Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.2, Apr. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.2.407

디지털 포렌식 관점에서의 인스타그램 사용자 행위 분석*

서 승 희,† 김 역, 이 창 훈‡
서울과학기술대학교 컴퓨터공학

Instagram Users Behavior Analysis in a Digital Forensic Perspective*

Seunghee Seo,† Yeog Kim, Changhoon Lee‡
Department of Computer Science and Engineering, Seoul National University of Science and Technology

요 약

인스타그램(Instagram)은 사람 간의 관계망을 구축하고 취미, 일상, 유용한 정보 등을 공유하는 인터넷 서비스인 소셜 네트워크 서비스(Social Network Service:SNS)로 최근 다양한 연령층에서 각광받고 있다. 하지만 업로드한 개인 정보를 불특정 다수가 열람할 수 있고 검증되지 않은 정보가 무방비하게 공유되기 때문에 이를 악용한 각종 사기, 스토킹, 명의 도용, 저작권 침해, 악성코드 유포 등의 문제가 발생 하고 있다. 이에 따라 인스타그램에 대한 디지털 포렌식적 관점에서의 분석이 필요하나 관련한 연구는 미약한 실정이다. 따라서 본 논문에서는 안드로이드 환경에서 인스타그램에 대해 디지털 포렌식 관점에서 역 공학 및 동적 분석을 수행하였고 그 결과 채팅 내용, 채팅 대상, 게시한 사진, 쿠키 정보 등의 사용자 행위 분석이 가능한 데이터가 담긴 3개의 데이터베이스 파일과 4개의 파일 저장 경로, 다양한 데이터 저장된 xml파일을 확인하였다. 또한 위의 분석 결과를 디지털 포렌식 조사에 활용할 수 있는 방안을 제시한다.

ABSTRACT

Instagram is a Social Network Service(SNS) that has recently become popular among people of all ages and it makes people to construct social relations and share hobbies, daily routines, and useful information. However, since the uploaded information can be accessed by arbitrary users and it is easily shared with others, frauds, stalking, misrepresentation, impersonation, an infringement of copyright and malware distribution are reported. For this reason, it is necessary to analyze Instagram from a view of digital forensics but the research involved is very insufficient. So in this paper, We performed reverse engineering and dynamic analysis of Instagram from a view of digital forensics in the Android environment. As a result, we checked three database files that contain user behavior analysis data such as chat content, chat targets, posted photos, and cookie information. And we found the path to save 4 files and the xml file to save various data. Also we propose ways to use the above results in digital forensics.

Keywords: Digital Forensic, Instagram, SNS, Android, Android reverse engineering

I. 서 론

소셜 네트워크 서비스(이하 SNS)는 사용자들에게 간단한 가입 절차와 사용을 제공한다. 또한 지인이나 제3자의 게시물을 간편하게 공유하거나 확인할 수 있어 많은 사람들이 SNS를 사용하고 있다. 미국

Received(03. 01. 2018), Modified(04. 16. 2018), Accepted(04. 16. 2018)
* 본 연구는 서울과학기술대학교 교내 연구비의 지원으로 수행되었습니다.
† 주저자, seunghee.seo.00@seoultech.ac.kr
‡ 교신저자, chlee@seoultech.ac.kr(Corresponding author)

시장조사회사 e마케터에 따르면 SNS 이용자 수는 2017년 24억 6000만명으로 세계 인터넷 이용자의 71%에 달할 것이라고 추산했다.[17] 또한 모바일 어플리케이션을 통한 서비스 제공은 폭발적인 SNS의 사용자 증가를 야기하였다.

하지만 사용자가 SNS에 제공한 개인 정보는 제3자에게 무방비하게 노출되기 쉽고 검증되지 않은 다량의 정보가 SNS 상에 공유되는 특성을 가지는데, 이를 이용한 다양한 범죄가 발생하고 있다. 예를 들어 SNS 상에 공개된 개인 정보를 도용하여 지인을 사칭하는 계정을 만들고 피해자에게 접근하여 금전적인 요구를 하거나[1] 각종 악성 링크, 악성 코드를 공유하여 유포할 수 있다.

또한 SNS는 소상공인들이나 기업에서 마케팅 전용 계정 또는 직원들의 개인 계정을 이용하여 노이즈 마케팅의 일환으로 사용되고 있으나 대부분의 기업들은 직원들에 대한 SNS 사용 관련 지침이 없어 이를 이용한 타직원의 명예 훼손, 기업 기밀 유출, 개인정보 도용 등의 범죄에 노출되어 있다.[13]

인스타그램(Instagram)은 웹과 모바일로 서비스를 제공하는 SNS 중 하나로 2010년 서비스를 시작하여[2] 최근 2017년 4월 사용자가 7억명에 달하였다. 국내 사용자는 2017년 천만명을 넘어섰으며 특히 젊은 연령층의 사용자들이 많이 선호하고 있다.[14] 또한 인스타그램은 게시물 공유, 팔로우, 채팅 등의 일반적인 SNS의 기능을 제공할 뿐 아니라, 사업자들을 대상으로 비즈니스 계정을 제공하여 스폰서 광고, 게시물 및 팔로워 통계 등 마케팅에 도움이 되는 기능을 지원하고 있다.

