

4주차 스터디

통합 분석 도구 소개 + 웹 브라우저, LNK (바로가기), Jumplist 분석

KEEPER CTF IR-2 문제 풀이

거의 모든 사람은 어떤 것이 자신에게 맞는다고 생각하면 그것만 사용하려고 한다.

처음에는 다른 포렌식 툴을 사용하지 않는 핑계들이 합리적으로 들릴 수 있겠지만 실제로는 전혀 그렇지 않다.

다른 툴에 대해서 배우는 것을 완전히 배제해서는 안 된다.

분석가가 수년간 닦아온 포렌식 능력을 활용하여 다양한 종류의 포렌식 프로그램을 사용해야 하는 것이다.

어떤 것이든 새로 시작하는 것은 어렵기 마련이다. 적어도 처음에는 어렵다.

자전거, 운전, 요리와 같은 활동들도 처음에는 어렵지만 시간이 지나가면 갈수록 익숙해져 나중에는 아무 생각 없이도 할 수 있게 되는 것들이다.

XWF를 이용한 포렌식 분석 - xii

단 하나의 프로그램으로 모든 것을 할 수 있는 프로그램이란 존재하지 않는다.
도구의 이해도가 높아짐에 따라 더 자주 사용할 수는 있겠지만.

하나의 프로그램만 사용하는 분석가들은 자신한테 미안해해야 한다.
대부분의 분석은 완전한 분석을 위해 여러 소프트웨어의 다양한 기능을 활용해야 하기 때문이다.

포렌식 소프트웨어와 하드웨어는 각각 서로 다른 목적을 가진 공구 상자에 있는 공구라고 생각하면 된다.

마치 못을 박을 때 망치만 필요한 것이 아니라 못을 빼는 도구도 필요한 것과 같은 이치다.

XWF를 이용한 포렌식 분석 - xv

통합 분석 도구란?

- 디지털 증거 수집, 분석 등 지금까지 수동으로 했던 작업들을 하나의 도구에서 모두 처리할 수 있다.
- 많은 기능들이 포함되어 있어 분석 도구의 용량이 크고, 사용법을 익히기가 어렵다. 또한 원활한 동작을 위해 고사양 PC가 필요하다.
 - 도구 개발 회사에서 별도의 자격증을 운영하고 있다.³
- 실무에서 거의 필수적으로 사용된다.
 - 분석 케이스가 방대하며, 빠르게 분석을 수행해야 한다. → 각각의 아티팩트 분석 도구를 수동으로 실행하여 보는 것은 비효율적

| Tool | Description |
|--|---|
| <u>X-Ways Forensics</u> (<u>WinHex</u>) | 파일시스템의 상세한 구조까지 모두 직접 확인 가능하고 필터링과 검색 기능이 뛰어나며 무엇보다도 가볍다. 파일시스템 해석 기능만 필요하다면 WinHex 제품으로도 충분하다. |
| <u>Magnet AXIOM</u> | 아티팩트 분석 기능과 레코드 복구 기능이 탁월한 도구로 파일시스템에 대한 이해 없이도 쉽게 사용 흔적을 확인할 수 있다. 하지만, 아티팩트 구조와 해석 방법에 대한 정확한 이해가 있어야 정확한 판단이 가능하다. |

¹ <https://blog.plainbit.co.kr/dforensics-specialist-tools/>

² http://forensic.korea.ac.kr/DFWIKI/index.php/통합_디지털_포렌식_도구

³ <http://www.forensic-artifacts.com/license/ace>

Autopsy

- 오픈소스, 공짜로 사용할 수 있는 종합 분석 도구 → 상용 도구에 비해 완성도, 기능은 떨어지지만 무료라는 장점이 있다.
- Autopsy 프로그램에 적용된 분석 플러그인들의 결과를 **Data Artifacts**, **Analysis Result**에서 확인할 수 있다.
 - 플러그인 개발 및 기여 가능 - [autopsy_addon_modules](#), [docs](#)

The screenshot shows the Autopsy 4.21.0 interface. The top menu bar includes Case, View, Tools, Window, and Help. The toolbar contains icons for Add Data Source, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report, and Close Case. On the left, a sidebar navigation tree shows Data Sources (240103.E01_1 Host, 240103.E01), File Views (File Types, Deleted Files, MB File Size), Data Artifacts (Installed Programs 41, Operating System Information 1, Recent Documents 24, Run Programs 474, Shell Bags 19, USB Device Attached 9, Web Bookmarks 1, Web Cookies 25, Web History 9), Analysis Results (Encryption Suspected 1, Web Categories 2). The main central area is titled 'Listing' under 'Web History' and shows a table of results. The table has columns: Source Name, S, C, O, URL, Program Name, Domain, Username, and Data Source. There are 9 results listed, all from Microsoft Edge Analyzer, User domain, and 240103.E01 source. The 'Web History' item in the sidebar is highlighted.

| Source Name | S | C | O | URL | Program Name | Domain | Username | Data Source |
|-----------------|---|---|---|---|-------------------------|----------|----------|-------------|
| WebCacheV01.dat | | | | file:///D:/autorun.ico | Microsoft Edge Analyzer | | User | 240103.E01 |
| WebCacheV01.dat | | | | file:///C:/Users/User/Downloads/2023년%208월%20회계부.png | Microsoft Edge Analyzer | | User | 240103.E01 |
| WebCacheV01.dat | | | | file:///C:/Users/User/Downloads/2023년%205월%20회계부.png | Microsoft Edge Analyzer | | User | 240103.E01 |
| WebCacheV01.dat | | | | file:///C:/Users/User/Downloads/2023년%209월%20회계부.png | Microsoft Edge Analyzer | | User | 240103.E01 |
| WebCacheV01.dat | | | | file:///C:/Users/User/Downloads/11월_회계부.rar | Microsoft Edge Analyzer | | User | 240103.E01 |
| WebCacheV01.dat | | | | file:///C:/Users/User/Downloads/x86%20x86_64%20아키텍처%20차이.pdf | Microsoft Edge Analyzer | | User | 240103.E01 |
| WebCacheV01.dat | | | | ms-gamingoverlay://kglcheck/ | Microsoft Edge Analyzer | | User | 240103.E01 |
| WebCacheV01.dat | 0 | | | https://login.live.com/oauth20_desktop.srf?lc=2066 | Microsoft Edge Analyzer | live.com | User | 240103.E01 |
| WebCacheV01.dat | 0 | | | https://login.live.com/oauth20_authorize.srf?client_id=00000000480728C... | Microsoft Edge Analyzer | live.com | User | 240103.E01 |

