JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 1 : 72~80 Jan. 2016

안드로이드 환경에서의 KakaoTalk 메신저의 포렌식 분석 방법론 제안 및 분석

윤종철[1] · 박용석[2*]

Forensic Analysis of KakaoTalk Messenger on Android Environment

Jongcheol Yoon[1] · Yongsuk Park[2*]

Graduate School of Information Security, SeJong Cyber University, 121 Gunja-ro, Gwangjin-gu, Seoul 05000, South Korea

요 약

최근 우리는 스마트폰을 활용하여 KakaoTalk IM(Instance Messenger)을 사용한다. IM 서비스에는 사용자/용의자의 생활패턴, 지리적 위치, 사상, 심리 상태 및 범죄 사실에 대한 흔적들이 존재하여 포렌식 분석이 필요하다. 하지만, KakaoTalk의 포렌식 분석은 미흡한 현실이다. 이에 본 논문은 KakaoTalk에 적합한 새로운 연구방법론을 제시하고, 흔적(Artifacts)의 위치 발견을 하고, 연락처・메시지의 칼럼 구조 분석하고, 사용자/용의자를 식별 하였으며, 추가한 연락처 정보들과 메시지의 타입을 파악하였고, 삭제한 연락처의 백업파일을 사용하여 복원하였다. 그 결과 분석한 정보와 방법론을 활용하면 Forensic Tool의 기본 플랫폼이 된다.

ABSTRACT

Recently, IM(Instant Messenger) of KakaoTalk is being used on smart devices such as smartphones. Because IM service can carry user and/or suspector's various information including life style, geographical position, psychology and crime history, forensic analysis on IM service is desirable. But, forensic analysis for KakaoTalk is not well studied yet. This paper studies a proper forensic method for KakaoTalks, finds artifacts location, reconstruct the list of contacts and the chronology of the messages that have been exchanged by users. Proposed methodology and analyzed information can provide a basic platform for forensic tool.

키워드 : 안드로이드 포렌식, IM(Instant Messenger), KakaoTalk, WhatsApp, SNS(Social Network Service)

Key word : Android Forensic, IM(Instant Messenger), KakaoTalk, WhatsApp, SNS(Social Network Service)

접수일자 : 2015. 12. 01 심사완료일자 : 2015. 12. 28 게재확정일자 : 2016. 01. 06

* **Corresponding Author** Yongsuk Park(E-mail:yongspark@sjcu.ac.kr, Tel: +82-2-2204-3894)
The Graduate School of Information Security, SeJong Cyber University, 121 Gunja-ro, Gwangjin-gu, Seoul 05000, South Korea

Open Access http://dx.doi.org/10.6109/jkiice.2016.20.1.72 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

인스턴트 메신저(IM : Instant Messenger)는 이동통신사 SMS, MMS 사용을 대신해 인터넷에 연결하여 메시지, 전화, 사진, 비디오 그리고 음성메시지를 주고받는 서비스이다. IM 서비스의 이용자들은 자유로운 의사소통과 정보 공유, 그리고 인맥 확대 등을 통해 사회적 관계를 맺어 일상 생활양식을 크게 변화시켰다[1-3]. IM은 사이버 수사에 증거로써 용의자 인적 네트워크 분석, 용의자 범죄동기 파악, 2차 범죄 사전 예측, 용의자 위치 파악, 알리바이 검증 등을 파악할 수 있는 중요한 정보이다[4]. 따라서 IM 포렌식 분석의 관심이 증가하고 있다. 국외 IM Apps은 포렌식 분석 연구가 활발하게 진행[5-9] 중 이지만, 국내 IM Apps은 포렌식 분석의 연구[10, 11]가 미흡한 실정이다.

이에 본 논문에서는 KakaoTalk App(국내 1위 IM App)을 사용흔적을 분석하기 위한 적합한 분석방법론을 제안하고, 제시한 방법론으로 포렌식 분석 연구를 진행한다.