하지만 인스타그램 사용자의 증가에 따라 SNS에 관련한 다양한 사이버 범죄 또한 함께 증가하고 있다. 인스타그램의 대표적인 검색 기능인 해시태그를 이용하여 사용자를 물색한 후, 성희롱적인 다이렉트 메시지를 전송하거나[15] 계정을 해킹하여 지인의 명예를 훼손하는 게시글이나 메시지를 전송하는 등[16] 다양한 범죄가 만연하고 있다.

인스타그램의 전 세계적인 사용자 및 국내 이용자의 증가와 현재 발생하고 있는 다양한 범죄들을 고려할 때, 인스타그램에 대한 디지털 포렌식 관점의 분석은 반드시 필요하다. 그러나 인스타그램에 대한 디지털 포렌식적인 분석은 국내외적으로 매우 미약한 실정이다. 국외의 관련한 연구는 5개 내외로 매우 적으며 국내에서는 관련 연구가 전무하다.

이에 따라 본 연구에서는 인스타그램에 대한 디지털 포렌식적 관점에서 분석을 수행하였다. 모바일 OS 시장의 점유율이 가장 높은 안드로이드 OS 환경에서 인스타그램 어플리케이션을 분석하였으며 모바일 기기 내 저장되어 있는 기본 정보 및 사용자의 행위에 따른 생성 정보에 초점을 맞추어 분석을 수행하였다. 또한 분석한 내용을 통해 인스타그램에서 사용자가 게시글 업로드, 메시지 송수신, 페이스북 연동 등의 사실을 알 수 있는 3개의 데이터베이스 파일과 4개의 파일 경로, 다수의 xml파일 등을 확인하였다.

II. 관련 연구

2.1 기존 연구

Daniel Walnyky, Ibrahim Baggili 외 4명[4]은 IM 기능을 제공하는 SNS를 포함한 Android의 가장 인기 있는 20개의 IM 어플리케이션을 대상으로 디지털 포렌식 관점에서 연구를 수행하였다. 20개의 어플리케이션에 인스타그램도 포함되어 있으며, 각 어플리케이션에서 가능한 사용자의 행동을 수행해보고 이에 따라 발생하는 네트워크 트래픽 및 디바이스 내 파일 변화를 분석하였다. 분석 결과, 인스타그램에서 IM 기능을 이용하여 사진을 상대방에게 전송할 때, 서버에 사진이 저장이 된다는 사실을 발견했다.

Reema Al Mushcab과 Pavel Gladyshev는[5] 인스타그램을 안드로이드 다음으로 가장 많이 사용하는 모바일 OS인 IOS 환경에서 디지털 포렌식 관점에서 분석하였다. iPhone 5s 디바이스를 사용하여 또 다른 SNS 어플리케이션인 Path와 함께 비교 분석하였다. 인스타그램을 분석한 결과 인스타그램 ID number, 프로필 내용 등 사용자의 팔로워들의 자세한 계정 정보를 백업한 파일, 인스타그램 알람 관련 백업 파일, 마지막 로그인된 유저 이름, 메인 피드를 동기화한 시간 등 다양한 어플리케이션 활동 정보가 저장된 백업 파일을 발견했다. 또한, 이 파일들이 제공하는 정보들을 디지털 증거자료로써 활용할 수 있는 방안을 제안하였다.

Reema Al Mushcab과 Pavel Gladyshev는 또한 안드로이드 환경에서 [5]에서와 같이 인스타그램과 Path의 디지털 포렌식 관점에서의 분석을 수행하였다.[6] 하지만 [5]와 다르게 4개의 backup 도구를 사용하여 두 어플리케이션에서 백업 파일을

찾아 내 분석하고, 각 backup 도구의 성능을 비교 평가하였다. 인스타그램 분석 결과로는 인터넷 쿠키 정보를 저장하는 데이터 베이스인 Cookies의 경로와 일시적으로 저장되는 비디오의 저장 경로, 암호화 되어 저장된 백업 파일이 있다.

