JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 4 : 777~785 Apr. 2016

KakaoTalk의 채팅 메시지 포렌식 분석 연구 및 WhatsApp의 Artifacts 와의 비교 분석

윤종철 · 박용석*

Forensic Analysis of chatting messenger service in KakaoTalk and Comparison Study of KakaoTalk and WhatsApp Artifacts

JongCheol Yoon · Yongsuk Park*

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

요 약

IM(Instant Messenger)의 채팅메시지는 이용자의 생활패턴, 지리적 위치, 심리 상태, 범죄 사실에 대한 흔적들이 존재하여 포렌식 분석이 필요하다. 하지만, KakaoTalk의 포렌식 분석은 주고받은 상세메시지에 대한 분석이 부족한 실정이다. 이에 본 논문은 우선 일반적인 IM 채팅메시지의 분석방법론을 정리 분석하였고, KakaoTalk의 상세 채팅 메시지의 테이블 구조를 분석하여 메시지를 재구성하였고, 채팅메시지를 복원하였다. 그 결과 분석한 정보를 활용하면 Forensic Tool의 기본 플랫폼이 된다. 추가적으로 분석한 KakaoTalk과 WhatsApp을 비교 분석하여 비슷한 IM App이지만, 다른 흔적의 차이를 논의하였다.

ABSTRACT

IM(Instant Messenger) chatting service can carry user's various information including life style, geographical position, and psychology & crime history and thus forensic analysis on the IM service is desirable. But, forensic analysis for KakaoTalk's chatting service is not well studied yet. For this reason, we study KakaoTalk's forensic analysis focusing on chatting service. This paper first details a general method of IM forensics investigating the previous articles about IM forensics although there are not many articles. Second, we discuss methodologies for IM forensics wherein we present analysis of table structure and method for reconstruction of chatting message. These result in the basic element of forensic tools of KakaoTalk chatting message. Last, we compare artifacts of KakaoTalk with that of WhatsApp. We conclude that these applications are, at least, different in that table structures and the ways to reconstruct chatting messages are not same and therefore digital evidences or artifacts are not same and somewhat distinct.

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)

Received 01 February 2016, **Revised** 28 February 2016, **Accepted** 20 March 2016

* **Corresponding Author** Yongsuk Park(E-mail:yongspark@sjcu.ac.kr, Tel: +82-2-2218-8452)
Graduate School of Information Security, Sejong Cyber University, 121 Gunja-ro, Gwangjin-gu, Seoul, 05000 Korea

Open Access http://dx.doi.org/10.6109/jkiice.2016.20.4.777 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

스마트폰은 항상 켜져 있고, 언제나 접속 가능한 상태로 전화, 메시지, 사진, 동영상 등을 주고받는 디바이스로 다양한 가치가 있는 디지털 증거들이 존재한다[1-6]. 인스턴트 메신저(IM: Instant Messenger)는 이동통신사 SMS, MMS 을 대신해 인터넷에 연결하여 메시지, 전화, 사진, 비디오 등을 주고받는 서비스이다[7,8]. IM 서비스 이용자는 자유로운 의사소통과 정보를 공유하여 서로 사회적 관계를 맺어 일상 생활양식을 크게 변화 시켰다[9,10]. 과거 휴대폰(피처폰)은 SIM 카드에 저장된 SMS가 중요 증거로써 포렌식 분석의 대상 이였으나, 변화한 생활양식에 따라 현재 휴대폰(스마트폰)은 IM Apps의 채팅 메시지, 사진, 음성메시지 등이 중요 증거로써 포렌식 분석의 대상이다[2,11,12]. IM은 사이버 수사의 증서로써 용의자의 인적 네트워크 분석, 범죄동기 파악, 위치정보 등을 파악할 수 있는 중요한 정보이다[4-6]. 따라서 IM 포렌식 분석의 중요도는 점차 증가하고 있다[13]. 이러한 연유로 IM Apps의 사용정보를 파악하기 위한 포렌식 연구가 필요하다.

스마트폰 이전 시대는 IM의 사용을 PC 기반에서 IM 프로그램 또는 웹 브라우저로 서비스를 이용하였다. 그에 따라 포렌식 분석 연구는 컴퓨터 포렌식 기술을 사용하여 AIM(AOL Instant Messenger)의 분석[14, 15], Facebook's Instant Messenger의 분석[16], MSN Messenger의 분석[17], 그 외 다양한 IM을 분석하였다[18,19].