Ⅱ. 관련 연구

IM Apps의 포렌식 연구는 일반적으로 iOS, 안드로이드의 분석 연구가 존재한다.

iOS의 IM 포렌식 연구는 Apple iTunes 백업/복원을 사용하여 획득한 사용자명, 메시지, 잔존하는 파일의 위치를 포렌식 분석하였다[5, 6]. 안드로이드의 IM 포렌식 연구는 세계에서 가장 많이 사용하는 WhatsApp 분석 연구가 활발하다. WhatsApp의 분석 연구는 VM(Virtual Machine)의 기반으로 잔존파일의 위치, 연락처・채팅 테이블의 구조 분석 등을 포렌식 분석하였다[8, 9]. 또한, WhatsApp의 암호화 Backup DB파일은 외부에서 공개한 복호화 프로그램(Xtract package)을 사용하여 복호화 후 얻은 평문의 과거 연락처・채팅메시지 정보를 포렌식 분석에 활용하였다[7].

하지만, KakaoTalk의 포렌식 분석연구는 기본적인 패키지 설치 위치를 소개하였고, 설치 위치에 존재하는 프리퍼런스(Preference), 데이터베이스(DataBase), 파일(File)의 기본적인 소개로 포렌식 분석연구가 미흡한 실정[10, 11]으로 KakaoTalk의 적합한 포렌식 분석 방법론과 분석이 필요하다.

Ⅲ. 분석 방법론

IM서비스는 1:1 또는 1:N 채팅방을 만들고 상호간 텍스트메시지, 멀티미디어 파일, 지도 등을 주고받는다. 주고받은 정보들은 단말기에 크게 나누어 휘발성 데이터, 비휘발성 데이터로 저장매체에 저장된다. 특히, 비휘발성 데이터의 정보는 단말기에 오랫동안 저장되어 잔존할 뿐만 아니라 휘발성 데이터 비해서 더 많은 정보들이 잔존한다. 이러한 이유로 본 논문에서는 IM 사용의 흔적인 비휘발성 데이터를 포렌식 분석한다. 이에 본 장에서는 KakaoTalk에 적합한 비휘발성 데이터의 포렌식 분석 방법을 제안한다.

3.1. 기존 포렌식 분석 방법의 한계

기존(WhatsApp)의 분석방법은 흔적파일의 분석 방법이 정확히 파악하기 어렵고(재연 불가능), 연락처·채팅 메시지 DB의 암호화 방식이 달라 다른 접근 방법이 필요하고, 제공하는 기능이 다르고, 분석 환경이 다르다. 따라서 KakaoTalk의 분석 방법은 다른 분석방법이 제공되어야한다. 파악된 WhatsApp과 KakaoTalk의 비교분석은 표 1 과 같다.

Table. 1 Comparison of WhatsApp and KakaoTalk

	WhatsApp	KakaoTalk
Artifacts Location	Replays are impossible	Introduction to basic
Contact・Chat DB	Plain text	Column Encryption
Contact・Chat Backup DB	File Encryption	Column Encryption
Features	Normal Chat	Normal Chat Secret Chat
Experiment Environment	Virtual Machine	Real Machine

3.2. 흔적 파일의 저장 위치 분석 방법

기본적으로 다양한 콘텐츠를 송・수신시키면, 교환한 콘텐츠의 새로운 파일이 파일시스템에 저장된다. 이러한 콘텐츠 파일의 저장 위치 분석방법은 콘텐츠 송・

수신 전(before) '디렉토리에 있는 파일과 하위디렉토리 목록'을 텍스트 파일로 루팅된 스마트폰에 저장하고, 콘텐츠 송・수신 후(after) '디렉토리에 있는 파일과 하위디렉토리 목록'을 텍스트 파일로 루팅된 스마트폰에 저장한다. 저장한 전・후 텍스트 파일은 분석PC에 저장하고, PC에서는 전・후 텍스트 파일을 비교하여 새롭게 생성한 파일을 발견한다. 하지만, 새롭게 생성한 파일은 KakaoTalk의 콘텐츠 파일, 시스템이 생성한 파일, 다른 App이 생성한 파일 등이 다량 발견되어, 분석의 어려움이 가중된다.

