

[포렌식툴 분석 보고서]

[KAPE]



작성일	2025.05.26
작성자	안서진
검토자	김예은

목차

I. 툴 기본 정보.....	3
II. 툴 소개 및 목적	3
III. 설치 매뉴얼	3
IV. 주요 기능 및 사용법	4
1. 기본 사용법	4
2. 기능 1: Target 기반 아티팩트 수집.....	5
3. 기능 2: Module 기반 아티팩트 수집	7
V. 참고 자료.....	8

I. 툴 기본 정보

항목	내용
툴 이름	KAPE(Kroll Artifact Parser And Extractor)
분석 카테고리	시스템 설치/실행, 파일 사용/조작, 사용자 위
사용 버전	v1.3.0.2
다운로드 경로	https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape
지원 포맷	.evtx, .log, .csv, .pf, .lnk 등 다양한 포맷 지원

[표 1. 툴 기본 정보표]

II. 툴 소개 및 목적

1. KAPE(Kroll Artifact Parser And Extractor)는 아티팩트 파서 및 추출 도구로, 법의학 조사를 신속히 처리하고 최적화하기 위해 제작된 포렌식 도구이다.
2. (1) 파일을 수집하고, (2) 수집된 파일을 하나 이상의 프로그램으로 처리하는 두 가지 기능을 제공한다.
3. 기능 확장성이 뛰어나며, 사건에 가장 중요한 시스템을 찾아 우선순위를 정하고 이미징을 시작하기 전에 주요 아티팩트를 수집할 수 있다.

III. 설치 매뉴얼

1. 지원 운영체제: Windows 7 이상(32/64비트)
2. 설치 방식: [KAPE 다운로드 링크](#) 에서 다운로드

3. 별도의 설치 없이 사용 가능하며, 압축을 푼 후 파일 내부의 **"kape.exe"** (CLI) 혹은 **"gkape.exe"**(GUI)를 실행하여 사용

다운로드 후 압축한 폴더의 내부는 다음과 같다.

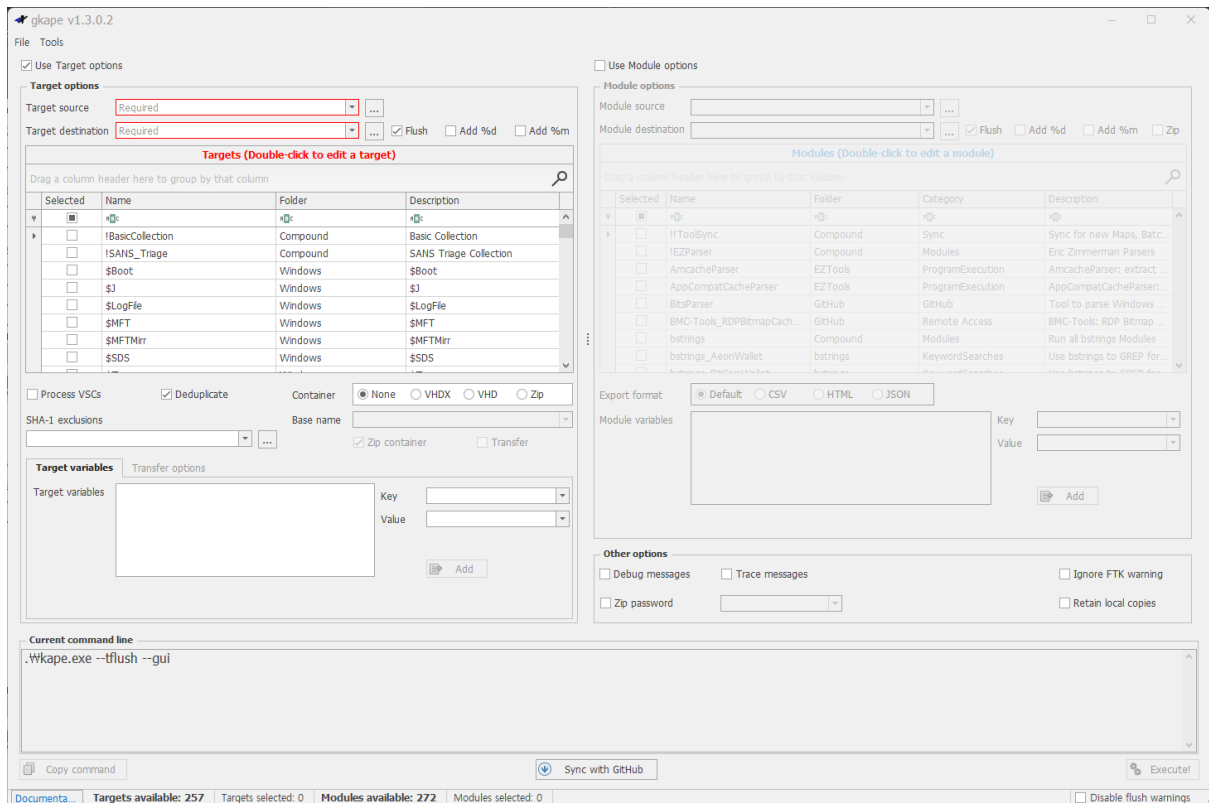
Documentation	2025-04-20 오후 1:39	파일 폴더	사용 계약 조항, 매뉴얼이 저장된 파일이 포함된 폴더
Modules	2025-04-20 오후 1:39	파일 폴더	모듈을 사전 정의한 .mkape 파일이 포함된 폴더
Targets	2025-04-20 오후 1:39	파일 폴더	타겟을 사전 정의한 .tkape 파일이 포함된 폴더
20250420045940_kape.cli	2025-04-20 오후 1:58	CLI 파일	1KB
ChangeLog.txt	2023-01-04 오전 1:47	텍스트 문서	21KB 버전 업데이트 정보
Get-KAPEUpdate.ps1	2023-06-22 오전 2:35	PS1 파일	20KB 최신 버전으로 업데이트 할 수 있는 powershell 스크립트
gkape.exe	2023-01-04 오전 1:47	응용 프로그램	61,654KB GUI 버전 KAPE
gkape.settings	2025-04-20 오후 5:21	Settings-Designer...	1KB 프로그램 설정 파일
kape.exe	2023-01-04 오전 1:47	응용 프로그램	6,840KB CLI 버전 KAPE

