논문 분석 보고서

작성일	25.05.22
작성자	배영혜, 김예은
검토자	김예은

목차

I. 논문 분석 개요

프로젝트 주제를 정하기 위해 각 팀원이 논문을 각각 3편씩 찾아보았으며, 논문을 협업 툴, 인스턴트 메신저, 웹, 기타로 분류하여 정리했습니다. 이를 통해 각 논문에서 다룬 아티팩트 유형과 경로를 명확히 파악할 수 있었으며, 특정 경로의 아티팩트를 대상으로 연구한 논문이 이미 존재하는 경우, 중복을 피하고 새로운 경로를 탐색할 수 있도록 하였습니다. 또한, 분석 대상 아티팩트의 경로를 표기하여 연구 범위를 명확히 하였으며, 이를 바탕으로 보다 효과적인 연구 주제 설정이 가능하도록 하였습니다.

II. 논문 요약 표

1. 협업 툴

제목	분석 대상 프로그램	관련 아티팩트 유형 (경로 포함)	논문 요약	방향성
Forensic investigation of Google Meet for memory and browser artifacts	Google Meet (Web 기반 화상회의 애플리케이션)	- 메신저 아티팩트 전송 기록, 캐시, 채팅 로그, 실행 기록, 메모리 덤프 (실행 중 RAM에서 획득) - 시스템 설치/실행 아티팩트 Prefetch, 레지스트리, 이벤트 로그, LNK 파일C:₩Users₩{User}₩AppData₩Roaming₩Microsoft₩Windows₩Recent₩ - 메모리 아티팩트: 프로세스 메모리, 명령어 이력 , 메모리 덤프 (실행 중 RAM에서 획득) - 사용자 행위 아티팩트: 최근 명령어, 로그인 기록, 탐색 기록 C:₩Users₩{User}₩AppData₩Local₩Google₩Chrome₩User Data₩Default₩Cache₩	- Google Meet 사용 중 메모리와 브라우저에 남는 아티팩트를 식별·분석하고, 이를 자동 추출하는 Python 도구를 개발함.	- 악용 가능성: Google Meet 메모리·브라우저에 남은 이메일, 채팅, 파일 정보가 피싱·사칭·유출에 악용될 수 있음. - 자동화 도구 개발: 이메일, 토큰 등 민감 정보를 시그니처 기반으로 자동 추출·위험도 분류.
노션프로그램 아티팩트 분석을 통한 위협 분석 및 대응방안 제시	Notion (PC 및 Android 앱)	- 메신저 아티팩트: 전송 기록, 캐시, 채팅 로그, 실행 기록 ₩Users₩{User}₩AppData₩Roaming₩Notion₩notion.유 - 사용자 행위 아티팩트: 최근 명령어, 로그인 기록, 탐색 기록C:₩Users₩{User}₩AppData₩Roaming₩Notion₩notion.db	- Notion 사용 중 PC와 Android 환경에서 수집된 사용자 정보와 작업 내용이 암호화 없이 저장되어 있어 유출 위험이 크다는 점을 확인하고, 이를 분석해 보안 위협과 포렌식 활용 가능성을 제시함.	- 악용 가능성: Notion에 저장된 이메일, 토큰, 삭제된 블록 등이 계정 탈취·문서 유출·사칭에 악용될 수 있음. - 자동화 도구 개발: 디스크 이미지에서 토큰, 삭제 기록 등 위험 아티팩트 자동 추출 및 분류 기능 개발.
메신저형 협업툴 어플리케이션 아티팩트 분석 - ChannelTalk을 중심으로	ChannelTalk	- 메신저 아티팩트 : 전송 기록, 캐시, 채팅 로그, 실행 기록 - 네트워크 아티팩트 : 방문 기록, 세션 토큰, 네트워크 연결 - 사용자 행위 : 최근 명령어, 로그인 기록, 탐색 기록	- 팀 메신저 등 모바일 어플리케이션 아티팩트를 분석해 사용자 행위와 사용 내역 기반 보안 사고 증거 수집	- 채팅 추출, MAC 타임 분석, 이상 접속 탐지 자동화 도구 개발