이에 분석의 시간을 단축하기 위해 방법을 제시한다. 일반적으로 응용프로그램은 시스템의 디렉토리에 파일을 저장을 할 수 없다. 따라서, 시스템이 생성한 디렉토리(하위 디렉토리 포함) 목록을 제거한다. 제거 후 남겨진 발견된 파일은 흔적 파일로 가정하여, PC에 파일들을 저장하고, 저장한 파일은 콘텐츠에 대응하는 뷰어 프로그램을 실행하고, 파일을 본 후 실행하여 볼 수 있는 파일은 흔적파일로 판단한다. 추가로 뷰어 프로그램으로 볼 수 없는 파일은 시그니처 분석을 하여, 흔적 파일의 저장 위치를 분석한다.

3.3. DB 암호 상태 구조・복호화 분석 방법

WhatsApp은 저장 중인 연락처・채팅 DB파일이 평문 값으로 이루어져 복호화 과정 없이 테이블의 구조 분석이 가능하지만, KakaoTalk은 저장 중인 연락처・채팅 DB파일이 평문 값과 칼럼 암호화(주요 개인정보인 메시지, 멀티미디어 주소, 휴대폰 연락 등의 정보)로 되어있는 것을 확인하였고 따라서 테이블의 구조 분석이 어렵다. 구체적으로 파악된 KakaoTalk의 연락처・채팅메시지 DB파일의 저장 경로(Directory), 암호화는 표 2 과 같다.

Table. 2 DB encryption status of KakaoTalk

	Directory	File Name	Encryption
DB	/data/data/com.kakao.talk/databases	KakaoTalk.db (chat)	Column Encryption
		KakaoTalk2.db (contact)	
Backup DB	/data/data/com.kakao.talk/files	103466717.backup (chat)	Column Encryption
		-1087431639.backup (contact)	

이에 KakaoTalk의 DB 복호화 연구가 필요하여, 새로운 복호화 분석 방법을 제시 및 기술한다.

KakaoTalk은 복호화 연구가 활발히 진행되지 않아 복호화 연구의 어려움을 가중시킨다. 복호화 로직을 분석하기 위해 디컴파일 후 소스코드를 분석도 가능하지만, 대량의 소스코드 및 소스코드 난독화가 존재하여, 암호로직의 파악이 어려워 복호화가 어렵다. 이에 복호화 방법을 제안하여 연락처, 채팅메시지 DB 테이블의 구조를 분석한다.

복호화 제안방법은 채팅메시지 테이블(chat_logs 테이블 message 칼럼)의 암호화 메시지 값들을 이용한다. 송신한 메시지 값은 암호 값으로 저장되어 있지만, KakaoTalk을 실행하면 평문으로 볼 수 있는 점을 착안하였다. 암호화된 주요 개인정보인 멀티미디어, 휴대폰 번호 등의 값과 송신한 chat_logs 테이블의 message 칼럼의 암호화 메시지 값을 서로 대체한 후 KakaoTalk을 재실행하여 평문 값을 얻는다. 이러한 복호화 방법론을 활용하여 DB 테이블의 구조를 분석한다.

3.4. 연락처 분석 방법

연락처 테이블의 구조 분석은 용의자/사용자를 식별 가능한 정보(이름, 휴대폰 번호, id 등)의 중심으로 분석이 필요하다. KakaoTalk의 연락처 DB파일은 KakaoTalk2.db 이고, 많은 테이블 중 용의자/사용자를 식별 가능한 테이블은 friends, block_friends로 주요 분석의 대상 테이블이다. 이 테이블의 구조 분석은 값의 변화를 주어 칼럼 및 상세 값의 의미를 분석해야한다.

