[논문 리뷰 보고서]

[윈도우 환경에서 카카오톡 데이터 복호화 및 아티팩트 분석 연구]

작성일	2025.05.26
작성자	안서진
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	윈도우 환경에서 카카오톡 데이터 복호화 및 아티팩트 분석 연구
저자 및 연도	조민욱, 장남수. (2023)
출처	한국정보보호학회/https://www.dbpia.co.kr/pdf/pdfView.do?nodeId=NODE11215974&googleIPSandBox=false&mark=0&minRead=15&ipRange=false&b2cLoginYN=false&icstClss=010000&isPDFSizeAllowed=true&accessgl=Y&language=ko_KR&hasTopBanner=true
분석 대상 프로그램	KakaoTalk
관련 아티팩트 유형	메신저 아티팩트, 파일 사용/조작, 사용자 행위

[표 1. 논문 개요표]

II. 논문 요약

이 논문에서는 카카오톡의 데이터 복호화 및 아티팩트 분석 방안을 제시하고자 하였다. 연구의 목적은 Windows 환경에서 카카오톡의 데이터가 암호화되어 저장되는 문제를 해결하고, 디지털 포렌식 수사에서 중요한 증거로 활용될 수 있는 사용자 행위 정보를 분석하는 것이다.

연구 결과, 썸캐시 파일 내에 저장된 썸네일을 추출하는 방안을 구현하였으며, 사진 촬영, 열람, 삭제 등 사용자의 각종 행위에 따른 썸네일의 변화를 분석하였다. 이를 통해 카카오톡의 데이터 복호화 및 아티팩트 분석의 중요성을 강조하고, 디지털 포렌식 분석의 효율성을 높일 수 있는 방법을 도출하였다.

연구는 카카오톡의 보안상의 이유로 데이터가 암호화되어 있는 점과 의도적인 조작, 은닉, 삭제 등의 행위가 증가하는 한계를 가지고 있으며, 후속 연구로는 이러한 문제를 해결하기 위한 개선 방향이 제안될 수 있다.

III. 상세 경로

항목	경로
Kakaotalk	"%LocalAppData%₩Kakao₩KakaoTalk₩users₩{userDir}₩chat_data₩chatLogs_{chatId}.edb
사용자 행위 정보	"%LocalAppData%₩Kakao₩KakaoTalk₩users
메신저 아티팩트	"%LocalAppData%₩Kakao₩KakaoTalk₩users₩chat_data
파일 사용/조작	"%LocalAppData%₩Kakao₩KakaoTalk₩users₩chat_data₩cl

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. 섬네일 자동 추출 도구 개발

기존 도구의 한계를 극복하기 위해, 썸네일을 자동 추출하고 다양한 사용자 행위를 분석할 수 있는 기능을 통합한 도구를 개발할 수 있을 것이다.

이를 통해 수사에 있어 증거 수집이 더욱 효율적이고 신속하게 이루어질 것으로 보인다.

더 나아가 암호화된 데이터를 복호화할 수 있는 도구를 개발하는 것 또한 효율적인 분석에 도움이 될 것이다.

V. 참고 문헌

[1] 조민욱, 장남수,「 윈도우 환경에서 카카오톡 데이터 복호화 및 아티팩트 분석 연구」, 정보보호학회논문지 제33권 제1호, 2023.2, 51-61