온라인 메신저 디지털 증거 수집과 분석 방법

이수연*, 샤흐저드*, 구형준**

성균관대학교 소프트웨어학과 (대학원생*, 교수**)

Investigating the Acquisition and Analysis of Digital Artifacts for Messaging Applications

Suyeon Lee*, Shakhzod Yuldoshkhujaev*, Hyungjoon Koo**

Department of Computer Science and Engineering, Sungkyunkwan University (Graduate student*, Professor**)

요 약

메신저 서비스는 다양한 플랫폼에서 활용되며, 사용자 행위에 따라 생성되는 디지털 흔적은 디지털 포렌식 분석에서 핵심적인 단서를 제공한다. 메신저 포렌식은 운영 체제, 저장 구조, 암호화 기법의 차이로 인해 데이터 보존 방식과 수집 가능 정보가 달라지고, 분석 전략 또한 서비스마다 상이하다. 본 연구는 주요 메신저 10종을 대상으로 저장 위치, 보안 구조, 아티팩트 유형, 분석 도구, 수집 절차를 체계적으로 정리하고 비교한다. 플랫폼 환경에 따라 아티팩트의 위치와 특성을 분석하고, 도구와 수집 방식의 조합이 복구 범위에 미치는 영향을 파악한다. 서비스별 분석 접근 방식을 분류하고 기술적 제약 요인을 식별함으로써, 환경별 분석 흐름을 구조화한다. 그 결과, 메신저 포렌식에서 일관된 절차 정립과 자동화 도구 설계가 필요한 지점을 도출하며, 다양한 플랫폼과 조건에 적용 가능한 분석 전략 수립의 기반을 제시한다.

I. 서론

메신저 서비스는 개인 간 소통은 물론 기업 활동과 사이버 범죄에도 활용되며, 이로 인해 생성되는 디지털 흔적은 법적 증거 확보와 보안 수사에서 핵심적인 자료로 기능한다. 특히 카카오톡, 텔레그램과 같은 주요 메신저 플랫폼은 사용자 활동 데이터를 로컬 또는 클라우드 저장소에 기록하며, 포렌식 분석의 주요 대상이 된다. 그러나 메신저 포렌식은 다양한 플랫폼과 암호화 정책, 저장소 구조의 차이로 인해 분석 전략과 복구 가능성에 큰 차이가 발생한다. 이러한 차이는 데이터 수집의 성공 여부뿐 아니라 복구 가능한 아티팩트 (Artifact)의 범위와 가능성에도 영향을 미친다. 기존 연구는 대부분 개별 메신저의 디지털 흔적에 대한 분석을 다양한 환경에서 수행했으나, 플랫폼 지원, 보안 기능, 저장 위치 등에 따른 분석 방법을 통합적으로 비교한 정리는 드물다. 본 연구는 최근 10년간의 포렌식 연구를 바탕으로 10종의 주요 메신저의 실험 환경, 저장 위치, 복구 대상, 분석 도구 사용 현황을 정리하고 복구 가능성의 차이와 기술적 한계를 비교 분석한다.

II. 메신저 포렌식

메신저 포렌식 (Messenger Forensics) [1]은 모바일 또는 데스크톱 환경에서 메신저 애플리케이션을 통해 생성된 디지털 흔적을 수집하고 분석하는 과정을 의미한다. 대표적인 분석 대상은 채팅 기록, 전송 파일, 계정 정보, 세션 토큰 등이 있다. 그러나 메신저는 서비스마다 플랫폼 (Android, iOS, Windows, Web 등), 저장 구조 (SQLite, 메모리, 브라우저 저장소 등), 보안 정책 (종단간 암호화 (End-to-End Encryption, E

본 논문은 2025년도 정부(과학기술정보통신부) 정보통신기획평가원 (No.RS-2022-II221199, 융합보안대학원(성균관대학교); No.RS-2024-00398745, 디지털 환경에서의 증거인멸행위 증명 및 대응기술 개발) 지원으로 수행한 연구임.

2EE), 자동 삭제 등)이 상이해 일관된 분석이 어렵다. 동일한 메신저라도 플랫폼에 따라 데이터가 저장되는 위치와 접근 방식이 다르며, 강력한 암호화나 클라우드 기반 설계로 인해 아티팩트 복구가 제한되는 경우도 많다.

이러한 구조적 차이로 인해 메신저 포렌식은 다양한 분석 전략과 도구가 필요하며, 복구 가능성 역시 환경에 따라 크게 달라진다. 선행 연구들은 이러한 제약을 극복하기 위해 SQLite 기반 데이터베이스 분석, 시스템 메모리 확보, 브라우저 저장소 접근, 포렌식 도구의 조합 등 다양한 방법론을 시도해 왔다.