이에 KakaoTalk 연락처 테이블의 영향을 주는 스마트폰의 주소록과 KakaoTalk App의 주소록을 변화를 주어 분석해야한다. 스마트폰 주소록의 경우는 주소록을 추가/수정/삭제하여 변화를 주고, KakaoTalk App 주소록(친구목록)의 경우는 친구목록을 즐겨찾기/숨김/차단하여 값의 변화를 유도한다.

Table. 3 Contact DB file name and Contact Table name and encryption of KakaoTalk

File Name	Table Name	Encryption
KakaoTalk2.db	・friends	Column Encryption
	・block_friends	X
-1087431639.backup	・friends	Column Encryption
	・block_friends	X

이를 반복하여, 칼럼 및 상세 값의 의미를 분석한다. 구체적으로 파악된 KakaoTalk App의 연락처 DB파일명, 테이블명 및 암호화 여부는 표 3 과 같다.

3.5. 교환한 메시지 분석 방법

용의자와 교환한 메시지의 중심으로 분석이 필요하다. KakaoTalk의 채팅메시지 DB파일은 KakaoTalk.db이고, 많은 테이블 중 메시지를 교환한 용의자/사용자의 테이블은 chat_logs, chat_rooms로 주요 분석의 대상 테이블이다. 이 테이블의 구조 분석은 값의 변화를 주어 칼럼 및 상세 값의 의미를 분석해야한다.

이에 메시지를 주고받을 때, 칼럼의 의미 및 상세 값의 의미를 분석한다. 구체적으로 파악된 KakaoTalk에서 채팅메시지 DB파일명, 테이블명 및 암호화 여부는 표 4 과 같다.

Table. 4 Chat DB file name and Chat Table name and encryption of KakaoTalk

File Name	Table Name	Encryption
KakaoTalk.db	· chat_logs	Column Encryption
	· chat_rooms	X
103466717.backup	· chat_logs	Column Encryption
	· chat_rooms	X

Ⅳ. 실험 및 분석환경

실험 디바이스는 스마트폰 3대, Windows 8.1 PC 1대를 사용한다. 실험에 참여한 스마트폰 디바이스의 Android, KakaoTalk, WhatsApp 버전과 루팅여부는 표 5 과 같다.

Table. 5 Smartphone Devices Environment

Model Number	Android Ver.	KakaoTalk Ver.	WhatsApp Ver.	Rooting
Nexus S	4.1.1	4.8.2	2.12.124	O
Nexus 4	5.1.1	4.8.2	2.12.124	O
IM-A880S	4.4.2	4.8.2	2.12.124	X

KakaoTalk에서 채팅방(1:1 및 1:N 그룹방 채팅)을 생성하고, 참여한 채팅방에서 분석할 기능은 표 6 과 같다. 그리고 Ⅲ장에서 언급한 분석방법들을 실현 수행하였다.

Table. 6 Analysis the features scope

Features	Normal Chat	Secret Chat
Direct/Group Chat	O	O
Photo	O	O
Video	O	O
Voice Note	O	X
Voice Calling	O	X
Location	O	X
Contact Info	O	X
Export Messages	O	X
File Sharing	△ (PC Only Send)	X

Ⅴ. 포렌식 분석결과

본 장에서는 KakaoTalk을 사용하면서 잔존하는 흔적의 파일 위치 분석, 연락처 정보 분석, 교환한 메시지 분석결과이다.

5.1. 흔적 파일의 저장 위치 분석

KakaoTalk을 사용하면서 잔존하는 파일의 저장 위치를 분석하며 아래와 같은 정보를 구한다.