[그림 1. KAPE 폴더 내부 파일]

IV. 주요 기능 및 사용법

1. 기본 사용법

- 1) **수집(Targets)**: 시스템에서 필요한 파일/아티팩트를 빠르게 수집할 수 있다.
- 2) **분석/파싱(Modules)**: 수집된 데이터를 다양한 도구를 이용해 자동으로 분석할 수 있다.
- 3) 수집과 분석은 별개/동시에 진행할 수 있다.
(예) Target 선택 → 수집 경로 지정 → Module 선택 → 출력 경로 설정 → 실행 및 결과 분석



[그림 2. gkape.exe 실행 화면]

2. 기능 1: Target 기반 아티팩트 수집

1) 특정 파일, 폴더, 레지스트리 키 등을 수집할 규칙을 정의한다.

(1) Use Target options → 타겟 설정 활성화

(2) Target Source → 타겟이 될 대상 볼륨 선택

(3) Target Destination → 추출된 아티팩트가 저장될 경로 선택

(4) Flush → 대상 디렉토리에 남아있는 기존 파일 삭제 후 새로 수집할 때 사용

(5) %d (date) → 현재 날짜를 자동으로 수집 경로에 포함, 진행 시점을 구분할 때 사용

(6) %m (Machine name) → 수집 대상의 호스트 이름을 수집 경로에 포함, 여러 시스템을 수집할 때 구분하기 위해 사용

- (7) Process VSCs → Volume shadow copy에 접근해 과거 시점의 데이터까지 수집 가능(파일 복구나 변경 추적에 용이)
- (8) Deduplicate → 수집이 진행되는 과정에서 중복되는 파일 제거 가능
- (9) Container → 수집 결과를 가상화 시스템이나 다른 분석 도구에 이용할 때 활용 가능

Target options

Target source: Required

Target destination: Required

☒ Flush ☐ Add %d ☐ Add %m

Targets (Double-click to edit a target)

