[논문 리뷰 보고서]

[A Study On Artifacts Analysis In Portable Software]

작성일	2025.05.26
작성자	정지윤
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	A Study On Artifacts Analysis In Portable Software
저자 및 연도	허태영, 손태식(2023.04.30)
출처	Journal of Platform Technology, 제11권 2호, 2023, pp.39–53, KoreaScience
분석 대상 프로그램	Opera, Notepad++
관련 아티팩트 유형	Prefetch 파일, JumpList, ShellBags, 메모리 데이터, MemCompression 기록, Windows Defender 로그 등

[표 1. 논문 개요표]

II. 논문 요약

위 논문은 설치가 필요 없는 포터블 프로그램의 사용 흔적을 분석하여 사용자 행위를 추적하는 방법을 제시한 연구이다. 포터블 프로그램은 별도의 설치 없이 실행되기 때문에 흔적이 적게 남으며 사용 후 삭제되면 일반적인 방식의 포렌식 분석으로는 증거 확보가 어렵다. 위 논문에서는 이러한 한계를 극복하기 위하여 가상 머신 상의 windows 10 환경에서 Opera(웹 브라우저)와 Notepad++(텍스트 에디터)를 대상으로 실험을 하였다.

저자는 운영체제 수준의 아티팩트 분서과 메모리 포렌식을 병행하여 다양한 분석을 수행하였는데, 운영체제 기반 분석을 통해 일부는 식별할 수 있었지만, 프로그램 종료 시 생성된 임시 파일이 삭제되는 경우가 많아 구체적인 아티팩트 분석에 한계를 가졌다. 이에 따라 저자는 메모리 포렌식을 활용하여 사용자가 접속한 웹사이트의 URL, 입력한 텍스트 파일 정보, Windows

Defender의 악성코드 탐지 기록, 접속 환경 정보, 실행 중이던 프로세스 등의 데이터를 얻을 수 있었다.

이 논문을 통하여 메모리 포렌식을 포함한 다양한 기법의 병행적 적용이 필수적임을 강조한다. 또한 Windows Defender와 MemCompression 프로세스 등 포렌식 분석에 활용될 수 있는 비전통적인 아티팩트의 중요성도 확인할 수 있다.

III. 상세 경로

항목	경로
Prefetch	C:₩Windows₩Prefetch₩*.pf
ShimCache (AppCompatCache)	HKLM₩SYSTEM₩CurrentControlSet₩Control₩Session Manager₩AppCompatCache
UserAssist	HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩UserAssist
MUICache	HKCU₩Software₩Microsoft₩Windows₩ShellNoRoam₩MUICache
LNK 파일	%APPDATA%₩Microsoft₩Windows₩Recent₩*.lnk 및 ₩AutomaticDestinations₩*.automaticDestinations-ms

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. 비전통적 아티팩트를 이용하여 포터블 프로그램에 대한 분석

포터블 프로그램에 대한 아티팩트 수집 및 분석 과정이 수작업이기 때문에 논문에서 언급된 Windows Defender, MemCompression, 메모리 내 문자열

등 비전통적 아티팩트를 이용하여 포터블 프로그램에 대한 분석 자동화 및 아티팩트 분석 도구 개발을 진행할 수 있을 것이다. 또한, 포터블 프로그램의 수는 다양하기 때문에 프로그램 수에 구애받지 않고 분석을 진행할 수 있을 것이다.

V. 참고 문헌

[1] 허태영, 손태식,「A Study On Artifacts Analysis In Portable Software(무설치 프로그램에서의 사용자 행위 아티팩트 분석)」, Journal of Platform Technology 제11권 제2호, 2023.04.30, KoreaScience.

[논문 리뷰 보고서]

[협업 툴 아티팩트 분석 및 삭제된 데이터 복구 연구]

작성일	2025.05.26
작성자	정지윤
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	협업 툴 아티팩트 분석 및 삭제된 데이터 복구 연구
저자 및 연도	신수민, 최용철, 김소람, 김종성 (2021)
출처	디지털포렌식연구 제15권 제2호 (2021.06), DOI: 10.22798/kdfs.2021.15.2.99
분석 대상 프로그램	잔디, 네이버 웍스
관련 아티팩트 유형	사용자 계정 정보, 대화 내역, 메시지 유형, 공유 파일, 투표 및 할 일 데이터, 삭제된 메시지, 썸네일, 설정 정보 등

[표 1. 논문 개요표]

II. 논문 요약

위 논문은 코로나 19로 인한 비대면 업무 확산에 따라 사용량이 급증한 협업 툴 '잔디'와 '네이버 웍스'에서 생성되는 사용자 행위 기반 데이터를 분석하고 삭제된 메시지의 복구 가능성을 확인하는 것을 목적으로 하였다. 협업 툴에는 계정 정보, 대화 내역, 파일, 투표, 할 일 등 다양한 정보가 저장되며 이 데이터가 혼재되어 있어 분석이 어렵기 때문에 위 논문에서는 주요 아티팩트를 식별하고, 그 상관관계를 통해 삭제 메시지 복구를 시도하였다.

위 연구는 안드로이드 환경이라는 제한적이 조건에서 어플리케이션을 실행하였으며 DB Browser, HxD 등을 활용해 분석을 수행하였다. 분석 결과, 두 앱 모두 메시지, 파일, 투표, 할 일 정보가 SQLite데이터베이스에 저장되고 있었으며 삭제된 메시지도 데이터베이스에 남아 있어 복구가 가능한 것으로 나타났다. 특히 JANDI는 평문 형태의 패스워드를 XML 설정 파일에 저장하고 있다는 것을 알 수 있었고 네이버 웍스는 비밀번호를 SHA256 + base64

형태로 저장했지만 4자리 숫자 제한으로 인해 GPU를 이용한 빠른 복호화가 가능하다는 것을 알 수 있었다.

III. 상세 경로

항목	경로
계정 정보	%AppData%₩[앱이름]₩settings.json, AppData₩Roaming, config.db, registry
채팅 내역	main.db, chat.db, IndexedDB, LevelDB, %AppData% 내부 DB
파일 업로드/다운로드 기록	%AppData%₩[앱이름]₩Cache, $MFT, $UsnJrnl, Downloads
캐시/임시 파일	%LocalAppData%₩Temp₩, %AppData%₩[앱]₩Cache
사용자 행위/기록	%AppData%₩[앱이름]₩Logs₩, Windows Event Logs, $Logfile, $UsnJrnl
앱 실행 흔적	refetch, Amcache.hve, UserAssist 레지스트리

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. 아티팩트 간 시간 정보와 키값을 활용해 악성 프로그램의 실행 흔적을 시간 순으로 재구성

   위 논문을 바탕으로 윈도우 악성 프로그램 아티팩트 분석 연구에서 악성 행위 발생 시 생성되는 다양한 시스템 아티팩트를 기능별로 분류하고, 삭제 또는 은폐된 활동 역시 추적 가능한 구조를 알 수 있다. 또한, 아티팩트 간 시간 정보와 키값을 활용해 악성 프로그램의 실행

흔적을 시간 순으로 재구성하는 분석 방법도 알 수 있다. 따라서 메시지 기반 협업 툴인 Slack이나 Microsoft Teams 등의 프로그램을 분석할 수 있다. 예를 들어 공격자가 slack을 통하여 내부자에게 악성 URL을 전달하는 상황에서 아티팩트 분석으로 메시지 복원이 가능한 상황을 생성할 수 있고, 공격자가 Microsoft Teams를 통해 내부방에 악성파일을 전송하였을때 아티팩트를 분석하며 실행 시간과 다운로드 시간의 상간관계를 알아낼 수 있다.

V. 참고 문헌

[1] 신수민, 최웅철, 김소람, 김종성,「협업 툴 아티팩트 분석 및 삭제된 데이터 복구 연구」, 디지털포렌식연구 제15권 제2호, 2021.06, DOI:10.22798/kdfs.2021.15.2.99

논문 리뷰 보고서]

[Microsoft Office 진단 로그 분석 및 포렌식 활용 방안]

작성일	2025.05.26
작성자	정지윤
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	Microsoft Office 진단 로그 분석 및 포렌식 활용 방안
저자 및 연도	임연재, 박정흠, 이상진 (2021)
출처	『디지털포렌식연구』 제15권 제2호, pp. 24-34
분석 대상 프로그램	Microsoft Word, Excel, PowerPoint
관련 아티팩트 유형	Office 진단 로그, File MRU 레지스트리, $UsnJrnl, LNK, JumpList, Prefetch 등

[표 1. 논문 개요표]

II. 논문 요약

위 논문은 Microsoft Office에서 자동으로 생성되는 진단 로그를 활용하여 문서 작성자의 작업 이력 추적이 가능한지를 분석하였다. 위 논문에서는 Office 진단 로그는 파일 이름, 경로, 내용 등을 포함하지 않아 단독으로 문서 식별이 어렵다는 점을 해결하기 위하여 진단 로그에서 기록되는 이벤트(파일 열기, 저장, 편집 등)의 유형을 정리하고 해당 로그를 File MRU 레지스트리 키와 연계하여 어떤 문서에 대한 작업 이력인지 추정할 수 있는 방법을 제시하였다.

실험을 통하여 Word, Excel, PoerPoint에서 발생하는 주요 사용자 행동을 6가지로 나누고, 각 행동에 따른 이벤트 발생 여부를 분석하였다. 특히 Word의 경우 Pdod와 UrlHash 값이 로그에 기록되어, 이를 기준으로 로그를 그룹화하여 하나의 문서 단위로 작업 이력을 추적할 수 있음을 나타내었다. 레지스트리의 File MRU 항목에 기록된 파일 열람 시각과 로그의 타임스탬프를 비교하여 특정 로그가 어떤 문서 파일에 해당되는지를

추적함에 따라서 문서 편집, 저장, 생성, 시점 등 정밀한 활동 내용을 복원할 수 있음을 알 수 있다.

III. 상세 경로

항목	경로
Office 진단 로그	C:₩Users₩<User>₩AppData₩Local₩Microsoft₩Office₩16.0₩Telemetry₩
임시 파일 (Office)	문서 저장 경로 또는 %AppData%₩Microsoft₩Word₩ 등
Shadow Copy / Volume Snapshot	삭제된 LNK, MRU, Prefetch가 백업본에 남아 있을 가능성

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. 사용자의 파일 작성, 생성 등의 구체적인 여부 등을 분석

위 논문에서 언급되었듯이 File MRU 이외에도 MS Word를 사용할때 주기적으로 생성되는 임시파일을 이용해서 문서 작업 이력을 추적할 수 있고, Ms Word내부에 생성되는 RSID라는 고유한 값을 이용하여 파일 이력을 추적하는 등 다양한 방법이 있다. Office 진단 로그에는 파일 이름, 경로, 내용 등을 포함하지 않는다는 점을 공격자가 이용하여 악성 행위를 하였을 때의 정보들을 진단 로그 에코드와 문서 파일을 연관시켜 사용자의 파일 작성, 생성 등의 구체적인 여부 등을 확인할 수 있다. 분석할 프로그램으로는 OneNote, OneDrive, Word, Excel 등이 있다.

V. 참고 문헌

[1] 임연재, 박정흠, 이상진,「Microsoft Office 진단 로그 분석 및 포렌식 활용 방안」, 디지털포렌식연구 제15권 제2호, 2021, pp. 24–34.