- 패키지 설치 경로(Directory)
- 채팅, 메시지 DB파일 위치
- 채팅, 메시지 Backup DB파일 위치
- 사진, 동영상 등의 저장 경로(Directory)

KakaoTalk을 설치하여 /data/data/ com.kakao.talk/에 패키지가 설치된다. 패키지의 하위경로 databases는 KakaoTalk.2db, KakaoTalk.db, Journal 파일이 저장된다. 패키지의 하위경로 files는 KakaoTalk.2db의 백업파일인 –1087431639.backup, KakaoTalk.db의 백업파일인 103466717.backup파일이 저장된다. (저장 경로는 표 7. Row 1-2)

Table. 7 Application and their artifacts location

Row #	Contents	Directory	File Name
1	Contact Databases	/data/data/com.kakao.talk/databases	· KakaoTalk2.db · KakaoTalk2.db-journal
		/data/data/com.kakao.talk/files	· -1087431639.backup (KakaoTalk.2db Backup File)
2	Chat Database	/data/data/com.kakao.talk/databases	· KakaoTalk.db · KakaoTalk.db-journal
		/data/data/com.kakao.talk/files	· 103466717.backup (KakaoTalk.db Backup File)
3	Photo	/sdcard/Android/data/com.kakao.talk/cache /{chat_id}/{Random Directory}	· various Files
		/sdcard/Android/data/com.kakao.talk/cache/imageEditor/{Random Directory}	
		/sdcard/Android/data/com.kakao.talk/contents/{chat_id}/{Random Directory}	
		/sdcard/Pictures/KakaoTalk (Photo Saved)	
		/sdcard/android/data/com.kakao.talk/cache/{-user_id}/{Random Directory} (When Chatroom Leave)	
4	Video	/sdcard/Android/data/com.kakao.talk/cache/{chat_id}/{Random Directory}	· various Files
		/sdcard/Android/data/com.kakao.talk/contents/{chat_id}/{Random Directory}	
		/sdcard/video/ (Video Saved)	
		/sdcard/android/data/com.kakao.talk/cache/{-user_id}/{Random Directory} (When Chatroom Leave)	· various Video Thumbnail Image Files
5	Voice Notes	/sdcard/Android/data/com.kakao.talk/contents/{chat_id}/{Random Directory}	· various Files
6	Location	/data/data/com.kakao.talk/cache/daummap/cache/0001	· various files
		/sdcard/android/data/com.kakao.talk/cache/default/{Random Directory}	· various files
7	Export Messages	/data/data/com.google.android.gm/cache (Send Text Only)	· {YYYY-MM-DD-hh:mm:ss}-{9-12 Digit}.attachment
		/data/data/com.google.android.gm/cache/{Gmail email address} (Send Text Only)	· KakaoTalkChats.txt
		/sdcard/KakaoTalk/Chats/KakaoTalk_Chats_{YYY-MM-DD_hh.mm.ss} (Save All Messages to SD Card)	· KakaoTalkChats.txt · various files
8	File Sharing	/sdcard/KakaoTalkDownload	· various down files
9	Package install	/data/data/com.kakao.talk	· various Files
10	Basic Package	/data/data/com.kakao.talk/shared_prefs	· KakaoTalk.more.perferences.xml · KakaoTalk.perferences.xml · various xml Files
		/data/data/com.kakao.talk/databases	· various SQlite DB Files

사진 송신은 '원본', '고화질', '일반 화질'의 3가지 기능을 제공하고, 사진을 송・수신 하면 /sdcard/Android/data/com.kakao.talk/ 하위 경로 cache, contents 하위 랜덤 경로에 사진파일을 저장한다. 채팅방에서 선택한 사진을 저장하면 /sdcard/Pictures/Kakao Talk/ 에 파일을 저장한 시각(13 Digit Unix Epoch Time)값의 파일이름이 생성된다. 사진을 '원본'파일로 송신한 사진을 저장 경우는 EXIF(Exchangeable Image File Format) 메타데이터의 정보(카메라 제조사, 카메라 모델명, 촬영시간 등) 값은 변경되지 않는다. 그러나 '고화질','일반 화질'로 송신한 사진을 저장 경우는 EXIF 메타데이터의 정보 값이 삭제된다. 추가로 채팅방을 나가면 채팅방에 존재하는 모든 사진 파일을 KakaoTalk Apps이 삭제하여 사진을 찾을 수 없다. 하지만 흔적파일로 송신한 사진만 /sdcard/android/data/com.kakao.talk /cache/{-user_id}/{Random Directory}에 파일이 존재한다. (저장 경로는 표 7. Row 3)