일반적인 스마트폰 IM Apps의 포렌식 분석 연구는 개별 App에 대한 연구와 다양한 IM Apps의 분석한 연구 결과를 비교하여 비슷한 IM App이지만 다른 흔적의 차이를 비교 분석하였다.

개별 IM Apps의 포렌식 분석 연구는 세계에서 가장 많이 사용하는 WhatsApp의 분석 연구가 활발하다. WhatsApp 연구에서는 VM(Virtual Machine)의 기반으로 App을 사용할 때 흔적파일의 위치, 연락처・채팅메시지 테이블의 구조 분석, 연락처・채팅메시지 복원 등을 포렌식 분석하였고[20,21], 암호화 Backup 연락처・채팅메시지의 DB파일을 외부에서 공개한 복호화 도구(Xtract Package)를 가지고 복호화 하여 얻은 평문의 과거 연락처・채팅메시지 정보들을 포렌식 분석에 활용하였다[21,22]. 하지만, 가상머신(VM)은 GPS 모듈 등이 없어, 일부 기능의 사용 제약이 존재하여 그로 인한 분석의 한계점이 존재한다[20].

한편, IM Apps의 비교 분석 연구에서는 WhatsApp과 Viber를 사용하고, 사용 흔적을 UFED(Universal Forensic Extraction Device) 물리적인 장비로 정보를 추출한 후 기존 연구한 분석결과를 토대로 App이 저장한 채팅 메시지・연락처 등의 DB파일의 위치 비교, 채팅 메시지의 테이블 비교, 연락처의 테이블 비교, 주고받은 멀티미디어(사진, 비디오 등) 파일의 위치 등을 비교하여 같은 IM 이지만 다른 흔적들을 연구하였다. 물리적인 장비로 정보를 얻고, 비교 분석의 기여는 하였지만 개별 WhatsApp, Viber의 포렌식 분석 연구는 진행하지 않았다[23].

또한, [24]에서는 WhatsApp, Facebook Messenger 등 IM App의 채팅메시지 DB파일 등의 위치를 비교 분석을 하였고, 평문 통신 경우 네트워크 스니핑 하여 사진, 동영상 등을 원본파일로 볼 수 있는 보안 약점을 포렌식 분석에 활용하여 얻은 그 분석결과를 비교하였다. [25] 에서는 국내 KakaoTalk(국내 1위 IM App)은 분석 방법론을 제시하고, 제시한 분석 방법을 수행하여 흔적 파일의 위치 분석, 연락처・채팅 테이블의 구조 분석 등을 하였지만, 그룹 채팅 및 비밀채팅 등의 상세한 채팅 메시지 분석이 진행되지 않아 분석이 필요하고, 다른 App과의 비교 분석이 필요하다.

이에 본 논문은 VM 아닌 실장비로 KakaoTalk의 그룹 채팅, 비밀채팅 등의 상세한 채팅 메시지 분석을 하고, 연구가 활발한 WhatsApp의 분석 결과를 비교하여 같은 IM 이지만 다른 흔적들을 비교한다[26].

본 논문의 구성은 Ⅱ장 분석 방법론에서는 IM App의 일반적인 채팅 메시지의 분석방법을 정리하고 수행한 분석방법을 소개하며, Ⅲ장 실험 및 분석환경에서는 실험에 참여한 장비와 분석할 기능을 소개하며, Ⅳ장 포렌식 분석결과에서는 KakaoTalk의 상세 채팅메시지 분석 결과 및 WhatsApp과 KakaoTalk의 비교분석의 결과를 논의하며 , Ⅴ장에서는 결론으로 정리한다.

Ⅱ. 분석 방법론

디지털 포렌식이란 디지털증거를 저장하는 정보기기에 내장된 디지털자료를 근거로 삼아 그 정보기기를

매개체로 하여 발생한 어떠한 행위의 사실관계를 규명하고 증명하는 일체의 절차를 말한다[27]. 일반적으로 IM App에서는 주고받은 텍스트메시지, 멀티미디어 파일 등의 흔적들은 DB파일, Backup DB파일에 저장된다. 따라서, 채팅메시지의 포렌식 분석은 IM 서비스를 사용하여 수정된 채팅 DB파일과 Backup DB을 위치를 찾고, 채팅메시지를 분석해야한다. 이를 위하여 IM 서비스는 1:1 또는 1:N 채팅방을 만들고 상호간 텍스트메시지, 멀티미디어 파일, 지도 등의 콘텐츠를 주고받게 하여, 채팅메시지의 '저장 중인 DB파일의 위치'와 'Backup DB파일의 위치'를 찾고, 분석해야한다.