[논문 리뷰 보고서]

[Conversational AI forensics: A case study on ChatGPT, Gemini, Copilot, and Claude]

작성일	2025.05.26
작성자	정지윤
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	Conversational AI forensics: A case study on ChatGPT, Gemini, Copilot, and Claude
저자 및 연도	Kyungsuk Cho, Yunji Park, Jiyun Kim, Byeongjun Kim, Doowon Jeong (Forensic Science International: Digital Investigation 52, 2025)
출처	Forensic Science International: Digital Investigation, Vol. 52 (2025), Article 301855. DOI: 10.1016/j.fsidi.2024.301855
분석 대상 프로그램	ChatGPT, Gemini, Copilot, Claude
관련 아티팩트 유형	메신저 아티팩트, 시스템 설치/실행, 사용자 행위

[표 1. 논문 개요표]

II. 논문 요약

최근 급성장한 대화형 AI(ChatGPT, Gemini, Copilot, Claude)를 기술 유출, 피싱, 악성코드 생성 등에 악용할 수 있다는 점을 고려하여 각 플랫폼이 사용자 대화와 첨부 파일, 웹 검색 결과 등을 어떻게 저장·전송하는지 기본 구조에 대하여 조사하였다.

chat gpt에서는 웹 브라우저 캐시와 데스크톱 앱의 로컬 캐시, 모바일 앱의 SQLite 데이터베이스에서 대화 이력과 메타데이터를 확보할 수 있었고, Gemini는 MyActivity JSON 과 브라우저 캐시를 통해 대화 제목과 전송 시간, 이미지 생성 기록을 추출할 수 있었다. Copilot과 Claude도 각기 REST API 호출 기록이나 브라우저 쿠키·스크립트 스니핑을 통해 대화 로그를 복원할 수 있음을 알 수 있었다.

이 연구에 대한 시나리오로는 랜섬웨어 제작에 악용된 'jailbreak prompt'를 Gemini 대화 로그에서 확인한 사례가 있고, ChatGPT Mac 앱의 로컬 캐시에서 이미지 생성 기록을 복원해 저작권 분쟁 증거로 활용한 사례도 있다. 이 시나리오를 바탕으로 향후 실시간 수집 자동화 도구 개발이나 이상 행위 탐지 모델 연구로 확장할 수 있다.

III. 상세 경로

항목	경로
ChatGPT (데스크톱 앱 로컬 캐시)	C:%APPDATA%₩ChatGPT₩Cache\
ChatGPT (모바일 앱 SQLite DB)	/data/data/com.openai.chatgpt/databases/chat_history.db
Gemini (MyActivity JSON)	C:%USERPROFILE%₩AppData₩Local₩Google₩MyActivity₩MyActivity.json

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. 대화형 AI의 프롬포트를 사용한 아티팩트 분석

대화형 AI의 프롬포트를 분석하여 사용자가 고의로 삭제한 로그를 재구성하거나 타임라인 등을 분석하여 피의자의 혐의를 입증하기 위한 아티팩트를 찾을 수 있다. 또한, 악성코드 제작 의뢰 및 기밀 문서 유출에 대한 이상 행위 탐지 모델을 개발하여 후속 연구로서 아티팩트 자동 파싱 툴에 대한 계획을 세울 수 있다.

V. 참고 문헌

[1] Kyungsuk Cho, Yunji Park, Jiyun Kim, Byeongjun Kim, Doowon Jeong, 「Conversational AI forensics: A case study on ChatGPT, Gemini, Copilot, and Claude」, Forensic Science International: Digital Investigation, Vol. 52, 2025, Article 301855. DOI: 10.1016/j.fsidi.2024.301855

[논문 리뷰 보고서]

[Forensic investigation of Google Meet for memory and browser artifacts]

작성일	2025.05.26
작성자	강지민
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	Forensic investigation of Google Meet for memory and browser artifacts
저자 및 연도	Farkhund Iqbal, Zainab Khalid, Andrew Marrington, Babar Shah, Patrick C.K. Hung (2022)
출처	Forensic Science International: Digital Investigation, Vol. 43, 2022, Article ID 301448 https://doi.org/10.1016/j.fsidi.2022.301448
분석 대상 프로그램	Google Meet (Web 기반 화상회의 애플리케이션)
관련 아티팩트 유형	메모리 및 브라우저 기반 아티팩트: – 메모리: 미팅 기록, 채팅 메시지, 이메일 주소, 프로필 사진, 다운로드 파일, 캡션 기록 등 – 브라우저: 히스토리, 쿠키, 캐시, 다운로드 정보, IndexedDB, 세션 로그 등

[표 1. 논문 개요표]

II. 논문 요약

이 논문에서는 Google Meet이 웹 기반 애플리케이션으로서 기존 데스크톱 클라이언트에 비해 포렌식 분석이 어렵다는 문제를 해결하고자, Google Meet 사용 중 메모리와 브라우저에 남는 포렌식 아티팩트를

식별하고 분석하는 것과 메모리 아티팩트 추출을 자동화 하는 도구를 개발하는 것을 연구 목적으로 제시했다.

실험 결과, Windows 10과 Linux 환경에서 Chrome, Firefox, Edge 브라우저를 통해 다양한 테스트 활동을 수행한 후 메모리 덤프와 브라우저 데이터를 분석한 결과, 다음과 같은 주요 아티팩트(Artifact Classes)를 확인하였다:

특히, RAM 용량이 클수록(12GB) 더 많은 송수신 메시지와 메타데이터가 연속된 형태로 추출되는 경향을 보여 RAM 크기가 메모리 아티팩트의 지속성과 형식에 영향을 미친다는 사실을 실험적으로 입증하였다.

이를 통해 Google Meet이 회의 종료 후 데이터 저장을 하지 않는다는 보안 특성에도 불구하고, 메모리와 브라우저에는 다양한 아티팩트가 남아 수사에 활용 가능한 디지털 증거로 기능할 수 있음을 결론지었으며, Python 기반 자동 추출 도구를 개발하여 문자열 기반 수작업 분석을 자동화하였다.

연구는 Google Meet이 폐쇄형 애플리케이션이기 때문에 소스 코드 기반의 구조적 분석이 불가능하고, 문자열 기반 분석에 의존해야 했다는 한계를 가지며, 수신 메시지가 일부 상황에서 식별되지 않는 등 일부 아티팩트의 완전성 문제도 존재한다.

후속 연구로는 다른 운영체제(macOS, Android, iOS)에서의 Google Meet 아티팩트 분석 확장이 제안될 수 있다.

III. 상세 경로

항목	경로 또는 위치 예시
Google Meet 사용 흔적	메모리 내 .lnk 파일 (google meet.lnk), Chrome IndexedDB (https_meet.google.com_0.indexeddb.leveldb), Top Sites, Web Applications 폴더 등
미팅 기록	메모리 내 미팅 이름, 이메일, 디바이스 ID, 타임스탬프 (meeting name, email address, device ID, timestamp)
채팅 메시지	메모리 및 Chrome 세션 로그(Sessions) 내 <chatTextInput>, <textarea> 태그 포함 내용
다운로드 파일 정보	Jamboard에서 생성된 PDF/JPG 정보: 메모리 및 Chrome 캐시(Cache) 폴더 내 저장 경로, 파일 이름, 사이즈 등
상대방 이메일 주소	메모리에서 추출된 in-call 메시지 교환 상대의 이메일 주소(Correspondence), Web Data, Login Data SQLite DB
캡션 기록	메모리 내 closed captioning transcripts (일부 포맷 없음, 수동 문자열 추출 필요)

[표 2. 아티팩트별 상세 경로표]

IV. 방향성 제시

1. 악의적인 사용 가능성

    1) 메모리 및 브라우저에 남은 Google Meet 아티팩트 중, 개인 식별 정보(PII) 및 회의 중 민감 정보(이메일, 채팅 내용, 파일 링크 등)는 유출 또는 악용될 위험이 있다.

    2) 예를 들어, 메모리 덤프에서 회의 참가자 이메일이나 채팅 메시지를 추출하면 사칭, 피싱 공격, 회의 내용 유출 등에 사용될 수 있다.

    3) 시나리오 예시

    (1) 회의 링크 + 이메일 조합 → 무단 접속 가능

    (2) 채팅 메시지 + 시간 정보 → 발언 추적 및 조작 시도

    (3) 다운로드 경로 + 파일명 → 외부 악성 파일 유포 경로 추적

2. 아티팩트 자동 탐지 기능 개발

    1) 특정 시그니처(문자열 패턴)를 자동 탐색하고, 잠재적 악용 가능성이 높은 항목(예: 평문 이메일, 토큰, 삭제된 데이터 등)을 우선 추출하는 기능을 개발한다.

3. 웹 기반 회의 서비스 전체로의 확장성

    1) Google Meet뿐 아니라 Zoom, Microsoft Teams 등 웹 회의 도구에서 유사한 방식으로 아티팩트가 남는 경우가 많다.

2) 분석 도구는 브라우저별 구조(Chrome, Firefox 등)와 IndexedDB, Cache, 쿠키를 공통 포맷으로 처리할 수 있도록 설계할 수 있다.

3) 각 서비스별로 "회의 도청", "채팅 감청", "파일 경로 수집"과 같은 위협 시나리오를 사전에 구성하여 자동 분석이 가능하도록 확장할 수 있다.

IV. 참고 문헌

[1] Wang, X., Zhang, J., & Zhang, Y.,「An artifact-centric approach for digital evidence analysis in collaborative platforms」, *Forensic Science International: Digital Investigation*, Vol. 43, 2022,

[논문 리뷰 보고서]

[노션프로그램 아티팩트 분석을 통한 위협 분석 및 대응방안 제시]

작성일	2025.05.26
작성자	강지민
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	노션프로그램 아티팩트 분석을 통한 위협 분석 및 대응방안 제시
저자 및 연도	한주현, 손태식 (2024.6)
출처	Journal of Platform Technology, Vol. 12, No. 3, June 2024
분석 대상 프로그램	Notion (PC 및 Android 앱)
관련 아티팩트 유형	- 사용자 정보 : 이메일, 이름, ID, 프로필 사진, 계정 토큰 등 - 사용자 행위 : 블록 생성/수정/삭제 기록, 마지막 접근 시간, 업로드 파일 정보 등 - 모바일 캐시 : 이미지, HTTP 네트워크 캐시 등 - SharedPreferences 파일(XML) 기반 설정 및 토큰 정보

[표 1. 논문 개요표]

II. 논문 요약

이 논문에서는 협업 프로그램(Notion 등) 사용 증가에 따라 사용자 정보 및 작업 내용이 유출될 위험성이 크다는 문제를 해결하고자, PC 및 모바일(Android) 환경에서 Notion 프로그램의 아티팩트를 수집·분석하여 보안 위협을 식별하고 대응방안을 제시하는 것을 연구 목적으로 제시했다.

실험 결과, 사용자 이름, 이메일, 프로필 사진, 계정 토큰, 작성 문서, 댓글, 업로드 파일 등 다양한 민감 정보가 암호화되지 않은 상태로 저장되어 있었으며, 특히 PC 환경에서는 삭제된 블록도 복구 가능하고, 모바일 환경에서는 인증 토큰이 평문으로 저장되어 장기적인 악용 가능성이 있음을 확인하였다. 이로써 Notion 사용 시 사용자 정보와 작업 내용이 디지털 포렌식 관점에서 추적 및 분석 가능함과 동시에, 보안 취약점이

존재함을 실험적으로 입증하였다.

이를 통해 Notion과 같은 협업 프로그램이 내부 감사나 사고 대응 시 아티팩트 분석을 통한 행위 추적이 가능하다는 점에서 디지털 포렌식적 의의를 지님과 동시에, 데이터 보호 관점에서는 암호화되지 않은 저장 방식이 심각한 보안 위협이 될 수 있음을 시사하였다.

연구는 Notion 단일 프로그램만을 대상으로 하였고, 실제 공격 시나리오에 기반한 실증 실험이나 기타 협업 도구들과의 비교가 부족하다는 한계를 가지고 있으며, 후속 연구로는 다양한 협업 도구(Microsoft Teams, Slack 등)의 아티팩트 분석, 실질적인 위협 시뮬레이션, 자동화된 분석 도구 개발이 제안될 수 있다.