2.2 기존 연구의 한계

기존 SNS에 대한 포렌적 관점에서의 분석 연구는 대부분 가장 사용자가 많고 유명한 facebook에 대한 연구이며[10][11][12], 인스타그램에 관한 연구는 다양한 SNS 어플리케이션과 비교 차원에서의 분석이거나[4][5][6] SNS 자체 기능보다는 Instant Message(IM) 기능에 초점을 맞추고 있다[4]

인스타그램의 백업 파일에 관한 연구도 일부 존재하나[5][6], 현재 모바일 OS 시장의 점유율이 가장 높은 안드로이드 플랫폼[7]에 대한 연구는 보다 미약하다. Reema Al Mushcab과 Pavel Gladyshev는[6] 안드로이드 환경에서 인스타그램의 백업 파일을 분석하였으나 백업 파일 자체에 대한 분석보다는 여러 백업 프로그램을 이용한 디지털 포렌식 수사의 필요성에 주안점을 두고 있어 백업 파일 안에 담긴 데이터에 대한 분석은 부족하다.

본 논문에서는 위와 같은 기존 연구의 한계를 보완하여 안드로이드 환경에서 인스타그램의 모든 백업 파일에 담긴 데이터와 IM 기능을 포함한 사진 및 동영상 게시, 댓글 남기기, 좋아요 누르기, 해시태그 걸기 등의 모든 기능에 대하여 디지털 포렌식 분석을 수행하였다.

III. 연구 방법

안드로이드 환경에서 어플리케이션을 분석하는 방법은 크게 두 가지로, 동적 분석과 정적 분석이 있다. 안드로이드 어플리케이션은 구조적 특성상 역공학이 가능하기 때문에 소스를 추출하여 정적으로 분석이 가능하다.[8]

3.1 안드로이드 역공학 (정적 분석)

안드로이드 어플리케이션의 경우, 개발자는 작성한 java 소스를 컴파일한 바이트코드로 구성되어 있는 Dex 파일을 기타 라이브러리 및 리소스와 함께 APK(Android Package)에 포함하여 배포한다.[9] 이에 따라 DEX 파일을 APK에서 따로 추출 가능하며 어셈블리어인 smali 코드 형태로 변경 할 수 있다. 또한 smali 코드는 디컴파일을 통해 고수준의 언어인 Java 코드로 변경가능하다. Fig. 1은 안드로이드의 자세한 빌드 과정과 디컴파일 과정을 나타낸다.

이런 안드로이드 어플리케이션의 구조 특성을 이용하여 DEX 코드를 java 코드로 디컴파일 해주는 다양한 도구들이 존재하며, 이를 통해 디컴파일 된 java 소스를 이용하여 어플리케이션의 실행의 흐름과 동작 방식을 정적으로 분석할 수 있다. 안드로이드 역공학에 주로 사용되는 대표적인 도구들로 APK 파일 및 기타 파일을 추출할 때 사용하는 ADB, 디어셈블 도구인 Apktool, Dex파일을 Java 코드로 변환하는 Dex2jar, 정적 분석을 쉽게 해주는 Java Decompiler GUI 등이 있다.

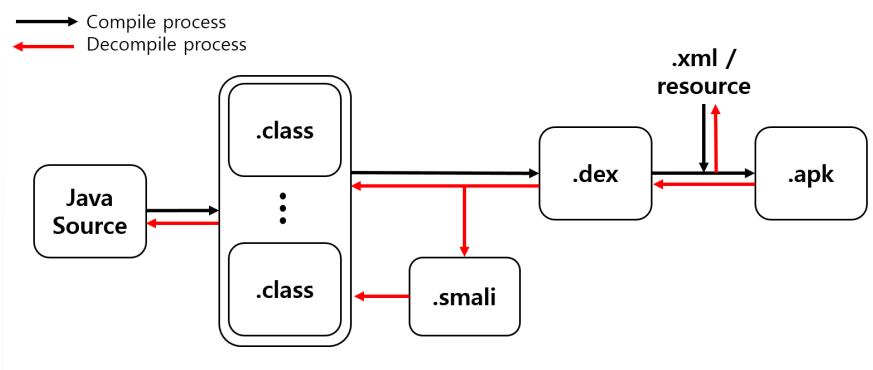

Fig. 1. Compile process and Decompile process on Android

3.2 동적 분석

동적 분석은 실제 어플리케이션을 실행하면서 발생하는 로그, 파일 디렉토리의 변화 등을 통해 앱의 코드 흐름을 추적하는 분석 방법이다. 동적 분석은 안드로이드 스튜디오 (Android Studio)의 기본 제공 도구인 Android Device Monitor 또는 DDMS(Dalvik Debug Monitor Service)를 사용한다. 또한 연결되어 있는 안드로이드의 디바이스의 내부 디렉토리를 확인 및 변경 가능한 ADB shell을 이용해서도 동적 분석이 가능하다.