'저장 중인 DB파일의 위치'와 'Backup DB의 위치'를 찾는 방법은 2가지 방법을 만들었다. 첫째, Backup App의 사용이다. Backup App을 사용하여 IM App을 백업하고, 백업 데이터 중 .db파일을 sqlite browser에서 보고, 채팅메시지로 보이면, 채팅메시지의 .db파일로 결정하여 찾는다. 그러나 .db파일이 아닌 경우는 찾을 수 없다(예: WhatsApp의 Backup DB는 .crypt파일). 따라서 둘째, 이 경우에는 수정된 파일의 검사를 사용한다. 메시지를 주고받기 전 파일시스템 상태를 텍스트로 저장하고, 메시지를 주고받은 후 파일시스템 상태를 텍스트로 저장되기 때문에, DB파일의 결정은 전/후 상태의 텍스트 파일을 비교하여 수정된 .db파일과 .backup 파일 등을 찾고, DB파일을 sqlite browser에 보고 채팅메시지로 보이면, 채팅 메시지 DB파일로 결정한다. 수정된 파일의 검사는 암호화 DB파일도 수정되기 때문에 감지가 되어 DB파일 위치를 찾는다.

발견한 '저장 중인 DB파일'과 'Backup DB파일'의 채팅 메시지를 분석을 위해 각각 다른 방법을 만들었다. '저장 중인 DB파일'의 분석방법은 다양한 콘텐츠 메시지를 주고받아, 값의 변화를 준 후 칼럼 및 값의 의미를 분석하였다. 추가적으로, 메시지 관련한 값들이 부분적 또는 전체적으로 암호화 되어 있을 경우에는 복호화 방법을 사용한다. 'Backup DB파일'의 분석방법은 '저장 중인 DB파일'과 비교하여 삭제 또는 수정한 메시지를 찾아 이를 분석한다[20,25]. 추가적으로, 메시지 관련한 값들이 부분적 또는 전체적으로 암호화 되어 있을 경우에는 복호화 방법을 사용한다.[20-22,25].

본 논문은 그룹 채팅메시지의 포렌식 분석에 초점을 두며, 기본 채팅메시지 분석과 그 방법 및 실험환경은 기존의 논문 [25] 에서 방법론을 참조 할 수 있다.

Ⅲ. 실험 및 분석환경

그룹채팅의 콘텐츠를 주고 받기위해 스마트폰은 3대를 사용하고, 분석PC 1대를 사용한다. 분석 스마트폰은 채팅메시지의 접근하고, 분석하기 위해 루팅한다. 실험에 참여한 스마트폰 디바이스의 Android, KakaoTalk, WhatsApp 버전은 표 1과 같다.

Table. 1 Smartphone Devices Environment

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

KakaoTalk에서 분석할 기능은 표 2와 같다. 추가로 그 외 실험 환경은 [25]을 사용하고, Ⅱ장에서 언급한 분석방법들을 실현 수행하였다.

Table. 2 Feature Analysis of WhatsApp & KakaoTalk

Features	WhatsApp		KakaoTalk	
	Normal Chat	Secret Chat	Normal Chat	Secret Chat
TEXT Chat	O	X	O	O
Group Chat	O	X	O	O
Photo/Video/ Voice Note	O	X	O	O
Voice Calling	O	X	O	X
Location	O	X	O	X
Contact Info	O	X	O	X
Export Messages	O	X	O	X
File Sharing	X	X	△	X

※ △: PC Only Send

Ⅳ. 포렌식 분석결과

4.1. 교환한 메시지 분석

KakaoTalk은 채팅메시지의 값의 변화를 주어 채팅메시지 테이블의 구조를 분석한다. KakaoTalk의 송·수신 메시지는 KakaoTalk.db파일 chat_logs, chat_rooms 테이블에 저장된다. 분석한 chat_logs 테이블 구조의 메시지 속성(Message Attributes)은 표 3과 같고, 메시지와

관련된 콘텐츠 (Concerning Message Contents)는 표 4와 같다. 분석한 chat_rooms 테이블 구조의 메시지와 관련된 콘텐츠 (Concerning Message Contents)는 표 5와 같고, 메시지 속성(Message Attributes)은 표 6과 같다. 분석한 테이블의 구조 분석은 아래와 같은 정보를 구한다.