III. 상세 경로

구분	경로
PC 사용자 정보	C:₩Users₩{UserID}₩AppData₩Roaming₩Notion₩notion.db 테이블: notion_user, space
PC 사용자 행위	C:₩Users₩{UserID}₩AppData₩Roaming₩Notion₩notion.db 테이블: block, comment
모바일 사용자 정보	data/data/notion.id/shared_prefs/ 파일: signin.xml, appid.xml, measurement.prefs.xml data/data/notion.id/files/PersistedInstallation.json
모바일 사용자 행위	data/data/notion.id/databases/data/data/notion.id/cache/image_manager_disk_cache.../Webview/Default/HTTP Cache

[표 2. 아티팩트별 상세 경로표]

IV. 방향성 제시

1. 악의적인 사용 가능성

1) Notion의 notion.db, shared_prefs, cache 등 다양한 경로에 저장된 사용자 정보(이름, 이메일, 계정 토큰 등)와 작성 문서, 댓글, 첨부파일 경로는 유출 시 피해로 이어질 수 있다.
2) 평문 상태로 저장된 access token이나 로그인 이메일은 계정 탈취, 세션 하이재킹, 사칭 행위로 악용될 수 있다.
3) 시나리오 예시

(1) access token + 로그인 이메일 → 계정 탈취 및 무단 로그인
(2) 삭제된 블록 + 작성자 ID → 삭제된 민감 문서 복구 및 책임자 추적
(3) 댓글 내용 + 시간 정보 → 발언 시점 조작 및 특정 사용자 음해
(4) 업로드 파일 경로 + 파일명 → 외부 파일 접근 또는 악성 파일 심기
(5) 프로필 사진 URL + 이름 → SNS 사칭 계정 생성 및 피싱 공격

2. 아티팩트 자동 탐지 기능 개발

1) 디스크 이미지(E01 등) 내에서 추출된 아티팩트(Registry, Prefetch, USN 등)를 대상으로, 사전 정의된 문자열 시그니처와 구조 기반 조건을 활용하여 악용 가능성이 높은 항목을 자동 탐지하는 기능을 구현한다.

3. 협업 툴 및 유사 소프트웨어로의 확장성

1) 이 논문은 협업 툴 특화 포렌식 연구로, 단순 메시징 앱이 아닌 업무 관리 플랫폼(Notion) 내 사용자 행위 분석을 중점적으로 다룬다는 점에서 차별성이 있다.
2) 향후 Slack, Trello, Confluence 등 다른 협업 플랫폼으로의 확장 적용이 용이하며, 공동 작업 중 생성되는 블록 기반 아티팩트의 시간 흐름 분석, 사용자 간 상호작용 분석 기능으로 확장 가능하다.
3) 특히 삭제된 데이터 복원 및 시각화 기능은 실무 감사, 내부 유출 조사, 규정 위반 탐지 등 실제 조직 내 수요에 적합하다.

IV. 참고 문헌

[1] 한주현, 손태식, 「노션프로그램 아티팩트 분석을 통한 위협 분석 및 대응방안 제시」, *플랫폼기술저널* 제12권 제3호, 2024년 6월, pp.27-40,

[논문 리뷰 보고서]

[디지털 포렌식 관점의 네이버 밴드 사용자 행위 수집 및 분석 연구]

작성일	2025.05.26
작성자	강지민
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	디지털 포렌식 관점의 네이버 밴드 사용자 행위 수집 및 분석 연구
저자 및 연도	안원석, 박명서 (2024.12)
출처	정보보호학회논문지, Vol. 34, No. 6, Dec. 2024 DOI: https://doi.org/10.13089/JKIISC.2024.34.6.1263
분석 대상 프로그램	네이버 밴드 (Naver Band, Android 환경)
관련 아티팩트 유형	- 사용자 정보: 사용자 번호, 프로필 이름, 성별, 나이, access token 등 - 채팅 기록: 송수신 메시지, 채널 ID, 메시지 상태, 삭제 여부 등 - 밴드 정보: 가입한 밴드 ID, 숨겨진 밴드 식별 정보 - 미디어 캐시: 이미지/동영상 파일 캐시 - 공유 파일: 공유 폴더 및 파일 메타정보 - API 정보: 요청 API를 통한 게시글, 미디어, 초대 링크 등 원격 데이터

[표 1. 논문 개요표]

II. 논문 요약

이 논문에서는 국내 이용자가 많은 폐쇄형 SNS인 네이버 밴드에서의 악성 행위(불법 촬영물 유포, 마약 거래 등)가 증가하고 있음에도 불구하고 관련 디지털 포렌식 연구가 부족하다는 문제를 해결하고자, 안드로이드 환경에서 네이버 밴드 애플리케이션의 로컬 아티팩트를 분석하고, API 재구성을 통해 포렌식 정보 수집을 확장하는 것을 연구 목적으로 제시했다.

실험 결과, /data 및 /shared_prefs, /cache 경로에서 사용자 정보(access_token, user_no, 성별, 나이 등), 채팅 기록(chat_message, channel_user 등), 밴드 정보(member 테이블, band_no 등), 이미지 및 동영상 캐시 등을 포함하는 다양한 로컬 아티팩트를 식별할 수 있었으며, 특히 삭제된 채팅(status = "RECLAIM") 또는 숨겨진 밴드 정보도 확인 가능함을 입증했다. 또한, Frida 후킹 기법을 이용한 API 재구성을 통해 서버 기반의 게시글, 미디어 파일, 가입 밴드 리스트, 초대 URL 등도 추가로 획득 가능함을 확인하였다.

이를 통해, 로컬 아티팩트 분석과 API 재구성의 병행을 통해 네이버 밴드 내 사용자 행위에 대한 디지털 포렌식 수집이 가능하며, 이는 폐쇄형 SNS 환경에서의 범죄 수사 및 내부 감사에 효과적으로 활용될 수 있음을 결론지었다.

연구는 로그아웃 시 사용자 관련 데이터가 완전히 삭제되는 등 로컬 데이터 보존이 제한적이며, 분석 대상이 안드로이드 앱에 한정되었다는 한계를 가지고 있으며, 후속 연구로는 PC 환경에서의 네이버 밴드 클라이언트 분석 및 로그아웃 후에도 데이터 확보가 가능한 포렌식 기법 개발이 제안될 수 있다.

III. 상세 경로

구분	경로 또는 API 위치
로컬 아티팩트 - 데이터 영역	/data/data/com.nhn.android.band/database/
	/data/data/com.nhn.android.band/database/member
	/data/data/com.nhn.android.band/shared_prefs/USER.xml
로컬 아티팩트 - 사용자 영역	/sdcard/Android/data/com.nhn.android.band/cache/IMAGE, /VIDEO
요청 API 기반 아티팩트	/v2.0.0/get_profile
	/v2.0.0/get_my_bands_for_search
	/v2.0.0/get_posts, /v2.0.0/get_posts_item
	/v2.0.0/get_photos, /v2.0.0/get_photo_videos
	/v2.0.1/get_files, /v2.0.0/get_folders, /v1.1/get_file_url
	/v1.0.0/get_file_url_by_message, /v1.1.0/get_video_url_by_message, /v1/chat/get_audio_url

[표 2. 아티팩트별 상세 경로표]

IV. 방향성 제시

1. 악의적인 사용 가능성

1) 네이버 밴드의 로컬 저장소(DB, SharedPreferences, Cache 등)에 저장된 사용자 번호, 채팅 메시지, 밴드 가입 정보, 이미지/동영상 캐시 등은 공격자에 의해 신원 도용, 불법 촬영물 유포, 대화 조작, 내부 자료 유출 등으로 악용될 수 있다.
2) 밴드 내 채팅 메시지, 밴드 ID(band_no), 사용자 번호(user_no), 이미지/동영상 캐시 등은 불법 거래 정황의 추적, 공범 간 대화 확인, 거래 증거 확보에 핵심적인 역할을 한다.
3) 삭제된 메시지 상태(status = "RECLAIM"), 숨겨진 밴드 비교(band_no 매칭) 등을 통해 사용자가 감추려 한 흔적까지 복원 가능하며, 이는 수사상 매우 중요한 단서가 될 수 있다.
4) 시나리오 예시
    (1) 사용자 신원 추적 및 정보 탈취
    (2) 삭제·은닉 정보 복원 및 조작
    (3) 불법 콘텐츠 유포 및 정황 분석
    (4) 불법 거래 정황 확인

2. 아티팩트 자동 탐지 기능 개발

1) Android 디바이스 이미지 내 /data/data/..., /sdcard/Android/data/... 경로에서 메시지 DB, 설정 XML, 캐시 이미지 등을 자동 탐색하여 디지털 포렌식 아티팩트를 분류·정리하는 기능을 개발한다.

3. 폐쇄형 SNS 및 유사 소프트웨어로의 확장성

1) 분석 대상인 네이버 밴드는 폐쇄형 구조로 운영되는 국내 특화 SNS로, Telegram, KakaoTalk, Band.us, LINE 등 유사한 앱에서도 유사한 방식의 사용자 활동 아티팩트가 생성됨.

2) 본 연구 및 분석 구조는 향후 다양한 폐쇄형 SNS 환경에도 적용 가능하며 메시지 구조 및 DB 패턴 분석, 사용자 권한 및 밴드(그룹) 정보 분석, API 요청 패턴 재구성 등으로 기능 확장이 가능하다.

IV. 참고 문헌

[1] 신수민, 박은후, 김소람, 김종성,「디지털 포렌식 관점에서의 Slack 및 Discord 메신저 아티팩트 분석」, 디지털콘텐츠학회논문지 제21권 제4호, 2020.4, pp. 799-809.

[논문 리뷰 보고서]

[원격 제어용 어플리케이션에서의 아티팩트 수집 및 분석]

작성일	2025.05.26
작성자	강지민
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	원격 제어용 어플리케이션에서의 아티팩트 수집 및 분석
저자 및 연도	박현재, 손태식 (2024.3)
출처	디지털포렌식연구, 제18권 제1호, DOI: 10.22798/kdfs.2024.18.1.46
분석 대상 프로그램	TeamViewer (QuickSupport), AnyDesk, AirDroid (모두 Android 환경)
관련 아티팩트 유형	원격 제어 로그 (TVLog.html), 전송된 파일 기록, 로그인 계정 및 닉네임, 앱 권한 설정 정보, 설치 앱 목록, 원격 요청된 권한 내역, 스크린샷 요청 여부, 디바이스 내 파일 인덱스 및 타임스탬프, 메시지 송수신 기록 등

[표 1. 논문 개요표]

II. 논문 요약

이 논문에서는 TeamViewer, AnyDesk, AirDroid와 같은 원격 제어 애플리케이션이 보이스피싱 범죄에 악용되고 있음에도 불구하고,

안드로이드 기반 포렌식 연구가 매우 부족하다는 문제를 해결하고자, 이들 앱에서 수집 가능한 디지털 아티팩트를 식별하고 수사에 활용 가능한 정보를 분석하는 것을 연구 목적으로 제시했다.

실험 결과, 각 앱의 /data/data/ 경로에서 다양한 파일과 로그를 확보할 수 있었으며, 특히 TeamViewer에서는 TVLog.html을 통해 제어자의 ID, 작업 로그, 파일 전송 기록, 스크린샷 요청 여부를, AirDroid에서는 계정 정보(account_backup), 전송 파일 기록(transfer.db), 설정 권한(main_preference_bk) 등 총 6개 이상의 아티팩트 경로에서 실질적인 포렌식 증거를 확보할 수 있었다. AnyDesk는 상대적으로 아티팩트가 적고 단일 파일 전송 기록만을 확인 가능했다.

이를 통해 원격 제어 앱이 범죄에 사용된 경우, 제어자의 로그인 정보, 전송 파일, 권한 요청 내역 등의 분석을 통해 사건 정황과 범인을 특정할 수 있는 실질적인 단서를 확보할 수 있음을 입증하였으며, 이는 디지털 포렌식 수사에서 해당 앱의 아티팩트가 중요한 증거로 기능할 수 있음을 시사한다.

연구는 제어자 IP 정보 확보가 어렵고, 실시간 네트워크 프로토콜 분석이 이루어지지 못했다는 한계를 가지며, 후속 연구로는 네트워크 레벨의 패킷 분석과 실시간 원격 제어 상황에서의 로그 및 데이터 흐름에 대한

추적 기법 개발이 제안될 수 있다.