		- 시스템 설치/실행 : Prefetch, 레지스트리, 이벤트 로그, LNK 파일		
안드로이드 환경에서의 Telegram X 메신저 아티팩트 분석	Telegram X	- 메신저 아티팩트 : 전송 기록, 캐시, 채팅 로그, 실행 기록 /data/data/org.thunderdog.challegram/files/tdlib → 경로에 위치하는 dp.sqlite파일 → messages 테이블 - 사용자 행위 아티팩트: 최근 명령어, 로그인 기록, 탐색 기록 /media/0/Android/data/org.thunderdog.challegram/files	- Telegram X의 다양한 메시지 유형과 로그를 분석하여 WAL 파일을 통한 삭제 메시지 복구 가능성을 확인	- WAL, SQLite 분석을 통한 데이터 변화 추적
화상 회의 애플리케이션 GoToWebinar 및 GoToMeeting 아티팩트 분석	GotoWebinar, GoToMeeting	- 메신저 아티팩트: C:₩Users₩<Username>₩Documents₩ChatLog[회의명]YYYY_MM_DD HH_mm.rtf - 파일 사용/조작: C:₩Users₩<Username>₩Documents - 사용자 행위	- 애플리케이션 데이터 특성과 차이 비교, 데이터 수집 및 분석 부족	- 실시간 화상회의 데이터 수집 자동화 툴 개발
윈도우 환경에서의 협업 도구 잔디 아티팩트 수집 및 분석 연구	JANDI(잔디)	- 메신저 아티팩트: Cache 폴더 - 시스템 설치/실행: C:₩Users₩[USERNAME]₩AppData₩Roaming₩JANDI - 사용자 행위: Cache와 Local Storage 폴더 하위에 존재	- 잔디의 아티팩트 수집 및 데이터 분석 기법 제시, API 기반 데이터 획득 방법 제안	- JANDI 내부 악용 기능 탐색 및 분석 자동화 툴 개발
협업 툴의 사용자 행위별 아티팩트 분석 연구 - Microsoft Teams	Microsoft Teams	- 메신저 아티팩트 %APPDATA%₩Microsoft₩Teams₩IndexedDB₩https_teams.microsoft.com_0.indexeddb.leveldb - 시스템 설치/실행 %APPDATA%₩Microsoft₩Teams - 사용자 행위 %APPDATA%₩Microsoft₩Teams₩Local Storage , %APPDATA%₩Microsoft₩Teams₩IndexedDB	- 디지털 포렌식 분석에서 운영 환경별 증거 확보 중요성 강조	- 협업툴 및 다양한 운영 환경에 대한 확장 연구 필요
협업 툴 아티팩트 분석 및 삭제된 데이터 복구 연구	잔디, 네이버 웍스	- 메신저 아티팩트 %LOCALAPPDATA%₩Microsoft₩Teams₩main.db, %LOCALAPPDATA%₩Microsoft₩Teams₩chat.db - 시스템 설치/실행 아티팩트₩Windows₩AppCompat₩Programs₩Amcache.h - 사용자 행위 아티팩트C:₩Windows₩System32₩winevt₩Logs	- 협업 툴 사용 증가로 인한 데이터 유출 위험 분석, 삭제 메시지 복구 가능성 확인	- 아티팩트 자동 파싱 도구 개발
Windows Telegram Desktop 애플리케이션에서 검색 가능한 메모리 아티팩트 추출 및 분석	Telegram Desktop	- 사용자 행위 아티팩트 - 메모리 아티팩트 UserData, HistoryMessage 객체 구조 분석을 통해 이름, 전화번호 등 추출 - 데이터베이스 아티팩트	- 메모리 덤프를 통해 계정 정보, 대화 내용, 삭제된 흔적을 추출하는 방법 제시	- 메모리 기반 포렌식 도구 개발

