정보에 대한 디지털 포렌식 연구는 스마트폰의 애플리케이션이나 내비게이션 기기 등에 대해 개별적으로 이루어지고 있고, 자동화된 포렌식 분석도구나 통합적 분석방법에 대해서는 제시하지 못하고 있다. 따라서 본 논문은 안드로이드 스마트폰에서 수집할 수 있는 위치정보를 다각적으로 분석하고, 계층적 군집화 알고리즘을 이용하여 위치정보에 대한 통합적 분석 모델 및 조사 절차를 제안한다.

본 논문은 2장에서 위치정보에 대한 관련연구에 대해 살펴보고, 3장에서는 안드로이드 스마트폰에 저장되는 위치정보를 시스템 로그 정보, 이미지의 GPS 메타데이터, 애플리케이션 측면으로 나누어 분석한다. 4장에서는 3장에서 분석된 내용을 토대로 위치정보 분석 모델을 제안하고, 5장에서는 위치정보 분석 도구의 구현 결과를 보여준다. 그리고 마지막 6장에서 결론을 맺고 향후 연구방향을 제시한다.

Ⅱ. 관련 연구

1. 위치정보에 관한 디지털 포렌식 연구

스마트폰에 존재하는 위치정보에 대한 디지털 포렌식 연구로는, Dohyun Kim 등이 스마트폰 지도 애플리케이션인 Google map, Daum map, Naver map을 대상으로 아이폰과 안드로이드 스마트폰에 저장된 시간정보와 위치정보를 분석하고 이를 토대로 'MapAn' 도구를 제안한 연구[2]와 Maus Stefan 등이 위도와 경도 형태의 좌표정보뿐 아니라 도시, 주소 등의 텍스트 형태의 위치정보 데이터에 대해서도 고려한 연구가 있다[3]. 그리고 사진파일에 저장되어 있는 GPS 정보 통해 유사한 파일을 탐지하고, GPS 정보 조작여부에 대해 판단하는 방법을 제안한 연구[4] 등이 있다.

또한 국외에서는 TomTom 내비게이션 기기의 좌표, 경로 등의 위치정보와 사용흔적에 대한 분석 방법 및 시각화 기법에 대해 지속적으로 연구가 진행되고 있으며[5], 국내에서도 국내 내비게이션 기기인 맵피, 아이나비, 지니, 아틀란에 남아 있는 사용흔적과 위치정보를 분석한 연구[6]가 있다.

이와 같이 기존의 위치정보에 대한 포렌식 연구는 위치정보를 이용하는 소프트웨어와 디바이스에 대해 개별적으로 그 사용흔적과 분석 방법에 대해 연구되고 있다. 따라서 본 논문에서는 안드로이드 스마트폰에서 발견할 수 있는 위치정보를 로그, 이미지, 애플리케이션 측면에서 다각적으로 분석하여, 수사기관에서 안드로이드 스마트폰 이용자의 위치정보에 대해 조사하는 경우에 다양한 출처로부터 위치정보를 확보하고 분석시간을 단축시키고자 한다.

2. 계층적 군집화 알고리즘 (Hierarchical Clustering)

통계적 분석 방법을 이용한 데이터 마이닝 기법 중 하나인 계층적 군집화 알고리즘은 K-means와 같은 비계층적 군집화 알고리즘과 달리 최종 군집 개수를 처음에 설정하지 않더라도 군집이 계층을 이루도록 군집화를 수행한 후, 덴드로그램을 통해 군집의 계층적 구조를 파악할 수 있는 방법이다[7]. 특히 계층적 군집화 알고리즘에서 병합적 방법은 각각의 데이터를 하나의 군집으로 보고 유사도에 따라 가장 가까운 군집을 찾아가는 방식으로, 군집간의 거리를 어떻게 정의하느냐에 따라 다양한 방법이 존재한다. 본 논문은 추출된 위치정보를 대상으로 이용자의 거점, 행동반경, 관심지역 등을 파악하기 위해 계층적 군집화 알고리즘을 활용한다. 계층적 군집화 알고리즘의 내용은 표 1과 같다.

표 1. 계층적 군집화 알고리즘

단 계	내 용
[Step 1]	각 데이터를 하나의 군집으로 형성 최초 N개의 데이터 집합 $\{x_1, x_2, \ldots x_N\}$과 군집 $\{C_1, C_2, \ldots C_N\}$
[Step 2]	Loop
[Step 3]	군집간의 거리를 계산 · $d(C_i, C_j) = \min_{x_i \in C_i, x_j \in C_j} d(x_i, xj)$
[Step 4]	거리가 가장 가까운 두 군집을 병합하여 새로운 군집을 생성 · $C_{ij} = C_i \cup C_j$
[Step 5]	until 하나의 군집이 남을 때까지 반복 End Loop

3. GPS와 안드로이드 위치정보

GPS (Global Positioning System)는 삼각측량의 원리를 이용하여 3개 이상의 GPS 위성으로부터 수신한 신호를 통해 GPS 수신기의 위치를 결정하는 시스템이다. GPS의 공식적인 기준좌표계는 WGS 84 (World Geodetic System 1984)지만, 기반이 되는 타원체와 평면 투영방식에 따라 다양한 좌표계가 존재한다. 그리고 스마트폰 애플리케이션의 저장 구조는 개발자에 의존적이기 때문에, 스마트폰에 저장되어 있는 좌표 정보의 경우에도 각 지역에 적합한 좌표계를 적용하기 위해서 지역좌표계로 변환하거나 고유 좌표계를 사용하는 경우가 있다[8]. 그러므로 위치정보를 나타내기 위해 사용되는 좌표계에 대해 미리 인지하고 대응할 필요가 있다.

또한, 안드로이드에서 현재 스마트폰의 위치정보를 측정하는 방법은 크게 GPS를 이용하는 방식과 Android's Network Location Provider를 이용하는 방식으로 나누어진다[9]. GPS는 스마트폰에 내장된 GPS 센서를 이용하는 방식으로, 높은 정확도를 가지고 있으나 실외에서만 작동하고 배터리 소모가 크며 업데이트되는 속도가 빠르지 않다는 단점이 있다. Android Network Location Provider는 기지국과 와이파이의 위치 및 신호 강도를 이용하여 스마트폰의 위치를 결정하는 방식으로, 실내와 실외에서 모두 작동이 가능하고 배터리 소모가 적으며 위치정보가 업데이트되는 속도가 빠르지만 상대적으로 오차범위가 큰 단점이 있다. 안드로이드에서는 위치 정보의 정확성, 배터리 소모 등을 고려하여 효율적으로 스마트폰의 위치정보를 얻기 위해 위의 방식들을 조합하여 사용한다.

4. 지리적 프로파일링 (Geographic Profiling)

지리적 프로파일링은 범죄자가 가장 소재할 가능성이 높은 장소나 다음 범죄지를 예측하는 장소지향적 수사기법으로, 연쇄사건, 실종사건과 같이 여러 장소와 관련된 사건이나 범죄유형 분석, 순찰차 배치와 같은 범죄예방활동 등에 활용되고 있다[10].

대표적인 지리적 프로파일링 시스템으로는 캐나다의 CGT (Criminal Geographic Targeting), 미국의 Crime Stat, 영국의 DRAGNET 등이 있다. 우리나라에서도 2009년에 국내 지역적 특성과 실정에 맞는 GeoPros를 개발하였고 최근 고도화 작업을 마쳐 범죄예방 및 검거활동에 적극적으로 활용하고 있다. 그림 1은 GeoPros를 이용한 범죄 다발지역을 분석한 화면을 보여준다[11].

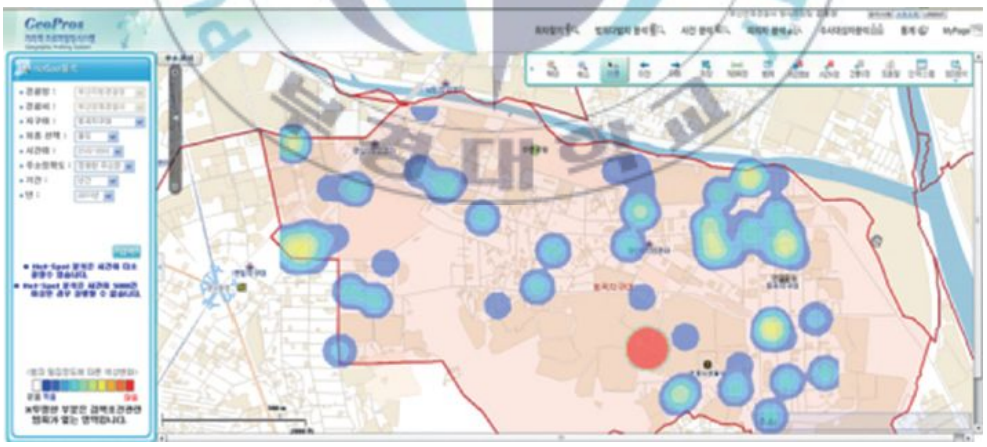

그림 1. 지리적 프로파일링 시스템을 이용한 범죄 다발지역 분석 (예시)

지리적 프로파일링과 관련된 연구로는 연쇄강력 범죄자의 주거지와 범행장소간에 연관성이 있음을 확인하고, 범행동기, 범인의 연령, 범행지속의

요인들이 범인의 평균 이동거리에 미치는 영향에 대해 분석한 연구[12]가 있고, 연쇄방화범을 대상으로 범행동기와 범죄자 유형에 따른 다양한 행동특성과 이동특성을 분석한 연구[13] 등이 있다.

또한 군집화를 이용한 지리적 프로파일링과 관련된 연구로는, 통계적 방법을 이용하여 공간적 패턴 분석뿐만 아니라 범행 위치의 공간적 분포와 범죄 발생의 시간적 분포 특성을 분석하여 연쇄 범죄 위치를 보다 정확하게 예측하는 알고리즘인 STA-BLP (Spatio-Temporal Analysis based Base Location Prediction)을 제안한 논문에서 지역적, 전역적 거점 위치를 예측하기 위하여 군집화된 범행위치를 이용한 연구가 있다[14]. 또한 범죄수법, 범죄 현장, 피해자 특징 등 범죄 장소에서 발견할 수 있는 50개의 기준을 선정한 뒤 유클리디안 제곱 거리 및 와드 연결법을 적용한 계층적 군집화 알고리즘을 적용하여 연쇄살인범을 체계적/비체계적 분류의 타당성을 살펴본 연구[15]도 있으며, 다음 범죄지를 예측하기 위해 K-means 알고리즘을 활용한 다중지점 공간평균 (Multi-point Centrography) 모델을 제안한 연구[16],, 그리고 범죄는 일반적으로 군집을 형성하므로 가장 적합한 군집 알고리즘을 결정하기 위하여 K-means, NNH, STAC (Spatio-temporal Analysis of Crime), fuzzy, ISODATA, GAM (Geographical Analysis Machine)의 다양한 군집 알고리즘을 대상으로 맨하탄, 유클리디안 거리를 각각 적용하여 군집의 유효성을 비교, 분석한 연구[17]가 있다.

기존의 지리적 프로파일링 연구에서도 범죄지, 사건 장소를 통해 범죄자의 거점 혹은 다음 범죄지를 예측하기 위하여 군집화 알고리즘을 많이 활용하고 있다. 본 논문에서는 범죄자의 스마트폰에 저장된 위치정보의 군집분석을 통해 거점을 파악하고 관심지역과 범죄지와의 연관성 등을 도출하고자 한다.