3.3 실험 환경

본 논문에서는 Android 4.4.2가 탑재된 Samsung Galaxy s4를 이용하여 버전이 10.27.1인 인스타그램을 분석하였다. 분석 시 사용된 도구는 Table 1.과 같다.

IV. 인스타그램의 포렌식 분석

인스타그램 어플리케이션은 Ⅲ.에서 설명한 바와 같이 정적 및 동적 방법으로 분석한 결과, 디지털 포렌식 관점에서 유의미한 데이터베이스 파일 3개, 파

Table 1. Tools used to analyze

Tool Name	Description
ADB (Android Debug Bridge)	a versatile command-line tool for communication with Android devices [18]
dex2jar	a tool for converting the dex file to jar file
JD(java decompiler) gui	a tool that visualizes the structure of jar files and Java source to provide an analysis environment with a user
Android Device Monitor	a tool to show the file directory structure for an android device and logs.
DB Browser for SQLite	a tool for showing the contents of SQLite Database file.

Table 2. Files and directories path of Instagram

Type	Name	Content	Path
Data base file	direct.db	Contents and related information of Direct Message	/data/data/com.instagram.android/dagabases/direct.db
	Cookies	Internet cookie values of the user	/data/data/com.instagram.android/app_webview/cookies
	Web Data	Private information related the business account of the user	/data/data/com.instagram.android/app_webview/Web Data
Directories	cache	Photos the user loads from gallery for uploading to feed	/data/data/com.instagram.android/cache/
	files	A photo that the user temporarily saves before uploading and saving related files, Edited photos the user uploaded	/data/data/com.instagram.android/files/
	images	Every photo presented to the main feed	/data/data/com.instagram.android/images
	shared prefs	XML files created and used by Preference API	/data/data/com.instagram.android/shared_prefs

일 저장과 관련된 3개의 디렉토리, 로그 파일이 저장되는 2개의 디렉토리를 확인할 수 있었다. Table 2.은 각각의 해당하는 파일 및 디렉토리의 내용와 경로를 정리한 표이다.

4.1 데이터베이스

4.1.1 direct.db

direct.db는 android_metadata, messages, sqlite_sequence, threads 총 4개의 테이블로 구성되어 있는 데이터베이스 파일로 인스타그램에서 제공하는 채팅 서비스인 direct message에 대한 정보들을 저장한다. messages 테이블에는 다른 이용자들과 주고받은 메시지의 내용, 메시지의 전송 시각, 수신자, 발신자 등의 정보가 기록되어 있다. 또한 threads 테이블의 tread_info 에는 사용자가 메시지를 마지막으로 확인한 시간, 메시지의 내용, 수발신자, 메시지 전송 시각이 저장된다. direct.db의 각 테이블에 대한 정리는 Table 3.와 같으며 채팅 메시지가 저장된 Message table은 Fig. 3 와 같다.

인스타그램은 현재 단말기가 아닌 이전 단말기 또는 동시 접속한 단말기 등을 이용하여 전송한 메시지는 Message table의 recipient_ids의 필드가 null로 저장되는 것을 확인하였다. Fig. 4와 같이 두 디바이스를 이용하여 같은 채팅방에서 메시지를 전송한 후 초록색으로 표시된 단말기에서 direct.db의 변화를 관찰한 결과, message table에 붉은 색으로 표시된 단말기로 전송한 메시지가 Fig. 2와 같

Table 3. Tables of direct.db

Table name	Content
android_metadata	Country version of Instagram application (ex. ko_KR)
messages	Information related direct messges (user id, thread id, timestamp, text, message code etc.)
sqlite_sequence	The total number of messages and threads
threads	Information related threads (user id, recipient id, last activity time, thread information etc.)

이 recipient_ids값이 null로 기록되어 저장되는 것을 확인하였다.

인스타그램은 이와 같이 여러 기기를 이용하여 동일 계정으로 동시 접속이 가능하고 동시 접속 시 기존 로그인한 사용자에게 별도의 알림이 제공되지 않으므로, 단말기 변경 후 이전 디바이스에 계정 정보가 남아있거나 해킹을 통해 계정 정보를 탈취당한 경우 제 3자에 의한 동시 사용이 가능하다. 만약 악의적인 목적을 가진 사용자에 의해 계정 정보를 탈취당한다면, 사용자를 사칭한 금전 사기, 불법 광고 및 악성코드 유포 등에 계정이 이용될 수 있다. 이때 동시 접속을 이유로 계정 정보 탈취 및 이용 사실에 부인할 수 있으나, 단말기 압수를 통한 recipient_ids 값 분석을 통하여 해당 사실을 입증할 수 있다.