- 메시지를 교환한 사람
- 메시지 이력(history), 메시지 콘텐츠 구분
- 멀티미디어(사진 동영상 등)의 정보
- 메시지 복원

Table. 3 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)

4.2. 채팅 메시지 이력

메시지의 이력의 설명에는 누가, 언제, 어떤 메시지를 주고받았는지 가능해야 한다. 채팅메시지를 설명에 필수인 chat_logs 칼럼명은 다음과 같다.

- 누가: 유저ID(user_id), 채팅방(chat_id)
- 언제: 메시지 생성시각(created_at)
- 메시지: 메시지(messages)
- 메시지 송・수신 구분: 장황한 정보(v)
- 콘텐츠 종류: 메시지 콘텐츠 종류(type)
- 콘텐츠: 멀티미디어 파일 정보(attachment)

위 7개 칼럼 중 6개의 값은 쉽게 구분이 되지만, v 칼럼의 값은 장황한 key:value 쌍(key value pair) 값으로 이루어져 있다. v 칼럼 값은 콘텐츠 종류(type), 메시지의 송・수신 구분, 메시지의 생성시각, 이모티콘 전송 여부, 사진 전송 크기 등의 쌍(key:value) 값이 존재한다.

Table. 4 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
attachment	• Encryption Data • multimedia information
v	• PlainText of key:value type • messages created time, sender/receiver smartphone separate, etc

Table. 5 Structure of the chat_rooms table: field storing information concerning message contents

Column Name	Meaning
type	• PlainText • chat room type: 'Directchat'=1:1 chat room, 'Multichat'=group chat room, 'SDirectChat'=secret chat room.
last_message	• PlainText • last message content in the chat room
v	• PlainText of key:value type • token key, created chat room time(10 Digit Unix Epoch Time), etc
last_chat_log_type	• PlainText • type of last message in the chat room
schat_token	• PlainText • Normal Chat is '0' value
last_skey_token	• PlainText • Normal Chat is '0' value
last_pk_tokens	• PlainText • Normal Chat is blank value

메시지 송・수신 구분의 key:value 값을 제외한 쌍(key:value) 값은 다른 칼럼과 중복 값이고, 송・수신 메시지의 구분은 isMine의 key이다. 송신 메시지는 'isMine:true' 이고, 수신 메시지는 'isMine:false'이다. 자세한 송신 메시지의 콘텐츠 구분 값은 표 7과 같다. 그 외 수신 메시지의 콘텐츠 구분 값은 [26]에서 참조한다.

Table. 6 Structure of the chat_rooms table: field storing message attributes

Column Name	Meaning
_id	• PlainText • sequence number of the record (set by SQLite)
id	• PlainText • unique chat room ID
members	• PlainText • KakaoTalk user ID in the chat room ※ Analysis devices is exclusive
active_member_ids	• PlainText • KakaoTalk user ID in the current chat room ※ Analysis devices is exclusive
last_log_id	• PlainText • unique message ID
last_updated_at	• PlainText • time of created message(10 Digit Unix Epoch Time)
unread_count	• PlainText • number of messages sent by this contact that have been received
last_read_log_id	• PlainText • last read unique message ID in the chat room
last_update_seen_id	• PlainText • last read unique message identifier in the chat room
active_members_count	• People participating in the current chat room ※ Analysis devices is include

Table. 7 Message Contents Separate of Sender

	ChatRoom	Contents	v Column Key		
			origin	pushAlert	isMine
Normal Secret	MultiChat	invited message	SYNCMSG	-	true
Normal Secret	DirectChat MultiChat	other contents	WRITE	-	true

다음은 그림 1 예시로 채팅 메시지는 'Hi'텍스트 메시지를 주고받았고, 분석단말기는 Nexus 4의 chat_logs 테이블이다. 채팅방은 일반 그룹 채팅방(chat_id=1xx92)과 비밀 그룹채팅방(chat_id=9xx30)이 존재한다. 일반 그룹방과 비밀 그룹채팅방은 Nexus4(user_id=1x73)가 최초 만들었고(type=0), Hi란 메시지를 송신하였다. Nexus4 일반 그룹채팅방의 메시지 송신시각은 2016. 1. 26. 오전 11:05:19(created_at= 1453773919)이고, 비밀 그룹채팅방의 메시지송신시각은 2016. 1. 26. 오전 11:10:55 (created_at=1453774255)이다. Nexus S (user_id=7x68)와 IM-A880S(user_id=1x06)은 Hi라는 메시지를 송신하였다.

