ISSN(Print) : 1976-5304, ISSN(Online) : 2713-931X
https://kdfs.jams.or.kr, DOI : 10.22798/kdfs.2022.16.1.37

중고거래 어플리케이션에서의 아티팩트 수집 및 분석

이 성 현*, 조 민 호*, 손 태 식**
아주대학교 사이버보안학과 (학부생)*, (교수)**

Collecting and analyzing artifacts in used trading applications

Seonghyeon Lee*, Minho Cho*, Taeshik Shon**
Dept. of Cybersecurity, Ajou University (Undergraduate Student)*, (Professor)**

요 약

중고거래는 원래 가격보다 싼 가격에 크게 흠이 없는 물품을 살 수 있다는 점에서 매년 수요가 급증하고 있고 이에 따라 중고거래 어플리케이션 사용자 수도 급증하고 있다. 하지만 개인 간의 거래인 만큼 사기 범죄가 많이 발생한다. 뿐만 아니라 마약 등 의약품의 불법 유통, 채팅을 통한 성희롱, 직접 만나서 거래를 하는 직거래를 하기 위해 실제 만남 이후 성범죄 또는 폭력 범죄가 발생하기도 한다. 따라서 어플리케이션에서는 이런 범죄들의 용의자 검거를 위한 단서를 제공할 가능성이 있다. 따라서 국내 중고거래 어플리케이션에서 가장 많이 사용되고 있는 당근마켓, 번개장터, 중고나라에서 다양한 범죄 상황을 고려하여 활동 기록을 남기고 아티팩트를 수집하여 분석을 진행했다. 그리고 사용자 정보, 마지막 사용 날짜 및 시간, 위치 정보, 채팅 정보 등과 같은 주요 아티팩트의 위치를 파악하여 정리했다.

주제어 : 중고거래 어플리케이션, iOS 포렌식, 안드로이드 포렌식, 모바일 포렌식, 디지털 포렌식

ABSTRACT

The demand for transactions of second-hand items is increasing every year in that you can buy items that are largely flawless at a lower price than the original price, and accordingly, the number of users of used traindg applications is also rapidly increasing. However, since it is an individual transaction, a lot of fraudulent crimes occur. In addition, sexual or violent crimes may occur after an actual meeting for illegal distribution of drugs such as drugs, sexual harassment through chatting, and direct dealings. Therefore, there is a possibility that the application may provide a clue for the arrest of the suspects of these crimes. Therefore, in consideration of various crime situations in daangn market, bungae jangter, and joonggonara, which are the most used in domestic used trading applications, we recorded activity records and collected artifacts for analysis. In addition, the location of major artifacts such as user information, last used date and time, location information, chat information, etc. were identified and organized.

Key Words : Used trading applications, iOS Forensics, Android Forensics, Mobile Forensics, Digital Forensics

▪ Received 30 December 2021, Revised 30 December 2021, Accepted 31 March 2022
▪ 제1저자(First Author) : Seonghyeon Lee (Email : ehdakstp2@ajou.ac.kr)
▪ 교신저자(Corresponding Author) : Taeshik Shon (Email : tsshon@ajou.ac.kr)

Ⅰ. 서 론

중고거래란 중고품을 사고 파는 행위로 일단 누가 먼저 샀었던 것을 파는 것이기 때문에, 당연하지만 개인 대 개인 간의 거래가 90% 이상이다. 따라서 중고거래는 보통 개인이 구입한 물건을 다시 사고 파는 것을 일컫는다. 이전에는 인터넷의 발달과 함께 카페나 사이트 등을 통해 중고거래가 이루어졌으나 최근에는 대부분의 사람들이 스마트폰을 들고 다니는 모바일시대가 도래함에 따라 중고거래 어플리케이션을 통해 거래가 이루어진다. 한국개발연구원이 분석한 중고거래 어플리케이션 월별 이용자 현황에 따르면 20년 1월 4,377만명이었던 어플리케이션 이용자 수는 21년 1월 기준 1억 588만 명까지 증가했다고 한다. 중고거래시장이 빠르게 커지고 있는 이유는 코로나19와 같은 특수한 환경적 요인, 중고거래에 대한 사람들의 긍정적인 인식 변화, 저렴한 가격에 물건을 구매하는 것은 합리적 소비라는 생각 때문이라는 분석이다[1]. 하지만 중고 거래가 활성화되면서 사기 피해 또한 급증하고 있다. 사기피해 정보공유 사이트 더치트는 중고나라와 당근마켓에서 발생한 누적 사기 피해가 각각 2만 705건, 5508건으로 파악했다[2]. 그러나 중고거래를 하다가 사기 피해를 당했을 경우 법적으로 구제받을 수 있는 길이 아직 없다. 현행법은 보이스피싱, 스미싱 등 특정 전기 통신사기에만 치우쳐져 있어 중고거래 사기를 다루지 못하고 있다. 현행법상 피해를 구제하는 장치가 없어 피해자들이 가장 요구하는 부당 수입 환수조차 이루어지지 않고 있다. 인터넷 거래 사기에 대해서 지급정지 등 긴급 조치와 피해 구제가 가능하도록 허용하는 내용을 담고 있는 통신사기 피해 환급법 개정안이 국회에 계류중이긴 하나 소액 사기의 경우 구제를 받기가 사실상 쉽지 않다. 또한 플랫폼을 믿고 중고거래 어플리케이션을 사용했는데, 문제가 발생하면 중고거래 플랫폼 운영자는 책임지는 모습을 보여주지 않기 때문에 본인이 모든 것을 증명해야하는 경우가 발생한다. 사기뿐만 아니라 채팅을 통한 성희롱, 직거래에서의 성범죄, 살인, 강도 등 강력범죄, 신분증 위조, 국민재난지원금을 더 낮은 가치의 현금과 바꾸는 이른바 지원금깡 등 불법 행위, 의약품 및 군용품 등 불법 판매 등 여러 범죄가 발생하고 있다[3].

위와 같은 사실을 비추어 볼 때 사기 행위나 성희롱, 금지 물품 불법 판매 등의 범행에 대한 사실을 입증하기 위한 증거나 직거래를 하기위해 만난 이후 발생되는 성범죄, 도난, 살인 등 강력 범죄의 해결을 위한 각종 단서가 어플리케이션 내에 또는 플랫폼 서버에 존재할 가능성이 있다. 예를 들어, 판매 및 구매 기록, 채팅 기록, 상대방의 프로필, 위치 정보 등을 직접적인 증거 및 정황 증거로 활용할 수 있다. 따라서 중고거래 어플리케이션의 아티팩트에 대한 분석연구가 필요하다.

이에 따라 본 논문에서는 국내 중고거래 시장을 선도하고 있는 3개 중고거래 어플리케이션인 당근마켓, 번개장터, 중고나라를 안드로이드와 iOS 환경을 대상으로 사용자 행위를 수행하고 이에 따라 생성되는 데이터를 식별하고 분석하였다. 본 논문의 구성은 다음과 같다. 2장에서는 관련 연구에 대해 서술하고, 3장에서는 분석 대상의 기능 및 특징과 분석 환경에 대해 서술한다. 4장에서는 아티팩트 분석, 5장에서는 주요 아티팩트 정리, 6장에서 결론으로 마무리한다.

Ⅱ. 관련 연구

모바일 어플리케이션에 관한 연구들은 다양한 연구가 진행되고 있다. 하지만 그 중 중고거래 어플리케이션과 관련된 연구는 존재하지 않아 본 연구를 진행하고자 하였다. 중고거래 어플리케이션은 물품에 관한 게시글을 올리고 거래 약속을 위해 개인 채팅을 한다는 점에서 SNS 또는 메신저 어플리케이션이랑 비슷하다고 볼 수 있다.