	client_item_id	thread_id	recipient_ids	timestamp	message_type	text
	필터	필터	필터	필터	필터	필터
137952	14AE3C48-7A···	340282366841···	NULL	149906638130···	text	마쟈
278656	NULL	340282366841···	NULL	149906637782···	text	잘됐음 좋겠다
349600	fb638919-406···	340282366841···	1268656491,452914297	149906636943···	text	넘나좋나

Fig. 2. Message table of the phone marked green line

	_id	user_id	server_item_id	client_item_id	thread_id	recipient_ids	timestamp	message_type	text	message
	필터	필터	필터	필터	필터	필터	필터	필터	필터	터
9	1123	822522775	272289758672···	8DB93495-F1B8-43B1-9···	340282366841···	NULL	147608573948···	media_share	NULL	content_typ···
10	1124	822522775	272289758672···	8DB93495-F1B8-43B1-9···	340282366841···	NULL	147608573948···	text	스크롤 내리다가 시선강탈 ···	content_typ···
11	1125	822522775	272290209819···	NULL	340282366841···	NULL	147608818516···	text	ㅜㅜㅜㅜㅜㅜㅜㅜㅜㅜ···	content_typ···

Fig. 3. Message table of direct.db

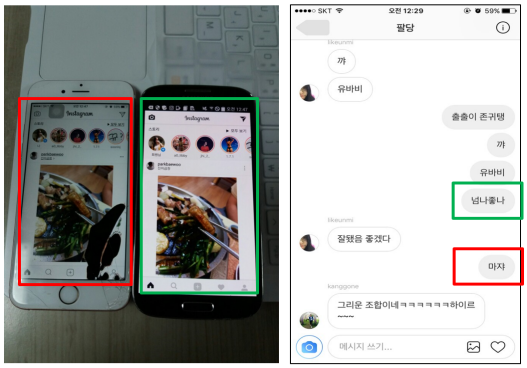

Fig. 4. The simultaneous login using different devices

4.1.2 Cookies

cookies는 확장자가 존재하지 않으나 같은 디렉토리 내 cookies-journal을 통하여 데이터베이스 파일임을 확인할 수 있다. cookies는 Table 4.와 같이 cookies와 meta라는 총 2개의 테이블로 구성되어 있고, sessionid, 서버에서 부여받은 사용자 고유 번호인 user_id, 각종 token 정보 등 인터넷 통신에 필요한 사용자의 정보 관련 정보가 저장된다. Fig. 5는 DB Browser를 사용하여 열어본 cookies의 cookies table의 모습이다.

cookies 테이블에 기록되는 ds_user 칼럼 값은 로그인한 유저의 실제 아이디 정보를 저장하며 사용자 고유 번호를 의미하는 ds_user_id는 사용자 관련 설정 파일 저장 및 direct 메시지의 수발신자 식별 등에 사용된다. 만약 불법 행위에 사용된 단말기를 압수하여 cookies 테이블에 대한 접근 권한을 얻는다면, 위의 두 칼럼을 이용하여 저장된 설정 파일들을 추적함으로써 인스타그램을 이용한 사용자의 행

Table 4. Tables of cookies

Table name	Content
cookies	The Internet use information of the host communicating with a user on network (host key, value, expiration date, last access time etc.)
meta	Version of cookies table

위를 입증할 수 있다. 또한 ds_user와 last_access_utc 칼럼 값을 조합하여 특정 아이디를 로그인한 시간을 추정하는 데 이용 가능하다.

4.1.3 Web Data

인스타그램은 개인, 기업의 마케팅을 위한 비즈니스 계정을 제공하고 있다. 개인계정에서 비즈니스 계정으로 전환할 경우, 비즈니스에 관련된 프로필 및 이메일 정보나 회사 또는 가게의 위치 정보 등을 사용자는 추가로 등록할 수 있다. 또한 인스타그램에 광고를 요청할 경우 결제되는 신용카드에 대한 정보를 입력해야한다. 인스타그램은 이런 비즈니스 계정에 관된 정보를 데이터베이스에 저장하여 사용하며, 해당 데이터베이스가 Web Data 라는 것을 확인하였다.

Web Data도 역시 앞서 설명한 cookies와 같이 확장자가 db로 되어 있지 않은 데이터베이스 파일로, 총 9개의 테이블로 구성되어 있다. 해당 데이터베이스는 이런 비즈니스 계정의 프로필 정보, 이메일, 위치정보, 핸드폰 번호, 신용카드 정보 등을 테이블 별로 나누어 저장하고 있다.

