[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