III. 디지털 증거 수집 및 분석 방법론

메신저 포렌식 실험은 사용자 행위 시나리오 정의, 디지털 증거 수집과 분석 세 단계로 구성된다. 그림 1은 전체 절차를 도식화한 것이다.

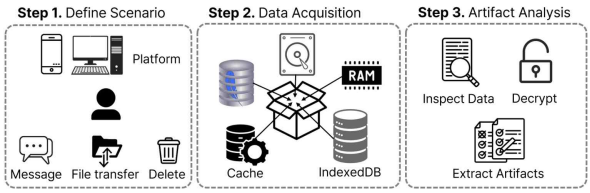

그림 1. 메신저 포렌식 연구의 일반적인 절차

3.1. 사용자 행위 시나리오 정의

실험 환경에서는 다양한 플랫폼에 메신저 애플리케이션을 설치하고, 사용자 행위를 시뮬레이션해 디지털 흔적을 생성한다. 시나리오는 메신저 사용 중 발생 가능한 행위를 중심으로 구성되며, 계정 생성, 텍스트 및 파일 송수신, 채팅방 생성과 탈퇴, 메시지 및 파일 삭제 등을 포함한다. 일부 시나리오는 삭제 후 재설치, 로그아웃 후 재로그인 등 복구 난이도가 높은 조건을 반영하며, 이를 통해 아티팩트의 잔존 여부를 확인한다. 이러한 시나리오는 저장 구조와 아티팩트 특성 비교를 위한 기준으로 작용한다.

3.2. 디지털 증거 수집

사용자 행위 이후, 대상 장치에서는 다양한 유형의 저장소로부터 디지털 증거를 수집한다. 주요 수집 대상은 애플리케이션의 로컬 저장소(SQLite 데이터베이스 (Database, DB), 캐시, 파일 시스템 등), 웹 애플리케이션의 클라이언트 저장소 (예: IndexedDB), 시스템 메모리 (RAM) 등이다. 일부 실험은 로그 파일과 네트워크 트래픽도 분석한다. 데이터 수집 시 ADB, FTK Imager 등 디지털 포렌식 도구를 활용하며, 저장소의 특성에 따라 물리 이미지 생성, 메모리 덤프, 논리 추출 방식 등을 선택한다.

3.3. 디지털 증거 분석

수집된 데이터는 채팅 로그, 계정 정보, 전송 기록, 삭제된 메시지, 인증 토큰, 세션 정보 등 다양한 유형의 아티팩트를 포함한다. 분석 단계에서는 SQL 쿼리와 메모리 검색을 통해 데이터를 열람하고, SQLCipher나 E2EE 해제 과정을 통해 암호화된 정보를 복구한다. 이후 아티팩트를 구조화하여 정리함으로써, 각 메신저에서 복구 가능한 정보의 범위, 저장 위치, 암호화 적용 여부를 체계적으로 파악한다.

IV. 실험 환경과 도구 비교

4.1. 실험 환경

메신저	지원 플랫폼					
	Android	iOS	Windows	macOS	Linux	Web
Wickr	✓	✓	✓	✓	✓	×
Signal	✓	✓	✓	✓	✓	×
Telegram	✓	✓	✓	✓	✓	✓
Naver Band	✓	✓	✓	✓	×	×
KakaoTalk	✓	✓	✓	✓	×	×
Wire	✓	✓	✓	✓	✓	×
Element	✓	✓	✓	✓	✓	✓
WeChat	✓	✓	✓	✓	×	×
Discord	✓	✓	✓	✓	✓	✓
WhatsApp	✓	✓	✓	✓	×	✓

표 1. 다양한 메신저 지원 플랫폼

실험 환경은 분석 대상 메신저의 플랫폼 지원 여부에 따라 구성되며, Android와 Windows 환경이 가장 널리 활용된다. 웹 기반 메신저의 경우 Chrome, Firefox, Edge 등 주요 브라우저가 사용되며, 가상환경과 실제 기기를 병행해 실험의 재현성과 범용성을 확보한다. 표 1은 선정한

10종 메신저의 지원 플랫폼을 정리한 것으로, 플랫폼 간 차이는 저장 위치와 분석 전략에 직접적인 영향을 미친다.