Web Data 데이터베이스에 구성되어 있는 table은 Fig. 6과 같다.

	creation_utc	host_key	name	value	path	expires_utc	secure	httponly	last_access_utc
	필터	필터	필터	필터	필터	필터	필터	필터	필터
1	131430398769···	.i.instagram.c···	mid	WVJOYAABAAGjVAU3-Pw5l6w5i8Jv	/	0	0	0	13143039876937751
2	131430398769···	.i.instagram.c···	sessionid	IGSC57f935281fe1c493f40d4171687bdc···	/	0	0	0	13143039876937861
3	131430398769···	.i.instagram.c···	ds_user	s_hee_s	/	0	0	0	13143039876937936
4	131430398786···	.i.instagram.c···	igfl	s_hee_s	/	0	0	0	13143039878622643
5	131430398854···	.facebook.com	fr	0tRMYGNTi0hAUIT1u.AWU_BPk0-s2oCq2SS8Jx2SDszh4.BZUk6F..AAA.0···	/	131508158854···	0	1	13143039885427909
6	131430997005···	.i.instagram.c···	is_starred_en···	yes	/	0	0	0	13143099700509656
7	131430998231···	.i.instagram.c···	rur	FTW	/	0	0	0	13143099823194201
8	131430998231···	.i.instagram.c···	csrftoken	c8xO7FMoX8MkqiFtQZEWm0wRH0bSb···	/	0	0	0	13143099823195787
9	131430998231···	.i.instagram.c···	ds_user_id	822522775	/	0	0	0	13143099823196696

Fig. 5. Cookies table of a cookies DB

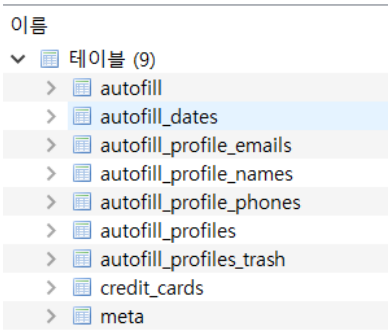

Fig. 6. Web Data Table list

4.2 파일 저장 관련 디렉토리

4.2.1 cache and files 디렉토리

cache와 files 디렉토리는 사용자가 업로드하는 게시물과 관련한 데이터를 저장한다. 인스타그램은 게시물에 반드시 사진을 포함해야하고, 사진은 앱 내에서 촬영 및 수정이 가능하다. 사용자가 게시물 업로드를 위해 사진을 앱에 로드하면 해당 사진은 cache에 복사되고 게시물 업로드를 완료하고 난 후 file 에 복사된다. 사용자가 사진을 수정할 경우, 업로드 완료 후 수정된 파일도 함께 file과 cache에 저장된다. 위의 사실은 단말기에서 특정 게시물에 대한 업로드 여부를 확인하는 데 활용될 수 있다. 예를 들어 악성 링크나 저작권에 침해되는 게시물을 업로드한 사용자의 단말기에서 cache와 file 내 사진 파일과 게시물 내 사진의 대조를 통해 업로드 사실을 입증할 수 있다.

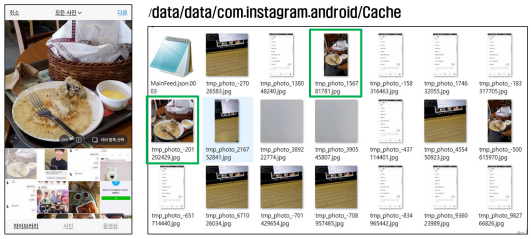

Fig. 7. Screen of uploading a post and photos saving in a cache folder

4.2.2 images 디렉토리

image는 메인 피드와 관련된 사진 파일들이 저장되는 경로로 메인 피드에 표시되는 이미지 파일들이 저장된다. image 내 파일들은 파일 확장자가 .clean으로 되어 있으나 분석한 결과, 'FF D8 FF E0'로 시작하는 JPEG 이미지 파일 포맷임을 확인하였다. 주로 다른 사람들의 프로필 이미지, 게시된 사진, 동영상 미리보기 사진 등이 저장되므로 이 경로 내 파일을 통해 사용자가 팔로우하고 있는 사용자, 주된 메인 피드 내용을 파악할 수 있다.

또한 이 파일들은 메인 피드 접속과 동시에 서버로부터 내려 받아 저장하므로 파일의 저장 시간과 메인 피드 접속 시간은 거의 일치한다. 이에 따라 사용자의 메인 피드 접속 시간을 추정 가능하다.