Drag a column header here to group by that column

Selected	Name	Folder	Description
<input checked="" type="checkbox"/>	\$MFT	Windows	\$MFT
<input type="checkbox"/>	\$MFTMirr	Windows	\$MFTMirr
<input type="checkbox"/>	\$SDS	Windows	\$SDS
<input type="checkbox"/>	\$LogFile	Windows	\$LogFile
<input type="checkbox"/>	\$J	Windows	\$J
<input type="checkbox"/>	\$Boot	Windows	\$Boot
<input type="checkbox"/>	!SANS_Triage	Compound	SANS Triage Collection
<input type="checkbox"/>	!BasicCollection	Compound	Basic Collection

☐ Process VSCs ☒ Deduplicate

Container: ☒ None ☐ VHDX ☐ VHD ☐ Zip

SHA-1 exclusions: []

Base name: []

☒ Zip container ☐ Transfer

Target variables | Transfer options

Target variables: []

Key: []

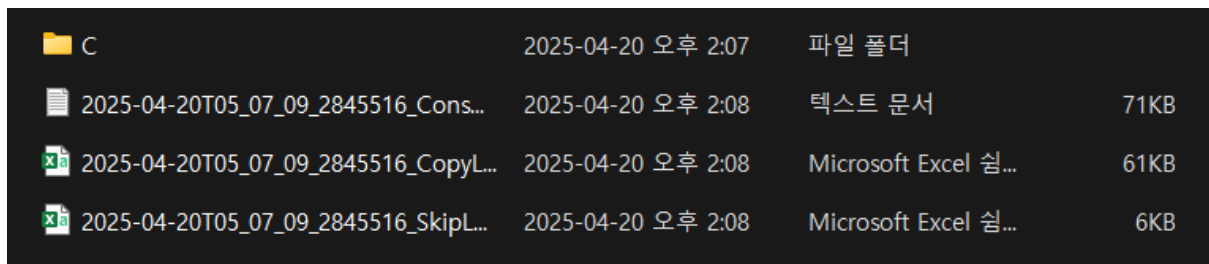
Value: []

[Add]

[그림 3. 타겟 옵션 설정 화면]

- 2) 관련 아티팩트로는 브라우저 기록(Chrome, Edge), 레지스트리 파일(NTUSER.DAT, SYSTEM), 이벤트 로그(.evtx) 등이 있다.