III. 상세 경로

구분	경로
권한 설정 정보	data/com.teamviewer.quicksupport.market/sharedprefs/com.teamviewer.quicksupport.market_preferences.xml
사용자 설정 정보 (SUID 등)	data/com.teamviewer.quicksupport.market/files/client.conf
원격 제어 로그 (시작~종료, 제어자 ID, 스크린샷, 파일 전송 등)	data/com.teamviewer.quicksupport.market/files/TVLog.html

[표 2. 아티팩트별 상세 경로표: TeamViewer]

구분	경로
원격 전송 파일 저장 경로	data/com.com.anydesk.anydeskandroid/files/downloads/[timestamp]/[filename]

[표 3.. 아티팩트별 상세 경로표: AnyDesk]

구분	경로
로그인 계정 닉네임, ID	data/com.sand.airdroid/files/account_backup

로그인 계정 상세 정보	data/com.sand.airdroid/files/account_preference
권한 요청 내역 및 세부 설정	data/com.sand.airdroid/files/main_preference_bk
디바이스 내 파일 인덱스	data/com.sand.airdroid/files/recursive_file_index_phone
설치 앱 목록, 메시지 송수신, 이벤트 기록 (DB)	data/com.sand.airdroid/databases/app.db
파일 전송 목록, 파일명·크기·PID 등 (DB)	data/com.sand.airdroid/databases/transfer.db
계정 권한 설정 (화면 미러링, 알림, 마이크 등)	data/com.sand.airdroid/shared_prefs/com.sand.airdroid_preference.xml

[표 4.. 아티팩트별 상세 경로표: AirDroid]

IV. 방향성 제시

1. 악의적인 사용 가능성

1) TeamViewer, AirDroid, AnyDesk 등 원격 제어 앱에서는 사용자의 접속 기록, 계정 정보, 전송된 파일 목록, 권한 요청 내역 등이 로컬에 저장되며, 이는 공격자에게 감청, 무단 제어, 내부 자료 탈취 등 악용 수단이 될 수 있다.

2) TVLog.html, transfer.db, account_preference 등에서 추출한 정보는 실제 원격 제어 중 수행된 행위 복원, 사용자 사칭, 전송 파일 분석을 통한 추가 공격 등에 사용될 수 있다.

3) 시나리오 예시

(1) TVLog.html + 접속 시간 → 사용자의 원격 제어 흔적 감시

(2) 전송 파일 목록 + 파일명 → 악성 파일 유포 경로 확인

(3) access_token + 계정 이메일 → 사용자 세션 탈취 및 감청

(4) 권한 설정 정보 + 요청 내역 → 화면 공유·마이크 도청 여부 분석

(5) 메시지 전송 로그 + 수신자 → 사칭 메시지 발송을 통한 피싱 시도

(6) 디바이스 파일 목록 + 전송 로그 → 민감 파일 복사 여부 추적

2. 아티팩트 자동 탐지 기능 개발

1) /data, /shared_prefs, 로그 파일 등에 흩어진 아티팩트를 자동 탐색하여 사용자 계정 정보, 접속 기록, 전송 파일 메타데이터, 권한 설정 내역 등을 자동 추출하는 기능을 구현한다.

2) 추출된 항목 중 민감 정보(e.g., access_token, 계정 ID, 닉네임) 또는 원격 요청 이력(e.g., 스크린샷 요청, 파일 접근 허용)은 우선 표시하고, 위험도에 따라 등급화(Risk Level)한다.

3. 원격 제어 앱 및 유사 소프트웨어로의 확장성

1) TeamViewer, AirDroid, AnyDesk 외에도 다양한 원격 제어 앱(e.g., Chrome Remote Desktop, VNC Viewer, Splashtop 등)에서 유사한 방식의 아티팩트가 생성된다.

2) 따라서 본 분석 방식은 로컬 설정 파일, 세션 로그, 전송 기록을 기반으로 한 통합 분석 도구로 확장 가능하며, 다양한 앱 구조에 대응 가능한 모듈 설계, 원격 접속 이벤트 기반 타임라인 분석, 전송 파일 위험도 판별 기능 등으로 발전시킬 수 있다.

IV. 참고 문헌

[1] 김동현, 김종성, 박은후, 「디지털 포렌식 관점에서의 원격 제어 애플리케이션 아티팩트 분석」, 디지털콘텐츠학회논문지, 제21권 제1호, 2020.1, pp. 135-144.

[논문 리뷰 보고서]

[메신저형 협업툴 어플리케이션 아티팩트 분석

- ChannelTalk을 중심으로]

작성일	2025.05.26
작성자	김신아
검토자	김예은

목차

Ⅰ. 개요

항목	내용
논문 제목	메신저형 협업툴 어플리케이션 아티팩트 분석 - ChannelTalk을 중심으로
저자 및 연도	홍리나(아주대) , 손태식(아주대) / 2024.03
출처	디지털 포렌식 연구 제18권 제1호 (p.79-96)
분석 대상 프로그램	ChannelTalk
관련 아티팩트 유형	메신저, 네트워크, 사용자 행위, 시스템 설치/실행

[표1. 논문 개요]

Ⅱ. 논문 요약

1. 논문 요약

이 논문에서는 어플리케이션 아티팩트 분석을 통해 보안 사고 발생 시 증거 수집의 중요성을 해결하고자 모바일 환경에서의 사용자 행위 및 사용 내역 분석을 통해, 기업 내부 정보 유출 및 개인정보 보호 침해와 같은 문제를 해결하는 것을 목표로 하였습니다.

실험 결과, 사용자 계정 정보, 채팅 기록, 파일 공유 기록이 중요한 증거 자료로 활용될 수 있음을 보여주었으며, 특히 팀 메신저와 같은 도구는 공격자에게 필요한 정보를 직관적으로 제공할 수 있다는 점에서 주의가 필요하다는 사실을 확인하였습니다. 이러한 아티팩트들은 기업의 내부 정보가 오고갈 가능성이 높다는 점에서, 보안 사고 발생 시 중요한 증거 수집의 기초가 될 수 있음을 입증하였습니다.

연구는 루팅된 Android 9 버전의 Galaxy Note 8을 사용하여 아티팩트

분석을 수행하였으며, 이는 특정 환경에 국한된 결과를 초래할 수 있다는 한계를 가지고 있었으며, 인터넷 연결이 없는 상태에서의 데이터 분석이 불가능하다는 점은 연구의 한계로 제시되었습니다.

후속 연구로는 다양한 모바일 환경과 인터넷 연결이 없는 상태에서도 접근 가능한 데이터에 대한 분석을 포함하여, 보다 포괄적인 아티팩트 분석이 이루어져야 합니다. 다양한 협업 툴과의 비교 분석을 통해 보안 취약점을 더욱 심층적으로 이해할 필요가 있습니다.

2. 주요 아티팩트 분석 내용

Path	찾을 수 있는 정보
com.zoyi.channel.desk.android.databases	사용자 계정, 채팅 등 데이터베이스
com.zoyi.channel.desk.android.cache.channel	채팅방 내에서 수/발신된 사진 캐시
com.zoyi.channel.desk.android.cache.image_cache	사용자 프로필 캐시 데이터
com.zoyi.channel.desk.android.cache.WebView.Defaul.HTTPCache	접근한 URL 관련 데이터
com.zoyi.channel.desk.android.shared_prefs	XML 형식의 파일로 사용자 설정, 환경 설정 및 간단한 데이터를 저장

[표2. 주요 경로별 수집 가능한 아티팩트 정보]

Ⅲ. 방향성

1. 채팅 로그, 첨부파일, 접속 이력 등 메신저 및 시스템 아티팩트를 중심으로 분석 진행
2. 유출 정황, 외부 접속 시도, 실행 기록 등을 포렌식적으로 재구성
3. 채팅 추출, MAC 타임 분석, 이상 접속 탐지를 지원하는 자동화 도구 개발

Ⅳ. 참고 문헌

[1] 홍리나, 손태식 「메신저형 협업툴 어플리케이션 아티팩트 분석 - ChannelTalk을 중심으로」디지털포렌식연구, 18(1), 2024, 79-96

[논문 리뷰 보고서]

[익명 커뮤니티 어플리케이션에서의 아티팩트 수집 및 분석]

작성일	2025.05.26
작성자	김신아
검토자	김예은

목차

Ⅰ. 개요

항목	내용
논문 제목	익명 커뮤니티 어플리케이션에서의 아티팩트 수집 및 분석
저자 및 연도	최재민(아주대), 손태식(아주대) / 2023.06
출처	디지털 포렌식 연구 제17권 제 2호 (p.45-61)
분석 대상 프로그램	익명 커뮤니티 어플리케이션(에브리타임, 디시인사이드, 네이트판)
관련 아티팩트 유형	메신저, 네트워크, 시스템 설치/실행, 사용자 행위,

[표1. 논문 개요]

Ⅱ. 논문 요약

1. 논문 요약

이 논문에서는 익명 커뮤니티에서 발생하는 범죄에 대한 수사적 접근의 필요성을 문제로 삼고, 이를 해결하고자 익명 커뮤니티 아티팩트를 수집 및 분석하는 연구 목적을 제시했습니다.

연구 결과, 익명 커뮤니티에서 수집된 아티팩트는 범죄 수사에 유의미한 단서를 제공할 수 있음을 보여주었습니다. 예를 들어, 댓글 목록, 게시물 제목, URL, 댓글 작성 시각 등의 데이터가 수집되었으며, 이를 통해 기존 연구에서 수집되지 않은 다양한 아티팩트를 발견할 수 있었습니다. 또한, 네트워크 분석을 통해 클라우드와의 통신 패킷을 분석하여 추가적인 정보를 확보할 수 있었습니다.

본 연구는 익명 커뮤니티에서의 디지털 포렌식 분석이 범죄 수사에 실질적인 기여를 할 수 있음을 입증하였습니다. 이는 향후 범죄 예방 및 수사 전략 수립에 중요한 기초 자료로 활용될 수 있으며, 익명 커뮤니티의 특성을 고려한 새로운 수사 접근법을 제시함으로써 범죄 수사 분야에

기여할 수 있는 가능성을 보여줍니다.

특정 커뮤니티에 국한되어 있으며, 다양한 커뮤니티를 포함하지 못한 점이 한계로 지적될 수 있으며, 수집된 데이터의 해석에 있어 주관적인 요소가 개입될 가능성이 있으며, 이는 결과의 신뢰성에 영향을 미칠 수 있다고 보여집니다.

향후 연구에서는 다양한 온라인 익명 커뮤니티를 포함하여 보다 포괄적인 데이터 수집이 필요합니다. 수집된 아티팩트의 분석 방법론을 더욱 정교화하고, 다양한 범죄 유형에 대한 맞춤형 접근법을 개발하는 것이 중요합니다.

Ⅲ. 방향성

1. 웹/클라이언트 아티팩트 수집.분석 , 사용자 활동 패턴 분석

Ⅳ. 참고 문헌

[1] 최재민, 손태식「익명 커뮤니티 어플리케이션에서의 아티팩트 수집 및 분석」디지털포렌식연구, 17(2), 2023, 45-61.

[논문 리뷰 보고서]

[포렌식 관점에서의 Element 인스턴트 메신저 아티팩트 분석]

작성일	2025.05.26
작성자	김신아
검토자	김예은

목차

Ⅰ. 개요

항목	내용
논문 제목	포렌식 관점에서의 Element 인스턴트 메신저 아티팩트 분석
저자 및 연도	조재민(고려대), 변현수, 윤희서, 서승희, 이창훈(과기대)
출처	정보보호학회논문지 제32권 제 6호 (p.1,113-1,120)
분석 대상 프로그램	Element
관련 아티팩트 유형	메신저, 네트워크,메모리, 사용자 행위

[표1. 논문 개요]

Ⅱ. 논문 요약

1. 논문 요약

이 논문에서는 사이버 범죄, 특히 피싱 범죄의 증가 문제를 해결하고자 디지털 포렌식 관점에서 보안 메신저와 관련된 데이터 분석을 통해 사이버 범죄의 예방 및 대응 방안을 모색하는 연구 목적을 제시하였습니다.