SNS 또는 메신저 어플리케이션 데이터 및 아티팩트에 대해 분석한 기존의 연구 결과는 다음과 같다. 모바일 메신저 어플리케이션 중 하나인 WeChat에서 데이터를 iOS에서 획득하는 방법과 WeChat의 주요 아티팩트를 분석한 연구가 제시된 바 있다[4]. iTunes 백업을 통해 WeChat의 데이터를 획득했으며, 음성 메시지, 텍스트 메시지, 사진, 동영상 등의 아티팩트들을 찾아 정리했다. 이미지나 비디오의 경우 서버로부터 다운로드 받은 것이 아닌 경우 썸네일만 찾을 수 있다. Android와 iOS 환경에서 채팅 어플리케이션 IMO의 아티팩트를 분석한 연구도 존재한다[5]. 아티팩트 분석뿐만 아니라 암호화된 네트워크 트래픽 또한 캡처하고 분석하여 IMO 트래픽 흐름을 감지하고 채팅 및 통화 관련 활동의 다양한 이벤트를 분류하였다. Kik이라는 메신저 어플리케이션을 포렌식으로 분석한 연구도 있다[6]. Kik의 아티팩트들은 유저 계정, 일반 텍스트 메시지, 첨부 파일로 나타났다. 삭제된 이미지를 장치에서 복구할 수 있을 뿐만 아니라 Kik 서버에서 찾아 다운로드할 수도 있었다. 또한 채팅 기록을 생성하는 여러 데이터베이스 테이블의 데이터를 연결하는 프로세스를 설명함으로써 채팅 기록을 정확히 확인할 수 있다. 사용자 입력 패스워드를 기반으로 데이터를 암호화한 보안메신저인 Sure

spot에서 암호화된 데이터를 복호화하는 방안 연구도 존재한다[7]. 암호화된 데이터에 대한 복호화 방안을 제시하고 복호화한 데이터를 토대로 패스워드 검증 방안을 제시하였으며 이를 토대로 사용자 로그인 패스워드를 복구하는 기술을 개발했다. 하지만 1000개의 메시지만 클라이언트에 저장하고 있으므로 최근 메시지를 제외하곤 데이터 획득에 어려움이 있었다. 전 세계적인 SNS 어플리케이션 중 하나인 Facebook에 대한 포렌식 분석 연구도 존재한다[8]. 안드로이드 에뮬레이터를 사용하여 가상 환경을 설정하여 데이터를 획득했으며, 사용자 이름, 유저 이름, 패스워드, 게시글, 친구 목록, 사용자 활동, 상세 프로필 등의 아티팩트를 분석했다. 다른 SNS 어플리케이션인 Twitter 사용 흔적을 분석한 연구도 존재한다[9]. 안드로이드는 루팅을 통해, iOS는 i Tunes를 이용한 백업으로 데이터 수집을 하였으며, iOS의 경우 사용자 id, userID, 디바이스 정보, 팔로워 등에 대한 아티팩트를, 안드로이드의 경우 사용자가 남긴 트윗 정보, 메시지 대화 내역 등에 대한 아티팩트도 확인할 수 있다.

다양한 어플리케이션에 대해 종합적으로 분석한 연구도 있다[10]. Line, Discord 등의 인스턴트 메시지 어플리케이션, Instagram, TikTok 등의 SNS 어플리케이션, Skype 등의 VoIP 어플리케이션 등 다양한 어플리케이션의 아티팩트를 그림 1과 같이 분석하고 얻을 수 있는 정보와 경로를 정리했다.

App\Artifacts	Version Number	Install Time	Username	Password	User Email & Phone Number	UserID	User Location	User IP Address	Text Messages	Shared Media	Phone Calls	Other People's Info	Logs
Discord	10.2.8	Yes-V	Yes-V	No	Yes-V	Yes-V	No	No	Yes-V	Yes-V	U	Yes-V*	Yes-V
Dust	6.1.3.2887	Yes-V	Yes-V	N/A	Yes-V	Yes-V*	U	No	U	U	N/A	Yes-V*	Yes-V*
Facebook Messenger	219.0.0.10.122	Yes-V	Yes-V	No	Yes-V	Yes-V*	Yes-V	No	Yes-V	Yes-V	Yes-V	Yes-V*	Yes-V*
GalleryVault	3.14.82	Yes-V	N/A	No	Yes-V	N/A	Yes-V	Yes-V	N/A	N/A	N/A	N/A	N/A
Imgur	4.5.9.12223	Yes-V	Yes-V	No	Yes-V	Yes-V	Yes-V	Yes-V	N/A	Yes-V*	N/A	Yes-V*	Yes-V
imo	9.8.000000010915	Yes-V	Yes-V	No	Yes-V	Yes-V	No	No	Yes-V	Yes-V	Yes-V	Yes-V	Yes-V
kik	15.19.0.22104	Yes-V	Yes-V	No	Yes-V	No	No	Yes-V	Yes-V	Yes-V	N/A	Yes-V*	Yes-V
Line	10.0.2	Yes-V	U	N/A	No	Yes-V	Yes-I.S.	No	Yes-V	Yes-V	Yes-V	Yes-V*	Yes-V*
MeWe	6.0.9.4	Yes-V	Yes-V	No	Yes-V	Yes-V	No	No	Yes-V	Yes-V*	U	Yes-V	Yes-V*
Signal	4.53.7	Yes-V	Yes-V	N/A	Yes-V	Yes-V	No	No	Enc	Yes-V	Enc	Enc	Enc
Silent Phone	6.10	Yes-V	Yes-V	No	Yes-V	Yes-V	No	No	Enc	Enc	Enc	Enc	Enc
Skout	6.17.0	Yes-V	Yes-V	Yes-V	Yes-V	Yes-V	Yes-V	No	Yes-V	Yes-V	Yes-V	Yes-V*	Yes-V
Telegram	5.14.0	Yes-V	U	No	Yes-V	Yes-V	No	Yes-V	Yes-M	Yes-M	Yes-M	Yes-M	Yes-V
TextNow	20.1.1.0	Yes-V	Yes-V	No	Yes-V	Yes-V	Yes-V	Yes-V	Yes-V	Yes-V	Yes-V*	Yes-V	Yes-V*
Threads	126.0.0.25.121	Yes-V	Yes-V	No	Yes-V	Yes-V	No	Yes-A	Yes-V	Yes-V*	Yes-V	Yes-V	Yes-V*
Instagram	126.0.0.25.121	Yes-V	Yes-V	No	No	Yes-V	No	Yes-A	Yes-V	Yes-V*	Yes-V	Yes-V	Yes-V*
WhatsApp	2.20.11	Yes-V	Yes-V	No	Yes-V	Yes-V	Yes-I.S.	Yes-V	Yes-V	Yes-V	Yes-V	Yes-V	Yes-V*
Wickr Me	5.45.4	Yes-V	Yes-M	No	No	No	Yes-M & I.S.	No	Yes-M	U	Yes-M*	Yes-M*	Enc
Wire	3.44.877	Yes-V	Yes-V	No	Yes-V	Yes-V	Yes-V	No	Yes-V	Yes-V	Yes-V	Yes-V	Yes-V*
TikTok	14.7.5	Yes-V	Yes-V	No	Yes-V	Yes-V	No	No	Yes-V	Yes-V*	N/A	Yes-V*	Yes-V*
Twitter	8.29.0-release.00	No	Yes-V	No	U	Yes-V	No	No	Yes-M	Yes-M	N/A	Yes-V*	Yes-V
Spotify	8.5.42.812	Yes-V	Yes-V	No	Yes-V	Yes-V	No	No	N/A	N/A	N/A	N/A	Yes-V
Snapchat	10.74.6.0	Yes-V	Yes-V	No	Yes-V	Yes-V	Yes-V	No	Yes-V	Yes-V	Yes-V*	Yes-V	Yes-V*
Skype	8.37.0.98/8.56.0.100	Yes-V	Yes-V	No	Yes-V	Yes-V	Yes-V*	Yes-V	Yes-V	Yes-V	Yes-V	Yes-V	Yes-V*
Viber	12.2.2.1	Yes-V	Yes-V	No	Yes-V	Yes-V	Yes-I.S	No	Yes-V	Yes-V	Yes-V	Yes-V	Yes-V
TOR Browser	68.4.1	Yes-V	N/A	N/A	N/A	N/A	No	No	N/A	N/A	N/A	N/A	N/A
Venmo	7.45.0	Yes-V	Yes-V	No	Yes-V	Yes-V	No	No	Yes-V*	N/A	N/A	Yes-V	Yes-V*

〈Figure 1〉 Summary of Recovered Android Artifacts

Ⅲ. 분석 대상의 기능 및 특징과 분석 환경

3.1. 분석 대상의 기능 및 특징

본 연구에서는 2021년 11월을 기준으로 최신 업데이트된 어플리케이션 3종에 대해 분석한다. 각 어플리케이션을 사용하고 어떠한 데이터가 남을 수 있는지 알기 위해 각 어플리케이션의 버전, 가입방법과 같은 기능과 특징들을 분석해보았다. 분석한 기능 및 특징은 〔표 1〕과 같다.