4.3. 채팅방 마지막 메시지

chat_rooms 테이블(채팅방 마지막 메시지)은 평문으로 되어 있어 상호간 나눈 대화를 쉽게 본다. chat_rooms 테이블은 용의자와 나눈 채팅방(id 칼럼), 대화에 참여한 유저ID(member 칼럼), 현재 채팅방에 참여하고 있는 유저ID(active_member_ids 칼럼), 메시지 생성 시각(last_update_at 칼럼) 등을 알 수 있다.

다음은 그림 1에서 주고받은 'Hi' 메시지의 chat_rooms 테이블을 그림 2 예시로 chat_rooms를 설명한다. 채팅방은 일반 그룹채팅방(id=1xx92)과 비밀 그룹채팅방(id=9xx30)이 존재한다. 현재 일반 그룹 채팅방에 참여자는 분석 단말기를 제외한 2명이(active_member_ids= 7x8,1x6) 참여 중이다. 일반 그룹채팅방의 마지막

	Model	_id	id	type	chat_id	user_id	message	attachment	created_at	deleted_at	client_message_id	v
Multi Chat	Nexus 4	6	1114315166399200000	1	136024800353492	195001573	tOG1rkeMB8	{}	1453773919	0	2075040070	{"origin":"WRITE","c":"01-26 11:05:
	Nexus 4	7	1114315164461440000	0	136024800353492	195001573	hwtkwTt5H5		1453773919	0	0	{"origin":"SYNCMSG","c":"01-26 11
	Nexus S	8	1114315682642520000	1	136024800353492	70557068	ZcSXAVjo6T		1453773980	0	2075103696	{"origin":"MSG","c":"01-26 11:06:1
	IM-A880S	9	1114315815014680000	1	136024800353492	194951906	SD0I0ZCNV		1453773996	0	2075118333	{"origin":"MSG","c":"01-26 11:06:3
Secret Multi Chat	Nexus 4	10	1114317975785970000	0	9143224398249030	195001573	hwtkwTt5H5		1453774254	0	0	{"origin":"SYNCMSG","c":"01-26 11
	Nexus 4	11	1114317990197600000	1	9143224398249030	195001573	tOG1rkeMB8	{}	1453774255	0	2075375170	{"skeyToken":11143179757859717
	Nexus S	12	1114318128190190000	1	9143224398249030	70557068	ZcSXAVjo6T		1453774272	0	2075394896	{"skeyToken":11143179757859717
	IM-A880S	13	1114318241721540000	1	9143224398249030	194951906	SD0I0ZCNV		1453774285	0	2075405533	{"skeyToken":11143179757859717

Fig. 1 Chat Messages History (chat_logs Table)

	_id	id	type	active_member_ids	last_log_id	last_message	last_updated_at	unread_count	last_chat_log_type	schat_token	last_skey_token
Group Chat	4	136024800353492	MultiChat	[70557068,194951906]	1114315815014680000	Hi	1453773996		1	0	0
Secret Multi Chat	5	9143224398249030	SMultiChat	[70557068,194951906]	1114318241721540000	Hi	1453774285		1	1114317975785970000	1114317975785970000

Fig. 2 Chat Messages History (chat_rooms Table)

으로 보낸 메시지ID(last_log_id)는 1x80000이고, 메시지를 보낸 사람은 chat_logs 테이블에서 찾아야한다. id=1x80000는 IM-A880S이다.

4.4. 메시지 콘텐츠 분석

KakaoTalk은 텍스트 메시지, 멀티미디어 파일(사진, 동영상, 음성메시지), 보이스톡, 지도 등 다양한 메시지 콘텐츠를 주고받는다. 다양한 메시지 콘텐츠는 KakaoTalk.db파일 chat_logs 테이블 type Column에 메시지 콘텐츠의 구분 값이 존재한다. 예를 들어 텍스트 메시지는 type='1', 사진은 type='2'값이 저장된다.