Autopsy

Ingest Modules

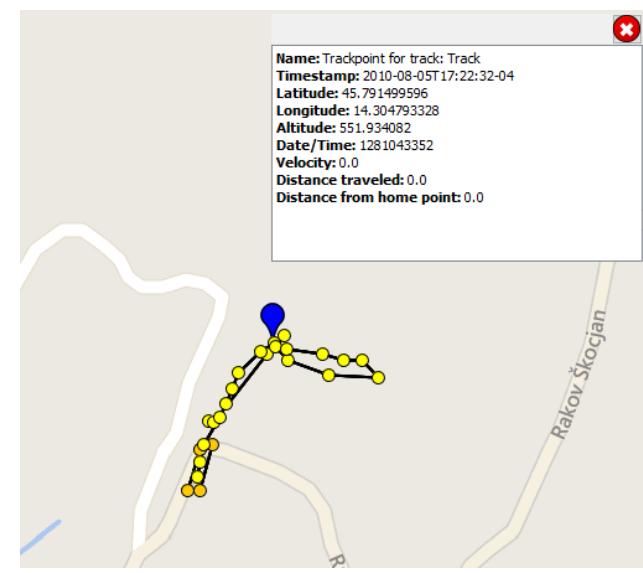
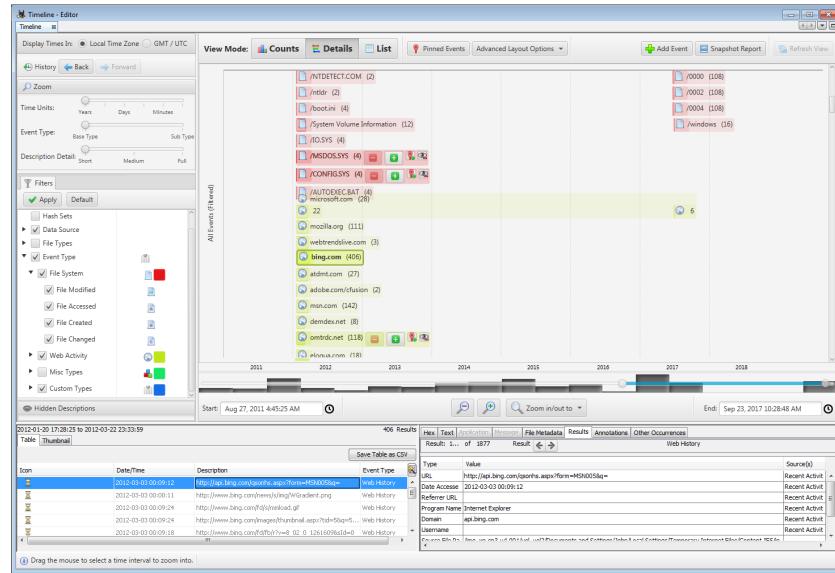
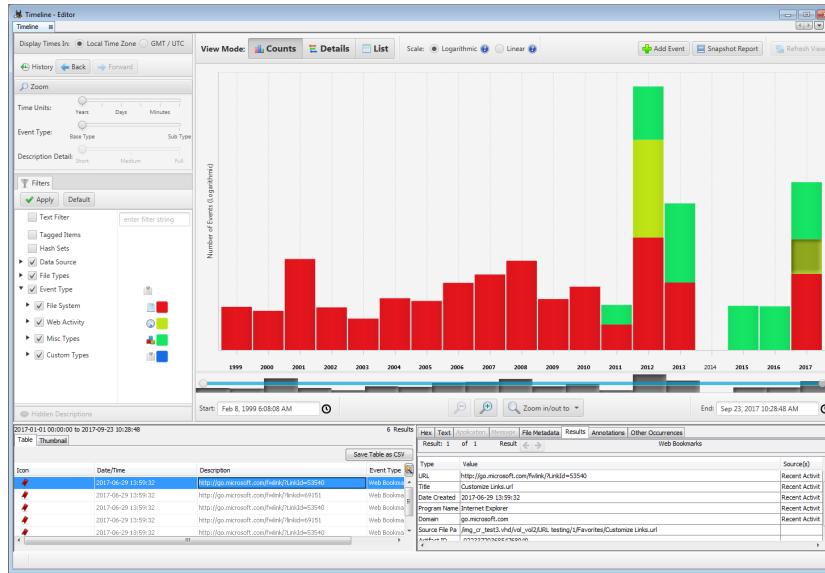
Ingest modules are responsible for analyzing the data source contents and will run in the background. The Ingest Modules analyze files in a prioritized order so that files in a user's directory are analyzed before files in other folders. Ingest modules can be developed by third-parties.

The standard ingest modules included with Autopsy are:

- **Recent Activity Module** extracts user activity as saved by web browsers and the OS. Also runs Regripper on the registry hive.
- **Hash Lookup Module** uses hash sets to ignore known files from the NIST NSRL and flag known bad files. Use the "Advanced" button to add and configure the hash sets to use during this process. You will get updates on known bad file hits as the ingest occurs. You can later add hash sets via the Tools -> Options menu in the main UI. You can download an index of the NIST NSRL from <http://sourceforge.net/projects/autopsy/files/NSRL/>
- **File Type Identification Module** determines file types based on signatures and reports them based on MIME type. It stores the results in the Blackboard and many modules depend on this. It uses the Tika open source library. You can define your own custom file types in Tools, Options, File Types.
- **Extension Mismatch Detector Module** uses the results from the File Type Identification and flags files that have an extension not traditionally associated with the file's detected type. Ignores 'known' (NSRL) files. You can customize the MIME types and file extensions per MIME type in Tools, Options, File Extension Mismatch.
- **Embedded File Extraction Module** opens ZIP, RAR, other archive formats, Doc, Docx, PPT, PPTX, XLS, and XLSX and sends the derived files from those files back through the ingest pipeline for analysis.
- **Picture Analyzer Module** extracts EXIF information from JPEG files and posts the results into the tree in the main UI. Also converts HEIC/HEIF files to JPEG format and extracts EXIF data from those JPEGs.
- **Keyword Search Module** uses keyword lists to identify files with specific words in them. You can select the keyword lists to search for automatically and you can create new lists using the "Advanced" button. Note that with keyword search, you can always conduct searches after ingest has finished. The keyword lists that you select during ingest will be searched for at periodic intervals and you will get the results in real-time. You do not need to wait for all files to be indexed before performing a keyword search, however you will only get results from files that have already been indexed when you perform your search.
- **Email Parser Module** identifies Thunderbird MBOX files and PST format files based on file signatures, extracting the e-mails from them, adding the results to the Blackboard.
- **Encryption Detection Module** looks for encrypted files.
- **Interesting Files Identifier Module** searches for files and directories based on user-specified rules in Tools, Options, Interesting Files. It works as a "File Alerting Module". It generates messages in the inbox when specified files are found.
- **Central Repository Module** adds file hashes and other extracted properties to a central repository for future correlation and to flag previously notable files.
- **PhotoRec Carver Module** carves files from unallocated space and sends them through the file processing chain.
- **Virtual Machine Extractor Module** extracts data from virtual machine files
- **Data Source Integrity Module** computes a checksum on E01 files and compares with the E01 file's internal checksum to ensure they match.
- **DJI Drone Analyzer** extracts data from drone files.
- **Plaso** uses Plaso to create **timeline** events.
- **Android Analyzer Module** allows you to parse common items from Android devices. Places artifacts into the BlackBoard.
- **GPX Analyzer** extracts geolocation data from .gpx files.
- **iOS Analyzer (iLEAPP)** extracts data from iOS data sources.

¹ https://sleuthkit.org/autopsy/docs/user-docs/4.19.3/quick_start_guide.html#s1c

Autopsy



- 위와 같이 시각화를 해주는 기능도 존재한다. (타임라인 시각화, 좌표 시각화 등)
- 그러나 잘 쓰이진 않는 것 같다. 더 좋은 도구들이 많이 있기 때문이다. (AXIOM, X-Ways 등)

¹ https://sleuthkit.org/autopsy/docs/user-docs/4.19.3/timeline_page.html

² https://sleuthkit.org/autopsy/docs/user-docs/4.19.3/geolocation_page.html

참고자료

- [Starting a New Digital Forensic Investigation Case in Autopsy 4.19+ - Part1](#)
- [Data Artifacts, Analysis Results and Reporting in Autopsy 4.19+ - Part2](#)
- [Disk Analysis with Autopsy | HackerSploit Blue Team Training](#)
- [Autopsy User Documentation](#)
- [Autopsy User's Guide](#)

- Windows, MAC, Memory, Mobile 등 다양한 환경의 아티팩트들을 분석하는 기능이 존재한다.¹
- 사용자에게 편의성을 제공하는 다양한 기능들과 UI 또한 깔끔하다.² → 실무에서 많이 사용한다고 한다.

컴퓨터 아티팩트

모두 지우기

- P2P (8/11)
- 맞춤형 아티팩트 (4/5)
- 메모리 (0/32)
- 문서 (18/18)
- 미디어 (12/12)
- 소셜 네트워킹 (8/9)
- 암호화 & 로그인 정보 (5/5)
- 애플리케이션 사용량 (9/9)
- 연결된 디바이스 (9/9)
- 운영 체제 (68/72)
- 웹 관련 (13/18)
- 위치 & 여행 (1/1)
- 이메일 및 캘린더 (13/14)
- 추가 소스 (4/4)
- 커뮤니케이션 (26/39)
- 클라우드 저장소 (6/6)
- 휴대폰 아티팩트 (1/1)

웹 관련

모두 보기

- Bing 도구 모음 웹 관련
- Chrome 웹 관련 옵션
- Edge/Internet Explorer 웹 관련 옵션
- Firefox 웹 관련 옵션
- Google 애널리틱스 웹 관련

컴퓨터 아티팩트

모두 지우기

- P2P (8/11)
- 맞춤형 아티팩트 (4/5)
- 메모리 (0/32)
- 문서 (18/18)
- 미디어 (12/12)
- 소셜 네트워킹 (8/9)
- 암호화 & 로그인 정보 (5/5)
- 애플리케이션 사용량 (9/9)
- 연결된 디바이스 (9/9)
- 운영 체제 (68/72)
- 웹 관련 (13/18)
- 위치 & 여행 (1/1)
- 이메일 및 캘린더 (13/14)

운영 체제

모두 보기

- PowerShell 운영 체제
- Shellbag 운영 체제
- Shim 캐시 운영 체제
- SRUM 운영 체제

¹ <https://blog.plainbit.co.kr/magnet-axiom-introduce/>

² <https://blog.plainbit.co.kr/axiom-messageanalysis-options/>

Magnet AXIOM Process 7.8.0.38310 - 1

파일 도구 도움말

증거 분석

사례 세부 정보

증거 소스 5

- 처리 세부 정보
- 아카이브 및 모바일 백업 검색 [켜기](#)
- 파일 기반 암호화 해제
- 검색 키워드 추가
- 파일에서 텍스트 추출 (OCR)
- 해시 및 일치 항목 찾기 [꺼기](#)
- Magnet.AI로 채팅 분석
- Magnet.AI로 사진 분석
- YARA 규칙으로 검색
- 추가 아티팩트 찾기

아티팩트 세부 정보 205

- 모바일 아티팩트
- 클라우드 아티팩트
- 컴퓨터 아티팩트 205/265
- 차량 아티팩트
- 아티팩트 구문 분석 및 카빙
- 권한 있는 콘텐츠
- 날짜 범위 필터