Ⅲ. 안드로이드 위치정보 분석

안드로이드 스마트폰에 저장되는 위치정보는 안드로이드의 시스템 로그, 사진에 저장된 GPS 메타데이터, 지도 및 내비게이션 등 위치정보를 사용하는 각종 애플리케이션에서 발견할 수 있다. 본 논문에서는 구글의 안드로이드 레퍼런스 스마트폰인 Nexus 4를 대상으로, 디지털 포렌식 도구인 EnCase와 PC에 연결된 안드로이드 기기를 제어하고 통신할 수 있는 ADB (Android Debug Bridge), 그리고 통계분석 도구인 R을 이용하여 안드로이드에 저장되는 다양한 위치정보에 대하여 분석한다. 표 2는 본 논문의 구체적인 위치정보 분석 대상과 환경을 나타낸다.

표 2. 위치정보 분석 대상 및 환경

종 류	이 름	버 전
DEVICE	Nexus 4	4.4.2
	Nexus 4 (Rooting)	4.4.2
SOFTWARE	EnCase Forensic	7.09.03.40
	ADB	1.0.31
	R	3.1.0
APPLICATION	Naver Map	4.0.3
	Daum Map	3.8.0
	Google Map	8.0.0
	Olleh Map	3.4.1
	Olleh Navi	3.4.1
	Kimgisa Navi	2.3.1
	Atlan3D Navi	2.3.041
	iNavi Air	2.00

1. 안드로이드 로그의 위치정보

안드로이드 로그는 휘발성 데이터로 주로 시스템 관리와 디버깅을 위한 정보로서 제공된다. 안드로이드 로그에 접근하는 방법으로는 시스템과 애플리케이션 디버그 메시지를 출력하는 logcat, 시스템 세부 정보에 대한 dumpsys, 디버그 로그와 시스템 정보를 연결시켜주는 dumpstate가 있으며, 이들 명령을 통합적으로 보여주는 bugreport가 있다[18].

bugreport의 location 서비스의 덤프에서 스마트폰의 마지막 위치정보(Last Known Location)를 확인할 수 있고, 이 위치정보는 각각 gps, network, passive, fused 방식으로 측정된 위치를 나타낸다.

그림 2는 안드로이드 기기의 Last Known Location 정보를 보여준다.

그림 2. 안드로이드 로그의 Last Known Location 정보

gps는 위성을 이용한 위치정보를 의미하고, network는 기지국과 와이파이 AP를 통해 측정된 위치정보를 말한다. passive는 다른 애플리케이션이나 서비스에서 업데이트된 위치정보를 수동적으로 가져는 것이고, fused는 위치정보 측정의 정확성과 배터리 소모 등 효율성 향상을 위해 GPS, 와이

파이, 기지국, 각종 센서 정보를 이용하여 지능적으로 최적의 위치를 나타내는 방식이다[19].

또한 안드로이드 시스템 로그에서도 위치정보를 확인할 수 있다. 그림 3은 구글의 뉴스와 날씨 정보를 제공해 주는 지니 위젯에서 사용한 위치정보를 나타낸다.

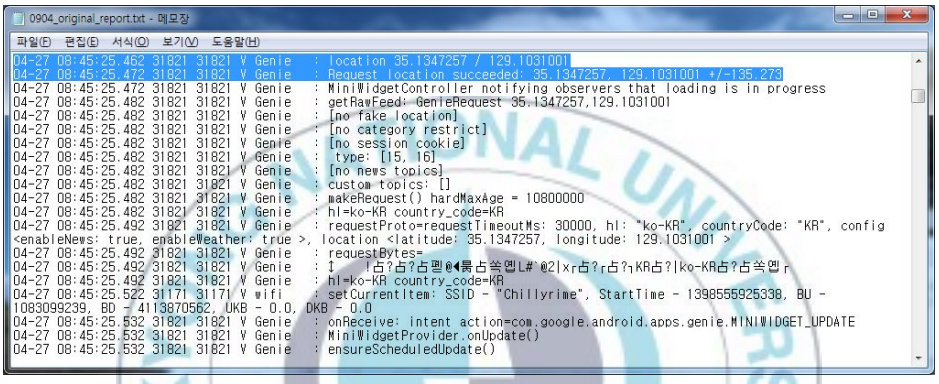

그림 3. 시스템 로그에 남아 있는 지니위젯의 위치정보

2. 이미지 메타데이터의 위치정보

스마트폰의 GPS 기능을 활성화시키고 사진을 촬영하면 해당 이미지에 촬영시간, 위/경도 등의 메타데이터가 EXIF (Exchangeable Image File Format) 형식으로 저장된다. 이 중 위치정보와 관련된 태그 정보는 표 3과 같다[20]. 스마트폰에는 직접 촬영한 사진뿐만 아니라 다운로드, 공유, 복사한 이미지도 존재할 수 있으므로 분석의 효율성을 위해서 제조사와 모델명 기준으로 필터링하는 작업도 고려한다.

표 3. 이미지에 저장된 위치정보와 관련된 태그

종 류	Tag ID	필 드 명	설 명
IFD	0x010F	Make	제조사
	0x0110	Model	모델명
	0x8825	GPSInfoIFD Pointer	GPS 포인터
GPS Info	0x0001	GPSLatitudeRef	북(N), 남(S)
	0x0002	GPSLatitude	위도
	0x0003	GPSLongitudeRef	동(E) / 서(W)
	0x0004	GPSLongitude	경도
	0x0007	GPSTimeStamp	GPS 촬영시간
	0x001D	GPSDateStamp	GPS 촬영날짜

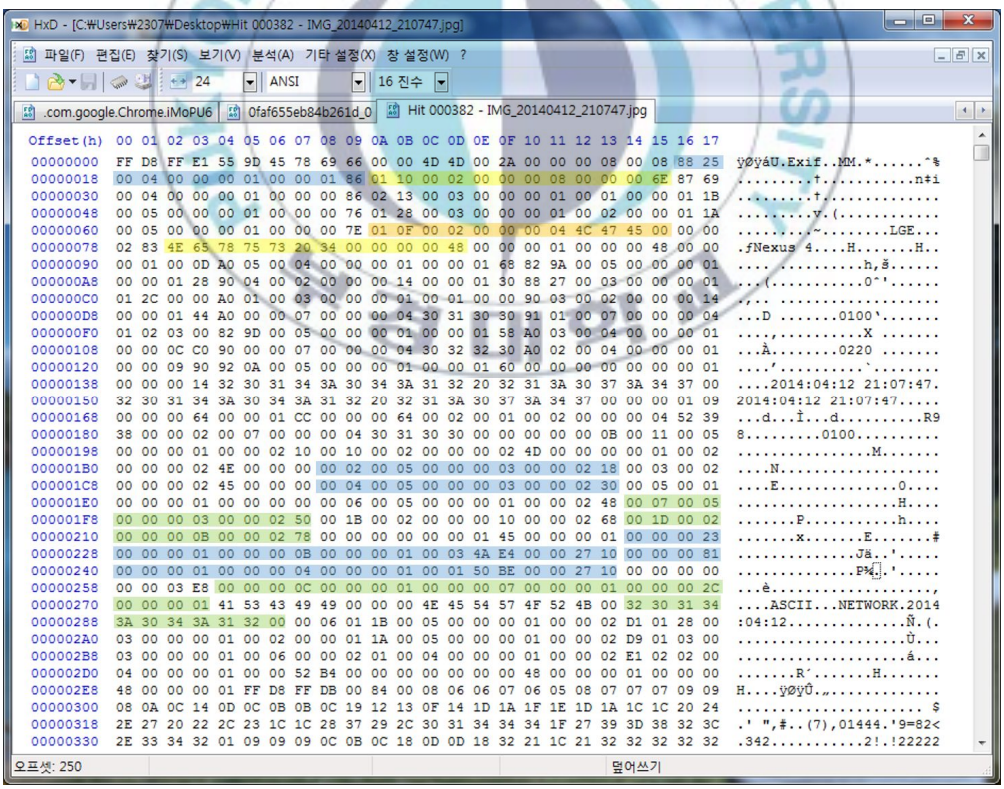

그림 4. 이미지에 저장되어 있는 위치정보 분석

그림 4는 헥사 에디터를 통해 이미지에 저장되어 있는 위치정보를 보여준다. 위도와 경도의 좌표 값은 24byte로 구성되어 있고, 각 8byte는 각각 도, 분, 초를 의미한다. 그리고 GPS 촬영시간 또한 24byte로 구성되어 있으며, 각 8byte는 각각 시, 분, 초를 의미한다. GPS 촬영날짜는 아스키 코드 형태로 저장된다.

3. 애플리케이션의 위치정보

지도와 내비게이션 애플리케이션은 지역 검색, 경로 탐색, 관심 지역 등록, 위치 공유 등의 기능을 제공하므로 스마트폰 이용자가 관심이 있는 지역이나 탐색하였던 경로 등을 파악할 수 있다. 안드로이드 애플리케이션의 인기 순위[21]에 따라, 지도 애플리케이션은 Naver Map, Daum Map, Google Map, Olleh Map, 내비게이션 애플리케이션은 Olleh Navi, Kimgisa Navi, Atlan3D Navi, iNavi Air를 선정하여 분석한다.

스마트폰 데이터를 수집하는 방법으로는 논리적으로 추출하는 방법과 물리적으로 추출하는 방법이 있다. 논리적 추출 방법은 USB 인터페이스를 이용하여 파일시스템이 관리하는 파일 및 디렉토리를 추출하는 방법이고, 물리적 추출방법은 dd 명령어, JTAG, 메모리 덤프, Boot loader를 이용하여 비할당 영역이나 슬랙 영역까지 추출하는 방법을 말한다[22]. 본 논문에서는 안드로이드 스마트폰을 대상으로 논리적 추출 방법을 이용하여 데이터를 수집한다.

애플리케이션 조사를 위해서 안드로이드의 내부저장소와 외부저장소를 확인한다. 안드로이드 애플리케이션의 내부 데이터 저장소는 /data/data/

<패키지명> 디렉토리의 하위에 위치하고, 일반적으로 shared_prefs, lib, files, cache, databases의 5가지 하위 디렉토리로 구성되며 루팅을 해야 접근이 가능하다. 외부저장소는 /sdcard/data/<패키지명> 디렉토리 하위에 위치하고 기본적으로 권한 제어가 적용되지 않아 루팅 없이도 확인이 가능하다[18].

표 4는 안드로이드 애플리케이션 분석을 위한 일반적인 안드로이드 내부저장소의 구조를 나타낸다.

표 4. 일반적인 안드로이드 내부저장소의 구조

종류	내용
shared_prefs	· 키, 값 형태의 XML 포맷 Shared Preferences 데이터를 저장
lib	· 애플리케이션이 사용하는 커스텀 라이브러리
files	· 개발자가 내부 저장소에서 사용하는 파일
cache	· 애플리케이션에 의해 캐시된 파일
databases	· SQL 데이터베이스 파일과 저널 파일

본 논문에서는 내부저장소 접근을 위해 스마트폰의 루트권한을 얻은 뒤 각 애플리케이션을 분석하였다. 또한 범용 디지털 포렌식 도구인 EnCase를 이용하여 스마트폰 이미지를 수집한 뒤 키워드, 인덱스 검색, 파일 구조 분석 등을 수행하였다. EnCase의 경우, 과거에는 Content Provider 방식[23]으로 안드로이드 스마트폰 데이터를 수집하였으므로 연락처, 통화기록, 인터넷 사용흔적, 설치된 애플리케이션 목록 등 제한된 정보만 수집이 가능하였으나, 현재는 백업 방식으로 데이터를 수집하므로 애플리케이션 데이터까지 모두 확인이 가능하다.

3.1 Naver Map

Naver Map의 패키지명은 com.nhn.android.nmap으로서, Naver Map에서 발견할 수 있는 사용흔적으로는 로그인 방식에 따른 이용자의 ID와 암호화된 패스워드가 있고, 가장 최근에 로그인한 ID를 식별할 수 있다. 그리고 위치정보에서 검색의 경우에는 이용자가 검색한 검색어, 검색 후 해당 위치를 확인하였는지 여부, 검색된 위치의 좌표, 검색 시간, 검색된 위치의 주소지 등을 알 수 있다. 또한 경로 탐색의 경우 출발지명과 도착지명, 출발지좌표와 도착지좌표, 시간정보를 확인할 수 있다.