또한 사진, 동영상, 음성메시지 등의 멀티미디어 파일은 chat_logs 테이블 attchment 칼럼의 값(암호값)에 콘텐츠의 접근하는 주소값이 저장된다. 다음은 예시로 사진을 송신한 attchment 값이다.

• 일반 채팅방

{"thumbnailUrl":"http://th-m3.talk.kakao.com/th/talkm/□□□/i_mg3acwi29q9b1_90x120.jpg","thumbnailHeight":120,"thumbnailWidth":90,"url":"http://dn-m.talk.kakao.com/talkm/□□□/i_mg3acwi29q9b1.jpg","k":"□□□/i_mg3acwi29q9b1.jpg","cs":"B403A1BF80C53C06D66A2145320A82A13D820F4F","s":79889,"w":960,"h":1280}

• 비밀 채팅방

{"thumbnailPath":"\/storage\/emulated\/0\/Android\/data\/com.kakao.talk\/cache\/-9223372036784218739\/93\/93dc6386c86a63440c4ce5034f103ff7f5b4e0da9edbf80bb1ad5a68c4f40520","w":960,"h":1280,"csk":{"sk":"GSrTwgIFQDIUMxT3vUwg+2i2FGx8lu6K9Ja7l1ae8tg=","mid":675834870,"hash":"K9BbBwTqjIog5+CzHm2BrMuWfXDOrc86acvIaRooQns="},"k":"c4wzg8\/oWlF4wmA0e\/kHJdHWUqPHbkSDkLiF7WP1\/i_wxhp8es5xai81.jpg","s":79889,"cs":"fb07ca853a20653ff1b3cf9c371b6ae3"}

일반 채팅방은 URL 주소로 사진 콘텐츠에 접근을 하고, 비밀 채팅방은 내부 저장 주소로 사진 콘텐츠에 접근한다. 즉, 일반 채팅방과 비밀 채팅방은 멀티미디어 콘텐츠에 다른 접근의 차이가 존재한다. 그 외 멀티미디어 파일, 지도, 연락처 보내기 등은 단순 텍스트 메시지가 아닌 URL 또는 내부의 저장 주소의 접근이 필요하여, attachment에 접근 주소가 저장된다.

4.5. 메시지 복원

메시지 삭제 및 채팅방을 나가면, chat_logs 테이블에 메시지들이 삭제된다. 일부 상황이지만, 채팅 백업

103466717.backup
16.01.26 11:11 Modify Time

_id	id	type	chat_id	user_id	message
Filter	Filter	Filter	Filter	Filter	Filter
6	11143151663...	1	13602480035...	195001573	tOG1rkeMB8lS...
7	11143151644...	0	13602480035...	195001573	hwtkwTt5H5u2...
8	11143156826...	1	13602480035...	70557068	ZcSXAVjo6T6p...
9	11143158150...	1	13602480035...	194951906	SD0I0ZCNV7q...
10	11143179757...	0	91432243982...	195001573	hwtkwTt5H5u2...
11	11143179901...	1	91432243982...	195001573	tOG1rkeMB8lS...
12	11143181281...	1	91432243982...	70557068	ZcSXAVjo6T6p...

KakaoTalk.db
16.01.28 21:41 Modify Time

```
C:Wchat>sqlite3 KakaoTalk.db
SQLite version 3.8.6 2014-08-15 11:46:33
Enter ".help" for usage hints.
sqlite> .tables
android_metadata   chat_rooms         public_key_info    secret_key_info
chat_logs          chat_sending_logs  schema_migrations
sqlite> select * from chat_logs;
sqlite>
```

Fig. 3 Message Restore

103466717.backup 파일로 복원 한다. 다음은 예시로 그림 3을 설명한다. 채팅방을 나가서 모든 메시지들이 삭제되었다. 하지만, Backup DB파일(103466717 .backup)에는 chat_logs 테이블에서 삭제메시지가 확인된다.

4.6. KakaoTalk 과 WhatsApp의 비교분석

KakaoTalk과 WhatsApp은 다른 App 이기 때문에 파일의 위치가 다르고, DB 암호화 상태 등이 다르다. 다른 점을 분석하기 위해 KakaoTalk과 WhatsApp이 제공하는 서비스를 반복 송수신 하였고, 이를 분석하였으며, 분석결과의 차이점을 비교하였다. 그 중 채팅메시지에 관한 주요 비교 분석은 표 8과 같다.

