디지털 포렌식을 위한 Android 및 Windows 환경에서 카카오톡 메시지의 아티팩트 분석 (Ⅰ)

이나비*, 김광조*

*KAIST 정보보호대학원

Analysis of Artifacts in KakaoTalk messages under Android and Windows Environments for Digital Forensics (Ⅰ)

Nabi Lee*, Kwangjo Kim*

*Graduate School of Information Security, KAIST.

요 약

다양한 채팅 애플리케이션 중 국내에서 압도적인 점유율을 가진 카카오톡은 사용자의 스마트폰 또는 PC에 저장된 사용자의 송·수신 메시지 흔적(아티팩트)을 통해 사용자의 생활패턴, 심리상태 등을 확인할 수 있어 포렌식 분야에 적극 활용되고 있다. 하지만 지금까지 발표된 논문들은 모두 Android 환경에서의 모바일용 카카오톡 또는 Windows 환경에서의 PC용 카카오톡 하나만을 분석하였다는 한계를 지닌다. 이에 본 논문에서는 모바일용 카카오톡과 PC용 카카오톡 아티팩트의 유형과 속성 정보를 비교 분석하고 이를 융합하여 포렌식 분야에 활용하는 방안을 살펴보았다.

I. 서론

카카오톡은 국내 스마트폰 사용자 중 97%가 애용하는 대표적인 채팅앱이다 [1]. 2010년 Android OS용, 2013년 Windows OS용 카카오톡이 출시되면서 사용자는 스마트폰과 PC를 구분하지 않고 텍스트, 사진, 음성, 동영상, 화상통화 등 다양한 콘텐츠로 소통하고 있다. 모든 송·수신 메시지는 사용자의 스마트폰과 PC에 DB형태로 저장되기 때문에 포렌식 연구에서 사용자의 스마트폰 또는 PC에 잔존하는 카카오톡 메시지 흔적 (아티팩트) 분석은 대단히 중요하다.

카카오톡은 WhatsApp, Facebook Messenger 등과 달리 [2] 국내에 그 인기가 국한되어 있어 상대적으로 연구가 활발하지 않고, 모바일용과 PC용으로 구분되어 있음에도 이를 동시에 다루는 논문을 찾아보기 힘들다. 국내 OS 시장에서 Android와 Windows의 점유율 [3]이 압도적이기 때문에 Android OS용 또는 Windows OS용 카카오톡에 대한 분석이 대부분이다. 본 논문에서도 iOS 및 MAC PC용 카카오톡 분석은 제외하였다. 문헌[4]는 Windows 7 환경에서 카카오톡, 네이트온, QQ 메신저 메시지의 암호화 알고리즘을 단계적으로 분석하였고, 문헌[5]는 30개의 인기 있는 Android OS용 채팅앱을 선별하여 메시지를 논리적으로 추출한 뒤 각각의 아티팩트를 분석하였다. 문헌[6]은 Android 환경에서 모바일용 카카오톡 DB파일 중 메시지를 SQLite browser를 통해 확인한 뒤 저장위치, 메시지 타입 등을 파악하였다.

문헌[4 - 6]은 모두 모바일용 카카오톡 또는 PC용 카카오톡 한 가지만을 연구하였고 특히 Android 환경에서의 아티팩트 분석방법을 기술한 문헌[5, 6]은 카카오톡 버전 4를 분석하여 최근 사용되는 카카오톡 버전 8 분석에는 일부 적합하지 않다. 따라서 본 논문은 Android 6 (마시멜로) 환경의 모바일용 카카오톡과 Windows 10 환경의 PC용 카카오톡 메시지를 각각 추출하여 아티팩트를 비교 분석하고 이를 효과적으로 포렌식에 활용하는 방안에 대해 고찰하였다.

II. 분석방법

1.1 분석환경

본 연구에서 사용한 장치와 카카오톡 버전은 Table 1과 같다. 카카오톡 계정 사용자의 ID와 PW는 사전 획득이 가능하다고 가정하였다.

Table 1. 본 연구의 분석 환경

	분석 기종	OS	카카오톡 버전
PC	Intel(R) Xeon(R) CPU E3-1230 v3	Window 10 Pro (64-bit)	3.0.4.2212
모바일	Samsung Galaxy Note5 (SM-N920)	Android 6.0 마시멜로	8.5.4

1.2 분석결과

카카오톡을 통해 생성된 데이터들은 /data/com.kakao.talk/databases와 /data/com.kakao.talk/files 경로 아래 'KakaoTalk.db'와 'KakaoTalk2.db' 파일에 구분되어 저장되어 있다. 카카오톡에 대한 메시지 추출(이미징)과 분석은 각각 상용 포렌식 도구인 MAGNET AXIOM 버전 3.3.1.14874의 Process (이미징)와 Examine (분석)을 활용하였다. 대상 데이터는 PC와 모바일에 카카오톡을 설치하고 '19. 6. 1.~'19. 6. 30. 1개월 동안 송·수신한 문자메시지, 동영상, 음성파일, 보이스톡 등 다양한 콘텐츠를 분석하였다.