실험 결과, 보안 메신저 앱인 Signal, Wickr, Threema의 암호화 메커니즘을 역공학을 통해 분석하였으며, 이를 통해 암호화된 정보의 복호화 방법을 제시하였습니다. 또한, Element와 같은 matrix 프로토콜을 사용하는 애플리케이션에 대한 포렌식 분석이 이루어졌으나, 암호화된 채팅 기록에 대한 평문 복구 방안은 제시되지 않았습니다.

이를 통해 사이버 범죄의 증가에 대한 경각심을 일깨우고, 보안 메신저의 암호화 메커니즘에 대한 이해를 높이며, 향후 연구 방향을 제시하는 데 기여하고 있습니다.

연구는 특정 보안 메신저 앱에 대한 분석에 국한되어 있으며, 다양한

플랫폼에 대한 포괄적인 분석이 부족하다는 한계를 가지고 있습니다. 또한, 암호화된 채팅 기록의 평문 복구 방안이 제시되지 않은 점은 연구의 한계로 지적될 수 있습니다.

후속 연구로는 다양한 보안 메신저 플랫폼에 대한 포괄적인 분석을 수행하고, 암호화된 데이터의 복호화 방법에 대한 연구를 심화시켜야 할 필요가 있으며, 사이버 범죄 예방을 위한 정책적 제안도 함께 고려해야 할 것입니다.

2. 논문 상세 경로

    1) Element 보안 채팅은 메시지 내용, 전송자, 전송 시각, 채팅방 ID 등이 C:₩Users₩user₩AppData₩Roaming₩Element₩EventStore 하위에 Events.db 파일에 저장되어있어, Events.db 파일의 암호화 프로세스를 분석하고 복호화 키를 찾는 방안을 연구함

Ⅲ. 방향성

1. 메타데이터, 비암호화 메타 정보중심 분석
2. 보안 기능 우회를 고려한 키 추출 및 메시지 해석 자동화 도구 개발

Ⅳ. 참고 문헌

[1] 조재민, 변현수, 윤희서, 서승희, 이창훈「포렌식 관점에서의 Element 인스턴트 메신저 아티팩트 분석」정보보호학회논문지, 32(6), 2022, 1113-1120.

[논문 리뷰 보고서]

[안드로이드 환경에서의 지도 애플리케이션 아티팩트 분석 및 복호화 방안 연구]

작성일	2025.05.26
작성자	김예은
검토자	김신아

목차

I. 개요

항목	내용
논문 제목	안드로이드 환경에서의 지도 애플리케이션 아티팩트 분석 및 복호화 방안 연구
저자 및 연도	(박귀은, 강수진, 김종성 , 2022)
출처	한국디지털포렌학회/https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE11083157
분석 대상 프로그램	네이버 지도, TMAP, 카카오 맵
관련 아티팩트 유형	위치, 이동 경로, 검색 기록 / 사용자 행위 중심 아티팩트

[표 1. 논문 개요표]

II. 논문 요약

이 논문에서는 디지털 포렌식 수사 관점에서 사용자 위치 추정에 활용하기 위해 지도 애플리케이션 아티팩트의 분석을 진행했다.

〈Table 2〉 Analysis result

Data type		Naver map	TMAP	Kakao map
Data encryption		O	X	X
Search history		*	O	O
Uesr information		O	O	O
Location	User's location	O	O	X
	Map location	O	X	O
Bookmark information		*	O	O
Home/Office information		X	O	O
Image	User confirmation	O	X	O
	User's subway screen	X	X	O

O : Plain data
X : Not exist
*: Encrypted data

[그림 1. 주요 분석 결과]

연구 결과 암호화 된 데이터 복호화 및 검색기록, 시간 등 아티팩트 분석 결과 사용자의 실시간 위치를 기반으로 생성되는 아티팩트는 디지털 포렌식 관점에서 활용 가치가 높아 수사에 지도 애플리케이션의 데이터를 활용할 수

있을 것이다는 결론을 도출하였다.

이 연구는 지도 애플리케이션에 분석된 결과의 범위는 한정적이고 아티팩트가 변경되거나 애플리케이션마다 저장되는 데이터의 형태가 다양하다는 한계 를 가지고 있으며, 후속 연구로 지도 애플리케이션에 저장되는 데이터를 활용하기 위해 최신 버전에서의 데이터 수집 방안 및 식별하는 연구의 필요가 제안될 수 있다.

III. 상세 경로

항목	경로
사용자 행위 아티팩트	databases 디렉토리 내 .db 형식으로 존재
	shared_prefs 디렉토리 내 .xml 형식으로 존재

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. 위치 인증 관련 악의적인 사용 탐지

위치 인증이 필요한 서비스(ex 출퇴근 인증, 배달)에서 GPS 데이터를 변조하여 허위 위치 정보를 제공하는 경우 GPS 로그파일, 위치 기록 캐시 등을 기반으로 위치 변동 패턴을 분석해 위치가 비약적으로 변동하는 경우 악의적인 사용을 탐지할 수 있다.

V. 참고 문헌

[1] 박귀은, 강수진, 김종성,「 안드로이드 환경에서의 지도 애플리케이션 아티팩트 분석 및 복호화 방안 연구」, 디지털 포렌식 연구 제 16권 제2호, 2022.06, 163-184

[논문 리뷰 보고서]

[안드로이드 환경에서의 Telegram X 메신저 아티팩트 분석]

작성일	2025.05.26
작성자	김예은
검토자	김신아

목차

I. 개요

항목	내용
논문 제목	안드로이드 환경에서의 Telegram X 메신저 아티팩트 분석
저자 및 연도	(김정민, 정병찬, 이상진, 박정흠, 2022)
출처	한국디지털포렌학회/https://www.scribd.com/document/774260539/1-%EC%95%88%EB%93%9C%EB%A1%9C%EC%9D%B4%EB%93%9C-%ED%99%98%EA%B2%BD%EC%97%90%EC%84%9C%EC%9D%98-Telegram-X-%EB%A9%94%EC%8B%A0%EC%A0%80-%EC%95%84%ED%8B%B0%ED%8C%A9%ED%8A%B8-%EB%B6%84%EC%84%9D
분석 대상 프로그램	Telegram X
관련 아티팩트 유형	연락처 정보, 채팅 메시지 기록, 삭제된 메시지 정보

[표 1. 논문 개요표]

II. 논문 요약

이 논문에서는 기존 메신저를 커스터마이징하여 개발된 Telegram X 메신저의 아티팩트를 분석하여 디지털 포렌식 수사에 활용할 수 있는 방법을 제시했다. 연구 목적은 안드로이드 환경에서 Telegram X 사용 시 생성되는 다양한 아티팩트를 수집하고, 삭제된 메시지를 복구하여 사용자 행위를 재구성하는 자동화 도구를 개발하는 것에 있다.

연구 결과, Telegram X의 일반 채팅, 그룹 채팅, 비밀 채팅 등 다양한 메시지 유형과 음성/영상통화 로그를 분석하여 WAL 파일을 통해 삭제된 메시지의 복구 가능성을 확인하였다. 이를 통해 사용자 연락처 및 메시지 데이터를 자동화 도구를 통해 SQLite와 CSV로 재구성할 수 있음을 도출하였다.

이 연구는 Telegram X와 같은 커스터마이징 메신저가 기존 메신저와 데이터 저장 구조가 달라 분석이 어려운 한계를 가지며, 후속 연구로 다양한 커스터마이징 메신저에 대한 포렌식 기법 연구가 제안될 수 있다.

III. 상세 경로

항목	경로
사용자 행위 아티팩트	/data/data/org.thunderdog.challegram/files/tdlib
메신저 아티팩트	/media/0/Android/data/org.thunderdog.challegram/files

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. 위치 인증 관련 악의적인 사용 탐지

본 논문에서는 Telegram X와 같은 커스터마이징 메신저의 아티팩트를 분석하여 삭제된 메시지 복구와 사용자 행위 재구성 가능성을 확인했다. 이를 바탕으로 우리는 악용 가능성이 있는 커스터마이징 메신저나 프로그램에서 정상 사용과 악용 상황을 구분할 수 있는 아티팩트 분석 기법을 연구할 수 있을 것으로 생각된다.

Telegram X의 WAL 파일을 복호화하여 삭제된 메시지의 흔적을 복구할 수 있던 것처럼 메신저의 WAL, SQLite 등을 분석하여 메시지 삭제, 수정 시 데이터 변화를 추적하는 방향성을 제시한다.

2. 정상 메시지 전송과 악성 메시지 전송 아티팩트 차이 분석

같은 메신저 애플리케이션의 채팅 기능에서 정상 메시지를 전송했을 때 남는 아티팩트와 악성 URL 전송 시 남는 아티팩트의 차이가 있다면 이를

분석하고 자동화로 탐지하는 연구를 추진 해볼 수 있을 것 같다.

V. 참고 문헌

[1] 김정민, 정병찬, 이상진, 박정흠,「 안드로이드 환경에서의 Telegram X 메신저 아티팩트 분석」, 디지털 포렌식 연구 제 16권 제4호, 2022.12, 2-14

[논문 리뷰 보고서]

[해외 직구 애플리케이션의 아티팩트 수집 및 분석]

작성일	2025.05.26
작성자	김예은
검토자	김신아

목차

I. 개요

항목	내용
논문 제목	해외 직구 애플리케이션의 아티팩트 수집 및 분석
저자 및 연도	(김송희, 손태식 , 2024)
출처	한국디지털포렌학회/https://www-dbpia-co-kr-ssl.access.inu.ac.kr/journal/articleDetail?nodeId=NODE11847671
분석 대상 프로그램	알리 익스프레스, 테무
관련 아티팩트 유형	국적, 장바구니 내역, 로그인 수단, 개인통관 고유부호, 카드번호 등

[표 1. 논문 개요표]

II. 논문 요약

이 논문에서는 해외 직구 애플리케이션에 대한 급증한 수요로 인해 증가하는 개인통관고부호와 같은 개인정보의 유출을 해결하고자 해외 직구 애플리케이션의 아티팩트 수집 및 분석을 진행했다. 아티팩트 분석을 통해 얻은 정보는 범죄자의 행위를 식별하는데 도움이 되거나 범죄자의 위치를 판별하는데 기여할 수 있기 때문이다.

연구 결과, 알리 익스프레스와 테무 간 수집하는 개인정보의 범위와 종류에 차이가 있다는 정보를 얻을 수 있었다. 이를 통해 해외 직구 플랫폼에서 수집되는 개인정보가 많을수록 유출 시 피해 규모가 커질 수 있으며, 알리 익스프레스와 같은 애플리케이션의 경우 데이터 보호 대책이 미흡하여 개인정보 침해 위험이 높다는 결론을 도출하였다. 반면, 테무는 수집하는 정보량이 적어 상대적으로 개인정보 보호 측면에서 안전하지만, 사용자 활동 파악에 필요한 데이터가 적어 디지털 포렌식 분석에 한계가 있다는 의의를 도출하였다.

연구는 안드로이드 5 버전에서 수행되어 최신 버전(Android 12 이후)의 환경에서는 분석 결과가 상이할 가능성이 있으며, iOS 플랫폼의 경우 탈옥 상태에서만 데이터 접근이 가능하여 iOS 디바이스에서의 아티팩트 분석이 어려운 한계를 가지고 있다. 또한, 해외 직구 플랫폼의 본사가 해외에 위치하여 국내 개인정보보호법의 적용을 받지 않는 문제도 있다. 후속 연구로 다양한 해외 직구 애플리케이션의 아티팩트 비교 분석, 최신 안드로이드 및 iOS 버전에서의 데이터 수집 특성 연구, 국내외 법률의 공조를 통한 데이터 보호 체계 구축 방안이 제안될 수 있다.