〈Table 1〉 Function and Features for each Application

Application	Version	가입방법	거래 소통 방법	어플리케이션 자체 결제기능	Function and Features
당근마켓	6.5.1	전화번호 기반	- 중고거래 글 작성 - 개인 간 채팅 및 전화	-	- 위치 인증 및 위치 기반 서비스 - 동네 생활 게시판, 동네 홍보 글 - 판매 및 구매 내역, 관심목록
번개장터	8.3.3	SNS(카카오톡, 네이버, 페이스북, 어플ID) 연동 기반	- 중고거래 글 작성 - 개인 간 채팅	번개페이	- 택배관리 - 본인인증 및 위치 인증
중고나라	4.6.6	전화번호 기반	- 중고거래 글 작성 - 개인 간 채팅	중고나라페이	- 본인인증 및 위치 인증 - 택배관리 - 자차 등록 - 카페 연동

3.2. 분석환경

본 연구에서 사용된 장치, OS, 분석도구와 같은 분석환경은 〔표 2〕과 같다. iPhone의 경우, 어플에서 제공하는 IPhone 관리 및 백업 프로그램인 iTunes를 이용해 데이터를 수집하였다. 어플리케이션 데이터를 분석하기 위해 HxD를 사용하였고 데이터베이스 내용을 확인하기 위해 DB Browser for SQLite와 MongoDB Realm Studio를 사용했다. 그리고 plist 내용을 확인하기 위해서 plist Editor Pro를 사용했다. Galaxy S8의 경우, Knox 버전은 3.2.1이었으며, TWRP, 삼성 오딘, Magisk를 이용한 루팅 방식으로 이미지를 얻어 Autopsy를 이용하여 분석하였다.

〈Table 2〉 Experiment Environment

	Name and Version
Device/OS	iPhone 12 pro / iOS 14.8.1 Galaxy S8 / Android 9
Data backup	iTunes ver 12.12.2 TWRP for dreamlte ver 3.52_9-0 Samsung Odin3 ver 3.14.4 Magisk ver 23.0
Analysis Tool (Viewer)	DB Browser for SQLite ver. 3.11.2 HxD Editor ver. 2.3.0.0 plist Editor Pro ver. 2.5 MongoDB Realm Studio ver. 11.1.0 Autopsy ver 4.19.1

Ⅳ. 아티팩트 분석

4.1. 당근마켓

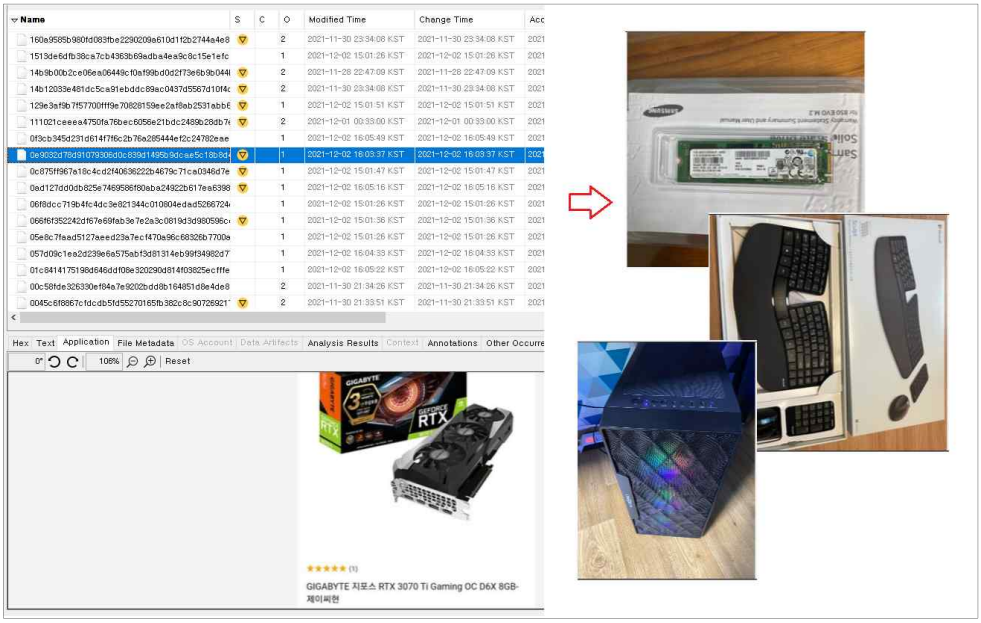
4.1.1. Android

당근마켓의 파일 저장 위치는 data/com.towneers.www이다. data/com.towneers.www 내의 폴더들에서 유의미한 정보를 찾아보았다.

〈Table 3〉 Android daangn market application data storage path and contents

Path	File Name	contents
data/com.towneers.www/shared_prefs	com.towneers.www.user.pref.xml	- 사용자 국적, 전화번호, 등록 위치, 이메일, 프로필 사진
data/com.towneers.www/databases	Colonies.db	- 최근 검색어
data/com.towneers.www/cache/image_manager_disk_cache	All file	- 캐시 이미지

첫 번째로, data/com.towneers.www/shared_prefs에 위치한 com.towneers.www.user.pref.xml 파일에서 사용자의 국적 및 휴대전화 번호, 등록한 동네 위치, 이메일, 프로필사진 등 다양한 정보를 얻을 수 있었다. 또한 data/com.towneers.www/databases에 위치한 Colonies.db 파일로부터 최근 검색어에 대한 정보를 찾을 수 있었다.



〈Figure 2〉 cache images

마지막으로 data/com.towneers.www/cache/image_manager_disk_cache 폴더에서는 그림 2와 같이 다양한 캐시 이미지들을 확인할 수 있었는데, 광고와 같은 사용자와 관련 없는 이미지도 포함되어 있지만 주로 나타난 물품의 이미지로부터 사용자의 관심 카테고리를 어느 정도 유추할 수 있다.

4.1.2. iOS

iOS의 당근마켓의 파일 저장 위치 또한 com.towneers.www였다. com.towneers.www에서 분석한 데이터의 경로 및 내용은 표 4과 같다.

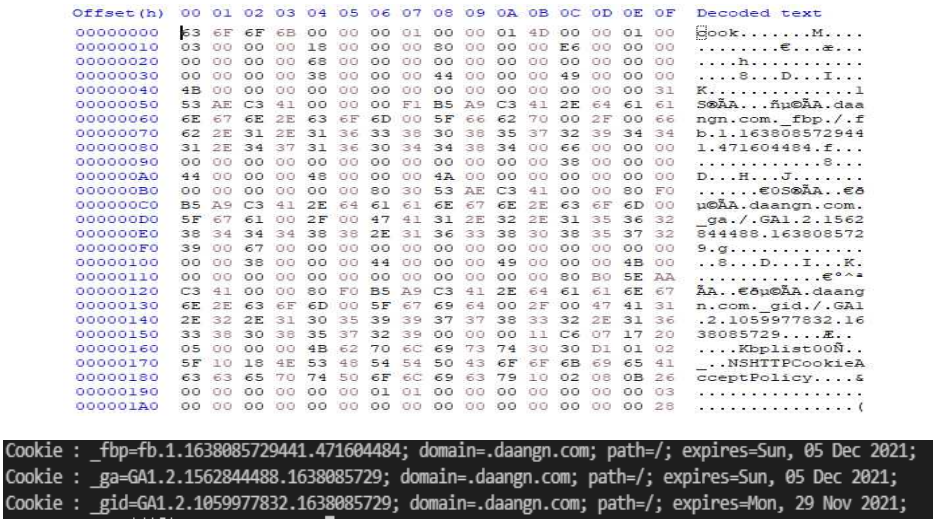
〈Table 4〉 iOS daangn market application data storage path and contents

Path	File Name	contents
com.towneers.www/Library	com-facebook-sdk-AppEventsTimeSpent.json	- 마지막 사용 날짜 및 시간 - 세션 ID - 마지막 소비 시간
com.towneers.www/Library/Application Support/io.branch	BNCPreferences.plist	- user agent 및 os 버전
net.quicket.app/Library/Cookies	Cookies.binarycookies	- HTTP Cookies(값, 도메인, 만료일, 플래그)
com.towneers.www/Library/Preferences	com.apple.AdSupport.plist	- 마지막 사용 날짜 및 시간
	com.google.gmp.measurement.plist	- App version - 마지막 사용 날짜 및 시간 - OS version
	com.towneers.www.plist	- 마지막 사용 날짜 및 시간 - 처음 사용 날짜 및 시간 - GMS(Google My Maps) cookie 값 - 최근 검색어 - 사용자 위치 정보 - 사용자 닉네임 - 사용자 프로필 이미지 - ID_identity - 사용자 전화번호
com.towneers.www/WebKit/WebsiteData/ResourceLoadStatistics	observations.db	- 사용 날짜

〈Figure 3〉 Facebook SDK spent time and session ID

com.towneers.www/Library/com-facebook-sdk-AppEventsTimeSpent.json에서는 마지막 사용 날짜 및 시간과 Facebook SDK에 사용되었던 세션 ID와 마지막 사용 때의 소비 시간을 확인할 수 있다. 그림 3과 같이 마지막 사용 날짜 및 시간은 Unix Timestamp로 표현되어져 있으며, 마지막 소비 시간은 초(second)로 표현된다. 따라서 2021.11.29. 오후 3:17가 마지막 날짜 및 시간이며 2분 24초 동안 사용했다는 것을 알 수 있다.