		메모리 상의 QString, PeerData, ChatData 추적		
Microsoft Office 진단 로그 분석 및 포렌식 활용 방안	Microsoft Word, Excel, PowerPoint	- 시스템 설치/실행 아티팩트: Prefetch, Amcache.hve, MFT, 임시파일 - 사용자 행위 아티팩트: Pdod, $UsnJrnl	- Microsoft Office 진단 로그를 활용해 작업 이력 추적 가능성 분석	- 진단 로그를 통한 문서 작업 흐름 복원 도구 개발
디지털 상호작용 디코딩: TeamViewer 포렌식 아티팩트 연구	TeamViewer	- 시스템 설치/실행 아티팩트 : Program Files₩TeamViewer - 파일 사용/조작 아티팩트 AppData₩Roaming₩TeamViewer₩Connections.txt AppData₩Roaming₩TeamViewer₩Connections_incoming.txt AppData₩Local₩TeamViewer₩Database₩tvchatfilecache.db AppData₩Local₩TeamViewer₩Database₩tvchatfiledownloadhistory.db - 메모리 아티팩트 : 동적 비밀번호, 채팅 내역 - 네트워크 아티팩트 TeamViewer15_Logfile.log (Android ↔ Windows 간 접속 IP 기록) - 데이터베이스 아티팩트 AppData₩Local₩TeamViewer₩Database₩tvchatfilecache.db AppData₩Local₩TeamViewer₩Database₩tvchatfiledownloadhistory.db	- Windows와 Android에서 TeamViewer 사용 시 남는 아티팩트 분석	- TeamViewer 사용 시 로그와 메모리 덤프 파싱 도구 개발
디지털 포렌식 관점에서의 협업 도구 네이버웍스의 데이터 수집 및 분석	네이버웍스	- 채팅 기록 - 파일 공유 - 캘린더/일정 - 사용자 계정 정보 - 삭제된 데이터, 로그 파일 C:₩Users[Username]₩AppData₩Local₩WorksMobile₩NaverWorks₩	- 네이버웍스에서 생성되는 다양한 사용자 행위 기반 데이터를 수집하고 분석함	- 안티포렌식 기능 우회 기술 연구 및 자동 분석 도구 개발
디지털 포렌식 관점의 네이버 밴드 사용자 행위 수집 및 분석 연구	네이버 밴드 (Android 환경)	- 메신저 아티팩트: /data/data/com.nhn.android.band/databases/chat_message - 네트워크 아티팩트: /v2.0.0/get_posts, /get_photos, /get_files - 사용자 행위 아티팩트: /databases/member, /shared_prefs/USER.xml, /cache/IMAGE, /cache/VIDEO	- Android 환경에서 네이버 밴드의 로컬 데이터와 API를 분석하여 사용자 정보, 채팅 기록 등을 수집	- 악용 가능성: 채팅, 이미지 캐시, user/band ID 등을 통한 신원 도용 및 삭제 대화 복원