III. 상세 경로

항목	경로
네트워크 아티팩트	com.alibaba.aliexpresshd₩databases₩cache.db
사용자 개인 정보	com.alibaba.aliexpresshd₩files₩DAI₩Database₩dege_compute.db
메신저 아티팩트	com.alibaba.iAliexpress₩Library₩Preferences

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. 개인정보 악용 가능성 탐지

개인통관고유부호와 연계된 구매 기록, 배송 주소 등을 분석하여 개인통관고유부호를 악용하여 타인의 명의를 도용해 물품을 구매하거나 불법 밀수입에 사용하는 행위를 탐지하거나 GPS데이터로 위치 조작 여부를 탐지할 수 있을 것 같다.

2. 정상 구매와 명의 도용 구매 아티팩트 차이 분석

정상구매와 명의도용구매를 비교했을 때 남는 아티팩트의 차이가 있다면 이를 분석하고 자동화로 탐지하는 연구를 추진 해볼 수 있을 것 같다. 또한 배송 패턴을 분석해 악용 가능성을 탐지하는 방법도 고려해볼수 있을 것 같다.

V. 참고 문헌

[1] 김송희, 손태식,「 해외 직구 애플리케이션의 아티팩트 수집 및 분석 」, 디지털 포렌식 연구 제 18권 제2호, 2024.06, 22-35

[논문 리뷰 보고서]

[디지털 상호작용 디코딩: Windows 및 Android 플랫폼에서 TeamViewer의 포렌식 아티팩트에 대한 광범위한 연구]

작성일	2025.05.26
작성자	배영혜
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	Decoding digital interactions: An extensive study of TeamViewer's Forensic Artifacts across Windows and android platforms
저자 및 연도	Nishchal Soni, Manpreet Kaur, Khalid Aziz (2024)
출처	Forensic Science International: Digital Investigation 51 301838 https://doi.org/10.1016/j.fsidi.2024.301838
분석 대상 프로그램	TeamViewer
관련 아티팩트 유형	레지스트리, 메모리 덤프, 세션 로그, 파일 전송 기록, 디스크 아티팩트

[표 1. 논문 개요표]

II. 논문 요약

이 논문은 원격 제어 프로그램인 TeamViewer의 포렌식 분석을 통해 윈도우 및 안드로이드 플랫폼에서 생성되는 다양한 아티팩트를 식별하고, 이를 통해 사이버 범죄 분석 및 디지털 증거 수집에 활용할 수 있는 방법을 제시한다.

원격 관리 및 제어 소프트웨어로 널리 사용되는 TeamViewer가 사이버 범죄에 악용되는 문제를 해결하고자 Windows 및 Android 환경에서 TeamViewer 사용 시 생성되는 다양한 시나리오를 실험하여, 프로그램이 남기는 디지털 아티팩트를 체계적으로 수집·분석하였다. 실험 결과, TeamViewer의 설치 및 실행 과정에서 다양한 위치에 증거가 남는다는 사실이 확인되었다. 예를 들어, Windows 환경에서는 레지스트리 키와 로그 파일에 TeamViewer 고유 ID, 세션 정보, 접속 계정, 파일 전송 내역 등이 기록되었으며, 메모리 덤프에서는 일시적으로 동적 비밀번호, 채팅 로그, 클립보드 데이터 등도 추출할 수 있었다.다만, TeamViewer의 통신 내용 자체는 강력하게 암호화되어 있어 세션 내 실제 데이터는 복구가 불가능하다는 한계가 있다.

III. 상세 경로

항목	경로
드라이버 설치 프로세스와 관련된 다양한 이벤트 및 활동 기록	C:₩Program Files₩TeamViewer ₩TeamViewer15_Hooks.log
Teamviewer 세션 내 이벤트 순서 재구성 시 필수적인 정보	C:₩Program Files₩TeamViewer₩TeamViewer15_Logfile.log
TeamViewer 계정 계정의 암호화된 인증 토큰, 계정 고유 값, 이메일 주소 등 사용 데이터	HKEY_CURRENT_USER₩SOFTWARE₩TeamViewer
상호작용, 시스템 구성 , 애플리케이션 동작에 대한 아티팩트	C:₩Users₩Research₩AppData₩Local₩TeamViewer₩Cache Files

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. TeamViewer에 대한 아티팩트 분석

본 연구는 TeamViewer 사용 시 생성되는 포렌식 아티팩트를 윈도우와 안드로이드 환경에서 각각 식별하고, 아티팩트의 저장 위치와 내용을 정리하는 데 중점을 두었다. 하지만 아티팩트의 변화 시점, 사용자 행위와의 상관관계, 악성 사용 여부에 대한 정량적 분석은 포함되어 있지 않다.

이를 보완하기 위해 아티팩트 변화 기반의 행위 분석을 중심으로 새로운 방향성을 제시한다. TeamViewer의 주요 기능(예: 파일 전송, 채팅, 클립보드 복사 등)을 수행한 후, 메모리·디스크·레지스트리의 변화를 비교 분석하여, 사용자의 실제 행위와 생성된 아티팩트 간의 관계를 파악한다.

이러한 방식은 단순한 아티팩트 식별을 넘어, 사용자 행위의 재구성 및

사이버 공격 탐지에 실질적으로 활용될 수 있다는 점에서 기존 연구와 차별화된다.

V. 참고 문헌

[1] Nishchal Soni, Manpreet Kaur, Khalid Aziz,「 Decoding digital interactions: An extensive study of TeamViewer's Forensic Artifacts across Windows and android platforms」, Forensic Science International: Digital Investigation 51 301838, 2024

[논문 리뷰 보고서]

[Digital Forensics in Google Drive: Techniques for Extracting Artifacts]

작성일	2025.05.26
작성자	배영혜
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	Digital Forensics in Google Drive: Techniques for Extracting Artifacts
저자 및 연도	Erika Ramadhani, Syafiq Irfan Isnaindar (2023)
출처	IIETA https://doi.org/10.18280/ijsse.140417
분석 대상 프로그램	Google Drive Desktop (버전 v66.0.3.0 추정)
관련 아티팩트 유형	계정 정보, 동기화 폴더 경로, 파일 해시, Google ID, 타임스탬프, 파일 생성/삭제/수정 이벤트

[표 1. 논문 개요표]

II. 논문 요약

본 논문은 Google Drive 데스크톱 애플리케이션에서 생성되는 디지털 아티팩트를 효과적으로 수집하고 분석하는 방법을 다루고 있다. 연구의 목적은 클라우드 기반 저장소의 특성상 증거 수집이 어렵다는 점을 극복하고, 실제 포렌식 수사에서 활용할 수 있는 체계적인 분석 절차를 제시하는 데 있다.

연구진은 sync_config.db, snapshot.db, sync_log.db 등 주요 데이터베이스 파일을 대상으로 NIST 표준 절차에 따라 실험을 진행했으며, 그 결과 파일 해시와 Google ID 등 일부 메타데이터는 추출할 수 있었지만, 활동 로그나 문서 수정 기록 등 핵심적인 증거는 확보하지 못했다.

이 논문은 로컬 아티팩트만으로는 Google Drive의 사용자 활동을 완전히 재구성하기 어렵다는 점을 보여주며, 클라우드 서비스의 특성상 구글과의 협력이나 API 기반 접근 등 추가적인 방법이 필요함을 강조한다. 또한, 암호화와 클라우드 의존성, 기존 포렌식 도구의 한계 등 실무적 제약도 함께 지적한다.

III. 상세 경로

항목	경로
sync_config.db 연결된 Google Drive 계정 정보와 동기화 폴더 위치 등을 담고 있는 SQLite 파일일	C:₩Users₩ACER₩AppData₩Local₩Google₩DriveFS
snapshot.db Google Drive에서 인식한 파일 목록, 해시값, Google ID, 타임스탬프 등 포함함	C:₩Users₩ACER₩AppData₩Local₩Google₩DriveFS
sync_log.db 파일 생성, 삭제, 수정 등의 이벤트 로그	C:₩Users₩ACER₩AppData₩Local₩Google₩DriveFS

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. TeamViewer에 대한 아티팩트 분석

본 연구는 Google Drive 로컬 클라이언트 환경에서 생성되는 아티팩트를 DriveFS 경로에 한정하여 분석하였으며, 주요 아티팩트로는 sync_config.db, snapshot.db, sync_log.db 등이 있다. 그러나 이러한 분석은 로컬 저장 경로에 국한되어 있어, Google Drive의 실제 사용자 행위나 다양한 흔적을 포괄적으로 파악하는 데에는 한계가 있었다.

이를 보완하기 위해, 분석 범위를 레지스트리, 메모리, 브라우저 캐시 등으로 확장할 필요가 있다. Google Drive 사용 시 로그인 정보, 세션 상태, 파일 접근 기록 등은 메모리나 브라우저 캐시 등 다양한 위치에 남을 수 있으며, 이를 함께 수집하고 분석함으로써 보다 풍부하고 정밀한 사용자 활동 추적이 이처럼 분석 범위의 확장과 행위 중심의 재구성 분석은 기존 연구와 차별화되는 방식으로, 보다 실질적이고 적용 가능한 포렌식 분석 모델을 제시할 수 있다.

V. 참고 문헌

[1] Erika Ramadhani, Syafiq Irfan Isnaindar,「Digital Forensics in Google Drive: Techniques for Extracting Artifacts」, IIETA, 2023

[논문 리뷰 보고서]

[Extraction and analysis of retrievable memory artifacts in IM applications: A case study of Telegram Desktop]

작성일	2025.05.27
작성자	배영혜
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	Extraction and analysis of retrievable memory artifacts in IM applications: A case study of Telegram Desktop
저자 및 연도	Pedro Fernández-Álvarez, Ricardo J. Rodríguez (2022)
출처	DFRWS (Digital Forensics Research Workshop) EU 2022 https://www.sciencedirect.com/science/article/pii/S2666281722000117
분석 대상 프로그램	Telegram Desktop (Windows 10, 버전 2.7.1)
관련 아티팩트 유형	계정 정보(사용자 ID, 전화번호), 대화 기록(채팅방 목록, 텍스트 메세지, 삭제된 메세지), 멀티미디어(파일 이름, 공유된 위치정보), 연락처(차단된 사용자, 삭제된 연락처)

[표 1. 논문 개요표]

II. 논문 요약

이 논문은 Windows 환경에서 동작하는 Telegram Desktop 애플리케이션의 메모리 기반 포렌식 분석을 수행하고, 해당 메신저 애플리케이션이 실행 중일 때 RAM 상에서 수집 가능한 아티팩트를 식별하고 분석하는 과정을 다룬다. 연구진은 추출, 분석, 보고의 세 단계를 포함하는 포렌식 분석 프레임워크를 구축하고, 이 과정에서 개발한 두 가지 도구인 Windows Memory Extractor와 IM Artifact Finder를 활용하여 Telegram에서 확보 가능한 다양한 사용자 관련 정보를 자동으로 추출할 수 있도록 설계하였다.

연구 결과, Telegram Desktop 실행 중 생성되는 메모리 아티팩트에는 사용자 계정 정보, 연락처 목록, 대화 내용, 전송 파일 이름, 지리적 위치 정보, 차단 사용자 정보 등이 포함될 수 있음이 확인되었다. 또한 대화 내용은 삭제된 이후에도 메모리 상 일부가 잔존하는 경우가 있으며, 이를 통해 사건 당시의

사용자 활동 흐름을 시간 순으로 재구성할 수 있다는 점에서 법적 증거로서의 활용 가능성이 크다.

이 연구는 기존의 디스크 기반 분석의 한계를 보완하고, 향후 다양한 인스턴트 메신저(IM) 애플리케이션에 적용 가능한 확장형 메모리 포렌식 프레임워크의 기초를 제시했다는 점에서 학술적, 실무적으로 중요한 기여를 한다.