추출된 카카오톡 아티팩트는 Table 2와 같이 5개의 유형으로 구분된다. Calls와 Shared Pictures는 각각 모바일용 카카오톡, PC용 카카오톡에서만 확인되었고 Chat Rooms, Messages, Contacts는 모바일용, PC용에서 동시에 확인할 수 있었는데 Table 3, 4, 5와 같이 세부 속성에는 공통점과 차이점이 있었다.

Table 2. 카카오톡 아티팩트 유형

아티팩트 유형	모바일	PC
카카오톡 Chat Rooms	○	○
카카오톡 Messages	○	○
카카오톡 Contacts (Friends)	○	○
카카오톡 Calls	○	×
카카오톡 Shared Pictures	×	○

Table 3. 카카오톡 Chat Rooms의 속성 정보

아티팩트 속성	모바일	PC
Chat ID	○	○
Room Name	○	○
Other Participants	○	△
Number of participants	×	○
Link ID	×	○
Chat Type	○	○
Last Message	○	○
Last Message Date/Time	×	○
Updated Date/Time	○	×
Unsent Message	○	×
Invitation Status	○	×
Room Status	×	○
Room Status Author	×	○
Status Updated Date/Time	×	○

Table 4. 카카오톡 Message의 속성 정보

아티팩트 속성	모바일	PC
Chat ID	○	×
Sender ID	○	○
Sender Name	○	×
Message	○	○
Message ID	×	○
Message Type	○	○
Created Date/Time	○	×
Message Direction	○	×
Message Sent Date/Time	×	○
Deleted Date/Time	○	×
Deleted	×	○
Attachment (Additional Information)	○	○
Latitude	○	×
Longitude	○	×

이는 카카오톡 메시지를 수사에 활용할 때 모바일용과 PC용 카카오톡을 동시에 활용한다면 차별성이 있는 정보획득이 가능함을 시사한다.

Table 5. 카카오톡 Contacts (Friends)의 속성 정보

아티팩트 속성	모바일	PC
ID	○	×
User ID	○	○
User Name (Screen Name)	○	○
Contact Name	○	×
Account Type	×	○
Status Message	○	○
Created Date/Time	○	×
Nickname	○	○
Favorite	○	○
Hidden	○	○
Phone Number	○	○
Profile Picture (image) URL	○	○
Link ID	×	○
Group Chat ID	○	×

예로 Table 2와 같이 모바일용에서만 추출 가능한 카카오톡 Calls 아티팩트를 통해 우리는 사용자의 보이스톡, 페이스톡 사용일자, 통화시간, 발신IP 등을 확인할 수 있다. 또한 Table 3과 같이 메시지를 생성/삭제한 시간은 모바일용 카카오톡에서, 메시지를 보낸 시간은 PC용 카카오톡에서 각각 확인이 가능하다.

III. 결론

본 논문에서는 카카오톡 모바일용 및 PC용 카카오톡 아티팩트 유형과 속성 정보의 공통점과 차이점을 분석하여 포렌식 분야에 활용하는 방안을 살펴보았다.

카카오톡 하나만 보더라도 추출 가능한 데이터의 양이 방대하고 수사관의 재량에 따라 획득 가능한 정보의 수준에 격차가 발생하는 만큼 다양한 수사기법의 융합이 필요하며, 향후에는 본 연구를 통해 추출한 카카오톡 메시지에 대한 구문 분석(자연어 처리)을 통하여 포렌식 업무에 유용한 정보를 추출하고자 한다.

[참고문헌]

[1] https://www.statista.com/statistics/984645/south-korea-kakaotalk-usage-by-age/

[2] https://gs.statcounter.com/os-market-share/all/south-korea/

[3] https://www.statista.com/statistics/258749/most-

[4] Choi, Jusop, et al. "Digital forensic analysis of encrypted database files in instant messaging applications on Windows operating systems: Case study with KakaoTalk, NateOn and QQ messenger." Digital Investigation 28 (2019): S50-S59.

[5] Azfar, Abdullah, Kim Kwang Raymond Choo, and Lin Liu. "An android communication app forensic taxonomy." Journal of forensic sciences 61.5 (2016): 1337-1350.

[6] 윤종철, 박용석. "KakaoTalk의 채팅 메시지 포렌식 분석 연구 및 WhatsApp의 Artifacts 와의 비교 분석." 한국정보통신학회논문지 20.4 (2016): 777-785.