증거 분석

처리할 소스

| 유형 | 이미지 - 위치 이름 | 증거 번호 | 검색 유형 | 시작 날짜/시간 - 현지 시간 |
|-----------|--|------------|------------|-----------------------|
| Partition | 240103.E01 - Partition 1 (Microsoft FAT32, 100 MB) NO NAME | 240103.E01 | 전체 | 2024-01-29 PM 9:02:06 |
| Partition | 240103.E01 - Partition 2 (16 MB) - 알려진 파일 시스템이 없음 | 240103.E01 | 섹터 레벨 | 2024-01-29 PM 9:03:43 |
| Partition | 240103.E01 - Partition 3 (Microsoft NTFS, 19.32 GB) | 240103.E01 | 전체 | 2024-01-29 PM 9:04:04 |
| Partition | 240103.E01 - Partition 4 (Microsoft NTFS, 573 MB) | 240103.E01 | 전체 | |
| Partition | 240103.E01 - 분할되지 않은 공간 | 240103.E01 | 분할되지 않은 공간 | |

검색 진행 중

경과된 시간: 3:12

현재 검색 위치

240103.E01 - Partition 3 (Microsoft NTFS, 19.32 GB) 검색 중 - Partition 3 (Microsoft NTFS, 19.32 GB) 10%

Search Definitions:

| | |
|--|--------------------|
| Partition 3 (Microsoft NTFS, 19.32 GB) | 완료 |
| Writing Filesystem Information | 검색 중 - 0% - (0:20) |
| pagefile.sys / swapfile.sys | 준비 |
| \$LogFile | 준비 |
| \$MFT | 준비 |
| All Files and Folders | 준비 |
| Volume Shadow Copies | 준비 |
| Unallocated Clusters | 준비 |
| File Slack Space | 준비 |
| hiberfil.sys | 준비 |
| Uninitialized File Area | 준비 |
| 중첩 컨테이너 발견: 0 | |

Thread Details:

취소 증거 분석

Magnet AXIOM Examine v7.8.0.38310 - 1

파일(F) 도구 프로세스 도움말(H)

필터 증거 아티팩트 콘텐츠 유형 날짜 및 시간 태그 및 주석 프로필 부분 결과 키워드 목록 스크립트 분석

검색 등록 입력... 이동 고급

증거 (382)

C:\Users\WUser\Downloads...

| 아티팩트 | 주요 세부 정보 | 지원 세부 정보 | 추가 세부 정보 |
|------------------|--|---|---------------------|
| 클라우드 서비스 URL | OneDrive | https://api.onedrive.com/v1.0/drive/items/[tab] | |
| 상세 결과 | 사이트 이름 | URL | |
| 소셜 미디어 URL | Teams | https://config.teams.microsoft.com/config/v1... | |
| 상세 결과 | 경로 | 경로 유형 | 액세스한 날짜/시간 - 현지 시간 |
| 로컬에서 접근한 파일 및... | D:\autorun.ico | Drive | 2024-01-03 16:53:01 |
| 상세 결과 | 경로 | 경로 유형 | 액세스한 날짜/시간 - 현지 시간 |
| 로컬에서 접근한 파일 및... | :Host: 내 PC | Virtual | 2024-01-03 16:53:01 |
| 상세 결과 | 경로 | 경로 유형 | 액세스한 날짜/시간 - 현지 시간 |
| 로컬에서 접근한 파일 및... | C:\Users\User\Downloads\2023년 8월 회계부.png | Drive | 2024-01-03 17:02:23 |
| 상세 결과 | 경로 | 경로 유형 | 액세스한 날짜/시간 - 현지 시간 |
| 로컬에서 접근한 파일 및... | C:\Users\User\Downloads\2023년 8월 회계부.png | Drive | 2024-01-03 17:02:23 |
| 상세 결과 | 경로 | 경로 유형 | 액세스한 날짜/시간 - 현지 시간 |
| 로컬에서 접근한 파일 및... | C:\Users\User\Downloads\2023년 5월 회계부.png | Drive | 2024-01-03 17:02:25 |
| 상세 결과 | 경로 | 경로 유형 | 액세스한 날짜/시간 - 현지 시간 |
| 로컬에서 접근한 파일 및... | C:\Users\User\Downloads\2023년 5월 회계부.png | Drive | 2024-01-03 17:02:25 |
| 상세 결과 | 경로 | 경로 유형 | 액세스한 날짜/시간 - 현지 시간 |
| 로컬에서 접근한 파일 및... | C:\Users\User\Downloads\2023년 9월 회계부.png | Drive | 2024-01-03 17:02:27 |
| 상세 결과 | 경로 | 경로 유형 | 액세스한 날짜/시간 - 현지 시간 |
| 로컬에서 접근한 파일 및... | C:\Users\User\Downloads\2023년 9월 회계부.png | Drive | 2024-01-03 17:02:27 |
| 상세 결과 | 경로 | 경로 유형 | 액세스한 날짜/시간 - 현지 시간 |
| 로컬에서 접근한 파일 및... | C:\Users\User\Downloads\11월_회계부.rar | Drive | 2024-01-03 17:04:29 |
| 상세 결과 | 경로 | 경로 유형 | 액세스한 날짜/시간 - 현지 시간 |
| 로컬에서 접근한 파일 및... | C:\Users\User\Downloads\11월_회계부.rar | Drive | 2024-01-03 17:04:29 |
| 상세 결과 | 경로 | 경로 유형 | 액세스한 날짜/시간 - 현지 시간 |
| 로컬에서 접근한 파일 및... | C:\Users\User\Downloads\x86_x86_64 아키텍처 차이.pdf | Drive | 2024-01-03 17:15:03 |
| 상세 결과 | 경로 | 경로 유형 | 액세스한 날짜/시간 - 현지 시간 |
| 로컬에서 접근한 파일 및... | C:\Users\User\Downloads\x86_x86_64 아키텍처 차이.pdf | Drive | 2024-01-03 17:15:03 |
| 상세 결과 | 경로 | 경로 유형 | 액세스한 날짜/시간 - 현지 시간 |
| 로컬에서 접근한 파일 및... | :Host: login.live.com | Virtual | 2024-01-03 17:18:26 |