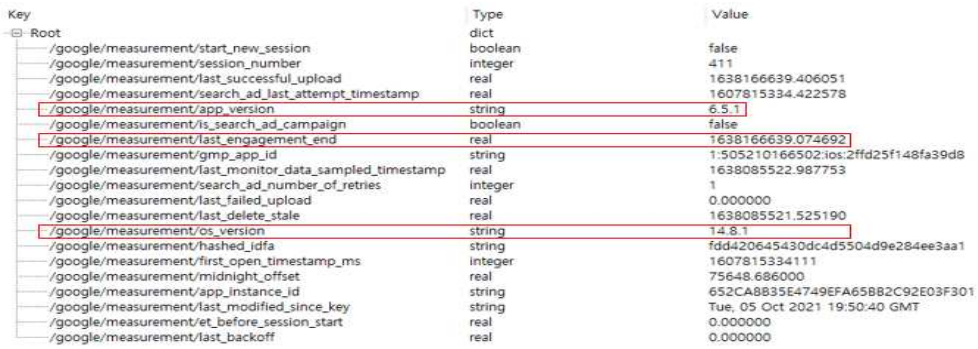
com.towneers.www/Library/Application Support/io.branchBNCPreferences.plist에서는 User Agent와 OS 버전을 확인할 수 있다. 각각 Mozilla 5.0, iPhone 14_8_1인 것을 확인할 수 있다.



〈Figure 4〉 binarycookies file and analysis result

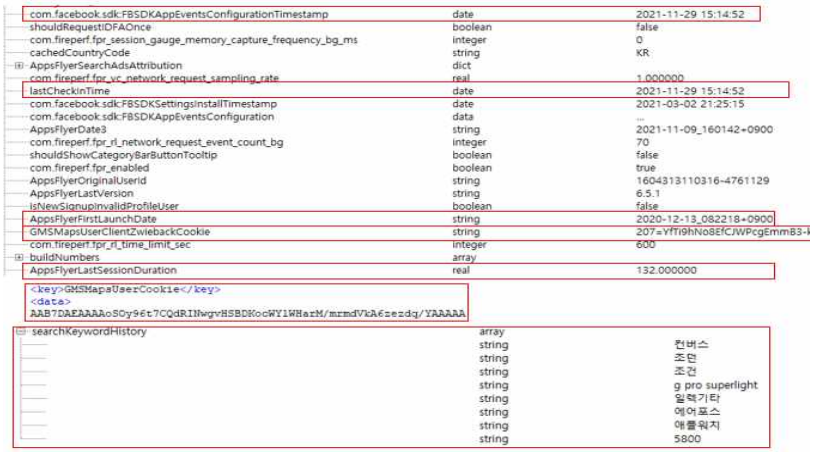
com.towneers.www/Library/Cookies/Cookies.binarycookies에서는 그림 4와 같이 쿠키 값과 도메인, 만료일, 쿠키 플래그를 확인할 수 있다. binarycookies 파일은 어느정도 일정한 형식이 존재하기 때문에 이에 따라 Python을 이용하여 분석했다[11].

com.towneers.www/Library/Preferences/com.apple.AdSupport.plist에서도 마지막 사용시간을 확인할 수 있었다.



〈Figure 5〉 com.google.gmp.measurement.plist

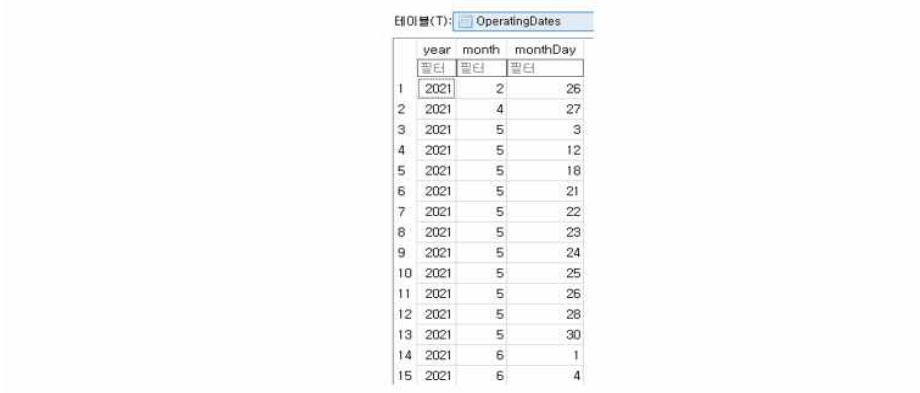
com.towneers.www/Library/Preferences/com.google.gmp.measurement.plist에서는 그림 5와 같이 현재 사용중인 App 버전, 마지막 사용시간, OS 버전을 확인할 수 있었다. 여기서의 마지막 사용시간도 com-facebook-sdk-AppEventsTimeSpent.json 파일과 같이 Unix timestamp 형식으로 표현되어있으며 2021.11.29. 오후 3:17로 같고, App 버전은 6.5.1인 것을 확인할 수 있다.



〈Figure 6〉 User Information(1)

〈Figure 7〉 User Information(2)

com.towneers.www/Library/Preferences/com.towneers.www.plist에서는 그림 6, 7과 같이 마지막 사용시간, 처음 사용시간, 마지막 소비 시간, 검색어 히스토리를 확인할 수 있었다. 마지막 사용 시간은 2021.11.29. 오후 3:14로 앞서 말한 파일들과 3분의 오차가 있고, 마지막 소비 시간은 2분 12초로 12초의 오차가 있다. 처음 사용시간은 2020.12.13. 오전 8:22이다. 검색어 히스토리로는 컨버스, 조던, 애플워치 등을 확인할 수 있다. 또한 위도, 경도, 주소 등 사용자 위치 정보를 확인할 수 있고, 자신의 닉네임 "수달"과 프로필 이미지, 폰 번호, ID tag 숫자도 확인할 수 있었다.



테이블(T): OperatingDates

	year	month	monthDay
	필터	필터	필터
1	2021	2	26
2	2021	4	27
3	2021	5	3
4	2021	5	12
5	2021	5	18
6	2021	5	21
7	2021	5	22
8	2021	5	23
9	2021	5	24
10	2021	5	25
11	2021	5	26
12	2021	5	28
13	2021	5	30
14	2021	6	1
15	2021	6	4

〈Figure 8〉 Dates of Use

com.towneers.www/Library/WebKit/WebsiteData/ResourceLoadStatistics/observations.db에서는 그림 8과 같이 OperatingDates 테이블에서 그 동안 당근마켓 App을 사용했었던 날짜들을 확인할 수 있었다.

4.2. 번개장터

4.2.1. Android

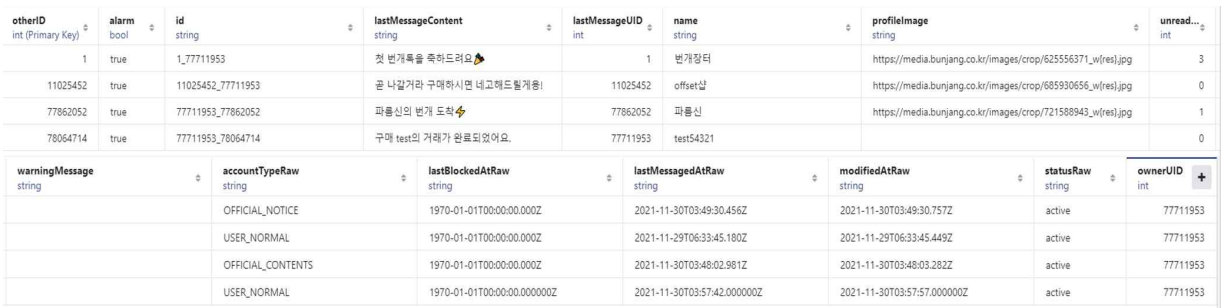
번개장터는 루팅 후 이용이 불가능하여 데이터를 가져오지 못하였다. 번개장터를 실행했을 때 “해킹 위험(루팅)이 탐지되었습니다. 보안정책에 따라 앱을 종료합니다.”라는 문구가 출력되며 확인을 누를 시 어플리케이션이 종료된다.

4.2.2. iOS

iOS의 번개장터의 파일 저장 위치는 net.quicket.app이다. net.quicket.app에서 분석한 데이터의 경로 및 내용은 표 5와 같다.