동영상을 송・수신 하면 /sdcard/Android/data/com.kakao.talk/ 하위 경로 cache, contents에 동영상 파일이 저장되고, 채팅방에서 선택한 동영상을 저장을 하면 /sdcard/video/ 에 파일을 저장한 시각(13 Digit Unix Epoch Time)값의 파일이름이 생성된다. 추가로 채팅방에 나가면 채팅방에 존재하는 모든 동영상 파일이 삭제되어 동영상을 찾을 수 없다. 하지만 흔적파일로 송신한 동영상의 썸네일 이미지 파일만 /sdcard/android/data/com.kakao.talk/cache/{-user_id}/{Random Directory}에 파일이 존재한다. (저장 경로는 표 7. Row 4) 이 외 음성메시지, 위치정보, 연락처 보내기 등의 흔적은 표 7 과 같다.

5.2. 연락처 정보 분석

연락처 정보를 분석하여 아래와 같은 정보를 구한다.

・연락처 리스트, 연락처 추가/삭제
・연락처 즐겨찾기/숨김/차단
・연락처 복원 (연락처 백업 파일 복원)

KakaoTalk 연락처의 정보는 KakaoTalk2.db 파일 friends, block_friends 테이블에 저장한다.(저장 경로는 표 7. Row 1)

friends 테이블은 개인을 식별 가능한 이름, 휴대폰 번호 등의 연락처가 저장된다. 특히, 용의자/사용자를 파악 가능한 주요 식별 가능한 값은 이름, 연락처, 유저ID가 존재하고, 주요 칼럼명은 다음과 같다.

・이름: name
・연락처: phone_number, raw_phone_number
・유저ID: id

block_friends 테이블은 차단한 유저의 이름, 프로필 이미지 URL 등이 저장된다. 분석한 block_friends 테이블의 구조는 표 8, friends 테이블의 구조는 표 9 과 같다.

Table. 8 Structure of the block_friends table

Column Name	Meaning
_id	・PlainText ・sequence number of the record (set by SQLite)
id	・PlainText ・KakaoTalk user ID
nickname	・PlainText ・KakaoTalk name of the contact (as set in communication partner profile)
profile_image_url	・PlainText ・URL of communication partner profile

Table. 9 Structure of the friends table

Column Name	Meaning
_id	・PlainText ・sequence number of the record (set by SQLite)
id	・PlainText ・KakaoTalk user ID
type	・PlainText ・user add type '1'=KakaoTalk ID add, '2'=Phone Number add.
phone_number	・Encryption Data ・phone number associated to the contact (type='2') or blank
raw_phone_number	
name	・Encryption Data ・KakaoTalk name of the contact (as set in communication partner profile)
profile_image_url	・Encryption Data ・KakaoTalk profile image of the contact (as set in communication partner profile)
full_profile_image_url	
original_profile_image_url	

Column Name	Meaning
status_message	・Encryption Data ・communication partner status message
chat_id	・PlainText ・Chat room ID (participate in Chat room)
favorite	・PlainText ・Add to favorites: ‘1’: Added to favorites, ‘0’: no favorites.
nick_name	・Encryption Data ・KakaoTalk nickname of the contact (as set in my KakaoTalk)
hidden	・PlainText ・hidden contact : ‘0’=normal contact, ‘1’=hidden contact.
involved_chat_ids	・PlainText ・Chat room ID at participate Chat room
enc	・PlainText ・encryption version ‘6’=v4.82.
created_at	・PlainText ・contact created time(13 Digit unix epoch)
new_badge_updated_at	・PlainText ・communication partner profile updated time(13 Digit unix epoch)
new_badge_seen_at	・new badge contact created unix epoch time(13 Digit unix epoch)

5.3. 연락처 복원 (연락처 백업 파일 복원)

삭제한 용의자/사용자의 연락처를 복원이 가능하면, 주고받은 사람의 연락처 정보를 얻을 수 있다. 휴대폰의 연락처를 삭제 후 KakaoTalk을 동기화를 하면 friends 테이블 phone_number, raw_phone_number 칼럼 등의 휴대폰 연락처 정보가 삭제된다. 일부 상황이지만, 연락처 백업 -1087431639.backup파일을 열어 연락처의 정보를 복원이 가능하다.

