[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