〈Table 5〉 iOS bungae jangter market application data storage path and contents

Path	File Name	contents
net.quicket.app/Documents	default.realm	- 개인 간 채팅 마지막 정보(상대 id, 상대 닉네임, 상대 프로필 이미지, 마지막 채팅 내용, 마지막 채팅 시간)
net.quicket.app/Library	com-facebook-sdk-AppEvents TimeSpent.json	- 마지막 사용 날짜 및 시간 - 세션 ID - 마지막 소비 시간
net.quicket.app/Library/Cookies	Cookies.binarycookies	- HTTP Cookie(값, 도메인, 만료일, 플래그)
net.quicket.app/Library/Preferences	adfit.session.plist	- 마지막 사용 날짜 및 시간
	com.google.gmp.measurement .plist	- App version - 마지막 사용 날짜 및 시간 - OS version
	net.quicket.app.plist	- 세션 ID - 연동 가입 종류 - 마지막 사용 날짜 및 시간 - 폰 정보(모델, OS version, SDK version, 통신사, 지역) - App version - user agent 및 ios 버전 - 최근 검색어 - 마지막 소비 시간 - 최근 본 상품(글 제목, 내용, 태그, 가격, 지역, 이미지, 판매자 닉네임, 작성 시간, 카테고리)
net.quicket.app/WebKitWebsiteData/ResourceLoadStatistics	observations.db	- 사용 날짜



otherID int (Primary Key)	alarm bool	id string	lastMessageContent string	lastMessageUID int	name string	profileImage string	unread... int
1	true	1_77711953	첫 번개톡을 축하드려요🎉	1	번개장터	https://media.bunjang.co.kr/images/crop/625556371_w{res}.jpg	3
11025452	true	11025452_77711953	곧 나갈거라 구매하시면 네고해드릴게용!	11025452	offset샵	https://media.bunjang.co.kr/images/crop/685930656_w{res}.jpg	0
77862052	true	77711953_77862052	파룡신의 번개 도착🚀	77862052	파룡신	https://media.bunjang.co.kr/images/crop/721588943_w{res}.jpg	1
78064714	true	77711953_78064714	구매 test의 거래가 완료되었어요.	77711953	test54321		0

warningMessage string	accountTypeRaw string	lastBlockedAtRaw string	lastMessagedAtRaw string	modifiedAtRaw string	statusRaw string	ownerUID int
	OFFICIAL_NOTICE	1970-01-01T00:00:00.000Z	2021-11-30T03:49:30.456Z	2021-11-30T03:49:30.757Z	active	77711953
	USER_NORMAL	1970-01-01T00:00:00.000Z	2021-11-29T06:33:45.180Z	2021-11-29T06:33:45.449Z	active	77711953
	OFFICIAL_CONTENTS	1970-01-01T00:00:00.000Z	2021-11-30T03:48:02.981Z	2021-11-30T03:48:03.282Z	active	77711953
	USER_NORMAL	1970-01-01T00:00:00.000000Z	2021-11-30T03:57:42.000000Z	2021-11-30T03:57:57.000000Z	active	77711953

〈Figure 9〉 person to person chat

net.quicket.app/Documents/default.realm에서는 그림 9와 같이 번개장터의 개인 간 채팅의 마지막 정보를 확인할 수 있었다. 상대방의 ID, 채팅 alarm 여부, 마지막 채팅 및 시간, 상대방 닉네임, 상대방 프로필 이미지, 안 읽은 개수 등을 확인할 수 있다.

net.quicket.app/Library/com-facebook-sdk-AppEventsTimeSpent.json에서는 당근마켓과 같이

마지막 사용 날짜 및 시간과 Facebook SDK에 사용되었던 세션 ID와 마지막 사용 때의 소비 시간을 확인할 수 있다.

```
Cookie : aid=4d2d10b8b1314b35a3209061bcfceb8e; domain=.ad.daum.net; path=/; expires=Wed, 30 Nov 2022; Secure; HttpOnly
Cookie : aid_ts=1634986561118; domain=.ad.daum.net; path=/; expires=Wed, 30 Nov 2022; Secure; HttpOnly
Cookie : _bun_buid=hMicKJ-1634819468; domain=.bunjang.co.kr; path=/; expires=Tue, 07 Dec 2021;
Cookie : _gcl_au=1.1.457247304.1638087068; domain=.bunjang.co.kr; path=/; expires=Sun, 05 Dec 2021;
Cookie : _ga=GA1.3.626872289.1638087166; domain=.bunjang.co.kr; path=/; expires=Tue, 07 Dec 2021;
Cookie : _gid=GA1.3.1856103088.1638087166; domain=.bunjang.co.kr; path=/; expires=Wed, 01 Dec 2021;
Cookie : _bun_session_id=1638243844-11e92R; domain=.bunjang.co.kr; path=/; expires=Tue, 30 Nov 2021;
Cookie : bunny_cookie=l0lxdpv3rb736e6vqamsuy0sviulqv7g; domain=.bunjang.co.kr; path=/; expires=Tue, 14 Dec 2021; HttpOnly
Cookie : csrftoken=hIu8oWHGaVcgsOfHJB64H1wpyxReqgn6U34WK5vNvDUwdpQeENBtRd65Ej39RPAV; domain=m.bunjang.co.kr; path=/; expires=Tue, 29 Nov 2022; Unknown
Cookie : SCOUTER=z7rkqi0vhnvp8r; domain=quickpay.kcp.co.kr; path=/; expires=Sat, 17 Dec 2089; Unknown
Cookie : _ga=GA1.4.626872289.1638087166; domain=.m.bunjang.co.kr; path=/; expires=Mon, 06 Dec 2021;
Cookie : _gid=GA1.4.1856103088.1638087166; domain=.m.bunjang.co.kr; path=/; expires=Tue, 30 Nov 2021;
```

〈Figure 10〉 binarycookies analysis result

net.quicket.app/Library/Cookies/Cookies.binarycookies도 당근마켓과 마찬가지로 Python을 이용해 분석하였으며 그림 10과 같이 쿠키 값과 도메인, 만료일, 쿠키 플래그를 확인할 수 있다.

Key	Type	Value
Root	dict	
firstVistsTimestampKey	date	2021-10-23 19:56:00
previousVistsTimestampKey	date	2021-11-29 15:21:47
sessionActive	boolean	true
appForeground	boolean	true
totalNumberOfVistsKey	integer	5
bgDrationSinceLaunchTimestampKey	real	0.001972
currentVisitTimestampKey	date	2021-11-30 12:47:54
transitionTimestampKey	date	2021-11-30 12:47:54

〈Figure 11〉 Last used date and time

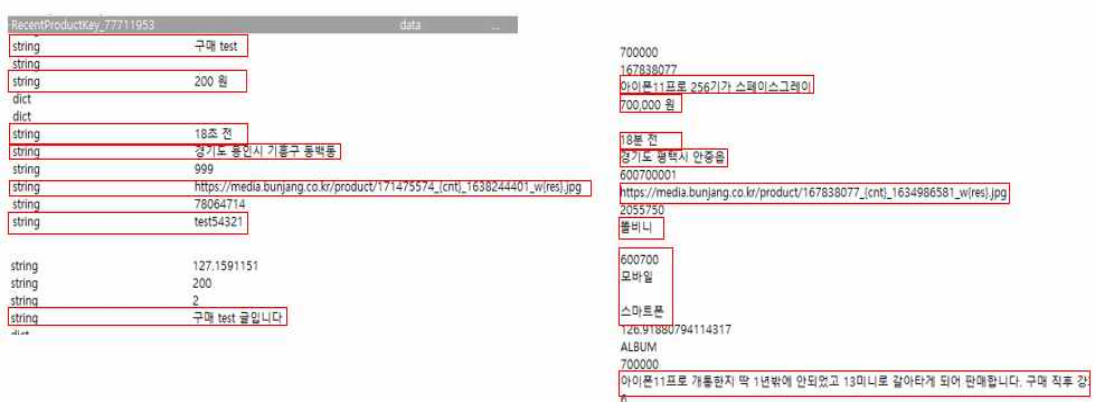
net.quicket.app/Preferences/adfit.session.plist에서는 그림 11와 같이 마지막 사용 날짜 및 시간을 확인할 수 있다. 그리고 net.quicket.app/Preferences/com.google.gmp.measurement.plist에서는 현재 App 버전이 8.3.3, 마지막 사용 날짜 및 시간이 2021.11.30. 12:47, OS 버전이 14.8.1인 것을 확인할 수 있다.