2. 인스턴트 메신저

제목	분석 대상 프로그램	관련 아티팩트 유형 (경로 포함)	논문 요약	방향성

포렌식 관점에서의 Element 인스턴트 메신저 아티팩트 분석	Element	- 메신저 아티팩트 - 네트워크 아티팩트 - 메모리 아티팩트 - 사용자 행위	- Signal, Wickr, Threema 등 보안 메신저 암호화 메커니즘 분석 및 일부 복호화 방법 제시	- 메타데이터 중심 분석 및 키 추출 도구 개발
윈도우 환경에서 카카오톡 데이터 복호화 및 아티팩트 분석 연구	KakaoTalk (카카오톡) PC 버전	- 파일 사용/조작: %LocalAppData%₩Kakao₩KakaoTalk₩users₩chat_data - 사용자 행위: %LocalAppData%₩Kakao₩KakaoTalk₩users - 메신저 아티팩트: %LocalAppData%₩Kakao₩KakaoTalk₩users₩chat_data	- 윈도우 환경에서 카카오톡 데이터를 복호화하고 아티팩트를 분석하는 방안을 구현함	- 썸네일 자동 추출 도구 및 데이터 복호화 자동화 도구 개발
카카오톡 메신저 백업 서비스 '톡서랍 플러스' 데이터 수집 방법 연구	KakaoTalk (카카오톡) PC 버전	- 네트워크 아티팩트 - 사용자 행위 - 데이터베이스 아티팩트	- 클라우드-동기화 서버 기반 '톡서랍 플러스' 데이터를 Internal API를 통해 수집하는 방안 제안	- 서버 백업 메시지 및 첨부파일 수집 도구 개발
Windows에서의 Wire 크리덴셜 획득 및 아티팩트 분석	Wire (암호화 메신저)	채팅 기록, 크리덴셜 데이터, 파일 공유 기록, 계정 정보 경로: %APPDATA%₩Wire₩logs₩electron.log	- Wire 메신저의 로그인 정보와 사용자 행위 기반 아티팩트를 분석하여 삭제 메시지 복원 가능성 확인	- 로그 기반 삭제 메시지 복원 기법 개발
윈도우 및 안드로이드 환경에서의 WeChat 메신저 아티팩트 분석 연구	WeChat (인스턴트 메신저)	채팅 기록, Moments, 타임캡슐, 사용자 계정 정보, 데이터베이스 파일	- Windows와 Android 환경에서 WeChat의 사용자 행위 기반 아티팩트를 분석하여 저장 경로 차이 비교	- 자동화된 아티팩트 수집 도구 및 삭제 메시지 복구 기법 연구
Windows Telegram Desktop 애플리케이션에서 검색 가능한 메모리 아티팩트 추출 및 분석	Telegram Desktop	- 메모리 아티팩트 : UserData, HistoryMessage 객체 구조 분석을 통해 이름, 전화번호 등 추출 - 데이터베이스 아티팩트 : 메모리 상의 QString, PeerData, ChatData 추적	Windows 환경에서 Telegram Desktop의 메모리 덤프를 분석하여 디스크로 접근할 수 없는 사용자 계정, 대화 내용 등을 추출하였다. 연구진은 Windows Memory Extractor와 IM Artifact Finder를 활용하여 주요 아티팩트를 효과적으로 식별하였다.	- Telegram과 같은 메신저의 메모리 덤프를 분석하여 계정 정보, 대화 내용, 삭제된 흔적 등을 자동으로 추출하는 메모리 기반 포렌식 도구를 개발

3. 클라우드

제목	분석 대상 프로그램	관련 아티팩트 유형 (경로 포함)	논문 요약	방향성
윈도우 환경의 아티팩트를 활용한 자동화된 사용자 분석 방안	Windows OS, Google Chrome	- 사용자 행위 아티팩트 : 프리패치, 레지스트리, 문서 목록, 이벤트 로그 - 시스템 설치/실행 아티팩트 - 데이터베이스 아티팩트	- 윈도우 시스템의 다양한 아티팩트를 수집하여 자동화된 사용자 행위 분석 기법을 제안 - 웹 브라우저 기록과 시스템 로그를 Mecab 형태소 분석기와 결합하여 관심 키워드 추출, 사용자 분류, 데이터 시각화 수행	자동화된 사용자 프로파일링 및 이상 행위 탐지 기반 마련
Google 드라이브의 디지털 포렌식: 디지털 아티팩트 추출 및 분석 기술	Google Drive	- 시스템 설치/실행 아티팩트 ACER₩AppData₩Local₩Google₩DriveFS - 파일 사용/ 조작 아티팩트ACER₩AppData₩Local₩Google₩DriveFS₩sync_config.db ACER₩AppData₩Local₩Google₩DriveFS₩snapshot.db ACER₩AppData₩Local₩Google₩DriveFS₩sync_log.db - 데이터 베이스 아티팩트 ACER₩AppData₩Local₩Google₩DriveFS₩experiments.db ACER₩AppData₩Local₩Google₩DriveFS₩metric_store_sqlite.db ACER₩AppData₩Local₩Google₩DriveFS₩root_preference_sqlite.db	- Google Drive의 클라우드 환경에서 디지털 포렌식 수행을 위해 NIST 방법론을 적용하여 주요 아티팩트(사용자 활동 로그, 문서 메타데이터, 권한 정보 등)를 식별	클라우드 포렌식 환경에서 NIST 기반의 단계별 절차 적용 가능성 평가, Google Drive File Stream의 구조적 한계와 도구 적합성에 대한 검토