Table. 8 Comparison of KakaoTalk and WhatsApp

	KakaoTalk	WhatsApp
Secret Chat	• Secret Chat	X
DB File	• Column Encryption • Rooting Access	• Plain Text • Rooting Access
Backup DB File	• Column Encryption • Rooting Access	• File Encryption • Rooting Access • Unrooting Access
time of deleted message	• deleted_at Column	• logs Files
Multimedia Artifacts	• Random Directory	• Static Directory

따라서, 표 8 의 1행과 같이 비밀채팅은 KakaoTalk만 지원하는 차별점이 있고, KakaoTalk 의 비밀채팅 분석은 일반 채팅메시지 분석과정과 동일하게 분석해야한다.

표 8의 2행과 같이 KakaoTalk DB파일은 WhatsApp의 평문 값과 다르게 칼럼 암호화로 되어 있어 복호화 방법론이 필요로 한다. KakaoTalk은 [25,26]의 방법론을 사용하여 암호화 값을 복호화 하여 분석해야한다.

표 8의 3행과 같이 WhatsApp의 파일 암호화 Backup DB파일은 외부에서 공개한 복호화 도구(Xtract Package) 의 방법론으로 외부 의존성을 가지나[21,22], KakaoTalk의 Backup DB파일은 DB파일과 동일한 암호화 방식으로 [25,26] 의 방법론을 사용하여 자체 App으로 복호화 하여 분석한다.

표 8의 4행과 같이 KakaoTalk 메시지 삭제 시각은 DB파일의 분석을 하여 시각 값을 파악하고, WhatsApp 경우는 DB파일에 삭제 시각 값이 미 존재로 DB파일 대신 logs 파일을 분석하여 시각 값을 분석해야한다.

표 8의 5행과 같이 WhatsApp의 멀티미디어 흔적파일은 정해진 경로에 파일들이 저장되나, KakaoTalk의 멀티미디어 흔적파일은 임의 경로를 생성하고 멀티미디어 파일들이 저장된다. 이에 KakaoTalk의 멀티미디어 흔적파일은 채팅방에서 주고받은 시각 값을 확인하고, 시각 값으로 전수 검사로 찾아야한다.

이를 기반으로 한 분석방법론은 2장에서 반영되어 있다.

Ⅴ. 결 론

IM Apps은 텍스트메시지, 사진, 동영상 등이 중요 증거로써 교환한 채팅메시지가 포렌식 분석의 대상이다. KakaoTalk은 그룹 채팅, 비밀채팅 등의 상세 채팅 메시지의 많은 분석 연구가 이루어지지 않았다. 이에 본 논문은 일반적인 IM App의 채팅메시지 분석 방법론을 분석 도출하였고, KakaoTalk 채팅메시지의 테이블 구조를 분석 수행하였다. 채팅메시지의 분석 내용은 다음과 같다. 채팅메시지의 유저를 식별하였고, 송・수신 구분과 콘텐츠를 구분하였고, 이력을 설명하였으며, 메시지 복원을 논의하였다. 분석결과는 분석한 정보를 바탕으로 Forensic Tool의 기본 플랫폼을 제공된다.

추가로 WhatsApp과 KakaoTalk을 비교 분석하였다. KakaoTalk의 DB파일은 WhatsApp과 달리 칼럼 암호화 상태로 복호화 방법이 필요로 하고, WhatsApp의 Backup DB파일 복호화는 KakaoTalk과 다르게 외부 사이트에 의존성을 보였다. 또한, WhatsApp은 채팅메시지의 삭제 흔적이 DB파일에 미 존재하여, logs파일 등의 추가 분석의 필요하다. 마지막으로 차후 PC 버전의 포렌식 분석은 제공하는 서비스에 대응하는 분석 방법론의 필요하다.

하지만 iOS의 KakaoTalk 분석 연구와 Android과 iOS의 KakaoTalk의 비교 분석 연구등 다양한 Platform에서의 각종 IM Forensics 비교 분석은 향후 연구로 남긴다.

REFERENCES

[1] Google. Consumer Barometer with Google [Internet]. Available: https://www.consumerbarometer.com/.

[2] Andrew Hoog, "Android Application and Forensic Analysis," in Android Forensics: Investigation, Analysis and Mobile Security for Google Android, 1st ed. Waltham, MA: Syngress Pub., ch. 7, pp. 285-363, 2011.