identifiers	dict	
sessionID	string	1638243844-11e92R
com.facebook.sdk:serverConfiguration1515207441905975	data	...
com.google.appinvite.openURL	boolean	true
INSIDER_FIRST_RUN	boolean	false
loginTypeKey	string	KAKAO
com.adobe.cc.sdk.cacheVersion	integer	9
AppsFlyerGetConversionDataTiming	real	2354.000000
kPushAllowPopupKey2	string	Y
com.facebook.sdk:FBSDKSettingsSetAdvertiserTrackingEnabledTimestamp	date	2021-11-30 12:58:33
insiderStaticAttributes	dict	
os_version	string	14.8.1
model	string	iPhone13,3
app_version	string	8.3.3
sdk_version	string	10.8.0
location_enabled	boolean	false
package_name	string	net.quicket.app
is_deliver_silently_enabled	boolean	true
device_token	string	fde345074e8bd6dcd2c2ff309377c0968bc858171d716f12396fec643428cdc0
push_enabled	boolean	false
platform	string	iOS
device_language	string	ko
apps	string	https,kakao934df846db7171e9bd5968621bdae46d,kakaokompassauth,kakaolink,kaka
timezone	string	Asia/Seoul
environment	string	production
carrier	string	LG U+
udid	string	2A34F26666CC43B098B808B278C4C955
AdFitStore	dict	
userAgent	string	Mozilla/5.0 (iPhone; CPU iPhone OS 14_8_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148

〈Figure 12〉 User Information(1)

RecentSearchKeyword	data	...
00000000: 5B 7B 22 6B 65 79 77 6F 72 64 22 3A 22 EA B5 AC EB A7	[{"keyword":"	
00000012: A4 22 2C 22 73 68 6F 70 22 3A 6E 75 6C 6C 7D 5D	","shop":null}]	
AppsFlyerLastSessionDuration	real	281.000000

〈Figure 13〉 User Information(2)



〈Figure 14〉 User Information(3)

net.quicket.app/Preferences/net.quicket.app.plist에서는 그림 12, 13, 14와 같이 가입 연동을 Kakao로 했다는 것, 마지막 사용 시간이 2021.11.30. 12:58으로 앞서 파일과 11분의 오차가, OS 버전이 14.8.1, App 버전이 8.3.3, 통신사가 LG U+ 그리고 세션 ID, User Agent 정보, 지역 등 사용한 폰에 대한 정보들을 확인할 수 있다. 폰 모델은 아이폰 13으로 잘못된 정보가 표시되어 있다. 그리고 최근 검색어, 마지막 사용 소비 시간이 4분 41초인 것을 확인할 수 있었으며, 최근 봤었던 상품에 대한 정보를 확인할 수 있었다. 최근 봤었던 상품에 대한 정보에는 상품 제목, 가격, 올린 시간, 지역, 이미지, 올린 사람의 닉네임, 상세글, 카테고리, 해시태그가 있다.

net.quicket.app/Library/WebKit/WebsiteData/ResourceLoadStatistics/observations.db에서는 당근마켓과 마찬가지로 OperatingDates 테이블에서 그 동안 번개장터 App을 사용했었던 날짜들을 확인할 수 있었다.

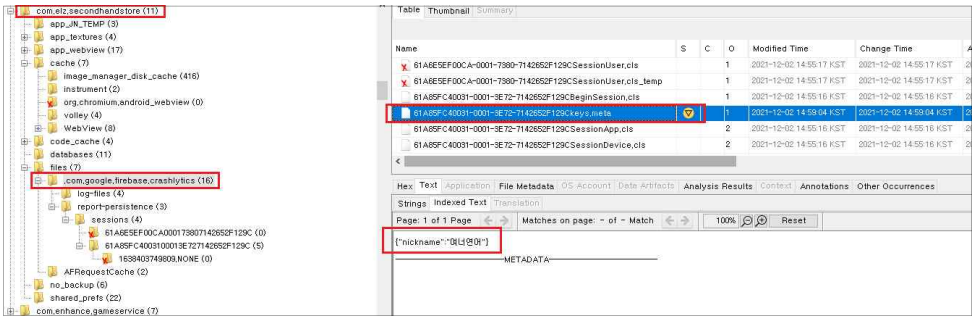
4.3. 중고나라

4.3.1. Android

중고나라의 파일 저장 위치는 data/com.elz.secondhandstore이다. 분석한 데이터의 경로 및 내용은 표 5와 같다.

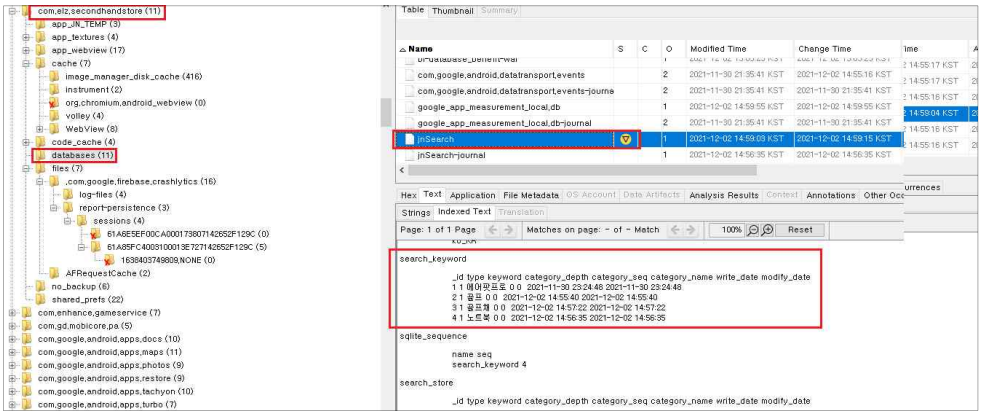
〈Table 5〉 Android joonggonara application data storage path and contents

Path	File Name	contents
data/com.elz.secondhandstore/.com.google.firebase.crashlytics	61A85FC40031-0001-3E72-7142652F129keys.meta	- 사용자 닉네임
data/com.elz.secondhandstore/databases	jnSearch	- 최근 검색어
data/com.elz.secondhandstore/app_webview/Default/Local Storage/leveldb	000003.log	- 사용자 이메일 주소
data/com.elz.secondhandstore/app_webview/BrowserMetrics	play_logger_context.pb	- 폰 화면 캡쳐 이미지
	1638403753673.NONE	
/data/com.elz.secondhandstore/cache/WebView/Default/HTTP Cache	125e3083582fceca_0	- 사용자 정보(이메일, 프로필 이미지, 전화번호, 성별, 연령대)



〈Figure 15〉 Nickname search

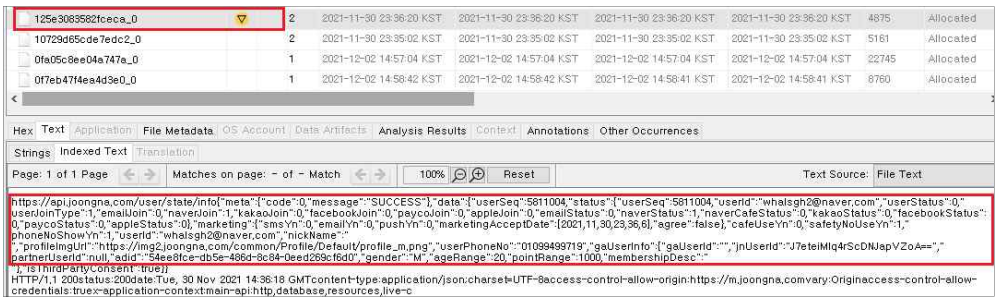
첫 번째로, 본인의 닉네임인 “여너연어”로 검색을 시도하였고, 그림 15과 같은 위치의 61A85FC40031-0001-3E72-7142652F129Ckeys.meta 파일에서 정보를 얻을 수 있었다.



〈Figure 16〉 Recent searches history

다음으로, 등록한 관심 키워드에 대해 검색해보았다. 중고나라에서는 “골프”와 “노트북”을 등록해두었다. 하지만, 검색 결과 등록한 관심 키워드에 대한 검색 결과는 나타나지 않았고 그림 16과 같이 최근 검색어에 대한 기록을 data/com.elz.secondhandstore/databases/jnSearch 파일에서 찾을 수 있었다.

추가적으로 계정 등록에 이용한 이메일 주소 또한 data/com.elz.secondhandstore/app_webview/Default/Local Storage/leveldb에 위치한 000003.log 파일에서 확인이 가능하였으며, data/com.elz.secondhandstore/app_webview/BrowserMetrics에 위치한 play_logger_context.pb 파일과 1638403753673.NONE 파일에서 스마트폰 캡쳐 화면을 확인할 수 있었다.



〈Figure 17〉 User Information

마지막으로 /data/com.elz.secondhandstore/cache/WebView/Default/HTTP Cache에 위치한 125e3083582fceca_0 파일에서 그림 17와 같은 사용자의 정보를 확인할 수 있었다. 등록 이메일과 프로필파일 이미지, 전화번호, 성별, 연령대 등 다양한 정보가 나타났다.

4.3.2. iOS

iOS의 중고나라 파일 저장 위치는 com.jnapp.usedMarket이다. com.jnapp.usedMarket에서 분석한 데이터의 경로 및 내용은 표 6와 같다.