세부 정보

아티팩트 정보

경로 C:\Users\User\Downloads\11월_회계부.rar
경로 유형 Drive
액세스한 날짜/시간 - 현지 시간 2024-01-03 17:04:29
사용자 User
액세스 횟수 1
유형 로컬에서 접근한 파일
항목 ID 64458
원본 아티팩트 Edge/Internet Explorer 10-11 Daily/Weekly History

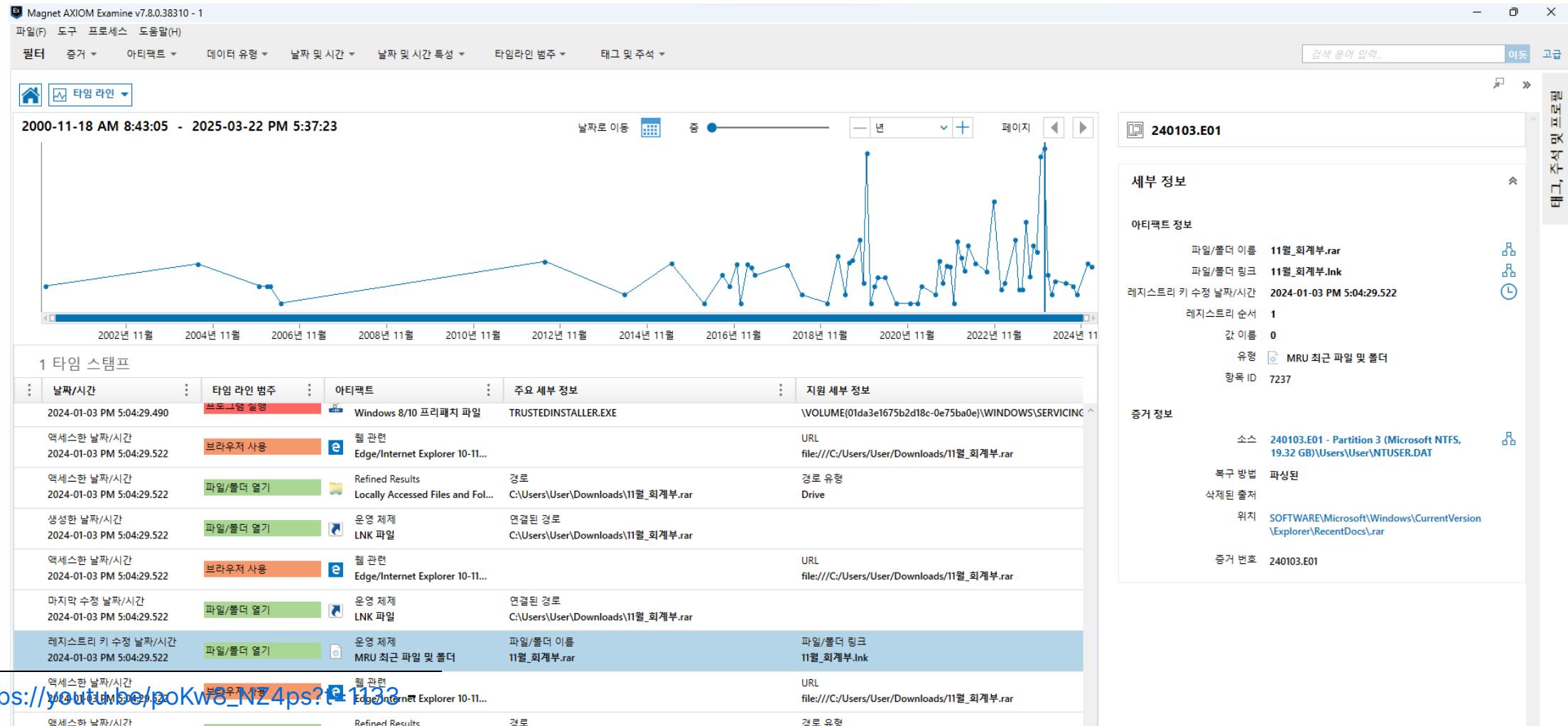
증거 정보

소스 240103.E01 - Partition 3 (Microsoft NTFS, 19.32 GB)\Users\WUser\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

복구 방법

삭제된 출처 위치 Table: Container_7 (UrlHash: 3475886728550291773)

- 타임라인 분석 기능¹



¹ https://youtube.be/poKw8_NZ4ps?t=1133

- 검색, 필터 기능¹

Magnet AXIOM Examine v7.8.0.38310 - 1

파일(F) 도구 프로세스 도움말(H)

