[포렌식툴 분석 보고서]

[NTFS Log Tracker]

작성일	2025.05.26
작성자	김신아
검토자	김예은

목차

Ⅰ. 툴 기본 정보

항목	내용
툴 이름	ntfslogtracker
분석 카테고리	시스템 설치/실행, 파일 사용/조작, 사용자 행위
사용 버전	1.8
다운로드 경로	https://sites.google.com/site/forensicnote/ntfs-log-tracker
지원 포맷	NTFS 볼륨의 $LogFile , $UsnJrnl , $MFT

[표1. 툴 기본 정보]

Ⅱ. 툴 소개 및 목적

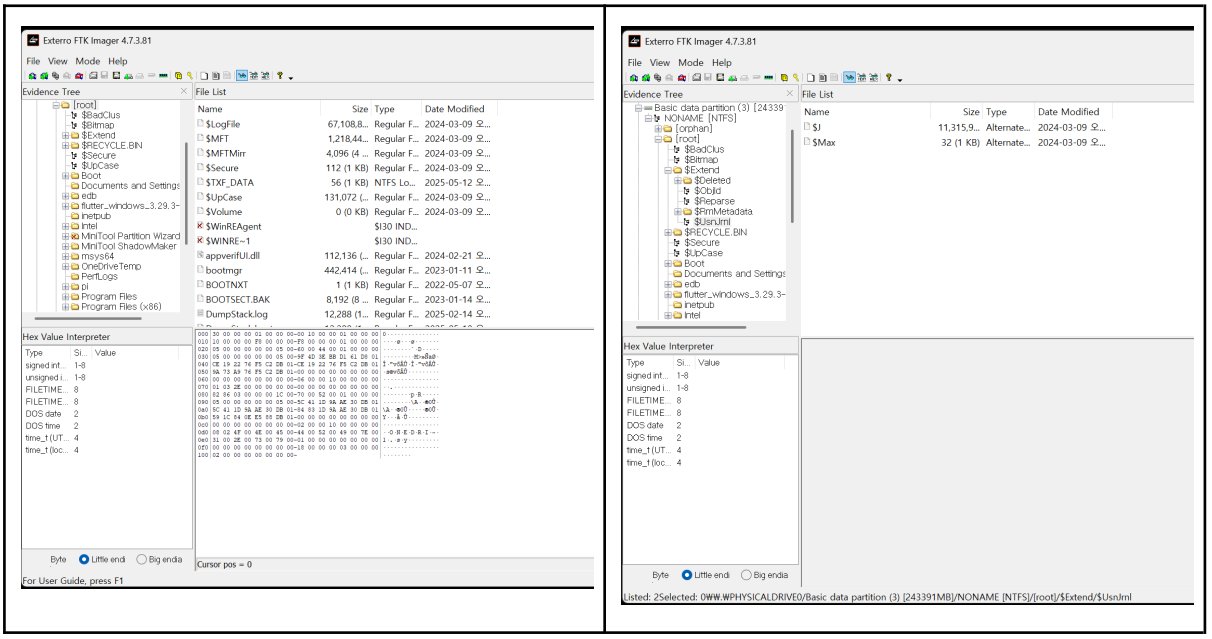
1. NTFS 파일 시스템에서 생성되는 $LogFile , $UsnJrnl , $MFT 핵심 로그 파일 분석하여 파일 생성, 수정, 삭제, 이동 등의 활동 이력을 추적하는 오픈소스 포렌식 분석 도구이다.

Ⅲ. 설치 매뉴얼

1. 지원 운영체제 : Windows 운영체제 전용 도구
2. 설치 방식
    1) NTFS Log Tracker v1.8 ZIP 파일을 다운로드
    2) 다운로드한 .zip 파일 압축 해제
    3) 압축을 푼 폴더 내 NTFSLogTracker.exe 실행 파일 클릭하여 실행

Ⅳ. 주요 기능 및 사용법

사용법1. FTK를 통해 $LogFile, $MFT, $UsnJrnl:$J 추출



[그림1. FTK를 이용한 로그 파일 추출 화면]

1) NTFS Log Tracker 사용 전 FTK 또는 EnCase 등의 디지털 포렌식 툴을 활용해 분석 대상 드라이브에서 로그 파일들을 추출해야 한다.