4. 기타

제목	분석 대상 프로그램	관련 아티팩트 유형(경로 포함)	논문 요약	방향성
안드로이드 환경에서의 지도 애플리케이션 아티팩트 분석 및 복호화 방안 연구	네이버 지도, TMAP, 카카오 맵 PC 버전	- 사용자 행위 아티팩트 databases 디렉터리의 bookmark.db, search-history.db, route-history.db, subwayMap.db파일 shared_prefs 디렉터리 내 pubtrans_cache.xml파일 NativeNaviDefaults.xml 파일	- 지도 애플리케이션에 분석된 결과의 범위는 한정적, 아티팩트가 변경되거나 애플리케이션마다 저장되는 데이터가 다양함. - 최신 버전에서의 데이터 수집 방안 연구 필요	GPS 데이터를 악용하는 경우 GPS 로그파일, 위치 기록 캐시 기반 패턴 분석
원격 제어용 어플리케이션에서의 아티팩트 수집 및 분석	TeamViewer, AnyDesk, AirDroid (모두 Android 환경)	- 메신저 아티팩트: app.db(AirDroid) - 네트워크 아티팩트: TVLog.html(TeamViewer), account_backup(AirDroid), main_preference_bk(AirDroid)	- Android 기반 원격 제어 앱의 로컬 아티팩트를 분석하여 제어자 정보·파일 전송·권한 요청 등 핵심 데이터를 식별	악용 가능성: 접속 기록, 계정, 전송 파일 등 감청·탈취·사칭 위험

		- 시스템 설치/실행 아티팩트: client.conf (TeamViewer), com.sand.airdroid_preference.xml(AirDroid) - 파일 사용/조작 아티팩트: downloads/ (AnyDesk), TVLog.html(TeamViewer) - 사용자 행위 아티팩트: TVLog.html(TeamViewer), app.db(AirDroid), recursive_file_index_phone(AirDroid)		
무 설치 프로그램에서의 사용자 행위 아티팩트 분석	Opera, Notepad++	- 메모리 아티팩트: 경로 X, 분석 도구는 Hex Fiend, Volatility - 시스템 설치/실행: C:₩Windows₩Prefetch - 파일 사용/조작: C:₩Windows₩Temp - 사용자 행위: %AppData%₩Roming₩Microsoft₩Windows₩Recent	- 포터블 프로그램에서의 사용자 행위 분석 방안 제시, 메모리 분석을 통해 증거 수집 가능	비전통적 아티팩트(windows Defender, MemCompression 등)를 파싱할 도구 개발
폴라리스 오피스 포렌식 아티팩트에 관한 연구	폴라리스 오피스	- 시스템 설치/실행 아티팩트 : C:₩Windows₩Prefetch₩[폴라리스 오피스 설치 파일명].pf (prefetch) - 사용자 행위 아티팩트 : C₩HKCU₩Software₩Infraware₩Polaris Office의 "FirstHomeAccessTime" 정보 - 파일 사용/조작 아티팩트 : %UserProfile%₩AppData₩Roaming₩PolarisOffice₩Database₩InfrawareRecentFiles.sqlite (최근 사용된 파일 목록) , %UserProfile%₩AppData₩Roaming₩PolarisOffice₩Database₩RecordCommand2.sqlite (작업 과정에 관여된 모든 파일에 대한 액세스 흔적), %UserProfile%₩AppData₩Roaming₩PolarisOffice₩Database₩InfrawareAutoRecover.sqlite (자동 복구 정보), %UserProfile%₩AppData₩Roaming₩PolarisOffice₩Recover₩Slide₩파일명, %UserProfile%₩AppData₩Roaming₩PolarisOffice₩Recover₩Word₩파일명 , %UserProfile%₩AppData₩Roaming₩PolarisOffice₩Recover₩Sheet₩파일명 - 데이터베이스 아티팩트 : %UserProfile%₩AppData₩Roaming₩Polaris Office₩Database₩InfrawareRecentFiles.sqlite, %UserProfile%₩AppData₩Roaming₩Polaris Office₩Database₩RecordCommand2.sqlite, %UserProfile%₩AppData₩Roaming₩Polaris Office₩Database₩InfrawareAutoRecover.sqlite	- Polaris Office 사용 시 Windows와 macOS에서 생성되는 아티팩트를 분석하여 작업 로그 DB 확인	문서 작성 및 수정 기능의 작업 로그 DB 분석을 통한 사용자 행위 재구성