〈Table 6〉 iOS joonggonara application data storage path and contents

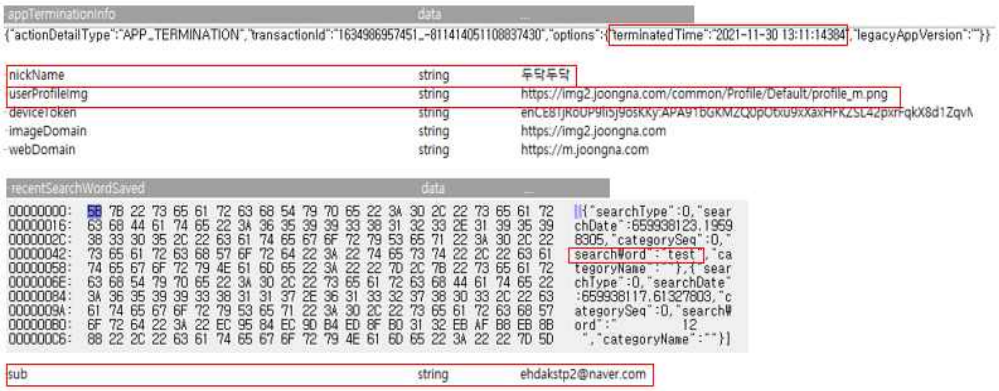
Path	File Name	contents
com.jnapp.usedMarket/Library	com-facebook-sdk-AppEventsTimeSpent.json	- 마지막 사용 날짜 및 시간 - 세션 ID - 마지막 소비 시간
com.jnapp.usedMarket/Library/Cookies	Cookies.binarycookies	- HTTP Cookies(값, 도메인, 만료일, 플래그)
com.jnapp.usedMarket/Library/Preferences	com.google.gmp.measurement.plist	- App version - 마지막 사용 날짜 및 시간 - OS version
	com.jnapp.usedMarket.plist	- 마지막 사용 날짜 및 시간 - 사용자 닉네임 - 사용자 프로필 사진 - 최근 검색어 - 사용자 아이디(이메일)
	com.sendbird.sdk.messaging.local_cache_preference.plist	- os Type - store(user) id - 사용자 닉네임 - App version - 사용자 프로필 사진

com.jnapp.usedMarket/Library/com-facebook-sdk-AppEventsTimeSpent.json에서는 다른 어플리케이션과 같이 마지막 사용 날짜 및 시간과 Facebook SDK에 사용되었던 세션 ID와 마지막 사용 때의 소비 시간을 확인할 수 있다.

〈Figure 18〉 binarycookies analysis result

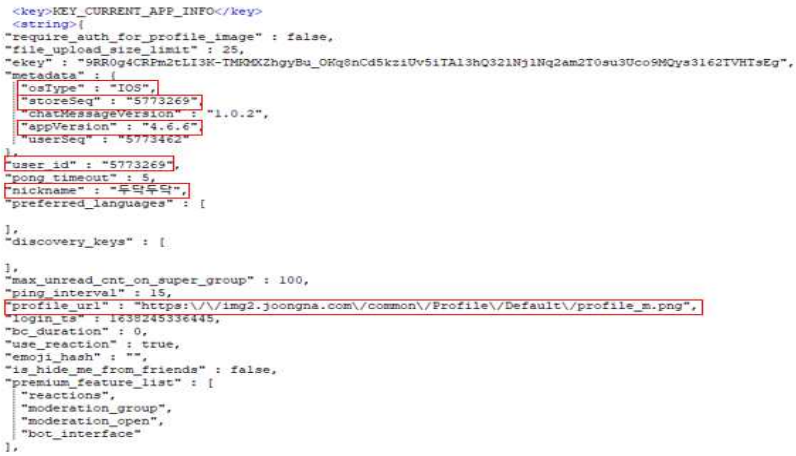
com.jnapp.usedMarket/Library/Cookies/Cookies.binarycookies도 다른 어플리케이션과 마찬가지로 Python을 이용해 분석하였으며 그림 18와 같이 쿠키 값과 도메인, 만료일, 쿠키 플래그를 확인할 수 있다.

com.jnapp.usedMarket/Library/Cookies/Preferences/com.google.gmp.mearsurement.plsit에서는 다른 어플리케이션들과 같이 현재 App 버전, OS 버전, 마지막 사용 날짜 및 시간을 확인할 수 있다.



〈Figure 19〉 User Information(1)

com.jnapp.usedMarket/Library/Cookies/Preferences/com.jnapp.usedMarket.plsit에서는 그림 19과 같이 마지막 사용 종료 날짜 및 시간인 2021.11.30. 13:11, 자신의 닉네임인 "두닥두닥", 프로필 이미지, 최근 검색어 "test", ID(이메일)을 확인할 수 있다.



〈Figure 20〉 User Information(2)

com.jnapp.usedMarket/Library/Cookies/Preferences/com.sendbird.sdk.messaging.local_cache_preference.plist에서는 그림 20과 같이 OS 종류, App 버전, 스토어(ID) 태그 숫자, 자신의 닉네임, 프로필 이미지를 확인할 수 있다.

Ⅴ. 주요 아티팩트를 통한 가상 시나리오

4장에서 국내 스마트폰 중고거래 어플리케이션 당근마켓, 번개장터, 중고나라 3종에서 사용자 관련 정보를 담고 있는 아티팩트의 분석을 진행했다. 3개의 어플리케이션 아티팩트에서 공통적으로 얻을 수 있는 주요 정보는 닉네임, 프로필 이미지, 이메일 등 사용자 정보, 마지막 사용 날짜 및 시간, 최근 검색어였다. 사용자 정보를 통해 사용자를 특정지을 수 있고, 마지막 사용 날짜 및 시간을 통해 사용자가 언제 해당 어플리케이션을 마지막으로 사용하였는지 알 수 있고, 최근 검색어를 통해 최근 어떤 상품에 관심이 있었는지 확인할 수 있다.

추가적으로 당근마켓은 위치 인증을 주력으로 하는 어플리케이션답게 사용자의 위치 정보를 획득할 수 있었다. 도/시/구/동까지만 나오기 때문에 정확한 주소는 알 수 없다. 하지만 대구광역시 중구 상덕동의 경우 약 0.003 km^2으로 50m 규격 수영장 두 개만 한 넓이로 비유된다. 이처럼 면적이 충분히 작은 동이라면 위치가 특정될 수 있다.

번개장터는 개인 간 채팅에 관한 마지막 정보와 최근 본 상품에 대한 정보를 획득할 수 있었다. 개인 간 채팅에 관한 마지막 정보는 각 개인 간 채팅 마지막 채팅의 정보로 마지막 채팅의 내용, 시간, 상대방 정보 등을 확인할 수 있고, 최근 본 상품에 대한 정보에는 최근 본 상품의 제목, 내용, 가격, 지역, 올린 사람 등을 알 수 있어 사용자가 어떠한 상품에 관심을 가지고 그 상품을 올린 사람과 채팅의 상대방을 대조함으로써 그 상품에 대해 채

팅을 나눴는지, 마지막 채팅을 통해 거래가 성사됐는지 실패했는지 등 어떻게 마무리되었는지 유추할 수 있다.

중고나라는 공통된 주요 정보 말고는 추가적인 정보가 없었다. 따라서 중고나라가 가장 개인정보의 노출이 적었다.

각 어플리케이션의 주요 아티팩트 요약은 다음 표 7과 같으며, 범죄를 저지른 사람이 판매자일 때와 구매자일 때를 나누어 시나리오를 가정하고, 각 상황에 활용될 수 있는 아티팩트 활용 방안을 제시하겠다.