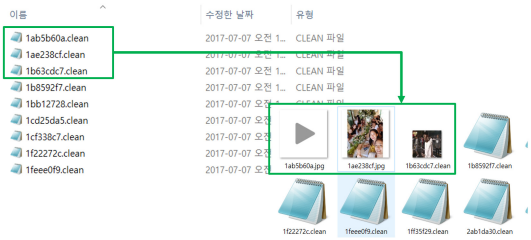

Fig. 8. The extension conversion of file saving in an images folder

4.2.3 shared_prefs 디렉토리

shared prefs는 안드로이드의 데이터 입출력 라이브러리인 Preference을 통해 생성된 xml파일들을 저장한다. Preference는 앱 설정과 같이 사용빈도가 높고 비교적 간단한 데이터를 xml 파일로 입출력하며 Fig. 9와 같이 SharedPreference 클래스를 선언하여 구현한다. 또한 이 클래스로 선언과 동시에 오픈된 xml 파일은 shared_prefs에 저장되고 파일명은 클래스 선언 시 생성자로 입력받은 문자열로 지정된다.

분석 결과 인스타그램은 앞서 언급한 사용자 고유번호를 이용하여 계정 별로 앱 설정 데이터를 구분 및 사용하고 이에 따른 파일명은 〔사용자 고유 번호〕_〔행위 및 서비스 이름〕.xml 형태임을 확인하였다. shared_prefs 내 xml파일은 클래스 선언 코드

```
public final class s
{
  public static s a;                                    Declare
  public SharedPreferences b = b.a("starredHidePreferences");
  public Set<String> c = new HashSet();
```

Fig. 9. SharedPreferences class variable declaration in the program source of Instagrm

Table 5. Xml files saved in the shared_prefs folderss

No.	File name	Description	Contents of file
1	[account number]_starred_view.xml	This file saves the information related video if a user watches video clips played automatically,	The id number of a video, UTC times a user watched
2	[account number]_AutoCompleteHashtabService.xml	This file stores relevant information if there is a hash tag on a commnet or post.	Contents of tag
3	[account number]_facebookPreferences.xml	The user information related login of Facebook is stored this file if a user logins using the facebook account.	An account name of Facebook, Oauth Access Token, The saved time and expired time of the token. user_id
4	[account number]_MainFeedSeenStateStore.xml	This file saves that posts of the main feed are seen or not. If a user look at posts, a post ID is written in 〈set name="seen_ids"〉 tag.	IDs of posts which a user saw and which a user not saw yet.
5	[account number]_starredHidePreferences.xml	This file saves the sync time when media files are synchronized.	The UTC time the media file is synchronized.
6	[account number]_USER_PREFERENCES.xml	This file saves the configuration information of a user.	Camera flash on/off setting, Photo auto save setting, sdn token
7	[account number]_usersBootstrapService.xml	The friend list of Facebook account is saved in this file, who use Instagam. This list presents on 'finding friend' tab	The name, profile of friend, Following or not
8	[account number]_video_view	If a user watches videos, this file saves the related information.	Video ID watched, Timestamp, The time of re-watched

가 호출되지 않으면 생성되지 않으므로 경로 내 존재하는 xml의 파일명 분석을 통해 계정 별 이용 서비스 내역을 추정할 수 있다.

또한 xml 내 저장된 데이터로 사용자 행위를 유추 가능하다. 예를 들어, AutoCompleteHash--tagService.xml 내 첫 태그의 Content 값이 'self'이고 파일 수정 시간이 '2017-06-31 13:51'이면 사용자가 해시태그 #self를 2017년 06월 31일 13:51에 사용했음을 알 수 있다.

인스타그램의 shared_prefs 내 저장되는 xml파일명 일부와 파일명에 따른 저장 데이터에 대한 정리는 Table 5.와 같다.

V. 결론 및 향후 연구

계속되는 SNS 이용자 수의 증가와 더불어 SNS를 활용한 다양한 범죄가 등장하고 있다. 또한 SNS는 많은 사람들의 생활에 밀접하게 연관되어 있기 때문에 사건의 중요한 단서가 될 수 있는 다양한 정보들을 SNS에서 획득할 수 있다. 인스타그램 역시 SNS로 해당 앱에서 범죄 입증에 관한 다양한 정보를 증거자료로 획득할 수 있다. 본 연구를 통해 확인된 정보를 활용하여 실제 사용자 본인이 업로드한 게시글인지 실제 전송한 다이렉트 메시지인지 등의 여부를 인스타그램 어플리케이션 분석을 통해 확인할

수 있다. 이러한 사항은 SNS을 이용한 도용이나 사칭 등을 확인하는 데 도움이 된다.

본 연구에서는 인스타그램의 일부 디렉토리와 shared_prefs 폴더 내의 일부 파일들의 분석을 통해 디지털 포렌식적으로 유의미한 다양한 정보를 확인하였다. shared_prefs 폴더에 저장되는 xml 파일의 경우, 관련 서비스 및 기능이 실행되지 않으면 xml 파일이 생성되지 않기 때문에 보다 많은 xml 파일이 생성될 가능성이 다분하며, 본 논문에서 확인한 디렉토리 외에 다른 디렉토리에서 추가적인 유의미한 정보가 확인 될 것이라고 기대한다.