Naver Map의 위치정보는 검색시간 (Epoch), 좌표 정보 (WGS 84), 기타 텍스트 형태의 검색어, 주소 등이 있다.

표 5. Naver Map의 사용흔적 및 위치정보

종류	파일명	설명
prefs	<모델명>.xml	· 마지막 로그인 ID, 암호화된 PW
	key_manual_<모델명>_<ID>.xml	· 수동 로그인 ID, 암호화된 PW
db	mapHistory.db - RecentHistory	· title: 검색어 · type: 검색 후 해당 지역 확인 여부 (0, 1) · **x y: 좌표 (WGS 84)** · **time: 검색 시간 (Epoch)** · addr: 검색된 지역의 주소 (type이 1인 경우) · **poix, poiy: addr의 좌표**
	mapHistory.db - RecentRoute	· start: 출발지명 · **startx, starty: 출발지 좌표** · end: 도착지명 · **endx, endy: 도착지 좌표** · **time: 검색 시간**

Table: RecentRoute

	uid	start	startx	starty	end	endx	endy	time
1	-2111292990	부경대학교대연캠퍼스2호관	129,1028361	35,1347469	부산사하경찰서	128,9781122	35,0856926	1394009194897
2	-2046159631	현대타운아파트	129,0694431	35,1891041	암남공원	129,020364	35,06375	1396751947716
3	-1872919787	이태원역 6호선	126,9945961	37,534542	천주교 한남동성당	127,00255	37,533725	1393491274928
4	-1686288753	몰만골역 3호선	129,0858591	35,1764712	이마트 연제점	129,0817884	35,1755714	1393491274895
5	-1481826063	부경대학교 용당캠퍼스	129,095839	35,1184	오토큐 용호점	129,1109091	35,1167025	1393491274886
6	-1218072054	한남마을마당	127,0038796	37,5389768	미트패킹레스토랑	126,9955422	37,5349877	1396083168058
7	-1142871391	부경대학교대연캠퍼스미래관	129,1022821	35,1344096	시실리	129,1009755	35,1321298	1393491274859
8	-1137227030	한강진역 6호선	127,0017552	37,5395247	서울한남초등학교	127,0047575	37,538338	1393491274913
9	-1090804998	센텀시티역 부산2호선	129,1316342	35,168903	더파티 센텀점	129,1258081	35,1742074	1395280285386
10	-929885981	부경대학교 용당캠퍼스	129,095839	35,1184	오토큐 대연점	129,0848698	35,1350292	1393491274890
11	-824112582	인제약국	129,0681638	35,1888131	사직쌍용예가아파	129,0557802	35,1969782	1393491274855
12	-693314084	종합운동장역(빅토리움)	129,0677757	35,1911263	거제동월드메르디	129,0827415	35,1927316	1393491274872
13	47135783	부경대학교대연캠퍼스3호관	129,1033949	35,1349584	김해국제공항국제	128,9490625	35,1737596	1393491274868
14	15354812	탐앤탐스커피부산장산역점	129,1756808	35,1696201	나라시스템	129,1280814	35,173289	1393491274881
15	365771318	광음교회	128,6853446	35,8367808	경산IC	128,7868292	35,8776802	1396314023296
16	420738258	한남마을마당	127,0038796	37,5389768	충청남도 서천군	126,691763	36,080283	1396086125851
17	720545328	참마트기린약국	129,0562651	35,1394388	부경대학교 대연캠	129,101239	35,133392	1395206653624
18	816748416	한강진역 6호선	127,0017531	37,5395269	더케이서울호텔	127,034141	37,468016	1393491274908

그림 5. mapHistory.db의 RecentRoute 테이블

표 5는 Naver Map에서 발견할 수 있는 사용흔적 및 위치정보를 정리한 것이고, 그림 5는 mapHistory.db의 RecentRoute 테이블을 나타낸다.

3.2 Daum Map

Daum Map의 패키지명은 net.daum.android.map으로서, Daum Map에서 발견할 수 있는 사용흔적으로는 이용자가 마지막으로 로그인한 ID가 있다. 그리고 Daum Map의 위치정보의 경우에는 시간정보와 함께 지역검색, 경로검색, 버스, 지하철 등으로 구분되어 저장이 된다. Daum Map에서 사용하는 좌표계는 Naver Map과 Google Map과는 달리, WGS 84 타원체를 기반으로 한 TM (Transverse Mercator) 좌표계의 변형인 wcongnamul 좌표계를 사용한다[24]. 이외에도 지도, 지하철 노선도의 캐시된 이미지가 저장된다.

Daum Map의 위치정보는 검색시간 (Epoch), 좌표 정보 (wcongnamul), 기타 텍스트 형태의 검색어, 주소 등이 있다.

표 6. Daum Map의 사용흔적 및 위치정보

종류	파일명	설명
prefs	net.daum.mf.ex.login.xml	· 마지막 로그인 ID · 해당 ID의 로그인 타입
	Preference.xml	· 최초 검색 경로 (출발지 및 도착지) · 해당 출발지와 도착지의 좌표
db	**map/data/search_history.db** **- search_history**	· type: 검색(100), 경로 검색 (200), 버스(300), 지하철(800) · key: 검색어, 검색된 지역명 · address: 검색된 지역의 주소 **· posX, posY: 검색지 좌표** **(wcongnamul)** **· startX, startY: 출발지 좌표** **· endX, endY: 도착지 좌표** · hitPoint: 검색 횟수 **· updatetime: 시간 (Epoch)**
	map/data/favorite.db map/data/<ID>/favorite.db - favorite	· name: 즐겨찾기 이름 · type: 검색(100), 경로(200), 버스(130), 지하철(150) · coords: 검색 (하나의 좌표) 경로 (두개의 좌표) · atime, mtime: 시간
cache	cache/map/cache/0001	· 지도, 지하철 노선도 등 캐시 이미지
	map/cache/0001/cache.db	· 캐시 이미지 관리

Table: search_history

	idx	type	key	chosungKey	address	posX	posY	itemid		startPoint	startX	startY	endPoint	endX	endY
1	1	100	부경대학교	ㅂㄱㄷㅎㄱ		0,0	0,0		1	1	-10000000,0	-10000000,0		-10000000,0	-10000000,0
2	2	100	부경대학교 대연캠퍼스	ㅂㄱㄷㅎㄱ ㄷ	부산 남구 대연	979940,0	460153,0	10464564	1	1	-10000000,0	-10000000,0		-10000000,0	-10000000,0
3	3	100	문화양곱창	ㅁㅎㅇㄱㅊ		0,0	0,0		1	1	-10000000,0	-10000000,0		-10000000,0	-10000000,0
4	4	100	문화양곱창	ㅁㅎㅇㄱㅊ	부산 부산진구	968532,0	465580,0	8988183	1	1	-10000000,0	-10000000,0		-10000000,0	-10000000,0
5	5	100	거제동 현대타운	ㄱㅈㄷ ㅎㄷㅌ		0,0	0,0		1	1	-10000000,0	-10000000,0		-10000000,0	-10000000,0
6	6	100	거제동 현대타운	ㄱㅈㄷ ㅎㄷㅌ		0,0	0,0		1	1	-10000000,0	-10000000,0		-10000000,0	-10000000,0
7	7	100	현대(1025번지)아파트	ㅎㄷ(1025ㅂㅈ)	부산 연제구 거	971179,0	475197,0	11201947	1	1	-10000000,0	-10000000,0		-10000000,0	-10000000,0
8	8	200				0,0	0,0		0	1	현대(1025번지)아파	971179,0	475197,0	문화양곱창	968532,0	465580,0
9	9	300	1001번 버스	1001ㅂ ㅂㅅ		0,0	0,0		1	1	-10000000,0	-10000000,0		-10000000,0	-10000000,0

그림 6. search_history.db의 search_history 테이블

표 6은 Daum Map에서 발견할 수 있는 사용흔적 및 위치정보를 정리한 것이고, 그림 6은 search_history.db의 search_history 테이블을 나타낸다.

3.3 Google Map

Google Map의 패키지명은 com.google.android.apps.maps으로서, Google Map에서는 구글계정 정보와 지역 검색에 대한 위도, 경도 좌표, 검색어에 대한 구글맵 연동 URL, 시간정보를 확인할 수 있고, 기타 구글 스트리트뷰에서 캐시된 이미지와 마지막 위정지도의 위치 좌표를 알 수 있다.

Google Map의 위치정보는 검색시간 (Epoch), 좌표 정보 (WGS 84), 검색어 (URL)가 있다.

표 7. Google Map의 사용흔적 및 위치정보

종류	파일명	설명
prefs	camera.xml	· 마지막 구글 위성지도의 위치 · lng: 경도 · lat: 위도
	settings_preference.xml	· 계정 및 환경설정정보
db	**gmm_myplaces.db** **- sync_item**	· key_string: 검색어에 대한 구글맵 연동 URL · **timestamp: 시간 정보 (Epoch)** · **latitude: 위도 (WGS 84)** · **longitute: 경도**
cache	tile_<문자열>	· 구글 스트리트뷰 이미지 캐시 파일
	cache_r.0	· 계정 사진 정보 (외부저장소)

Table: sync_item

	corpus	key_string	timestamp	merge_	featur	latitude	longitude
1	1	http://maps.google.com/?q=%EB%B6%	1392024059666	38827012	817514	35189297	129069217
2	8	1:0	1388416274261	0		35134763	129108109
3	1	http://maps.google.com/?cid=15870869	1400146045795	58141321	983684	35888800	128610281
4	1	http://maps.google.com/?cid=15199383	1400148072285	57111656	580895	35846829	127129363
5	1	http://maps.google.com/?cid=1198878E	0	0	627931	35189331	129069003
6	1	http://maps.google.com/?cid=1203133E	0	0	932653	35205523	129059781
7	1	http://maps.google.com/?cid=13707832	0	0	044052	35420264	128989117

그림 7. gmm_myplaces.db의 sync_item 테이블

표 7은 Google Map에서 발견할 수 있는 사용흔적 및 위치정보를 정리한 것이고, 그림 7은 gmm_myplaces.db의 sync_item 테이블을 나타낸다.

3.4 Olleh Map

Olleh Map의 패키지명은 com.kt.ollehmap이다. Olleh Map에는 지역검색 및 경로검색으로 검색된 지역의 위치명과 UTM-K 방식으로 기록된 좌표정보가 저장되어 있지만, 시간정보는 확인할 수 없다.

Olleh Map의 위치정보는 좌표 정보 (UTM-K)와 지역명이 있다.

표 8. Olleh Map의 사용흔적 및 위치정보

종류	파일명	설명
db	**ollehmap2.db**	· address: 주소 · display_name: 검색지 (출발지) **· position_x: 검색지 경도 (UTM-K)** **· position_y: 검색지 위도** · end_name: 도착지 **· end_position_x: 도착지 경도** **· end_position_y: 도착지 위도**
text	latest_list.txt	· 텍스트 형태의 검색, 경로 정보

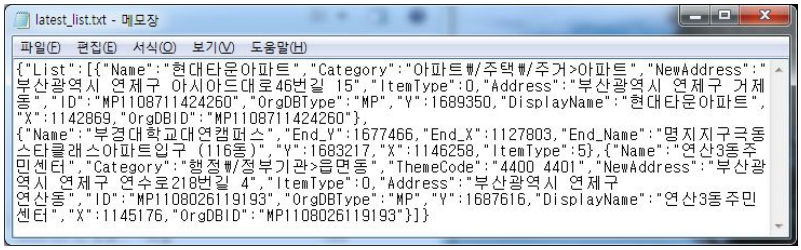

그림 8. latest_list.txt

표 8은 Olleh Map에서 발견할 수 있는 사용흔적 및 위치정보를 정리한 것이고, 그림 8은 latest_list.txt 파일 내용을 나타낸다.