〈Table 7〉 Each used trading application important data storage path and contents

Application	OS	Path and File Name	contents
당근마켓	Android	data/com.towneers.www/databases/ Colonies.db	최근 검색어
		data/com.towneers.www/shared_prefs/com.towneers.www.user.pref.xml	사용자 전화번호, 위치 정보, 이메일, 프로필 사진
	iOS	com.towneers.www/Library/Preferences/com.towneers.www.plist	처음 및 마지막 사용 날짜 및 시간, 최근 검색어, 사용자 위치 정보, 닉네임, 프로필 이미지, ID_identity, 전화번호
번개장터	iOS	net.quicket.app/Documents/default.realm	- 개인 간 채팅 마지막 정보(상대 id, 닉네임, 프로필 이미지, 마지막 채팅 내용, 마지막 채팅 시간)
		net.quicket.app/Library/Preferences/net.quicket.app.plist	마지막 사용 날짜 및 시간, 최근 검색어, 마지막 소비 시간, 최근 본 상품(글 제목, 내용, 태그, 가격, 지역, 이미지, 판매자 닉네임, 작성 시간, 카테고리)
중고나라	Android	data/com.elz.secondhandstore/files/.com.google.firebase.crashlytics/61A85FC40031-0001-3E72-7142652F129Ckeys.meta	사용자 닉네임
		data/com.elz.secondhandstore/databases/jnSearch	최근 검색어
		/data/com.elz.secondhandstore/cache/WebView/Default/HTTP Cache/125e3083582fceca_0	사용자 이메일, 프로필 이미지, 성별, 연령대, 전화번호
	iOS	com.jnapp.usedMarket/Library/Preferences/com.jnapp.usedMarket.plist	마지막 사용 날짜 및 시간, 사용자 닉네임, 프로필 사진, 최근 검색어, 아이디(이메일)
		com.jnapp.usedMarket/Library/Preferences/com.sendbird.sdk.messaging.local_cache_preference.plist	사용자 store(user) id, 닉네임, 프로필 사진

5.1. 판매자가 범죄를 저질렀을 때 시나리오

판매자가 중고거래 어플리케이션을 통해 범죄를 저지를 수 있는 경우는 판매 물품을 다른 물품으로 바꿔치거나 설명한 상태와 다른 물품을 파는 사기 범죄, 의약품 및 군용품 등과 같이 개인 또는 중고 거래가 금지된 물품 판매 등이 있는데, 이 중 사기 범죄의 경우로 시나리오를 작성하였다.

구매자 A는 판매자 B의 물품을 택배 거래로 구매하기로 하였다. A는 먼저 돈을 B에게 보내고 B는 돈을 확인하고 A에게 택배를 보냈다. 며칠 뒤 택배를 받은 A는 구매하기로 한 물품이 아닌 다른 물품을 받았고 경찰에 B를 신고했다. 하지만 B는 자신은 A와 거래하기로 한 적이 없으며, 최근 중고거래 어플리케이션을 사용한 적이 없다고 주장했다. 이때 B의 폰을 압수하여 포렌식 분석을 통해 B의 중고거래 어플리케이션의 마지막 사용 날짜 및 시간을 파악할 수 있다. 그리고 어플리케이션에 따라 다르지만 마지막 채팅 내용 정보를 확인할 수도 있다. 비록 중고거래 어플리케이션이 삭제될지라도 파일시스템 비할당 영역에 존재하는 데이터를 복구하여 사용 흔적을 파악할 수 있다.

5.2. 구매자가 범죄를 저질렀을 때 시나리오

구매자가 중고거래 어플리케이션을 통해 범죄를 저지를 수 있는 경우는 채팅으로 인한 성희롱, 직거래를 위한 만남에서 도난, 폭행, 살인 등이 있다. 이 중 채팅으로 인한 성희롱의 경우로 시나리오를 작성하였다.

판매자 C는 여성 옷을 판매한다고 글을 올렸다. 그러자 구매자 D는 개인 간 채팅으로 "판매자 실제 착용 사진을 보고 싶다"고 했고, C는 옷을 입고 사진을 찍어 D에게 보내줬다. 그러자 D는 C의 몸매를 언급하며 성희

롱성 발언이 담긴 메시지를 보냈다. 이에 C는 D를 성희롱으로 고소했다. 하지만 D는 본인이 메시지를 보내지 않았고, 해킹당한 것이라고 주장했다. 이때 D의 폰을 압수하여 포렌식 분석을 통해 D의 마지막 사용 날짜 및 시간과 최근 검색어를 파악할 수 있다. 그리고 어플리케이션에 따라 다르지만 마지막 채팅 내용 정보와 최근 본 상품의 정보를 확인할 수도 있다. 비록 중고거래 어플리케이션이 삭제될지라도 파일시스템 비할당 영역에 존재하는 데이터를 복구하여 사용 흔적을 파악할 수 있다.

Ⅵ. 결론

스마트폰 중고거래 어플리케이션의 사용자 수가 점차 늘어가고, 이미 수많은 사용자가 존재함에 따라 다양한 범죄가 발생하였다. 하지만 범죄와 같은 문제가 발생하면 중고거래 플랫폼 운영자는 책임을 지지 않는 경우가 많기 때문에 본인이 모든 것을 증명해야하는 경우가 발생했다. 따라서 이를 증명해줄 수 있는 데이터를 얻기 위해 중고거래 어플리케이션에서 저장하는 데이터의 내용을 파악해 분석하는 것이 필요하다.

본 논문에서는 국내에서 가장 많이 사용되고 있는 중고거래 어플리케이션인 당근마켓, 번개장터, 중고나라를 대상으로 분석을 진행하였으며, 각 어플리케이션에 대한 아티팩트 수집 및 분석을 수행하였다. 각 어플리케이션의 아티팩트를 분석함으로써 디바이스 내에 어떤 데이터가 저장되는지 그 데이터가 어느 경로로 저장되는지 파악할 수 있었고 주요 아티팩트를 정리하였다. 분석된 데이터를 통해 사용자 정보와 사용자의 최근 검색어, 마지막 사용 시간을 확인할 수 있고, 또한 어플리케이션에 따라 다르지만 위치, 최근 본 상품 정보, 마지막 채팅 정보, 거래 상대 정보 등을 확인할 수 있다. 이러한 정보들를 제시한 시나리오와 같이 범죄에 대한 증거로 활용할 수 있다. 해당 논문에서 각 어플리케이션들의 아티팩트 위치와 내용을 제시함으로써 더욱 빠른 분석 및 증거 수집에 도움이 될 것으로 예상된다.

구매 및 판매 내역, 게시글 그리고 모든 채팅 내용을 얻을 수 있다면 더 정확한 증거들로 사용할 수 있을 것이다. 하지만 인터넷 연결 없이는 어플리케이션에서조차 이 내용들을 볼 수 없는 것으로 보아 디바이스 내에 저장되지 않는 것으로 파악된다. 따라서 향후 아티팩트 분석에서 얻을 수 없었던 구매 및 판매 내역, 게시글, 모든 채팅 내용 등을 얻기 위해 각 어플리케이션의 네트워크 패킷 등에 관한 연구가 필요하다.

참 고 문 헌 (References)

[1] "Statistics Korea blog", https://blog.naver.com/hi_nso/222300521250

[2] "Maeil Business News Korea", https://www.mk.co.kr/news/business/view/2021/03/201453/

[3] "cpbc News", http://www.cpbc.co.kr/CMS/news/view_body.php?cid=810075&path=202109

[4] Feng Gao, Ying Zhang, "Analysis of Wechat on IPhone", Advances in Intelligent Systems Research, 2013.

[5] M. Sudozai, S. Saleem, W. J. Buchanan, N. Habib and H. Zia, "Forensics study of imo call and chat app", Digit. Invest., vol. 25, pp. 5-23, Jan. 2018.

[6] K. M. Ovens and G. Morison, "Forensic analysis of kik messenger on ios devices", Digit. Invest, vol. 17, pp. 40-52, Oct. 2016.

[7] Giyoon Kim, Uk Hur, Sehoon Lee, and Jongsung Kim, "Forensic Analysis of the Secure Instant Messenger Surespot," Journal of Digital Forensics, 13(3), pp. 175-188, Sep. 2019

[8] A. K. Agrawal, A. Sharma and P. Khatri, "Digital Forensic Analysis of Facebook App in Virtual Environment," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), 2019, pp. 660-664.

[9] Gi-Hwan Ryu, Sang-Jin Lee.(2014).Research on Analysis of Artifacts from Twitter.Journal of Digital Forensics ,8(2),15-29.

[10] FE Salamh, MM Mirza, S. Hutchinson, YH Yoon, U. Karabiyik, "What's on the Horizon? An In-Depth Forensic Analysis of Android and iOS Applications," in IEEE Access, vol. 9, pp. 99421-99454, 2021.

[11] as0ler, "BinaryCookieReader", https://github.com/as0ler/BinaryCookieReader

저 자 소 개

이 성 현 (Seonghyeon Lee)
준회원

2017년 3월~현재 : 아주대학교 사이버보안학과 학사과정
관심분야 : 사이버 보안

조 민 호 (Minho Cho)
준회원

2016년 3월~현재 : 아주대학교 사이버보안학과 학사과정
관심분야 : 사이버 보안

손 태 식 (Taeshik Shon)
평생회원

2000년 : 아주대학교 정보및컴퓨터공학부 졸업(학사)
2002년 : 아주대학교 정보통신전문대학원 졸업(석사)
2005년 : 고려대학교 정보보호대학원 졸업(박사)
2004년~2005년 : University of Minnesota 방문연구원
2005년~2011년 : 삼성전자 통신· DMC 연구소 책임연구원
2017년~2018년 : Illinois Institute of Technology 방문교수
2011년~현재 : 아주대학교 정보통신대학 사이버보안학과 교수
관심분야 : Digital Forensics, ICS/Automotive Security