5.4. 교환한 메시지 분석

메시지 정보를 분석하면 아래와 같은 정보를 구한다.

・메시지 송신자
・메시지 콘텐츠 구분

KakaoTalk의 모든 송・수신 메시지는 KakaoTalk.db 파일 chat_logs, chat_rooms 테이블에 저장한다.

chat_logs 테이블은 유저가 송・수신한 메시지들은 chat_logs 테이블에 저장되고, chat_rooms 테이블은 개별 채팅방의 마지막 메시지가 저장된다. chat_logs의 테이블 구조는 메시지 속성(Message Attributes)은 표 10과 같고, 메시지와 관련된 콘텐츠 (Concerning Message Contents)는 표 11 와 같다.

Table. 10 Structure of the chat_logs table: field storing message attributes

Column Name	Meaning
_id	・PlainText ・sequence number of the record (set by SQLite)
id	・PlainText ・unique message ID
chat_id	・PlainText ・unique chat room ID
user_id	・PlainText ・unique KakaoTalk user ID
created_at	・PlainText ・time of created message(10 Digit Unix Epoch Time)
deleted_at	・PlainText ・time of deleted message(10 Digit Unix Epoch Time) or ‘0’ (no delete)

Table. 11 Structure of the chat_logs table: field storing information concerning message contents

Column Name	Meaning
type	・PlainText ・message content type: ‘0’ = invited message, ‘1’ = text message & satic emoticon, ‘2’ = photo, ‘3’ = video, ‘4’ = send contact, ‘5’ = voice note, ‘9’ = PC login message, ‘12’ = dynamic emoticon, ‘16’ = location, ‘17’ = send KaKao Talk Profile, ‘18’ = file sharing, ‘51’ = vocie calling.
message	・Encryption Data ・message content

Ⅵ. 결 론

KakaoTalk 포렌식 분석은 국외 IM Apps 포렌식 분석 연구에 대비하여 연구가 미비하다. 본 논문은 Kakao Talk App의 적합한 분석방법을 제시하였고, 제안한 분석방법을 진행하여 그 결과로 아티팩트(Artifacts)를 보였다.

KakaoTalk의 분석방법은 흔적 파일의 위치분석방법과, 흔적 파일의 접근 권한 분석방법과, 연락처・채팅메시지 DB의 암호화를 복호화 하는 방법과, 연락처・채팅메시지의 테이블 구조를 분석방법을 제시하였다.

흔적 파일의 위치 분석은 다양한 콘텐츠를 송・수신의 전 파일시스템 상태와 파일시스템 후 상태를 텍스트 파일로 저장하고, 저장한 파일의 내용을 비교하여 다양한 콘텐츠의 저장 위치를 파악하였다. 추가로, 흔적 파일의 접근 권한 분석방법은 콘텐츠의 저장 위치에 언루팅 단말기로 콘텐츠 접근을 하여 접근가능 여부를 파악하였다.

연락처・채팅메시지 DB의 암호화를 복호화는 채팅메시지 테이블(chat_logs 테이블 message 칼럼)의 암호화 메시지 값을 이용하여 평문 값을 얻었다. 얻은 평문 값으로 연락처・채팅메시지 테이블의 구조분석은 연락처・채팅메시지의 값을 변화를 주어 테이블의 구조를 분석하였다. 연락처 테이블의 구조 분석은 용의자를 식별 가능한 주요 연락처 테이블 구조 분석을 하였고, 채팅메시지 테이블의 구조분석은 주고받은 메시지의 콘텐츠 타입을 분석을 하였다.