취약점 별 아티팩트 사례 분석을 통한 아티팩트 그룹핑 연구	Adobe Flash Player	- 시스템 설치/실행 아티팩트 : Prefetch, Event log, - 파일 사용/조작 아티팩트 : $MFT, $LogFile, $UsnJrnl, %Appdata% ₩Roaming₩Microsoft₩windows₩Recent₩AutomaticDe stinations , - 사용자 행위 아티팩트 : %Appdata%Roaming₩Adobe₩F lash Player₩NativeCache(Flash Cache), %Appdata%Roaming%Macromedia₩Flash Player ₩#Shared Objects (Shared Objects), %Appdata%Roaming₩Macrom edia₩Flash Player ₩macromedia.com₩support₩flashplayer₩sys(Setting Info)	- Adobe Flash Player의 취약점 활용 침해사고 사례 분석 - 초기 침해 대응을 위한 '아티팩트 그룹핑' 방안 제시	CVE 취약점 공격 발생 시 Prefetch 및 Web Cache 분석을 통한 공격 흔적 확보
Conversational AI forensics: A case study on ChatGPT, Gemini, Copilot, and Claude	ChatGPT, Gemini, Copilot, Claude	- 메신저 아티팩트: C:₩Users₩<User>₩Downloads₩chatgpt_export_<YYYY-MM-DD>₩conversations.json - 네트워크 아티팩트: C:₩Users₩<User>₩Documents₩Wireshark₩chatgpt_traffic.pcap	- 대화형 AI 플랫폼의 대화 이력과 메타데이터를 수집·분석하여 악성 코드 제작 행위를 입증할 수 있는 아티팩트 식별	대화형 AI에 입력된 프롬프트와 삭제된 대화 로그를 분석하여 이상 행위 탐지 모델 개발

※ 참고 문헌

[1] Farkhund Iqbal, Zainab Khalid, Andrew Marrington, Babar Shah, Patrick C.K. Hung, 「Forensic investigation of Google Meet for memory and browser artifacts」 , Forensic Science International: Digital Investigation, Vol. 43, 2022, Article ID 301448 「」

[2] 한주현, 손태식,「노션프로그램 아티팩트 분석을 통한 위협 분석 및 대응방안 제시」, Journal of Platform Technology, Vol. 12, No. 3, June 2024

[3] 홍리나 , 손태식, 「메신저형 협업툴 어플리케이션 아티팩트 분석 - ChannelTalk을 중심으로」, 디지털포렌식 연구 제18권 제1호 (p.79-96) 2024

[4] 김정민, 정병찬, 이상진, 박정흠,「안드로이드 환경에서의 Telegram X 메신저 아티팩트 분석」, 고려대학교 정보보호대학원 2022

[5] 강수진, 김기윤, 이양선,「화상 회의 애플리케이션 GoToWebinar 및 GoToMeeting 아티팩트 분석」, 한국정보보호학회 2023