3.5 Kimgisa Navi

Kimgisa Navi의 패키지명은 com.locnall.KimGiSa이다. Kimgisa Navi에는 이용자의 ID 정보, 평문의 패스워드와 함께, 마지막으로 GPS를 수신한 위치와 검색한 도착지가 KTM (TM 128) 좌표계 형태로 저장되어 있지만, 시간정보는 확인할 수 없다.

Kimgisa Navi의 위치정보는 좌표 정보 (KTM)와 도착지명이 있다.

표 9. Kimgisa Navi의 사용흔적 및 위치정보

종류	파일명	설명
prefs	KimGiSaPreferences.xml	· user_id: ID · user_pass: 평문의 PW · **last_known_location_x_key: 경도** · **last_known_location_y_key: 위도** **마지막 위치의 좌표 (KTM)** · navi_recent_path_name_key: 도착지 · **navi_recent_path_x_key: 도착지경도** · **navi_recent_path_y_key: 도착지위도**

<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<map>
<string name="navi_recent_path_name_key"/>
<long name="month_traffic_key" value="778389"/>
<int name="navi_recent_path_x_key" value="-1"/>
<string name="current_destination_group_key">20130925171004876610-48617</string>
<string name="user_udid">355136051692658</string>
<string name="init_traffic_date_key">2014년 5월 15일</string>
<string name="user_id">say4ever</string>
<string name="push_key">APA91bHX1KW8vGdpLLAk_bRcB5D6eTS3wDBDmN577APSC360d3sveXK_NRubZbHUriaOaJao-2ijs9IgFiY-klU22-s8reGGQht8kpVvFyGFRu_pgXtDnxMqhUvblvn26_JhjiDD9N95ct17h4rUrwrbDX6TUN5e9Q</string>
<string name="current_destination_key">20140516064820591058-89255</string>
<int name="navi_recent_path_rpflag_key" value="-1"/>
<long name="total_traffic_key" value="778389"/>
<boolean name="navi_recent_path_freeway_key" value="false"/>
<int name="navi_recent_path_y_key" value="-1"/>
<string name="user_pass">[redacted]</string>
<boolean name="new_install" value="false"/>
<boolean name="current_displayed_beehive_key" value="false"/>
<int name="traffic_monthly_key" value="5"/>
<int name="last_known_location_x_key" value="500670"/>
<boolean name="data_folder" value="true"/>
<boolean name="navi_recent_path_key" value="false"/>
<boolean name="new_item_square_key" value="false"/>
<boolean name="navi_time_gubun_key" value="false"/>
<int name="last_known_location_y_key" value="282316"/>
</map>

그림 9. KimGiSaPreferences.xml

표 9는 Kimgisa Navi에서 발견할 수 있는 사용흔적 및 위치정보를 정리한 것이고, 그림 9는 KimGiSaPreferences.xml 파일 내용을 나타낸다.

3.6 Atlan3D Navi

Atlan3D Navi의 패키지명은 kr.mappers.AtlanSmart으로서, 사용흔적과 위치정보는 외부저장소로부터 확인할 수 있고 도착지점 및 등록지점의 위도, 경도 좌표와 주소, 연월일시분초 형태의 검색시간 등이 UTF-8 형태의 텍스트로 인코딩되어 ‘;’으로 항목을 구분하여 저장되어 있다.

Atlan3D Navi의 위치정보는 검색시간 (YMDHMS), 좌표 정보 (WGS 84), 검색어가 있다.

0;0;0;7233921;129.1317082;35.1689357;129.1317082;35.1689357;센텀시티역(부산2호선);;부산 해운대구 우동(우2동);부산 해운대구 우동(우2동);부산 해운대구 센텀남대로 76;1291-27;;4613;99;0;0;0;;;11;1;1;0;2014;4;30;12;57;8
0;0;12;0;129.10237503051758;35.15618324279785;129.10237503051758;35.15618324279785;부산 수영구 광안동;;부산 수영구 광안동;;;;;2388;0;0;0;0;;;0;1;0;0;2014;4;30;12;56;31
0;0;0;6317924;129.0689431;35.1893634;129.069046;35.1889076;거제현대타운아파트;;부산 연제구 거제동(거제2동);부산 연제구 거제2동;부산 연제구 아시아드대로46번길 15;1025;;6815;8;0;0;0;;;2;1;1;0;2014;4;30;12;35;18

그림 10. AtlanSmartRecentDest.archive

표 10. Atlan3D Navi의 사용흔적 및 위치정보

종류	파일명	설명
External /sdcard/atlan3D/UserData/	**AtlanSmartRecentDest.archive**	· 도착지 정보 · **위도, 경도 (WGS 84)** · 검색지 주소 · **검색시간 (YMDHMS)**
	AtlanSmartRegHomeOffice.archive	· 등록 지점 · **위도, 경도 (WGS 84)** · 등록지 주소 · **검색시간**
	AtlanSmartSearchHistoryInfo.archive	· 검색어 히스토리 · 검색어 및 검색날짜
	AtlanSmartUserData.archive	· 이용자 ID

표 10은 Atlan3D Navi에서 발견할 수 있는 사용흔적 및 위치정보를 정리한 것이고, 그림 10은 AtlanSmartRecentDest.archive 파일을 나타낸다.

3.7 iNavi Air

iNavi Air의 패키지명은 com.thinkware.inaviair으로, 최종 수신된 위치정보의 위치와 시간정보, 검색어 및 검색된 지역명이 저장되어 있다. iNavi Air에서는 고유의 지도 좌표를 사용하고 있고 이에 대한 위치는 아이나비 지도 서비스에서 http://map.inavi.com/?rx=<x값>&ry=<y값>을 입력함으로써 확인할 수 있다.

iNavi Air의 위치정보는 GPS 수신시간 (Epoch), 고유 좌표 정보, 검색어가 있다.

표 11. iNavi Air의 사용흔적 및 위치정보

종류	파일명	설명
prefs	AFK_Frame_Gps_Info.xml	· 마지막으로 GPS를 수신한 위치의 **좌표 (고유좌표)** · **수신시간 (Epoch)**
	SearchResultSharedPreferences.xml	· 검색어 및 **좌표**

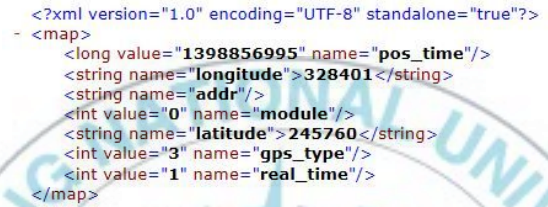

그림 11. AFK_Frame_Gps_Info.xml

표 11은 iNavi Airi에서 발견할 수 있는 사용흔적 및 위치정보를 정리한 것이고, 그림 11은 AFK_Frame_Gps_Info.xml 파일을 나타낸다.

3.8 Olleh Navi

Olleh Navi의 패키지명은 kt.navi으로서, 가장 최근에 검색한 경로에 대한 좌표 정보와 시간 정보를 확인할 수 있고, 또한 공유지, 도착지 각각에 대해서 저장된 좌표 정보와 검색어 목록이 저장되어 있다.

Olleh Navi의 위치정보는 시간정보 (YMDHMS), 좌표 정보 (KTM), 검색어가 있다.

표 12. Olleh Navi의 사용흔적 및 위치정보

종류	파일명	설명
prefs	**kt.navi_preferences.xml**	· 최근 출발, 경유, 도착지 및 등록지점의 **좌표 (KTM)** · **시간정보 (YMDHMS)**
db	**Db_DestinationSendList**	· 공유지의 위치 정보 · **time: 공유 시간** · **posX, posY: 좌표**
	Db_RecentDestination	· 도착지의 위치정보 · name: 검색지 (등록지명) · addr: 주소 · **posX, posY: 좌표**
	Db_RecentSearchListDbControl	· 검색어

그림 12. kt.navi_preferences.xml의 좌표정보

표 12은 Olleh Navii에서 발견할 수 있는 사용흔적 및 위치정보를 정리한 것이고, 그림 12은 kt.navi_preferences.xml 파일을 나타낸다.

4. 기타 위치정보

4.1 Google의 위치 기록

안드로이드 스마트폰에서 'Google 위치 정보 전송 기능'을 활성화한 경우에는 구글에서 해당 기기의 위치정보를 주기적으로 저장한다. 구글에 로그인된 기기의 위치는 https://maps.google.com/locationhistory에서 확인할 수 있다. 구글의 위치정보는 시간정보와 함께 저장되고 시각화 기능을 제공하므로 타임라인 분석이 가능하다. 또한 위치정보가 짧은 시간 단위로 축적되므로 용의자의 실거주지와 거점을 파악하는데 용이하며, 구글에서 지리 데이터를 표시하는데 사용하는 KML 포맷으로 내보내기를 할 수 있어 다른 도구와도 연계할 수 있다[25]. 다만, 계정에 등록된 모든 안드로이드 기기의 위치정보를 나타내므로 이를 고려해야 한다.

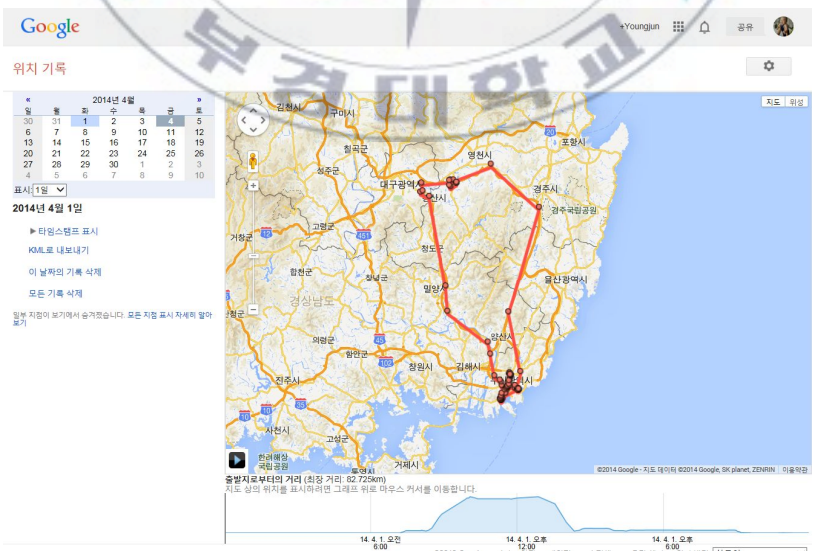

그림 13. 구글의 위치 기록 화면

4.2 날씨 애플리케이션

날씨정보는 일반적으로 이용자의 위치가 특정되어 있어야 서비스가 가능하므로 해당 애플리케이션에 위치정보가 남아 있을 가능성이 높다. 구글의 지니 위젯은 뉴스와 날씨정보를 제공하는 애플리케이션으로 패키지명은 com.google.android.apps.genie.geniewidget이다. 위치정보는 해당 애플리케이션의 weather.db을 통해서 확인할 수 있는데, 시간정보와 '시'와 '구' 단위의 위치정보를 확인할 수 있다.