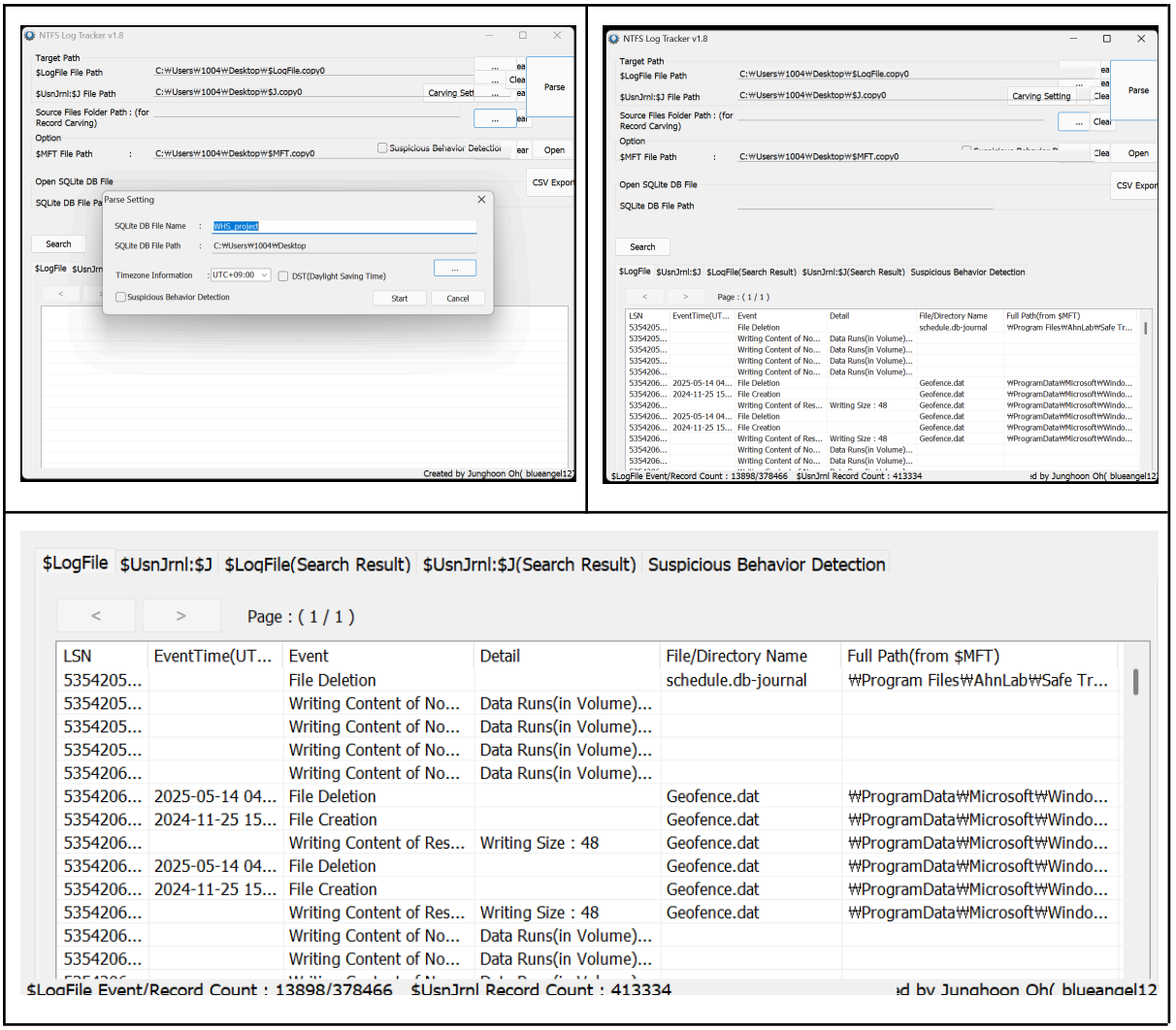
2) 추출 방법

   (1) FTK Imager에서 대상 디스크 이미지 마운트

   (2) $LogFile, $MFT, $UsnJrnl:$J 파일을 추출

   (3) NTFS Log Tracker에 불러와 분석 시작

사용법2. 데이터 파싱



[그림2,3. NTFS Log Tracker 실행 화면 및 데이터 로드]

[그림4. 로그 데이터 파싱 결과 예시]