[6] 위다빈, 김한결, 박명서,「윈도우 환경에서의 협업 도구 잔디 아티팩트 수집 및 분석 연구」, 한국정보보호학회 2024

[7] 김영훈, 권태경,「협업 툴의 사용자 행위별 아티팩트 분석 연구- 운영환경에 따른 differential forensic 개념을 이용하여」, 한국정보보호학회 2021

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

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

[10] 김한결, 위다빈, 박명서,「디지털 포렌식 관점에서의 협업 도구 네이버웍스의 데이터 수집 및 분석」, 한국정보보호학회 2024

[11] 안원석, 박명서,「디지털 포렌식 관점의 네이버 밴드 사용자 행위 수집 및 분석 연구」, 정보보호학회논문지, Vol. 34, No. 6, Dec. 2024「」

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

[13] 조재민, 변현수, 윤희서, 서승희, 이창훈,「포렌식 관점에서의 Element 인스턴트 메신저 아티팩트 분석」, 정보보호학회논문지 제32권 제 6호 (p.1,113-1,120)

[14] 조민욱, 장남수,「윈도우 환경에서 카카오톡 데이터 복호화 및 아티팩트 분석 연구 」, 한국정보보호학회 2023

[15] Dayeon Lee, Sueun Jung, Sangjin Lee, Jungheum Park,「카카오톡 메신저 백업 서비스 '톡서랍플러스'데이터수집 방법 연구」, 디지털포렌식연구 제17권 제2호,한국디지털포렌식학회

[16] 신수민, 김소람, 윤병철, 김종성,「Windows에서의 Wire 크리덴셜 획득 및 아티팩트 분석」, 한국정보보호학회 2021

[17] 박은후, 김소람, 김종성,「윈도우 및 안드로이드 환경에서의 WeChat 메신저 아티팩트 분석 연구」, 한국디지털포렌식학회 2020

[18] 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

[19] 김진성, 은창오, 정임영,「윈도우 환경의 아티팩트를 활용한 자동화된 사용자 분석 방안」, 한국통신학회 학술대논문집 (한국통신학회 2017년도 하계종합학술발표회 논문집), 2017.6, pp. 1,437–1,438 (2 pages)

[20] Erika Ramadhani, Syafiq Irfan Isnaindar,「Digital Forensics in Google Drive: Techniques for Extracting and Analyzing Digital Artifacts」, International Journal of Scientific & Engineering

Research, 2024, pp. 1203–1211 (9 pages). DOI: 10.18280/ijsse.140417 (Received 30 Oct 2023; Revised 2 Jul 2024; Accepted 17 Jul 2024; Available online 30 Aug 2024)

[21] 박귀은, 강수진, 김종성,「안드로이드 환경에서의 지도 애플리케이션 아티팩트 분석 및 복호화 방안 연구」, 디지털포렌식연구 제16권 제2호 (p.163–184) 2022.6

[22] 박현재, 손태식,「원격 제어용 어플리케이션에서의 아티팩트 수집 및 분석」, 디지털포렌식연구 제18권 제1호 (p.46–62) 2024.3

[23] 허태영, 손태식,「무 설치 프로그램에서의 사용자 행위 아티팩트 분석」, A Study On Artifacts Analysis In Portable Software, p.39, 20__

[24] 이연주, 김정민, 이성진,「폴라리스 오피스 포렌식 아티팩트에 관한 연구」, 디지털포렌식연구 Vol. 14, No. 4, 통권 30호 (pp.368–378) 2020

[25] 송병관, 김선광, 권은진, 진승택, 김종혁, 김형철, 김민수,「취약점 별 아티팩트 사례 분석을 통한 아티팩트 그룹핑 연구 : 어도비 플래시 플레이어 취약점을 이용하여」, 융합보안논문지 KOCOSA Vol. 19, No. 1, 통권 84호 (pp.87–95) 2019

[26] 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, March 2025, Article ID 301855