References

[1] Sns Fraud, http://www.fnnews.com/news/201402041721133241

[2] Instagram history, https://instagram-press.com/our-story/

[3] Instagram active user monthly, https://www.statista.com/statistics/253577/number-of-monthly-active-instagram-users/

[4] Daniel Walnycky, Ibrahim Baggili, Andrew Marrington, Jason Moore, Frank Breitinger, "Network and device forensic analysis of Android social-messaging applications", , DFRWS 2015 USA, Digital Investigation, vol. 14, no. 1, pp. S77-S84, Aug. 2015

[5] Reema AL Mushcab, Pavel Gladyshev, "Forensic Analysis of Instagram and Path on an iPhone 5s Mobile Device",Computers and Communication (ISCC), 2015 IEEE Symposium, pp. 6-9, Jul. 2015

[6] Reema AL Mushcab, Pavel Gladyshev, "The Significance of Different Backup Applications in Retrieving Social Networking Forensic Artifacts From Andrroid-Based Mobile Devices", Information Security and Cyber Forensics (InfoSec), 2015 Second International Conference, pp.15-17, Nov. 2015

[7] Worldwide Smartphone OS Market, http://www.idc.com/promo/smartphone-market-share/os

[8] Jong-Won Choi, Jeong-Hyun Yi. "Analysis on Personal Information Leakage of Google Account App on Android." Journal of Digital Forensics , vol. 8, no. 2, pp. 65-81, Dec. 2014

[9] Sanghyung Kim, Android Programming Conquest, 4th Ed., vol. 1,Hanbit Media, pp. 19

[10] Miroslav Vaca, Jasmin Cosic, Zoran Cosic, "Forensic Analysis of Social Networks", Proceedings of the ITI 2013 35th, International Conference on Information Technology Interfaces, pp.24-27, Jan. 2013

[11] Noora Al Mutawa, Ibrahim Baggili, Andrew MArrington. "Forensic analysis of social networking applications on mobile devices", DFRWS 2012, Digital Investigation. vol. 9, pp. s24-s33, Aug. 2012

[12] Farhood Norouzizadeh Dezfouli, Ali dehghantanha,Brett Eterovic-Soric, Kim-Kwang Raymond Choo "Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms", Australian Journal of Forensic Sciences , vol. 48, pp. 469-488, Aug 2015

[13] Taylor, Mark, et al. "Forensic investigation of social networking applications." Network Security vol. 2014, no. 11 pp. 9-16, Nov.2014

[14] Korea sns statistics 2017,http://www.mobiinside.com/kr/2017/08/24/korea-sns-2017-1/

[15] Instagram Stocking, http://www.civicnews.com/news/articleView.html?idxno=5057

[16] Instagram Direct hacking, https://m.blog.naver.com/PostView.nhn?blogId=mintkiwi24&logNo=220412395650&pro

xyReferer=https%3A%2F%2Fwww.google.co.kr%2F
〔17〕 Sns user number, http://news.joins.com/article/21770960
〔18〕 ADB, https://developer.android.com/studio/command-line/adb.html

〈저자소개〉

서 승 희 (Seunghee Seo) 학생회원
2012년 3월: 서울과학기술대학교 컴퓨터공학과 학사
2017년 3월: 서울과학기술대학교 컴퓨터공학과 석사과정
〈관심분야〉 정보보호, 역공학, 디지털 포렌식, 암호학

김 역 (Yeog Kim) 정회원
1992년 3월: 성신여자대학교 전산학과 (이학사)
2003년 3월: 고려대학교 정보보호대학원 (공학석사)
2010년 3월: 고려대학교 정보경영전문대학원 (공학박사)
2005년 3월~2007년 8월: 동양미래대학교 전임강사
2017년 9월~현재: 서울과학기술대학교 전기정보기술연구소 연구원
〈관심분야〉 정보보호, 디지털 포렌식, 암호모듈평가 등

이 창 훈 (Changhoon Lee) 종신회원
2001년 3월: 한양대학교 자연과학부 수학전공 학사
2003년 3월: 고려대학교 정보보호대학원 석사
2008년 3월: 고려대학교 정보경영전문대학원 정보보호전공 박사
2008년 4월~2008년 12월: 고려대학교 정보보호연구원 연구교수
2009년 3월~2012년 2월: 한신대학교 컴퓨터공학부 조교수
2012년 3월~2015년 3월: 서울과학기술대학교 컴퓨터공학과 조교수
2015년 4월~현재: 서울과학기술대학교 컴퓨터공학과 부교수
〈관심분야〉 정보보호, 사이버 보안, CTI, IoT보안, 디지털포렌식, 암호학 등