필터 증거 아티팩트 콘텐츠 유형 날짜 및 시간 태그 및 주석 프로필 부분 결과 키워드 목록 스크립트 분석 11월 X

필터 지우기 11월 이동 고급

일치하는 결과 (67,809개 중 27개) 열 보기

| 아티팩트 | 주요 세부 정보 | 지원 세부 정보 | 추가 세부 정보 | 날짜 및 시간 | 항목 ID |
|----------------------------|---|------------------------------------|---|---|-------|
| 상세 결과 로컬에서 접근... | 경로 C:\Users\User\Downloads\11월_회계부.rar | 경로 유형 Drive | 액세스한 날짜/시간 - 현지 시간 2024-01-03 17:04:29 | | 64458 |
| 상세 결과 로컬에서 접근... | 경로 C:\Users\User\Downloads\11월_회계부.rar | 경로 유형 Drive | 액세스한 날짜/시간 2024-01-03 PM 5:04:29.522 | | 62613 |
| 상세 결과 로컬에서 접근... | 경로 C:\Users\User\Downloads\11월_회계부.rar | 경로 유형 Drive | 액세스한 날짜/시간 - 현지 시간 2024-01-03 17:04:29 | | 62626 |
| 상세 결과 로컬에서 접근... | 경로 C:\Users\User\Downloads\11월_회계부.rar | 경로 유형 Drive | 액세스한 날짜/시간 2024-01-03 PM 5:04:29.522 | | 64588 |
| e 웹 관련 Edge/Internet... | 사용자 User | URL file:///C:/Users/User/Do... | 액세스 횟수 1 | | 64457 |
| e 웹 관련 Edge/Internet... | 사용자 User | URL file:///C:/Users/User/Do... | 액세스 횟수 1 | | 62624 |
| e 웹 관련 Edge/Internet... | 사용자 User | URL file:///C:/Users/User/Do... | 액세스 횟수 1 | | 64758 |
| e 웹 관련 Edge/Internet... | | URL file:///C:/Users/User/Do... | 사용자 User | 액세스한 날짜/시간 2024-01-03 PM 5:04:29.522 | 64773 |
| e 웹 관련 Edge/Internet... | | URL file:///C:/Users/User/Do... | 사용자 User | 액세스한 날짜/시간 2024-01-03 PM 5:04:29.522 | 62603 |
| e 웹 관련 Edge/Internet... | | URL file:///C:/Users/User/Do... | 사용자 User | 액세스한 날짜/시간 2024-01-03 PM 5:04:29.522 | 64587 |
| 문서 텍스트 문서 | 파일 이름 AppCache133487434468756669.txt | 크기(바이트) 90945 | 생성한 날짜/시간 2024-01-03 PM 5:17:27.000 | 마지막 수정 날짜/시간 2024-01-03 PM 5:17:27.000 | 63852 |
| 문서 텍스트 문서 | 파일 이름 AppCache133487435096486503.txt | 크기(바이트) 90948 | 생성한 날짜/시간 2024-01-03 PM 5:18:32.000 | 마지막 수정 날짜/시간 2024-01-03 PM 5:18:32.000 | 63853 |
| 문서 텍스트 문서 | 파일 이름 AppCache133487427280512612.txt | 크기(바이트) 90910 | 생성한 날짜/시간 2024-01-03 PM 5:16:27.000 | 마지막 수정 날짜/시간 2024-01-03 PM 5:16:27.000 | 63849 |

C:\Users\User\Downloads... 240103.E01

세부 정보

아티팩트 정보

경로 C:\Users\User\Downloads\11월_회계부.rar
경로 유형 Drive
액세스한 날짜/시간 - 현지 시간 2024-01-03 17:04:29
사용자 User
액세스 횟수 1
유형 로컬에서 접근한 파일
항목 ID 64458

원본 아티팩트 Edge/Internet Explorer 10-11 Daily/Weekly History

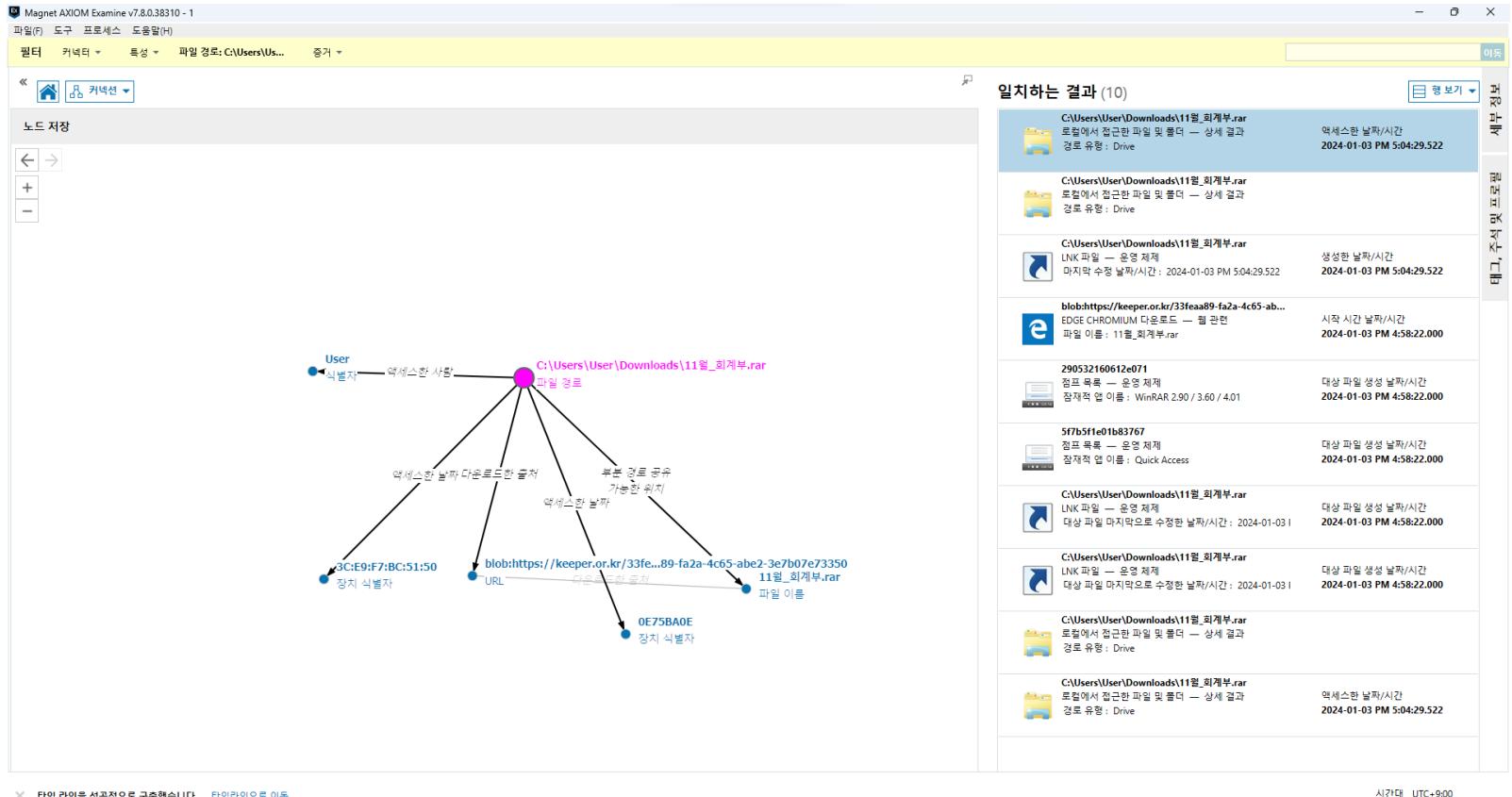
증거 정보

소스 240103.E01 - Partition 3 (Microsoft NTFS, 19.32 GB)\Users\User\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