(예) Use Target options → 소스 및 저장 경로 지정 → \$MFT, EventLogs
선택 → Execute



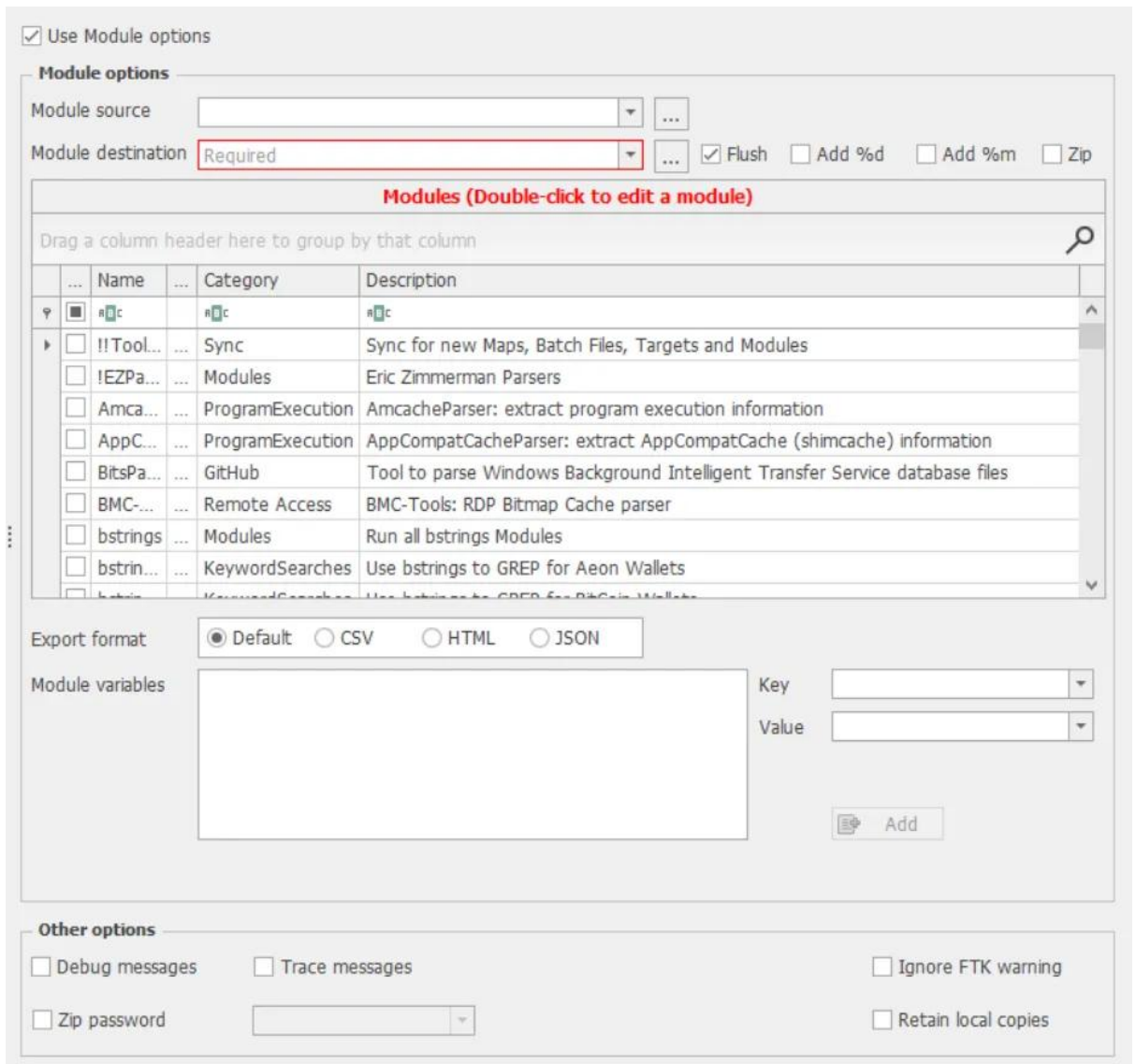
C	2025-04-20 오후 2:07	파일 폴더	
2025-04-20T05_07_09_2845516_Cons...	2025-04-20 오후 2:08	텍스트 문서	71KB
2025-04-20T05_07_09_2845516_CopyL...	2025-04-20 오후 2:08	Microsoft Excel 실...	61KB
2025-04-20T05_07_09_2845516_SkipL...	2025-04-20 오후 2:08	Microsoft Excel 실...	6KB

[그림 4. 추출된 폴더 내부의 아티팩트 파일]

3. 기능 2: Module 기반 아티팩트 수집

1) 수집된 데이터를 여러 분석 도구(Module)를 통해 자동으로 분석한다.

- (1) Use Modules options → 모듈 설정 활성화
- (2) Module Source → 모듈이 될 대상 볼륨 선택
- (3) Module Destination → 모듈 수행 결과물이 저장될 경로 선택
- (4) Flush → 대상 디렉토리에 남아있는 기존 파일 삭제 후 새로 수집할 때 사용
- (5) %d (date) → 현재 날짜를 자동으로 수집 경로에 포함, 진행 시점을 구분할 때 사용
- (6) %m (Machine name) → 수집 대상의 호스트 이름을 수집 경로에 포함, 여러 시스템을 수집할 때 구분하기 위해 사용
- (7) Export format → Module 처리된 데이터를 출력할 형식 지정
- (8) Module variables → .mkape 파일에서 변수 교체에 사용할 key:value 쌍 목록 지정
- (9) Other options → 디버그/추적 메시지 출력 여부, FTK 경고 무시 여부, ZIP 암호 설정, 파일 전송 후 로컬 사본 유지 여부



[그림 5. 모듈 옵션 설정 화면]

2) 관련 아티팩트는 레지스트리 분석 결과, 파일 메타데이터, 시스템 구성 정보 등이 있다.

(예) Use Module options → RECcmd(레지스트리 분석 도구) 선택 → 소스 및 저장 경로 지정 → Execute

V. 참고 자료

[1] Kroll, 「Kroll Artifact Parser and Extractor (KAPE)」, Kroll Inc, N/A, 2023.

[2] Kroll, 「KAPE Documentation and Resources」, Kroll Inc, N/A, 2023.

[3] Kroll, 「KAPE: Artifact Parser and Extractor Tool Overview」, Kroll Inc, N/A, 2023.