Table: tblHourlyWeather

	_id	fakeLocation	location	timestamp	begins	ends	description	temperature
7	12572		Busan	1394050923644	1394118000000	1394121600000	Partly Cloudy	1
8	12573		Busan	1394050923644	1394121600000	1394125200000	Partly Cloudy	1
9	12574		Busan	1394050923644	1394125200000	1394128800000	Clear	0
10	12575		Busan	1394050923644	1394128800000	1394132400000	Clear	0
11	12576		Busan	1394050923644	1394132400000	1394136000000	Clear	-1
12	12793		Saha-gu	1394158860786	1394161200000	1394164800000	Sunny	5
13	12794		Saha-gu	1394158860786	1394164800000	1394168400000	Sunny	6
14	12795		Saha-gu	1394158860786	1394168400000	1394172000000	Sunny	6
15	12796		Saha-gu	1394158860786	1394172000000	1394175600000	Sunny	6
16	12797		Saha-gu	1394158860786	1394175600000	1394179200000	Sunny	6
17	12798		Saha-gu	1394158860786	1394179200000	1394182800000	Partly Cloudy	6
18	12799		Saha-gu	1394158860786	1394182800000	1394186400000	Partly Cloudy	5
19	12800		Saha-gu	1394158860786	1394186400000	1394190000000	Partly Cloudy	4
20	12801		Saha-gu	1394158860786	1394190000000	1394193600000	Partly Cloudy	3
21	12802		Saha-gu	1394158860786	1394193600000	1394197200000	Partly Cloudy	3
22	12803		Saha-gu	1394158860786	1394197200000	1394200800000	Partly Cloudy	3
23	12804		Saha-gu	1394158860786	1394200800000	1394204400000	Mostly Cloudy	2
24	12805		Saha-gu	1394158860786	1394204400000	1394208000000	Mostly Cloudy	2
25	12806		Saha-gu	1394158860786	1394208000000	1394211600000	Mostly Cloudy	2
26	12807		Saha-gu	1394158860786	1394211600000	1394215200000	Mostly Cloudy	2
27	12808		Saha-gu	1394158860786	1394215200000	1394218800000	Mostly Cloudy	1
28	12809		Saha-gu	1394158860786	1394218800000	1394222400000	Mostly Cloudy	1
29	12810		Saha-gu	1394158860786	1394222400000	1394226000000	Mostly Cloudy	1
30	12811		Saha-gu	1394158860786	1394226000000	1394229600000	Mostly Cloudy	1
31	12812		Saha-gu	1394158860786	1394229600000	1394233200000	Mostly Cloudy	2
32	12813		Saha-gu	1394158860786	1394233200000	1394236800000	Partly Cloudy	2
33	12814		Saha-gu	1394158860786	1394236800000	1394240400000	Partly Cloudy	3
34	12815		Saha-gu	1394158860786	1394240400000	1394244000000	Partly Cloudy	5
35	12816		Saha-gu	1394158860786	1394244000000	1394247600000	Partly Cloudy	6
36	13249		Dongnae-gu	1394364071751	1394366400000	1394370000000	Clear	3
37	13250		Dongnae-gu	1394364071751	1394370000000	1394373600000	Clear	3
38	13251		Dongnae-gu	1394364071751	1394373600000	1394377200000	Clear	2

그림 14. 지니 위젯의 weather.db

4.3 메신저 애플리케이션

메신저 애플리케이션은 채팅 기능뿐 아니라 위치 공유, 주변 위치 등의 서비스를 제공하고 있다. Facebook은 메신저 상에서 송신자의 위치를 보낼 수 있고, 이를 활성화한 경우에는 송신자 위치의 좌표가 남는다. 카카오톡은 특정 위치를 검색하여 상대방과 공유할 수 있는데, 대부분의 데이터가 암호화되어 있다.

표 13. Facebook의 사용흔적 및 위치정보

종류	파일명	설명
db	prefs_db - preferences	· 이용자 ID · 계정 정보 (이름, 전화번호, 이메일, 프로필 사진 등)
	threads_db2 **- messages**	· text: 메시지 내용 · **coordinates: 송신자 위치의 좌표 (WGS 84)** · **timestamp_ms: 시간 (Epoch)**
	nearby_tiles_db - nearby_tiles	· 근처 장소 (동서남북 좌표) · 주소, 지역명, 이름 등

표 14. KakaoTalk의 사용흔적 및 위치정보

종류	파일명	설명
prefs	KakaoTalk.perferences.xml	· 이용자 ID, 전화번호, 이메일, 상태 메시지, 프로필 사진
db	KakaoTalk.db	· 채팅메시지, 첨부 (암호화) · 와이파이 SSID

5. 안드로이드 위치정보 요약

안드로이드 로그, 이미지, 각종 애플리케이션으로부터 확인한 위치정보는 다양한 좌표계와 시간표기 방식을 이용하고 있다. 그리고 당시 이용자의 위치를 나타내는지 아니면 이용자가 관심이 있는 검색지, 경로를 나타내는지에 따라서도 구분될 수 있다. 표 15에서 안드로이드에서 발견할 수 있는 위치정보를 정리하였다.

표 15. 안드로이드의 위치정보 요약

종류	위치정보 형태	시간정보 형식	속성 구분
Android Log	WGS 84	YMDHMS, ET	현재 위치
Image's Metadata	WGS 84	EPOCH	현재 위치
Naver Map	WGS 84	EPOCH	검색, 경로
Daum Map	wCongnamul	EPOCH	검색, 경로
Google Map	WGS 84	EPOCH	검색
Olleh Map	UTM-K	X	검색, 경로
Kimkisa Navi	KTM	X	현재 위치, 경로
Atlan3D Navi	WGS 84	YMDHMS	경로
iNavi Air	고유좌표	EPOCH	현재 위치
Olleh Navi	KTM	YMDHMS	검색, 경로
Genie Wiget	시군구별 지역	EPOCH	현재 위치
Facebook	WGS 84	EPOCH	현재 위치
KakaoTalk	암호화	EPOCH	위치 공유

Ⅳ. 위치정보 분석 모델

본 논문에서는 3장에서 분석된 안드로이드 위치정보를 기반으로 계층적 군집화 알고리즘을 적용한 스마트폰 위치정보에 대한 포렌식 분석 모델과 조사 절차를 제안한다.

1. 제안 모델의 구조

본 논문에서 제안하는 모델은 크게 3가지 모듈로 구성된다. 스마트폰 데이터 중 위치정보를 추출하는 위치정보 추출 모듈 (Location Data Extractor), 위치정보가 가지고 있는 속성에 따라 구분해서 저장 및 관리하는 공통 포맷 모듈 (Common Format Module for Location Data), 추출된 위치정보를 분석하는 분석 모듈 (Analysis Module)로 구성된다. 그림 15는 제안 모델의 전체 구조를 나타낸다.

1.1 위치정보 추출 모듈 (Location Data Extractor)

위치정보 추출 모듈은 EnCase, Xry, Oxygen 등의 디지털 포렌식 도구나 포렌식적으로 검증된 수집방법을 이용하여 획득한 스마트폰 데이터에서 위치정보를 추출하는 모듈이다. 시스템 로그, 이미지의 메타데이터, 각종 애플리케이션으로부터 위치정보를 추출한다.

시스템 로그는 휘발성 데이터이므로 가장 먼저 추출하는 것이 바람직하

고, 이미지는 스마트폰 이용자가 촬영한 사진이 맞는지 확인하기 위하여 스마트폰의 제조사와 모델명으로 필터링한다. 그리고 애플리케이션의 저장 구조가 개발자에 의존적이므로 업데이트 현황 등 버전을 관리한다.

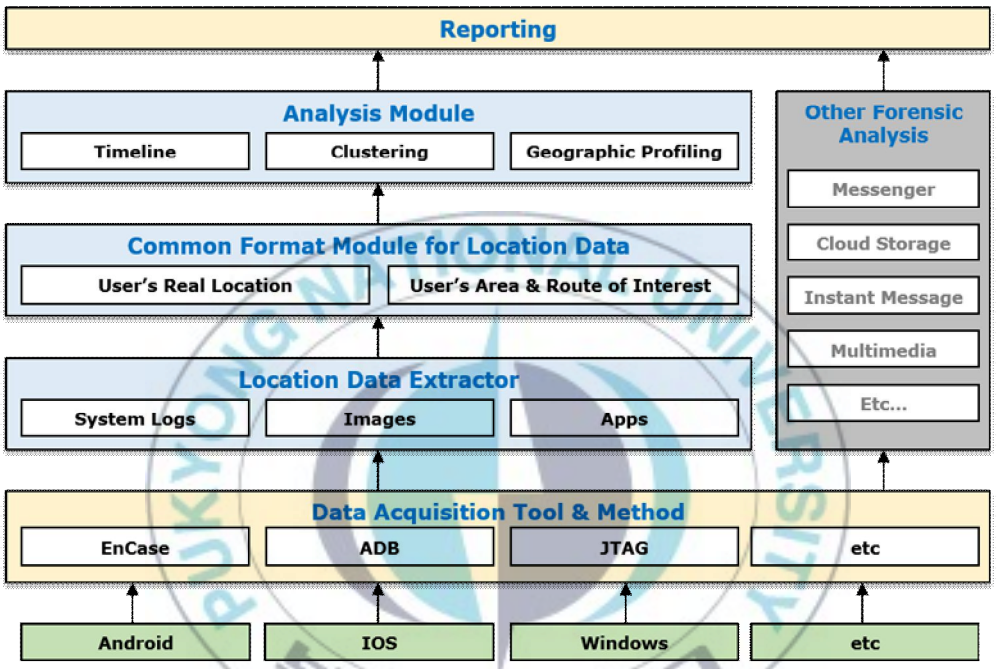

그림 15. 제안 모델의 아키텍처

1.2 위치정보 처리를 위한 공통포맷 모듈 (Common Format Module for Location Data)

일반적으로 시스템 로그나 이미지에서 추출한 위치정보의 경우에는 특정 시점의 이용자의 위치를 나타내지만, 지도, 내비게이션 애플리케이션에 저장된 위치정보의 경우에는 특정시점에 해당 지역을 검색하거나 경로를 탐색하였다는 것을 의미한다. 그러므로 이를 서로 구분하여 저장하고 각각

분석할 필요가 있다.

이 모듈에서 관리하는 위치정보는 기본적으로 시간정보와 위도, 경도의 좌표 데이터이다. 기타 검색어, 검색지 주소, 경로 좌표 등은 애플리케이션에서 저장하는 방식에 따라 선택적으로 포함되며, 최종적으로 XML 포맷을 활용하여 저장한다. 시간정보는 Epoch 타임으로 통일하고, 위치정보는 GPS 기준좌표계인 WGS 84로 변환하여 처리한다.

1.3 위치정보 분석 모듈

수사에 도움이 되는 정보로 가공하기 위하여 앞서 추출된 위치정보를 토대로 군집화, 타임라인, 지리적 프로파일링 분석을 수행한다. 계층적 군집화의 입력은 추출된 위치정보의 위도와 경도 데이터로서, 2차원 공간에서 장소지향적으로 군집화를 수행한다.

타임라인 분석은 시간정보를 통해서 범죄자의 위치 또는 행위를 재구성하며, 각종 사건 정보를 통해 지리적 프로파일링을 수행한다. 지리적 프로파일링은 범죄자의 거점 또는 다음 범죄지를 예측이 가능하므로, 앞서 군집화 분석을 통해 도출한 범죄자의 위치정보와 비교, 분석이 가능하다. 이러한 분석 내용을 종합하여 추후 조사지역에 대한 우선순위를 선정한다.

2. 제안 모델의 알고리즘

제안 모델의 알고리즘은 디지털 포렌식의 일반적인 수행 절차인 수집, 조사, 분석, 보고서 작성의 순서에 따라 구성된다[26].