¹ <https://youtu.be/lB-YcOGsBHM?t=956>

- 커넥션 탐색 기능¹

| 아티팩트 정보 | |
|-------------|---|
| 다운로드 소스 | blob: https://keeper.or.kr/33feaa89-fa2a-4c65-abe2-3e7b07e73350 |
| 파일 이름 | 11월_회계부.rar |
| 시작 시간 날짜/시간 | 2024-01-03 PM 4:58:22.000 |
| 종료 시간 날짜/시간 | 2024-01-03 PM 4:58:45.000 |
| 다음 대상에 저장 | C:\Users\User\Downloads\11월_회계부.rar |



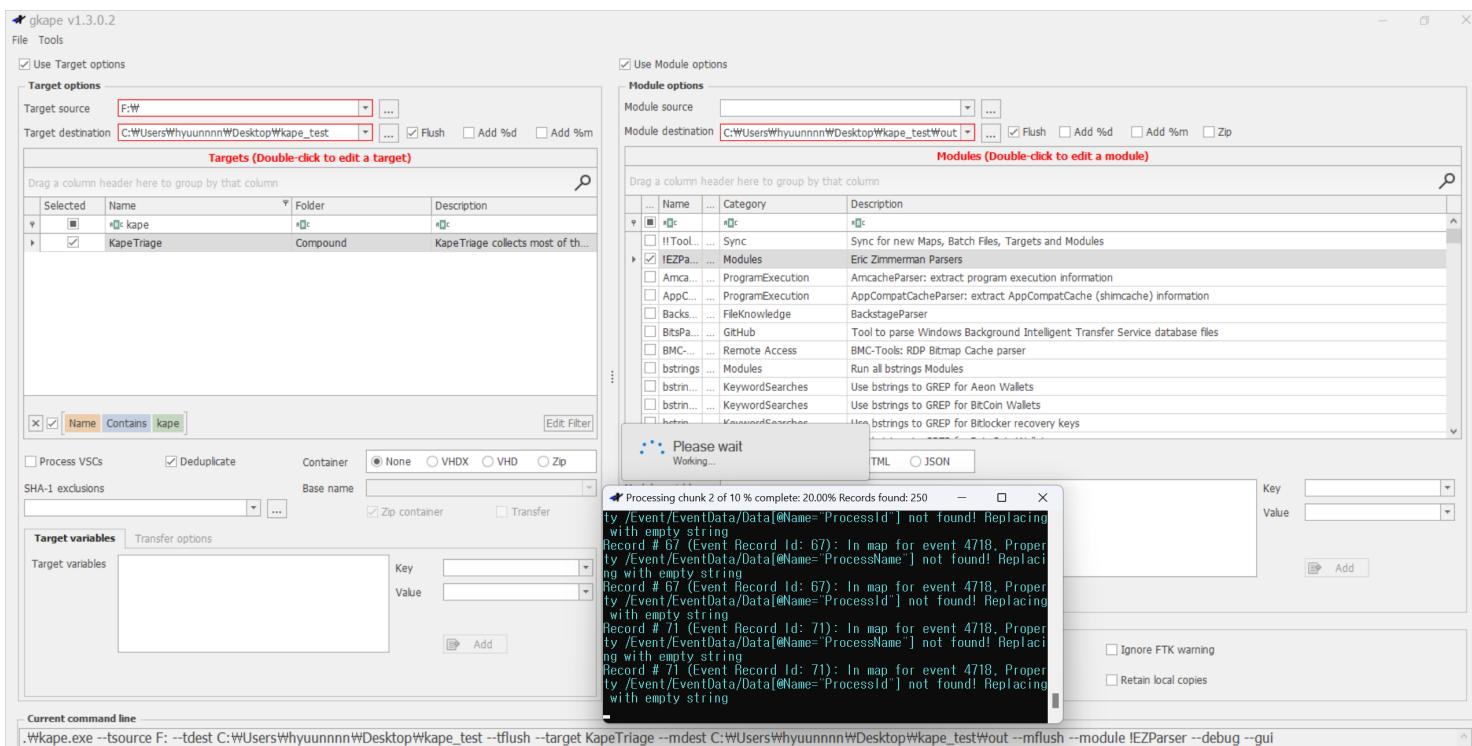
¹ https://youtu.be/poKw8_NZ4ps?t=879

참고자료

- Magnet AXIOM - system32
- AXIOM - plainbit
- AXIOM 실무 활용 가이드
- Getting Started with Magnet AXIOM
- MAGNET AXIOM PRODUCT DOCUMENTATION
- Magnet AXIOM User Guide

KAPE

- one-click 으로 아티팩트 수집과 분석을 한 번에 해주는 도구
- AXIOM, EnCase와 같은 프로그램을 대체하기 위한 프로그램이 아니라고 한다.¹
→ 빠른 수집 및 분석을 보완해주는 또 다른 도구일 뿐이다.



¹ <https://youtu.be/DXE0INTu9ek?t=360>

KAPE

- 특정 경로에 접근하여 파일들을 수집한 후 수동으로 아티팩트 분석 도구에 업로드하여 분석했었지만, KAPE를 사용하면 모든 과정을 자동으로 수행한다. → 반복 작업이 줄어든다.
- 수집해야 하는 경로는 고정되어 있다. (레지스트리, 이벤트 로그 등) → 이러한 정보들을 기록하여 사용

The screenshot shows the KAPE configuration interface. On the left is the 'Target options' panel, which includes fields for 'Target source' (set to F:\) and 'Target destination' (set to C:\Users\hyuunnnn\Desktop\kape_test). It also contains sections for 'Targets' and 'Modules'. On the right is the 'Module options' panel, which includes fields for 'Module source' and 'Module destination' (both set to C:\Users\hyuunnnn\Desktop\kape_test\out). It also contains sections for 'Targets' and 'Modules'.