4.2. 실험 도구

분류	용도	도구
메모리 포렌식	RAM 획득	Belkasoft, FTK Imager, WinPmem
	RAM 분석	RAMAS
종합 포렌식	종합 디지털 포렌식	AccessData, Autopsy, Magnet AXIOM, Paraben E3
	디스크 및 파일 시스템 포렌식	X-Ways
모바일 포렌식	모바일 포렌식 통합	Oxygen Detective, Cellebrite, MSAB
	모바일 아티팩트 파서	aLEAPP, Andriller, ADB
	모바일 데이터 수집	Magnet Acquire, Oxygen Extractor
SQLite 포렌식	데이터 복구	bring2lite, FQlite, SQLECmd
	분석 및 시각화	DB Browser Forensic Toolkit, KS DB, Oxygen SQLite Viewer
브라우저 포렌식	기록 수집	Capturer Examiner
	기록 분석	Viewer

표 2. 분석 대상 위치별 메신저 포렌식 도구

데이터 수집과 아티팩트 분석에는 다양한 범주의 포렌식 도구가 활용된다. 메모리, 파일 시스템, 로컬 DB, 브라우저 저장소 등 각 저장 구조에 적합한 도구를 선택하며, 수집 목적과 분석 단계에 따라 구분해 적용한다. 표 2는 메신저 포렌식 실험에서 활용된 주요 도구들을 용도별로 분류한 내용을 나타낸다.

V. 메신저별 디지털 증거 분석

메신저는 플랫폼, 저장 구조, 보안 정책에 따라 분석 접근 방식과 복구 가능 정보의 범위에 차이가 있다. 다음은 조사한 연구들 가운데 가장 구체적인 아티팩트가 확인된 플랫폼을 기준으로 기술한다.

Wickr. [2,3] 자체 암호화된 `.wic` 키 파일과 사용자 설정 기반 인증 구조를 가진다. Windows 환경에서는 SID 기반으로 키를 파생해 복호화를 수행하며, WAL 로그 분석을 통해 삭제 전후 메시지 상태를 비교한다.

Signal. [3] 복호화 키는 Android Keystore에 저장되며, 키 확보 시 E2EE 상태의 채팅 내용, 그룹 키, 전송 파일까지 추출 가능하다. 이외에도 로그 파일을 통해 채널 변경 이력 등 앱 내 활동 정보를 확인할 수 있다.

Telegram. [4,5] Web 버전에서는 IndexedDB와 Cache에 이미지와 메타데이터가 저장되며, 일부 텍스트 메시지가 암호화되지 않은 형태로 포함된다. Desktop 버전에서는 메모리에 텍스트 메시지가 일시적으로 남아 있어, 메모리 덤프를 통해 대화 내용을 확인할 수 있다. Android에서는 루팅을 통해 DB를 확보하고, 계정 정보와 메시지 로그를 추출할 수 있다.

Naver Band. [6] Android 기반에서 SQLite DB의 status='RECLAIM' 값을 통해 삭제된 메시지를 식별한다. shared_prefs의 USER.xml에는 access_token과 사용자 식별자가 평문으로 저장되며, Frida 후킹으로 복호화한 인증 키를 사용해 서버 채팅 이력을 추가 확보할 수 있다.

KakaoTalk. [7] macOS 버전은 사용자 비밀번호 기반 AES 암호화를 적용하며, 복호화 키 생성 절차 분석을 통해 메시지 DB 접근이 가능하다. 내부에는 메시지 본문, 전송 이력, 삭제 여부 등을 포함한 구조화된 기록이 저장된다.

Wire. [8] Windows 환경에서 Device ID와 세션 쿠키 기반의 인증 구조를 사용하며, 쿠키 파일 확보만으로 인증을 우회한다. LevelDB에는 메시지 본문, 삭제 여부, 자동 삭제 시각 등이 포함된 로그가 저장된다.

Element. [9] Matrix 프로토콜을 기반으로 한 구조를 따르며, Windows 환경에서는 Events.d

b 파일 내에서 room_id를 포함한 채팅 로그, 전송 기록, 사용자 정보 등 구조화된 데이터를 확보한다. 삭제 여부는 해당 데이터베이스의 전용 필드 값을 기준으로 구분된다.

WeChat. [10] Android, Windows 환경에서 SQLCipher 암호화를 적용하고 IMEI, UIN, 사용자 ID 기반 키 파생 알고리즘을 사용한다. 삭제 메시지는 FTS 인덱스에 일부 정보가 남아 있으며 색인 분석을 통해 원문 일부를 추출한다.