III. 상세 경로

항목	경로
사용자 전화번호, 사용자 이름 (firstName, lastName, username), 사용자 식별자 (ID)	QString 객체 형태로 메모리에 존재
HistoryMessage 객체 (메시지 기록) 메시지 내용 (QString 형식), 전송 시간 (_timeText – UTF-16 문자열), 메시지 발신자, 수신자 정보	사용자가 최근에 열람한 대화 내용만 메모리에 상주
ChatData, ChannelData	해당 그룹이나 채널을 사용자가 접근한 경에만 메모리에서 name, participants 등 확인

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. Telegram Desktop에 대한 아티팩트 분석

기존 연구는 Telegram Desktop 애플리케이션이 실행 중일 때 메모리 내에 존재하는 사용자 정보, 대화 내용, 전송 파일명 등 다양한 아티팩트를 식별하고 분석할 수 있음을 보여주었다. 그러나 분석 대상은 단일 버전(2.7.1)의 Telegram Desktop에 한정되어 있으며, 메모리 내 데이터 구조를 수작업으로 식별한 후 전용 도구(IM Artifact Finder)를 통해 분석하는 방식이기 때문에 적용 범위와 실시간성에 제한이 있다.

이를 보완하기 위해 향후 분석에서는 Telegram 버전 업데이트에 따른 메모리 구조 변화에 자동 적응 가능한 분석 환경을 구축할 필요가 있다. 즉, 정적인 클래스 구조 분석에 의존하기보다, 메모리 내 공통 패턴(QString, 연락처 ID, 시간 포맷 등)에 기반한 동적 탐지 로직을 강화함으로써 도구의 버전 독립성을 확보해야 한다.

이러한 방향성은 메모리 기반 포렌식 분석을 정적 식별에서 실시간 추론 및 사용자 행위 재구성 중심으로 발전시키는 기반이 될 수 있다.

V. 참고 문헌

[1] Pedro Fernández-Álvarez, Ricardo J. Rodríguez,「Extraction and analysis of retrievable memory artifacts in IM applications: A case study of Telegram Desktop」DFRWS (Digital Forensics Research Workshop) EU 2022

[논문 리뷰 보고서]

[협업 툴의 사용자 행위별 아티팩트 분석 연구- 운영환경에 따른 differential forensic 개념을 이용하여]

작성일	2025.05.26
작성자	안서진
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	협업 툴의 사용자 행위별 아티팩트 분석 연구- 운영환경에 따른 differential forensic 개념을 이용하여
저자 및 연도	김영훈, 권태경. (2021)
출처	한국정보보호학회/https://koreascience.kr/article/JAKO202118350309351.page
분석 대상 프로그램	Microsoft Teams
관련 아티팩트 유형	메신저 아티팩트, 시스템 설치/실행, 사용자 행위

[표 1. 논문 개요표]

II. 논문 요약

이 논문에서는 협업 도구인 Microsoft Teams에서 발생하는 사용자 행동과 관련된 디지털 증거(아티팩트)를 분석하고, 운영체제별(윈도우와 안드로이드)로 남는 증거의 차이점을 규명하여 증거 수집 및 분석의 효율성을 높이기 위한 해결책을 제시하고자 하였다.

실험 결과, 윈도우와 안드로이드 환경에서 각각의 아티팩트 획득률이 유의하게 차이 나며, 두 환경을 비교 분석할 때 증거의 범위와 신뢰도가 향상될 수 있음을 확인하였다.

이를 통해, 차분 포렌식을 적용하면 협업 도구 내 사용자 행위에 대한 이해를 높이고, 디지털 증거 수집의 효율성을 증대시킬 수 있음이 도출되었다.

연구는 디지털 포렌식 분석에 있어 운영 환경별 차별적 증거 확보의 중요성을 강조하며, 향후 다양한 협업툴과 운영 환경에 대한 확장 연구와 증거 자동화 수집 기술 개발이 필요하다는 한계를 가지고 있다.

III. 상세 경로

항목	경로
Teams	C:₩Users₩%USERPROFILE%₩AppData₩Roaming₩Microsoft₩Teams
애플리케이션 구동 및 사용자 행위 로그, 캐시	IndexedDB, Local Storage, Cache 디렉터리 등에 저장
Teams Channel의 메시지 전송 관련 행위 정보	%USERPROFILE%₩Microsoft₩Teams₩IndexedDB₩https_teams.microsoft.com_0.indexddb.leveldb 디렉터리 내의 [0-9]{6}.log 파일/Cache 디렉터리의 data_#(0~3) Data block files
파일전송 관련 아티팩트	%USERPROFILE%₩Microsoft₩Teams₩IndexedDB₩https_teams.microsoft.com_0.indexddb.leveldb
이미지 파일 전송	Cache 디렉터리 내의 f_(0)(4)([0-9]|[a-z]){2}) 파일/%USERPROFILE%₩Microsoft₩Teams₩Local Storage₩leveldb 디렉터리의 [0-9]{6}.log 파일

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. twitter space에 대한 아티팩트 분석

트위터 스페이스에 대한 연구 사례는 매우 제한적이다. 또한 모바일과 PC 두 가지 버전이 사용이 가능하다는 점이 있다. 음성 데이터와 메타데이터, 네트워크 트래픽 그리고 API를 분석하여 보안 취약점을 찾아내고 사용자의 행동 패턴을 추적하거나 이상 징후를 감지할 수 있을 것이다.

추후 툴 개발에서는 사용자의 행동 패턴을 파악하고 이를 자동화 도구를 통해 감지할 수 있는 시스템을 만들 수 있을 것이다.

그 결과로 자동화를 통해 효율적으로 신속한 증거 수집이 가능할 것이다.

V. 참고 문헌

[1] 김영훈, 권태경,「 협업 툴의 사용자 행위별 아티팩트 분석 연구 - 운영환경에 따른 differential forensic 개념을 이용하여」, 정보보호학회논문지 제31권 제3호, 2021, 353-363

[논문 리뷰 보고서]

[윈도우 환경에서의 협업 도구 잔디 아티팩트 수집 및 분석 연구]

작성일	2025.05.26
작성자	안서진
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	윈도우 환경에서의 협업 도구 잔디 아티팩트 수집 및 분석 연구
저자 및 연도	위다빈, 김한결, 박명서. (2024)
출처	한국정보보호학회/https://www.dbpia.co.kr/pdf/pdfView.do?nodeId=NODE11956128&googleIPSandBox=false&mark=0&minRead=15&ipRange=false&b2cLoginYN=false&icstClss=010000&isPDFSizeAllowed=true&accessgl=Y&language=ko_KR&hasTopBanner=true
분석 대상 프로그램	JANDI(잔디)
관련 아티팩트 유형	메신저 아티팩트, 시스템 설치/실행, 사용자 행위

[표 1. 논문 개요표]

II. 논문 요약

이 논문에서는 협업 도구를 사용하는 과정에서 발생하는 다양한 아티팩트의 수집과 분석의 어려움을 해결하고자, 윈도우 환경에서 잔디의 아티팩트 수집 방법과 데이터 분석 기법을 제시하는 것을 연구 목적로 삼았다.

연구 결과, 잔디의 로컬 저장 데이터와 API 요청 재구성을 통해 주요 메시지, 채팅 기록, 사용자 활동 로그 등을 수집할 수 있었으며, 이를 활용하여 디지털 포렌식적 분석이 가능함을 보여줬다. 이를 통해, 기업 내 협업 도구 활용 시 보안 확보와 디지털 수사에 기여할 수 있다는 결론을 도출하였다.

이 연구는 윈도우 환경에서 수집할 수 있는 아티팩트의 범위를 확장하고, API 기반 데이터 획득 방법을 적용하여 기존의 한계를 극복하는 데 의의가 있다. 다만, 일부 데이터는 클라우드 서버에 저장된 경우 수집이 어려운 한계가 존재하며, 향후 클라우드 데이터 분석 및 실시간 수집 방안을 모색할 필요가

있다.

III. 상세 경로

항목	경로
JANDI	C:₩Users₩[USERNAME]₩AppData₩Roaming₩JANDI
사용자 행위 정보	Cache와 Local Storage 폴더 하위에 존재
메신저 아티팩트	Cache 폴더

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. 잔디 내 특정 악용이 가능한 기능 탐색

기존 논문에서는 클라우드 서버의 한계를 지적했으나, 클라우드 서버 분석은 본 프로젝트 주제에 맞지 않다고 판단하여, 프로그램 내부의 비정상 트래픽을 Fiddler와 Wireshark로 분석하여 네트워크 행위를 분석하는 방향을 제시하고자 한다.

추후 툴 개발에서는 정상 활동과 악성 활동 간의 네트워크 및 파일 시스템 접근 패턴을 학습하여, 이상 행위를 자동으로 탐지하고 분석하는 자동화 도구를 개발할 수 있을 것이다.

그 결과로 정상 프로그램을 악용한 공격 시도에 대한 조기 탐지 및 대응이 가능할 것이다.

V. 참고 문헌

[1] 위다빈, 김한결, 박명서,「 윈도우 환경에서의 협업 도구 잔디 아티팩트 수집 및 분석 연구」, 정보보호학회논문지 제34권 제5호, 2024.10, 915-925

[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

[논문 리뷰 보고서]

[무 설치 프로그램에서의 사용자 행위 아티팩트 분석]

작성일	2025.05.26
작성자	안서진
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	무 설치 프로그램에서의 사용자 행위 아티팩트 분석
저자 및 연도	허태영, 손태식. (2023)
출처	한국정보보호학회/https://www.dbpia.co.kr/pdf/pdfView.do?nodeId=NODE11419018&googleIPSandBox=false&mark=0&minRead=15&ipRange=false&b2cLoginYN=false&icstClss=010000&isPDFSizeAllowed=true&accessgl=Y&language=ko_KR&hasTopBanner=true
분석 대상 프로그램	Opera, Notdpad ++
관련 아티팩트 유형	메모리 아티팩트, 시스템 설치/실행, 파일 사용/조작, 사용자 행위

[표 1. 논문 개요표]

II. 논문 요약

이 논문에서는 포터블 프로그램에서의 사용자 행위 분석이 부족함을 판단하고, 이를 위한 아티팩트 분석 방안을 제시했다.

연구 결과, 포터블 프로그램의 Prefetch, JumpList, ShellBags 등의 운영체제 분석과 메모리 분석을 통해 증거 수집이 가능함을 확인하였다. 특히, 메모리 분석을 통해 구체적인 사용자 행위 분석이 가능하다는 점을 강조했으며, 이를 통해 향후 포터블 프로그램의 포렌식 분석에 있어 중요한 기초 자료로 활용될 수 있음을 도출하였다.

연구는 특정한 환경에서의 분석이 아닌 포터블 프로그램 전반에 걸친 연구가 필요하다는 한계를 가지고 있으며, 후속 연구로 다양한 환경에서의 포터블 프로그램 분석을 위해 추가 연구가 제안될 수 있다.

III. 상세 경로

항목	경로
메모리 아티팩트	경로 X, 분석 도구는 Hex Fiend, Volatility
프리패치 (시스템 설치/실행)	C:₩Windows₩Prefetch
파일 사용/조작	C:₩Windows₩Temp
사용자 행위	%AppData%₩Roming₩Microsoft₩Windows₩Recent

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. 다양한 포터블 프로그램 분석 및 자동화 도구 개발

   다양한 포터블 프로그램에 대한 행위를 분석한 뒤, 패턴을 파악하고 이 분석을 토대로 종합적인 접근 방식을 도출해낸다.

   추후 툴 개발에서는 이를 기반으로 분석 과정을 자동화한 도구를 개발할 수 있을 것이다.

   이를 통해 증거 수집의 신속성과 정확성을 크게 향상시킬 수 있을 것이다.

V. 참고 문헌

[1] 허태영, 손태식,「무 설치 프로그램에서의 사용자 행위 아티팩트 분석」, JOURNAL OF PLATFORM TECHNOLOGY Vol.11 No.2, 2023, 39-53

[논문 리뷰 보고서]

[화상 회의 애플리케이션 GoToWebinar 및 GoToMeeting 아티팩트 분석]

작성일	2025.05.26
작성자	안서진
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	화상 회의 애플리케이션 GoToWebinar 및 GoToMeeting 아티팩트 분석
저자 및 연도	강수진, 김기윤, 이양선. (2023)
출처	한국정보보호학회/https://www.dbpia.co.kr/pdf/pdfView.do?nodeId=NODE11397727&googleIPSandBox=false&mark=0&minRead=15&ipRange=false&b2cLoginYN=false&icstClss=010000&isPDFSizeAllowed=true&accessgl=Y&language=ko_KR&hasTopBanner=true
분석 대상 프로그램	GotoWebinar, GoToMeeting
관련 아티팩트 유형	메신저 아티팩트, 파일 사용/조작, 사용자 행위

[표 1. 논문 개요표]

II. 논문 요약

이 논문에서는 GoToWebinar 및 GoToMeeting 애플리케이션을 분석하여, 이들 애플리케이션에서 생성되는 데이터의 특성과 차이를 통해 수사에 기여할 수 있는 정보를 제공하였다.