표 16. 제안 모델의 알고리즘

Stage 1 Collect & Extract location data
Step 1 Acquire smartphone's data
Step 2 Extract location information in smartphone's data from system logs from image's metadata from applications
Step 3 Examine other parts where location information may exist
Return timestamp, location coordinates and other related data
Stage 2 Export the extracted location information
Step 1 Store real location and interesting area such as search history separately for efficient analysis
Step 2 Verify integrity using hash value
Return 2 XML files and hash value
Stage 3 Analyze the extracted location information
Step 1 Perform Hierarchical Clustering (1) Table 1 shows Specific algorithms (2) Similarity Measure : Euclidean distance (3) Linkage Method ① SLM (Single Linkage Method) ② ALM (Average Linkage Method) (4) Determine the number of clusters with certain height in dendrogram (5) Return the cluster values
Step 2 Geographic Profiling (1) Timeline Analysis (2) Compare with the clusters and the criminal area predicted from analysis of crime occurrence places
Step 3 Analyze with other forensic results such as contacts, SMS, calendar, call logs, SNS, etc.
Return the priority of investigation places and investigation directions
Stage 4 Reporing and Finding Evidence

제안 모델은 우선 스마트폰의 데이터를 수집한 뒤, 스마트폰에 저장된 위치정보에 대하여 시스템 로그, 이미지, 애플리케이션으로부터 위치정보를 추출하고, 기타 위치정보가 존재할 수 있는 부분에 대해서도 조사한다. 이를 통해 스마트폰의 다양한 출처로부터 위치정보와 관련된 시간정보, 좌표정보, 검색어 등 관련 데이터를 추출한다.

추출된 위치정보는 특정시점의 이용자의 실제 위치를 나타내는 경우와 특정시점에서 검색한 위치의 경우로 구분된다. 그러므로 위치정보를 실제 위치와 관심지역으로 구분하여 관리하며, 시간과 좌표단위는 각각 통일하여 XML 포맷으로 저장한다. 무결성 보장을 위하여 추출된 파일과 생성된 파일의 해시값을 보존한다.

추출된 위치정보의 위도와 경도의 좌표값은 계층적 군집화 알고리즘의 입력으로 이용한다. 계층적 군집화 알고리즘은 유사성을 근거로 새로운 군집을 생성해 나가는 방식으로 초기에 군집 수를 결정해주지 않아도 군집의 계층적인 모습을 확인할 수 있다.

계층적 군집화 결과에서 주어진 데이터에 적합한 덴드로그램의 높이를 결정함으로써 최종 군집된 결과를 얻을 수 있다. 스마트폰은 GPS, aGPS, 와이파이, 기지국 등을 통해 현재 기기의 위치를 측정하므로 각 방식에 따른 오차범위가 존재한다[3]. 그러므로 덴드로그램의 높이를 설정함에 있어 이용자의 행동반경과 함께 위치정보의 오차범위도 고려하여 결정하다.

제안 모델은 계층적 군집화에서 대표적으로 사용되는 유클리드 거리(Euclidean distance)를 기준으로 최단연결법 (Single Linkage Method)과 평균연결법(Average Linkage Method)을 이용한다. 최단연결법은 가장 가까운 데이터 쌍 간의 거리를 이용하는 방식으로 고립된 특정 군집을 찾는데 유용하고, 평균연결법은 모든 데이터 쌍들의 거리의 평균을 이용하는 방식으로 작은 분산을 가지는 군집을 형성하는 특징이 있다[7].

기타 위치정보의 시간 속성을 이용하여 사건발생 시간 및 지역과의 연관성, 범죄자의 이동경로, 이동패턴 등 타임라인 분석과 함께 사건발생 지역을 통해 예측한 용의자의 거점과 실제 위치정보가 군집된 거점을 비교하는 지리적 프로파일링 분석을 수행한다. 그리고 위의 과정으로 분석된 결과는 일정, SMS, 통화, 연락처 등 다른 디지털 포렌식 분석 결과와 종합한다.

제안 모델에서 분석된 위치정보는 조사지역 우선순위를 선별하거나 초기 수사 방향을 제시하는데 활용된다. 우선순위 결정요인으로는, 첫째, 범죄 발생 시간과 장소에 가장 근접한 데이터가 포함된 군집의 경우로, 범죄 발생지와 용의자 위치정보의 관계를 파악할 수 있다. 둘째, 빈도가 상대적으로 많은 군집의 경우로, 용의자의 거점 및 관심지역을 도출할 수 있다. 셋째, 검색지, 경로 등의 속성을 가진 군집의 경우로, 용의자의 이동패턴, 행동반경, 관심지역 등을 추측할 수 있다.

표 16는 제안 모델의 전체 알고리즘을 나타낸다.

3. 위치정보에 대한 수사절차

우선, 범죄수사 시 위치정보가 필요한 사건인지 여부를 판단한다. 만약 위치정보가 사건해결에 중요한 역할을 한다면 특정 용의자가 사용하는 휴대전화 번호를 이용하여 해당 통신사에게 통신사실확인자료를 요청한다. 이로써 기지국 기반의 위치정보를 확보가 가능하지만, 기지국 기반의 위치정보는 오차범위가 크기 때문에 용의자의 대략적인 위치를 나타내는 자료로 활용한다. 추후 수사 과정에서 특정 용의자의 스마트폰을 압수한 후에는 그림 16과 같이 제안 모델의 알고리즘을 적용한 수사 절차를 활용한다.

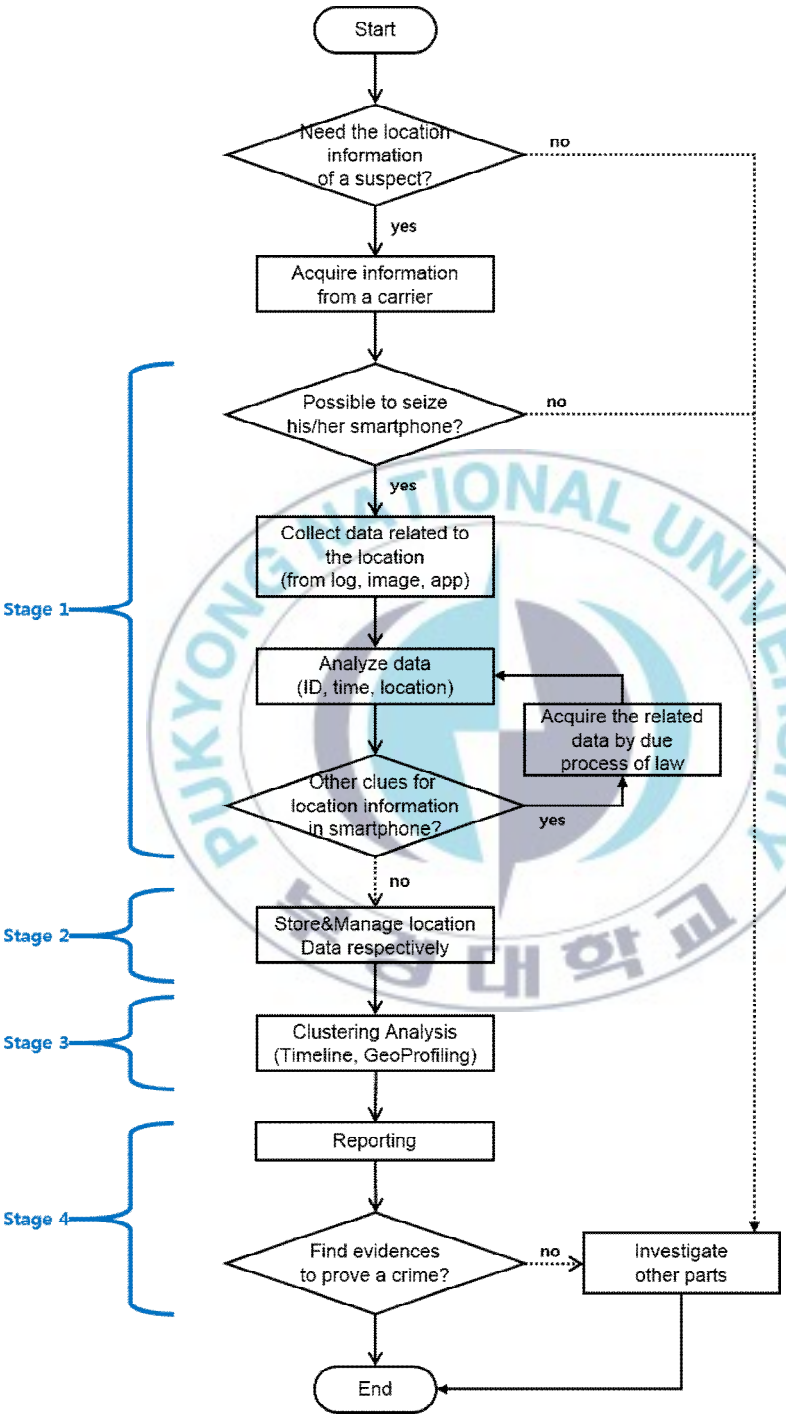

그림 16 . 위치정보 조사절차의 순서도

3.1 Stage 1

사건과 관련된 증거와 단서를 얻기 위하여 압수수색영장을 발부받은 뒤 용의자의 스마트폰을 압수한다. 최근 원격에서 데이터를 삭제하거나 스마트폰을 초기화할 수 있으므로 유의한다.

압수한 스마트폰을 대상으로 스마트폰에 저장된 위치정보를 추출한다. 현재 사진 이미지에서 GPS 정보를 가져오는 도구들이 많이 존재하고 있지만, 애플리케이션의 경우에는 데이터 저장구조가 제작자에 의존적이므로 신속한 조사가 어렵다. 그러므로 제안 모델의 위치 정보 추출 모듈에서 기 분석된 내용을 토대로 위치정보를 추출한다.

3.2 Stage 2

추출된 위치정보를 실제 위치를 나타내는 경우와 검색한 경우로 구분하여 저장 및 관리한다. 지도와 연계된 시각화 도구를 이용하면 이 데이터를 통해서도 대략적인 위치정보를 파악할 수 있다. 또한 스마트폰의 위치정보는 기지국 기반 위치정보보다 오차범위가 적으므로 신뢰성이 높다.

3.3 Stage 3

추출된 위치정보에 대하여 용의자의 행동반경과 위치정보의 오차범위를 고려하여 위도와 경도에 대해 계층적 군집화 알고리즘을 적용한다. 군집은 수집된 용의자의 위치정보 사이의 거리에 대해 공간적 특성을 나타내므로 용의자의 자백에 의존하지 않더라도 군집의 빈도수를 통해 용의자의 거점 및 관심지역을 파악할 수 있다.

또한, 사건발생지역 부근의 군집 분석과 지리적 프로파일링에서 범죄발생지역을 통해 예측한 범인의 거점 지역과도 비교, 분석한다. 이러한 정보들을 종합적으로 판단하여 범죄수사지역의 우선순위를 선정하고 범죄자에 대한 구증 자료로 활용한다.

3.3 Stage 4

전체적인 포렌식 분석결과를 정밀 검토하여 보고서를 생성한다. 보고서에는 위치정보를 가지고 있는 파일과 실제 경로, XML 포맷의 추출된 위치정보 리스트, 위치정보의 군집 결과와 범죄지의 분석 내용 등이 포함된다. 군집의 경우 거리값, 군집 연결방법 등 해당 군집 결과를 얻게 된 경위를 기술한다.

만약 수사에 도움이 될 만한 증거를 찾지 못한 경우에는 다른 부분에 대해 수사를 하고, 최종 범죄자를 검거한 경우에는 추출한 위치정보를 지리적 프로파일링 등 범죄데이터로 활용한다.

Ⅴ. 구현 및 평가

1. 구현

본 논문에서 제안한 위치정보 분석 모델을 기반으로 i5-3450 CPU와 8GB 램이 장착된 Windows7 PC에서 위치정보 분석도구를 구현하였다. 위치정보 추출 모듈의 경우, EnCase의 EnScript를 통해 구현하였고, EnCase에서 수집한 Nexus 4 이미지를 대상으로 위치정보를 추출하였다.