Discord. [11] Windows 환경에서 SQLite 기반의 main.db, Friends.db, guilds.db에 사용자 정보, 대화 기록, 친구 목록, 길드 참여 정보 등이 관계형 구조로 저장된다. 메시지 삭제 여부는 deleted 필드를 통해 식별하며, 전송된 이미지와 파일은 Cache 디렉터리에서 추출 가능하다.

WhatsApp. [5,12] Web 환경에서 브라우저의 IndexedDB와 Cache에 대화 이미지 및 관련 메타데이터가 저장된다. 탭이 열린 상태에서 RAM을 덤프하면 URL, 발신자, 메시지 내용 등을 평문 형태로 추출할 수 있으며, 잔존 여부는 브라우저 종료 방식에 따른 차이를 보인다.

VI. 기술적 한계 및 향후 과제

메신저 포렌식은 대개 탈옥, 루팅, 로그인 유지와 같은 제한된 실험 환경에 의존해 실무 적용성과 일반화에 한계가 있다. 웹 기반 메신저는 데이터 휘발성이 높고, 수집 시점이나 브라우저 동작 방식에 따라 아티팩트의 잔존 여부가 달라질 수 있다. 메시지 암호화는 수집보다 해석 과정에서 더 큰 제약을 야기한다. 복호화 키가 An-droid Keystore 등 보안 영역에 저장될 경우, 데이터를 확보하더라도 실제 해석이 불가능한 사례가 빈번하다. 따라서, 권한 제한 환경에서도 적용 가능한 수집 전략, 플랫폼 및 버전별 저장 구조에 따른 분석 절차의 정립, 그리고 다양한 조건을 자동으로 감지해 절차를 수행하는 포렌식 도구의 자동화가 요구된다.

VII. 결론

본 연구는 10종의 주요 메신저를 대상으로 진행된 포렌식 연구를 조사하고, 각 서비스의 저장 구조, 암호화 방식, 아티팩트 특성을 비교하였다. 플랫폼과 보안 설계에 따라 수집 가능한 정보와 분석 방법에 차이가 있음을 확인했으며, 환경별 분석 절차 정립과 자동화 도구 개발의 필요성을 제안한다. 이 연구가 메신저 포렌식 절차의 체계화와 분석 전략 수립을 위한 기초 자료로 활용될 것으로 기대한다.

[참고문헌]

[1] Barradas, Diogo, et al. "Forensic analysis of communication records of messaging applications from physical memory." Computers & Security 86 (2019): 484-497.

[2] 정수은, et al. "윈도우 환경에서의 Wickr 메신저 포렌식 분석." 디지털포렌식연구 16.4 (2022): 42-55.

[3] Son, Jihun, et al. "Forensic analysis of instant messengers: Decrypt Signal, Wickr, and Threema." Forensic Science International: Digital Investigation 40 (2022): 301347.

[4] Raza, Ahmed, et al. "Forensic analysis of web browsers lifecycle: A case study." Journal of Information Security and Applications 85 (2024): 103839.

[5] Fernández-Álvarez, Pedro, and Ricardo J. Rodríguez. "Extraction and analysis of retrievable memory artifacts from Windows Telegram Desktop application." Forensic Science International: Digital Investigation 40 (2022): 301342.

[6] 안원석, and 박명서. "디지털 포렌식 관점의 네이버 밴드 사용자 행위 수집 및 분석 연구." 정보보호학회논문지 34.6 (2024): 1263-1272.

[7] 박범준, and 이상진. "macOS 용 카카오톡 데이터베이스 복호화 방안." 정보보호학회논문지 33.5 (2023): 753-760.

[8] 신수민, et al. "Windows에서의 Wire 크리덴셜 획득 및 아티팩트 분석." 정보보호학회논문지 31.1 (2021): 61-71.

[9] 조재민, et al. "포렌식 관점에서의 Element 인스턴트 메신저 아티팩트 분석." 정보보호학회논문지 32.6 (2022): 1113-1120.

[10] 허욱, 박명서, and 김종성. "WeChat 메신저의 향상된 복호화 방안과 SQLite Full Text Search 데이터를 이용한 삭제된 메시지 복구에 관한 연구." 정보보호학회논문지 30.3 (2020): 405-415.

[11] 신수민, et al. "디지털 포렌식 관점에서의 Slack 및 Discord 메신저 아티팩트 분석." 디지털콘텐츠학회논문지 21.4 (2020): 799-809.

[12] Kim, Giyoon, et al. "Analyzing the Web and UWP versions of WhatsApp for digital forensics." Forensic Science International: Digital Investigation 52 (2025): 301861.