제시 및 기술한 분석방법으로 흔적파일의 저장 위치를 찾았고, 흔적파일의 접근 권한 분석을 하였으며, 연락처 테이블의 구조를 분석하여 용의자/사용자를 식별을 하였고, 교환한 메시지의 콘텐츠 구분 등을 분석하였다. 추가로, 연락처 Backup DB파일을 이용하여 삭제한 연락처 정보를 발견하여 증거로서 사용 가능성을 보였다.

본 논문의 가치는 실제 단말기에서 KakaoTalk의 비활성데이터 흔적을 포렌식 분석하여 기초정보의 제공과 주요 연락처의 칼럼 구조 분석, 복원(recovery)을 하여 KakaoTalk의 적합한 포렌식 분석을 하였다. 분석한 정보와 방법론을 바탕으로 Forensic Tool의 기본 플랫폼을 제공하였다.

하지만 KakaoTalk과 WhatsApp의 iOS 스마트폰 포렌식 분석을 미래연구로 남기며, 자세한 chat_rooms, chat_logs의 채팅메시지 분석과 WhatsApp 와 Kakao Talk의 비교 분석연구를 현재 진행 중이다.

REFERENCES

[1] J. M. Lee, “The Effect of Personal Communication Activities using Smart Phone Instant Messenger on Job Performance,” *Journal of Korean Socieity for Internet Information*, vol. 13, no. 6, pp. 17-24, Oct. 2012.

[2] Wikimedia Foundation, Inc. Instant Messaging [Internet]. Available: https://en.wikipedia.org/wiki/Instant_messaging.

[3] H. S. Jung, “The evolution of Korean social network service focusing on the case of Kakao talk,” *The Journal of Digital Policy and Management*, vol. 10, no 10, pp. 147-154, Nov. 2012.

[4] Yu Jong Jang, Jin Kwak, “Mobile Digital Forensic Procedure for Crime Investigation in Social Network Service,” *The Journal of Korea Navigation Institute*, vol. 17, no. 3, pp. 325-331, Jun. 2013.

[5] Mohammad Iftekhar Husain, Ramalingam Sridhar, “iForensics: forensic analysis of instant messaging on smart phones,” in *The First International Conference on Digital Forensics & Cyber Crime*, pp. 9-18, Sept. 2009.

[6] Yu-Cheng Tso, et al., “iPhone social networking for evidence investigations using iTunes forensics,” in *Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication*, ACM New York, article no. 62, Feb. 2012.

[7] Shubham Sahu, “An Analysis of WhatsApp Forensics in Android Smartphones,” *International Journal of Engineering Research*, vol. 3, no. 5, pp. 349-350, May 2014.

[8] Neha S. Thakur, “Forensic analysis of WhatsApp on Android smartphones,” M.S. Thesis, University of New Orleans Theses and Dissertations, 2013.

[9] Cosimo Anglano, “Forensic analysis of WhatsApp Messenger on Android smartphones,” *Digital Investigation*, vol. 11, no. 3, pp. 201-213, Sept. 2014.

[10] JaeWan Jo, “Study Android lock features analysis of Digital Forensic focus,” M.S. Thesis, KOREA University Theses and Dissertations, 2013.

[11] HoSeung No, “Logical Forensic Technique on Android Smartphone,” M.S. Thesis, KOREA University Theses and Dissertations, 2014.

윤종철(Jongcheol Yoon)

세종사이버대학교 정보보호대학원 정보보호학과 석사 과정
※관심분야 : IT 서비스 및 보안, 포렌식, 클라우드, IoT 등

박용석(Yongsuk Park)

서강대학교 컴퓨터공학 (학사)
뉴욕(POLY)대 (석사, 박사)
AT&T (Bell) Labs, 삼성전자
현재 세종사이버대학교 정보보호 대학원 주임교수
현재 세종사이버대학교 IT학부 교수
※관심분야 : IT 서비스 및 보안, 산업보안, 클라우드, IoT 등