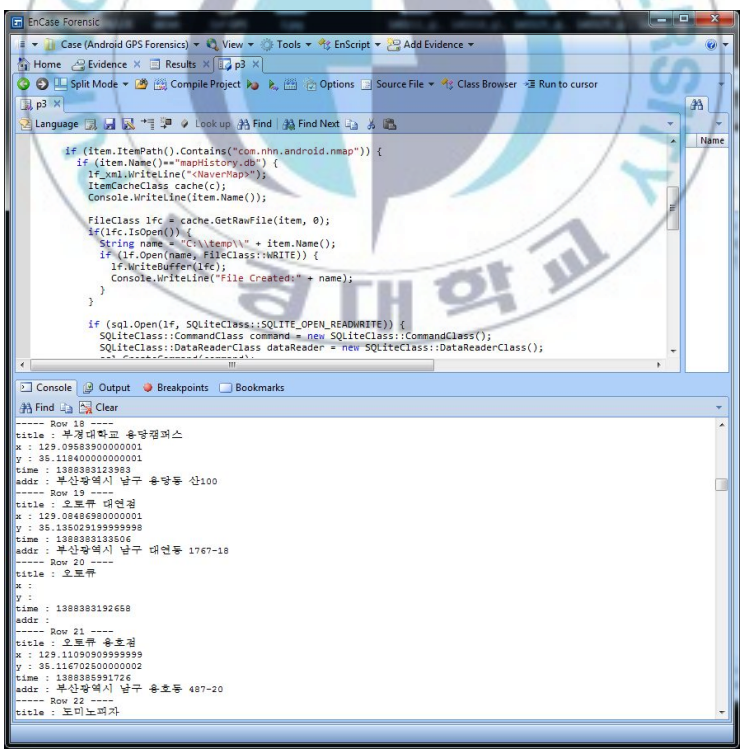

그림 17. 위치정보 추출도구의 구현

위치정보 추출도구에서 검색된 위치정보는 시간정보와 좌표계가 변환된 뒤 XML 포맷으로 내보내어진다. 또한 위치정보가 검색된 파일의 이름과 경로, 무결성 보장을 위한 해시 값이 저장된다.

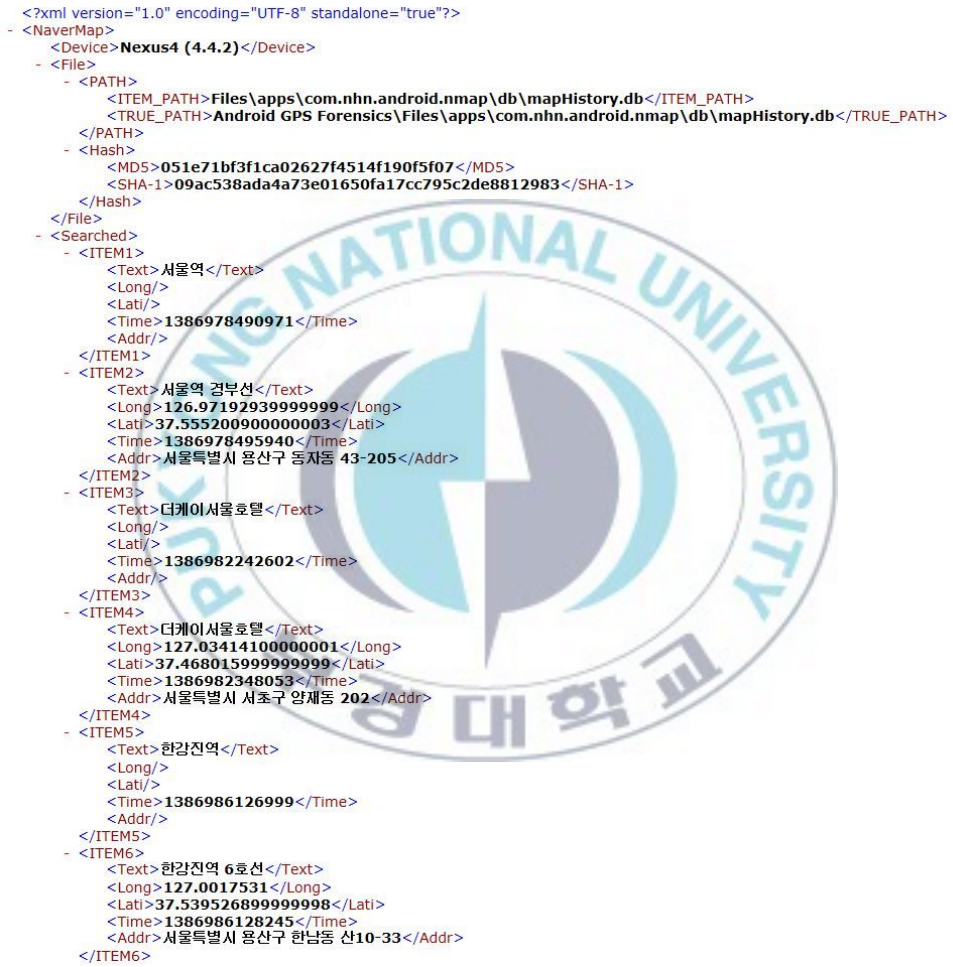

그림 18. XML 형태로 추출된 위치정보 (Naver Map)

실험에서는 이미지에 저장되어 있는 GPS 데이터를 대상으로 위치정보를 추출하였고, 총265개의 데이터 중에서 해외지역을 제외한 245개의 좌표를

이용하였다.

위와 같이 추출된 위치정보 데이터를 유클리드 거리와 최단연결법 및 평균연결법을 적용하여 계층적 군집화하고, 덴드로그램의 높이는 이동범위와 위치정보의 오차를 고려하여 300m로 가정하였다. 최단연결법은 데이터들 사이의 거리를 계산하고 가장 작은 값으로 군집을 구성하는 방식이므로, 이는 거리가 300m 이내의 데이터는 하나의 군집을 이루게 된다. 그림 19는 통계분석 도구인 R을 통해 최단연결법을 적용한 계층적 군집화 결과를 나타내고, 그림의 붉은 실선은 덴드로그램에서 높이를 300m로 설정하였을 때 14개의 군집이 형성된 모습을 보여준다.

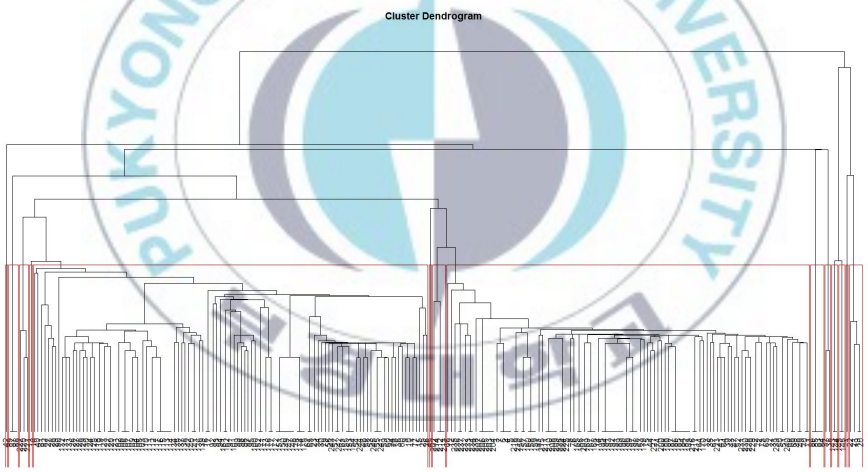

그림 19. 계층적 군집화 결과 (덴드로그램)

그림 20은 덴드로그램에서 높이를 300m로 설정하였을 때의 군집 결과로, 부산광역시의 일부 지역을 나타낸다. A군집의 경우는 104개의 위치정보를, B군집의 경우는 113개의 위치정보를 포함하고 있다. 이들 군집의 경우 다른 군집의 경우보다 상대적 빈도가 매우 높으므로 A지역과 B지역은 거점, 주 활동지역 또는 관심지역이라는 사실을 도출할 수 있다. 또한, 만

약 D지역이 사건발생 지역이라고 한다면 가까운 군집인 C지역과 A지역을 우선적으로 조사해야 할 것이고, 군집을 이루는 개체 수가 적더라도 사체 유기장소, 공범의 거점, 범죄 일정 파악 등 수사 과정 중 도움이 될 만한 정보를 얻을 수 있으므로 고려한다.

그림 20. 덴드로그램에서 높이를 300m로 설정하였을 때의 군집 결과

그리고 계층적 군집분석을 통해 도출된 군집의 수에 대한 타당성 검증을 위해서 분산분석 (ANOVA: Analysis of variance)을 수행하였다. 분산 분석은 평균값을 기초로 여러 집단을 비교하고 이들 집단간에 차이점이 있는지에 대해 가설 검증을 통해 관계를 파악하는 통계분석 기법이다.

위 실험 데이터의 위도, 경도 좌표값에 따른 군집의 변화에 대해 분산분석을 수행하였다. 분석 결과 F값이 충분히 크고 P값이 낮으므로 군집 간에 유의한 차이가 있다는 사실을 알 수 있다.

```
            Df Sum Sq Mean Sq F value   Pr(>F)
LNG          1  137.7  137.71   27.43 3.54e-07 ***
LAT          1  155.4  155.36   30.95 7.01e-08 ***
Residuals  242 1214.9    5.02
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1
```

그림 21. ANOVA 분석 결과

또한 추출된 위치정보의 시각화를 위하여 Naver 지도 API를 이용하여 시각화 도구 프로토타입을 구현하였다.

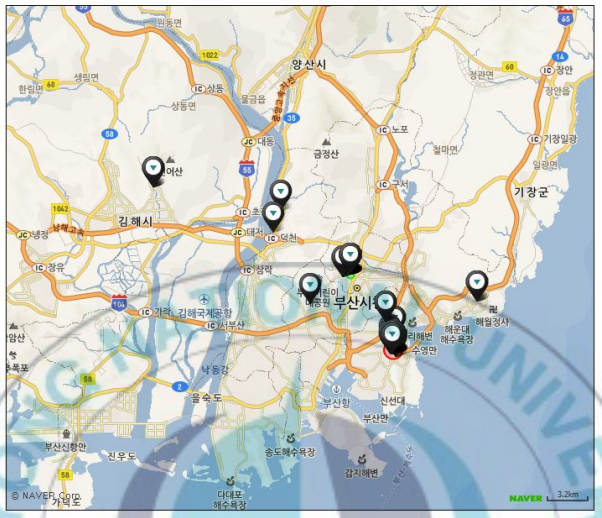

그림 22. 위치정보 시각화 (1)

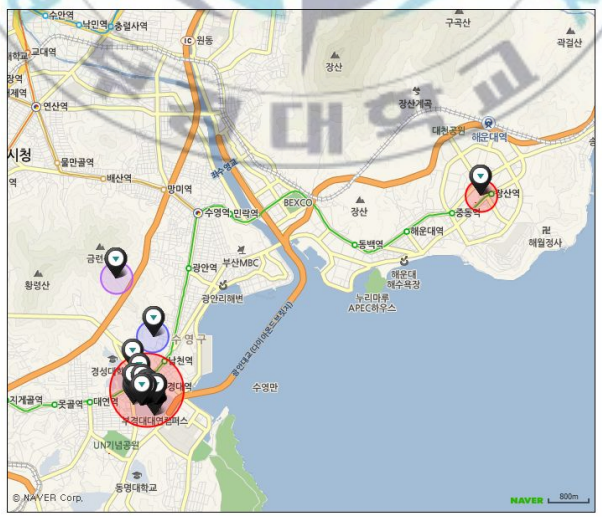

그림 23 위치정보 시각화 (2) - 군집 형성

2. 평가

본 논문에서 제안한 스마트폰 위치정보 분석모델의 기대효과는 다음과 같다. 첫째, 자동화된 위치정보 추출도구를 통해 기존에 수작업으로 관리하였던 피의자의 거주지, 회사, 사건 발생 위치, 사체 유기 장소 등의 위치정보를 효율적으로 관리할 수 있다. 둘째, 위치정보의 군집화를 통해 피의자의 실거주지, 회사 등의 거점과 관심지역을 파악하는데 용이하다. 셋째, 군집이 포함하고 있는 범죄와 관련된 장소, 군집의 빈도수, 기타 지리적 속성 등을 통해 수사가 필요한 지역을 선별할 수 있다. 넷째, 수사가 종결된 후에도 범죄자의 거점장소, 이동패턴 등 확보된 다양한 위치정보를 경찰 지리적 프로파일링 시스템에 적용하여 향후 프로파일링 알고리즘의 개선과 범죄데이터 축적에도 많은 도움이 될 것으로 기대된다.