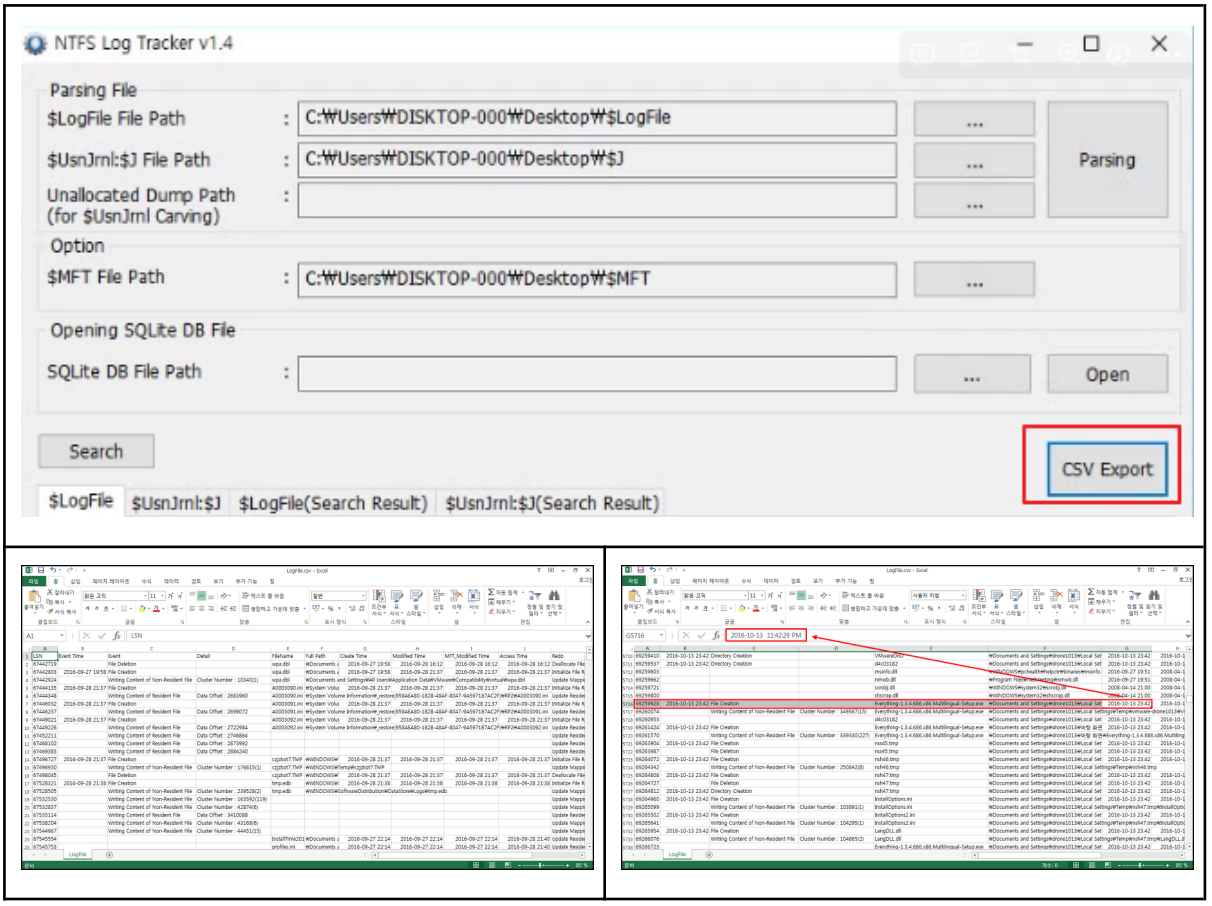
1) 추출한 로그 파일들을 로딩하면 자동으로 이벤트 데이터를 파싱해 GUI에 출력한다.

2) 출력 방법

   (1) 로그 파일 선택

   (2) 자동으로 분석 수행 후, 결과 탭에서 각 이벤트 확인

기능1. CSV Export (파일 변경 사항 시간 추적)



[그림5. CSV Export 기능 실행 화면]

1) 분석 결과를 CSV 형식으로 내보내 시간 순으로 정렬된 파일 변경 이력을 저장할 수 있다.

2) 사용법

(1) Export > CSV Export 클릭

(2) 저장 위치 선택 후 CSV 파일 생성

Ⅴ. 참고 자료

[1] 오정훈, 황현욱「NTFS 로그 분석을 통한 사용자 의심 행위 탐지에 관한 연구」디지털포렌식연구, 15(3), 2021, 54-71.

[2] https://croas.tistory.com/88