연구 결과, 각 플랫폼마다 저장되는 데이터의 형태가 다름을 확안하였고 사용자 아티팩트로는 로그인 기록, 전송된 파일 정보, 채팅 내역 등이 포함되었다.

이 연구를 통해 화상 회의 애플리케이션의 데이터 수집 및 분석이 디지털 포렌식 수사에 필수적임을 강조했다.

연구는 특정 애플리케이션에 국한되어 포괄적인 분석이 부족하다는 한계를 가지고 있으며, 후속 연구로는 다양한 화상 회의 애플리케이션을 포함한 비교 분석이 제안될 수 있다.

III. 상세 경로

항목	경로
메신저 아티팩트	C:₩Users₩<Username>₩Documents₩ChatLog[회의명]YYYY_MM_DD HH_mm.rtf
파일 사용/조작	C:₩Users₩<User name>₩Documents
사용자 행위	

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. 실시간 화상회의 데이터 수집 자동화 툴 개발

화상회의 데이터는 별도의 도구를 통해 수작업으로 수집하는 경우가 대부분이다.

화상 회의가 진행중인 동안 네트워크 패킷과 메모리 덤프를 자동 수집 및 분석하여 로그인 정보, 채팅, 파일 공유 내역을 실시간으로 추출하는 도구를 개발할 수 있을 것이다.

2. 가상 배경(Background) 및 필터 사용 흔적 분석 툴 개발

다양한 화상 회의 애플리케이션에서 가상 배경이나 얼굴 필터 기능을 제공한다.

이 기능 사용 여부를 통해 포렌식 분석에 있어 중요한 증거를 찾을 수도

있다고 생각한다.

회의 기록, 캐시, 메모리 등을 통해 가상 배경 이미지 파일, 필터 설정 정보 등을 찾고 조작이나 위조 여부를 분석하는 툴을 개발할 수 있을 것이다.

V. 참고 문헌

[1] 강수진, 김기윤, 이양선,「화상 회의 애플리케이션 GoToWebinar 및 GoToMeeting 아티팩트 분석」, JOURNAL OF PLATFORM TECHNOLOGY Vol.11 No.1, 2023.2, 11-22

[논문 리뷰 보고서]

[폴라리스 오피스 포렌식 아티팩트에 관한 연구]

작성일	2025.05.27
작성자	전소현
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	폴라리스 오피스 포렌식 아티팩트에 관한 연구
저자 및 연도	YeoonJoo Lee, JeonMin Kim, SungJin Lee (2020)
출처	한국디지털포렌식학회 디지털포렌식 연구 제14권 제4호 / https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002675185
분석 대상 프로그램	폴라리스 오피스
관련 아티팩트 유형	파일 사용/조작, 시스템 설치/실행, 사용자 행위

[표 1. 논문 개요표]

II. 논문 요약

이 논문에서는 폴라리스 오피스 프로그램 사용 시 시스템에 남는 포렌식 아티팩트를 규명하는 것을 목적으로 한다. 이를 위해 Windows 10과 macOS 환경에서의 문서 편집 작업 후 남겨지는 흔적을 수집 및 비교 분석한다. 윈도우에서는 대부분의 아티팩트가 SQLite 기반 DB 파일에 저장되며, RecordCommand2.sqlite 파일을 통해 사용자 문서 작업의 시간 흐름까지 추적할 수 있었다. 반면에, macOS는 plist와 dat 파일을 중심으로 아티팩트가 기록되며, 사용자 계정 정보도 plist로 별도 보관된다는 차이점이 있었다. 이를 통해, 폴라리스 오피스가 남기는 아티팩트는 디지털 범죄 수사 시 문서 작업 이력을 추적하는 데 유의미한 증거로 사용될 수 있음을 입증한다. 다만, 클라우드 상에서만 파일을 열람하고 저장하는 경우에는 로컬 아티팩트가 남지 않는다는 한계가 있으며, 후속 연구로는 모바일 운영체제 아티팩트 분석 및 복구 가능성 평가 도구 개발이 제안되었다.

III. 상세 경로

항목	경로
프로그램 최초 실행 흔적	₩HCKU₩Software₩Infraware₩PolarisOffice의 "FirstHomeAccessTime" 정보
프로그램 실행 흔적	C₩Windows₩Prefetch₩응옹프로그램명{-랜덤숫자}.pf
최근 사용된 파일 목록(계정사용/미사용시 동일)	%UserProfile%₩AppData₩Roaming₩PolarisOffice₩Database₩InfrawareRecentFiles.sqlite
작업과정에 관여된 모든 파일에 대한 액세스 흔적 (계정사용/미사용시 동일)	%UserProfile%₩AppData₩Roaming₩PolarisOffice₩Database₩REcordCommand2.sqlite
자동 복구 정보 (계정사용/미사용시 동일)	%UserProfile%₩AppData₩Roaming₩PolarisOffice₩Database₩InfrawareAutoRecover.sqlite
자동 복구 임시 파일 (계정사용/미사용시 동일)	%UserProfile%₩AppData₩Roaming₩PolarisOffice₩Recover₩Slide₩파일명, %UserProfile%₩AppData₩Roaming₩PolarisOffice₩Recover₩Word₩파일명, %UserProfile%₩AppData₩Roaming₩PolarisOffice₩Recover₩Sheet₩파일명

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

폴라리스 오피스를 문서 열람 및 저장 기능을 중심으로 RecordCommand2.sqlite 를 통한 사용자 작업 이력을 추적한다.

V. 참고 문헌

[1] 이연주, 김정민, 이성민,「 폴라리스 오피스 포렌식 아티팩트에 관한 연구」, 한국디지털포렌식학회 디지털포포렌식연구 2020, vol.14, no.4,

통권30호, 368-378.

[논문 리뷰 보고서]

[취약점 별 아티팩트 사례 분석을 통한 아티팩트 그룹핑 연구 : 어도비 플래시 플레이어 취약점을 이용하여]

작성일	2025.05.27
작성자	전소현
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	취약점 별 아티팩트 사례 분석을 통한 아티팩트 그룹핑 연구 : 어도비 플래시 플레이어 취약점을 이용하여
저자 및 연도	ByungKwan Song, SeonKwang Kim, EunJin Kwon, SeungTaek Jin, JongHyck Kim, HyeongCheol Kim, Minsu Kim (2019.03)
출처	융합보안논문지, 제19권 제1호 / https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002455074
분석 대상 프로그램	어도비 플래시 플레이어
관련 아티팩트 유형	파일 사용/조작, 시스템 설치/실행, 사용자 행위

[표 1. 논문 개요표]

II. 논문 요약

이 논문은 소프트웨어 취약점을 이용한 공격 시 윈도우 시스템에 남는 아티팩트를 사례별로 분석하고 이를 유입경로 및 공격 유형에 따라 그룹핑하는 방식을 제시한다. 특히, 어도비 플래시 플레이어의 취약점(CVE-2018-4878, CVE-2015-7645, CVE-2015-8651)을 분석 대상으로 하여, 공격 방식에 따라 공통 아티팩트와 차등 아티팩트를 분류한다. 공통적으로 생성되는 아티팩트로는 crossdomain.xml, Flash 캐시 (Native Cache), Shared Objects, Setting.Sol 등이 있으며 공격 도구에 따라 문서 기반 공격에서는 jumplist, 웹 기반 공격에서는 prefetch 및 SWF 로드 흔적이 남는다는 점을 확인했다. 이를 바탕으로 아티팩트들을 문서 기반과 웹 기반으로 나누어 그룹핑하고 공격 유입 경로를 빠르게 추정할 수 있도록 하는 초기 침해 대응 전략의 유용한 틀을 제시한다.

III. 상세 경로

항목	경로
시스템 설치/실행	Prefetch, Eventlog
파일 사용/조작	$MFT, $LogFile, $UsnJrnl, %Appdata%₩Roaming₩Microsoft₩windows₩Recent₩AutomaticDe stinations
사용자 행위	%Appdata%Roaming₩Adobe₩Flash Player₩NativeCache(Flash Cache), %Appdata%Roaming%Macro media₩Flash Player ₩#Shared Objects (Shared Objects), %Appdata%Roaming₩Macromedia₩Flash Player ₩macromedia.com₩support₩flashplayer₩sys (Setting Info)

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

어도비 플래시 플레이어 프로그램에서 취약한 SWF 파일 실행 기능을 중심으로 crossdomain.xml, NativeCache, Setting.Sol, jumplist, prefetch 등을 활용하여 공격 경로를 식별함

V. 참고 문헌

[1] 송병관, 김선광, 권은진, 진승택, 김종혁, 김형철, 김민수, 「 취약점 별 아티팩트 사례 분석을 통한 아티팩트 그룹핑 연구 : 어도비 플래시 플레이어 취약점을 이용하여」, 융합보안 논문지 제19권 제1호 97-95.

[논문 리뷰 보고서]

[윈도우 환경의 아티팩트를 활용한 자동화된 사용자 분석 방안]

작성일	2025.05.26
작성자	전소현
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	윈도우 환경의 아티팩트를 활용한 자동화된 사용자 분석 방안
저자 및 연도	Jinseong Kim, Jeong Im Y (2017)
출처	2017년 한국통신학회 하계종합학술발표회
분석 대상 프로그램	Windows 10, Chrome
관련 아티팩트 유형	시스템 실행, 파일 사용/조작, 사용자 행위

[표 1. 논문 개요표]

II. 논문 요약

이 논문에서는 윈도우 사용자 데이터 환경에서 수작업 기반 아티팩트 분석의 비효율성 문제를 해결하고자 자동화된 사용자 분석 시스템 구성 방안을 제시한다. 윈도우 시스템에 남아 있는 다양한 아티팩트들로부터 사용자 행위를 추적하고 이를 시각화 기반으로 그룹화한다. Chrome 싱크 데이터를 활용해 모바일과 PC 웹 기록을 통합 분석하는 방식이 중요한 특징이다. 윈도우에 존재하는 다양한 아티팩트들의 핵심 정보만 추출하여 데이터베이스화한 후, Mecab 을 통해 관심 키워드 추출 및 사용자 관심군 분류화가 가능하다.

GUI 기반 시각화 및 자동 키워드 그룹화를 통해 다중 아티팩트 기반의 사용자 행위 분석의 실용성을 제시했다. 다만, 모바일은 구글 계정 싱크 데이터에 한정되고, 단순 키워드 분석 방식의 한계가 존재해 향후 가중치 기반 분류 및 NLP 도입이 제안되었다.

III. 상세 경로

항목	경로
사용자 행위	문서 목록, 디폴트 다운로드 경로, 크롬 History 다운로드 경로, Chrome Login Data, Chrome History, Chrome Sync
시스템 설치/실행	Prefetch, 레지스트리, 이벤트 로그
파일 사용/조작	MFT Attibutes Flags

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

Chrome의 싱크 아티팩트에서 추출된 웹 URL 및 검색어 데이터를 Mecab (형태소 분석) 한 후 명사 기반으로 분류하여, 사용자가 최근에 자주 탐색한 관심사 주제와 시점을 식별 가능하며 PC 및 모바일 통합 분석이 가능한 포렌식 도구를 제시함

V. 참고 문헌

[1] 김진성, 은창오, 정임영,「윈도우 환경의 아티팩트를 활용한 자동화된 사용자 분석 방안」, 2017년도 한국통신학회 하계종합학술발표회 논문집 1437-1438.