표 17. 위치정보에 대한 기존의 조사 방식과 제안 방식의 비교

기준	기존 방식	제안 방식
신속성	위치정보 종류별로 각각 추출하고 관리	위치정보 종류별로 통합적으로 추출 및 관리가 가능
정보성	추출된 위치정보를 그대로 제공하므로 추후 별도의 전처리 및 분석 작업 요구	군집화를 통해 가공된 수사정보(거점, 관심지역, 우선수사지역)를 제공 가능
활용성	수집되는 위치정보의 수가 많지 않고, 수작업으로 위치정보를 입력, 관리하므로 활용성이 떨어짐	다양한 출처로부터 자동적으로 위치정보를 추출하므로 범죄데이터의 축적 및 지리적 프로파일링 등 범죄 연구에 활용이 가능

향후에는 범행 위치의 특징, 토지 유형, 인구통계, 도로 등의 지리적 거리 요인들과 실제 사례 및 범죄 데이터를 통해 제안 모델의 성능을 검증하고 보다 정확한 결과를 얻고자 한다. 또한 K-means, FCM 등 다양한 군집화 알고리즘을 적용하여 가장 적합한 알고리즘에 대해 연구하고[27,28], 조사지역 우선순위 결정에 있어서는 의사 결정 문제를 계층적으로 분석하여 최적의 대안을 선정하는 기법인 AHP (Analytic Hierarchy Process) 적용에 대해 연구하고자 한다[29].

Ⅵ. 결론 및 향후연구

기존의 스마트폰 위치정보에 대한 디지털 포렌식은 주로 수작업으로 관련된 파일을 일일이 확인하거나 일부 구현된 추출 도구를 개별적으로 이용하는 방식으로 이루어졌다. 이로 인해 디지털 포렌식 조사의 신속성, 정보성, 활용성을 담보하기 어려웠다. 따라서 디지털 포렌식 분석이 효율적으로 범죄 수사를 보조하기 위해서는 위치정보에 대해 통합적으로 관리하고 분석할 필요가 있다.

본 논문에서는 안드로이드 스마트폰의 사용자 위치정보에 대해서 시스템 로그, 이미지의 메타데이터, 각종 애플리케이션 측면에서 다각적으로 접근하였고, 이를 토대로 계층적 군집화 알고리즘을 이용하여, 안드로이드 스마트폰의 위치정보에 대한 분석 모델 및 조사 절차를 제안하였다. 구현 결과 다양한 출처로부터 위치정보를 자동적으로 수집할 수 있었고, 계층적 군집화로 도출된 군집들은 서로 유의한 차이가 있다는 사실을 통해 이용자의 지역 정보를 추정할 수 있었다.

본 논문에서 제안한 분석 모델은 범죄자의 거점 및 관심지역 파악이 가능하고, 수사가 필요한 지역의 우선순위를 선정할 수 있으며, 기타 효율적인 위치정보의 관리와 범죄 데이터 축적 등의 효과가 있을 것으로 기대된다.

향후에는 다양한 지리적 요인과 실제 데이터를 이용하여 보다 정확한 결과를 가지는 알고리즘에 대해 검토하고, 의사결정기법 적용을 통해 구체적인 우선순위를 도출하여, 효율적인 수사지원 기법에 대해 계속 연구하고자 한다.

참고문헌

[1] 임재영, 유지열, 장세정, 김민영, 유재민, “2012년 스마트폰이용 실태 조사 최종보고서,” 한국인터넷진흥원, 2013.

[2] Dohyun Kim, Jewan Bang, and Sangjin Lee, "Analysis of Smartphone-Based Location Information," *Computer Science and Convergence. LNEE*, vol. 114. Springer. pp. 43-53, 2012.

[3] Maus Stefan, Hans Hofken, and Marko Schuba. "Forensic Analysis of Geodata in Android Smartphones," *Int'l Conf. on Cybercrime, Security and Digital Forensics*, Jun, 2011; http://www.schuba.fh-aachen.de/papers/ 11-cyberforensics.pdf

[4] SungJin Hong and Kyunghyune Rhee , “An approach for the similar file detection with GPS information,” *2011 First ACIS/JNU Int'l Conf. on Computers, Networks, Systems and Industrial Engineering* (CNSI), May. 2011, pp.320,324,

[5] B. Nutter, “Pinpointing TomTom location records: A forensic Analysis,” *Digital Investigation*, Vol. 5, Sep, 2008, pp. 10-18.

[6] 최용석, “디지털 포렌식 관점에서의 내비게이션 사용흔적 정보 분석,” 석사학위논문, 고려대학교 정보경영공학전문대학원 정보경영공학과, 2010.

[7] 박혜영, 이관용, *패턴인식과 기계학습*, 이한출판사, 2011.

[8] B. Hofmann-Wellenhof, H.Lichtenegger, and J.Collins, *GPS Theory and Practice*, Springer-Verlag Wien New York, 2001.

[9] *Android Location Strategies*; http://developer.android.com/guide/topics/location/strategies.html

[10] 임준태, 이도선, “지리적 프로파일링을 통한 연쇄강력범죄의 공간적 특성분석,” 한국경찰연구, 제8권, 제4호, 2009, pp. 199-224.

[11] 신신애, 김성현, 송경빈, 류승희, 정규진, 송리라, *창조경제 실현을 위한 2013 빅데이터 국내 사례집*, 한국정보화진흥원 빅데이터 분석활용센터, 2014.; http://www.bigdataforum.or.kr/?Act=bbs&subAct=filedown&bid=example&seq=869&file_seq=169

[12] 임준태, “지리학적 프로파일링을 통한 한국의 연쇄강력범죄 분석,” 한국경찰연구, 제5권, 제2호, 2006, pp. 161-188.

[13] 임준태, “연쇄방화범 프로파일링과 이동특성,” 한국 공안행정학보, 제37권, 2009, pp. 369-402.

[14] 홍동숙, 김정준, 강홍구, 이기영, 서종수, 한기준, “시공간 분석 기반 연쇄 범죄 거점 위치 예측 알고리즘,” 한국공간정보시스템학회 논문지, 제10권, 제2호, 2008, pp. 63-79.

[15] Sandie Taylor et al., “Cluster Analysis Examination of Serial Killer Profiling Categories: A Bottom-Up Approach,” *Journal of Investigative Psychology and Offender Profiling*, Vol. 9, No. 1, Jan. 2012, pp. 30-51.

[16] Jiaji Zhou, Le Liang, and Long Chen, “Geographic Profiling Based on Multi-point Centrography with K-means Clustering,” *World Academy of Science, Engineering and Technology* (WASET), Vol. 6, Jan. 2012, pp. 1363-1396.

[17] Esra Polat, “Spatio-temporal Crime Prediction Model Based on Analysis of Crime Clusters,” Master’s Thesis, Dept. of Geodetic and Geographic Information Technologies, Middle East Technical Univ. Sep. 2007.

[18] 앤드류 후그, *안드로이드 포렌식: 구글 안드로이드 플랫폼 분석과 모바일 보안*, 에이콘 출판사, 2013.

[19] *Android Location APIs*; https://developer.android.com/google/play-services/location.html

[20] JEITIA, *Exchangeable image file format for digital still cameras: Exif Version 2.2*; http://www.kodak.com/global/plugins/acrobat/en/service/digCam/exifStandard2.pdf

[21] *Androidrank Open Market Statistics*; http://www.androidrank.org

[22] 최우용, 은성경, "스마트폰 포렌식 기술 동향," 한국전자통신연구원 전자통신동향분석, 제28권, 제3호, 2013, pp1. 1-8.

[23] 오정훈, "안드로이드 스마트폰 포렌식 분석 방법에 관한 연구," 석사학위논문, 고려대학교 정보보호대학원 정보보호학과, 2012.

[24] *다음 API 좌표체계*; http://dna.daum.net/apis/local/ref

[25] *Google KML*; https://developers.google.com/kml/

[26] Karen Kent, Suzanne Chevalier, Tim Grance, and Hung Dang, "Guide to Integrating Forensic Techniques into Incident Response," *NIST Special Publication 800-86*, Sep. 2006, pp. 1-7.

[27] J. Bezdek, "A convergence theorem for the fuzzy ISODATA clustering algorithm," *IEEE Trans. Pattern Anal. Machine Intelligence*, PAMI2(1), 1980, pp. 1-8.

[28] 양석환, 정목동, "이 기종 네트워크에서 퍼지 알고리즘과 MAUT에 기반을 둔 적응적 보안 관리 모델", 전자공학회논문지 제47권 CI편, 제1호, 2010, pp. 104-115.

[29] 키노시타 에이조, 오오야 타카오, *전략적 의사결정기법 AHP*, 청람출판사, 2012.

감사의 글

컴퓨터 공부를 하고 싶어 다니던 직장을 휴직하고 대학원에 입학한 지도 어느덧 2년이란 시간이 흘렀습니다. 그 동안 제가 학업에 열중하고 대학원 생활을 무사히 마칠 수 있도록 곁에서 도와주시고 관심을 가져주신 모든 분들께 감사의 인사를 드리고자 합니다.

우선, 부족한 저를 이끌어주시고 관심과 사랑으로 지도해주신 정목동 교수님께 진심으로 감사드립니다. 그리고 바쁘신 와중에도 논문을 심사해 주신 서경룡 교수님과 신상욱 교수님, 그리고 열정이 넘치는 강의를 해 주신 여정모 교수님과 박승섭 교수님께도 진심으로 감사드립니다.

또한, 대학원 생활 중에 동고동락하며 좋은 추억을 만든 연구실 멤버들에게도 감사드립니다. 제 멘토가 되어 주셨던 재천 선배를 비롯하여 석환 선배, 현동 선배, 영희 누님, 준호 형, 상곤 선배, 지영이 그리고 부족한 저를 믿고 따라준 찬진, 크리스, 상헌, 은영, 보미, 창연, 양훈, 민규, 민승, 재윤 모두 정말로 고맙습니다. 앞으로도 이 소중한 인연을 잘 간직하겠습니다.

그리고 사랑하는 우리 가족들에게도 감사의 인사를 드립니다. 먼저, 저를 믿고 묵묵히 따라준 아내에게 고마움을 전하고 싶습니다. “사랑하는 미소야! 남편의 꿈을 위해 기꺼이 희생해주고 힘들 때마다 격려해줘서 정말로 고마워요. 앞으로도 우리 귀여운 아들 이주 잘 키우고 더 많이 사랑해요.” 그리고 졸업 때까지 뒷바라지해 주시고 조언과 격려를 아끼지 않으셨던 아버지, 어머니, 장인어른, 장모님, 할아버지, 할머니, 큰아버지, 큰어머니께도 진심으로 감사드립니다.

마지막으로, 초심을 잃지 않고 열심히 노력할 것을 저 스스로 다짐하고, 대학원 생활 2년이 밑거름이 되어 우리나라 발전에 보탬이 될 수 있는 사람이 되도록 최선을 다하겠습니다. 감사합니다.

2014년 8월

손영준 드림