[3] Jeff Lessard, Gary C. Kessler, "Android Forensics: Simplifying Cell Phone Examinations," *Small Scale Digital Device Forensics Journal*, vol. 4, no. 1, pp. 1-12, Sept. 2010.

[4] Federal Court of Australia. Ashby v Commonwealth of Australia (No 4) [2012] FCA 1411 [Internet]. Available: http://www.austlii.edu.au/cgi-bin/sinodisp/au/cases/cth/FCA/2012/1411.htm.

[5] SAFLII. S v Oscar Pistorius (CC113/2013) [2014] ZAGPPHC 793 (12 September 2014) [Internet]. Available: http://www.saflii.org/za/cases/ZAGPPHC/2014/793.html.

[6] 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.

[7] TTA. Instant Messaging [Internet]. Available: http://word.tta.or.kr/main.do.

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

[9] 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.

[10] 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.

[11] Svein Yngvar Willassen, "Forensics and the GSM mobile telephone system," *International Journal of Digital Evidence*, vol. 2, no. 1, pp. 1-17, Spring. 2003.

[12] Mark Taylor, et al., "Digital evidence from mobile telephone applications," *Computer Law & Security Review*, vol. 28, no. 3, pp. 335-339, Jun. 2012.

[13] KIPO(Korean Intellectual Property Office), Digital forensics technology, patents increase. [Internet]. Available: http://www.kipo.go.kr.

[14] M. Dickson, "An examination into AOL Instant Messenger 5.5 contact identification," *Digital Investigation*, vol.3, no. 4, pp. 227-237, Dec. 2006.

[15] J. Reust, "Case study: AOL instant messenger trace evidence," *Digital Investigation*, vol. 3, no. 4, pp. 238-243, Oct. 2006.

[16] Noora Al Mutawa, et al., "Forensic artifacts of Facebook's instant messaging service," in *Conference of the 6th International Conference on Internet Technology and Secured Transactions*, Abu Dhabi, pp. 771-776, 2011.

[17] M. Dickson, "An examination into MSN Messenger 7.5 contact identification," *Digital Investigation*, vol. 3, no. 2, pp. 79-83, Apr. 2006.

[18] H. Carvey, "Instant messaging investigations on a live Windows XP system," *Digital Investigation*, vol. 1, no.4, pp. 256-260, Dec. 2004.

[19] Matthew Kiley, et al., "Forensic analysis of volatile instant messaging," in *Conference of The Fourth Annual IFIP WG 11.9 Conference on Digital Forensics*, Kyoto, pp. 129-138, 2008.

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

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

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

[23] Aditya Mahajan, et al., "Forensic analysis of instant messenger applications on android devices," *International Journal of Computer Applications*, vol. 68, no.8, Apr. 2013.

[24] Daniel Walnycky, et al., "Network and device forensic analysis of Android social-messaging applications," *Digital Investigation*, vol. 14, pp. S77-S84, Aug. 2015.

[25] Jongcheol Yoon, Yongsuk Park, "Forensic Analysis of KakaoTalk Messenger on Android Study of KakaoTalk," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 20, no. 1, pp. 72-80, Jan. 2016.

[26] Jongcheol Yoon, "Forensic Analysis of KakaoTalk Messenger on Android and Comparison Study of KakaoTalk and WhatsApp Artifacts," M.S. Thesis, SeJong Cyber University, 2016.

[27] Sei-Youen OH, "The application of digital forensic investigation for response of cyber-crimes," Journal of Digital Convergence, vol. 13, no. 4, pp. 81-87, Apr. 2015.

윤종철(JongCheol Yoon)

세종사이버대학교 정보보대학원 졸업 (석사)
※관심분야 : IT 서비스 및 보안, 산업보안, 포렌식, IoT 등

박용석(Yongsuk Park)

서강대학교 컴퓨터공학 (학사)
뉴욕(POLY)대 (석사, 박사)
미국 AT&T (Bell) Labs 연구소 연구원 (internet business 서비스 및 보안)
삼성전자 연구소 연구원 (모바일 및 DTV 응용 보안 및 서비스)
현재 세종사이버대학교 정보보호대학원 주임교수
현재 세종사이버대학교 IT 학부 교수
※관심분야 : IT 서비스 및 보안, 산업보안, 클라우드, IoT 등