| Selected | Name | Folder | Description |
|-------------------------------------|-----------|---------|-------------|
| <input checked="" type="checkbox"/> | mft | File | |
| <input type="checkbox"/> | \$MFT | Windows | \$MFT |
| <input type="checkbox"/> | \$MFTMirr | Windows | \$MFTMirr |

| Sel... | Name | Folder | Category | Description |
|-------------------------------------|----------------|----------|------------|---|
| <input checked="" type="checkbox"/> | mft | File | FileSystem | MFTECmd: process all files handled by MFTECmd |
| <input type="checkbox"/> | MFTECmd | Compound | FileSystem | MFTECmd: process \$Boot files |
| <input type="checkbox"/> | MFTECmd_\$B... | MFTECmd | FileSystem | MFTECmd: process \$Boot files |

- Target: 어떤 경로에 있는 파일들을 수집할 것인지
 - .tkape 확장자 사용 - /Targets 폴더
- Module: 어떤 파일을 어떤 도구로 분석할 것인지, 커맨드 라인은 어떻게 입력할 것인지
 - .mkape 확장자 사용 - /Modules 폴더

With that being said, gather your image(s) and mount them via [Arsenal Image Mounter](#), it's free! Do not use [FTK Imager](#) for mounting your images as your images will be mounted as a network share rather than a physical disk like with Arsenal Image Mounter. The benefit to being mounted as a physical disk is that it allows you access to Volume Shadow Copies. Both are the same price so you might as well use the tool that does the job better!

Mounting forensic images for use with KAPE

Use [Arsenal Image Mounter \(AIM\)](#) to access E01s and other forensic images. While there are other tools out there to mount images, AIM exposes the image as a physical device, which means the Volume Shadow Copies are made available to KAPE. AIM is free, so there is no reason to not use it.

WARNING: Do not use FTK Imager, Dokan, or similar! They will not work properly!

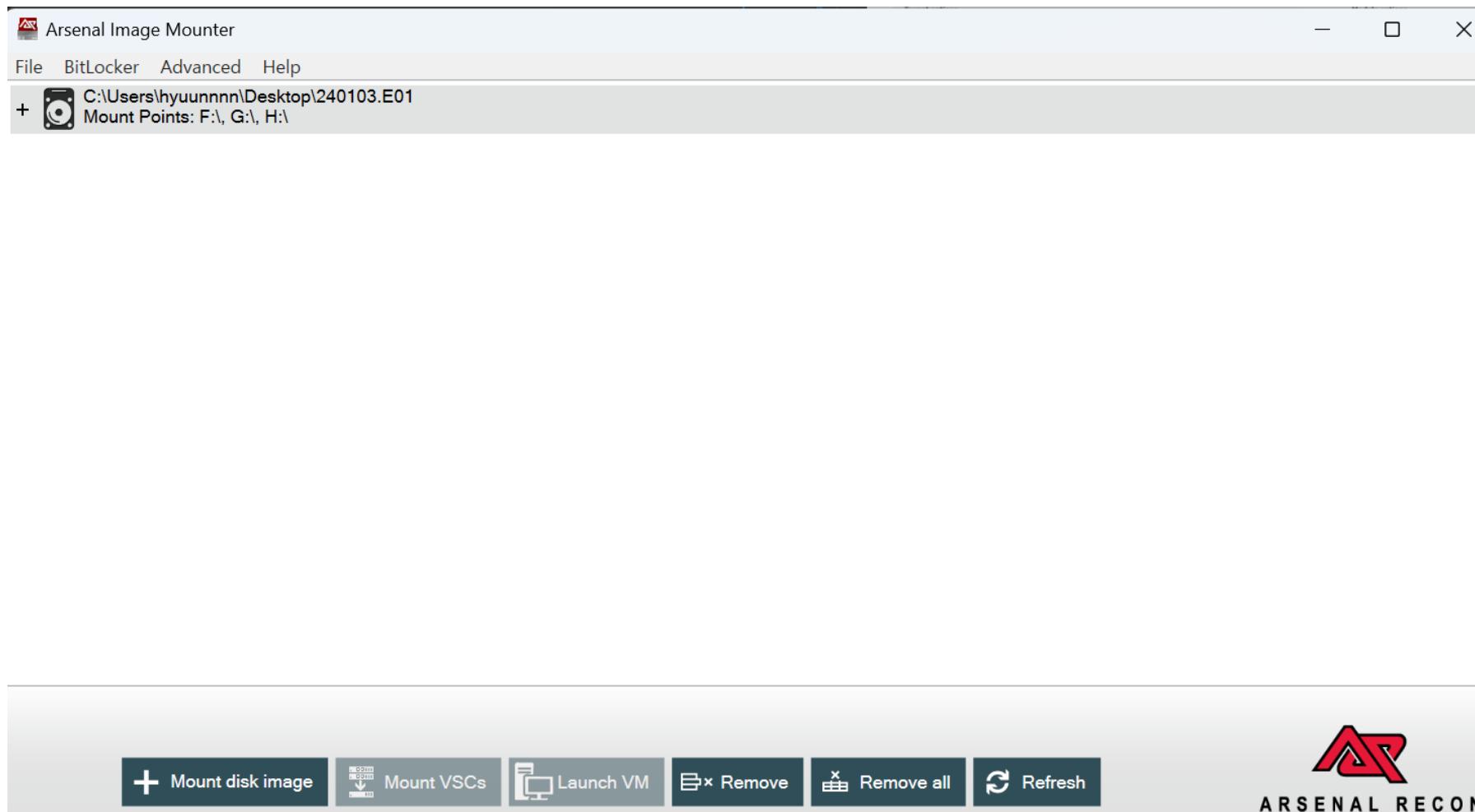
It is also recommended to mount E01s that are local to the system where KAPE will be run. Mounting image files over a network can cause issues if there is any disruption to the network connection, which can result in errors.

이미지 파일에 있는 파일들을 수집하려면 드라이브에 마운트를 해야 하는데,
이때 [FTK Imager](#)가 아닌 [Arsenal Image Mounter](#)를 사용하라고 한다.

¹ <https://aboutdfir.com/toolsandartifacts/windows/cape/2/>

² <https://ericzimmerman.github.io/KapeDocs/#!Pages\2.-Getting-started.md#some-basics>

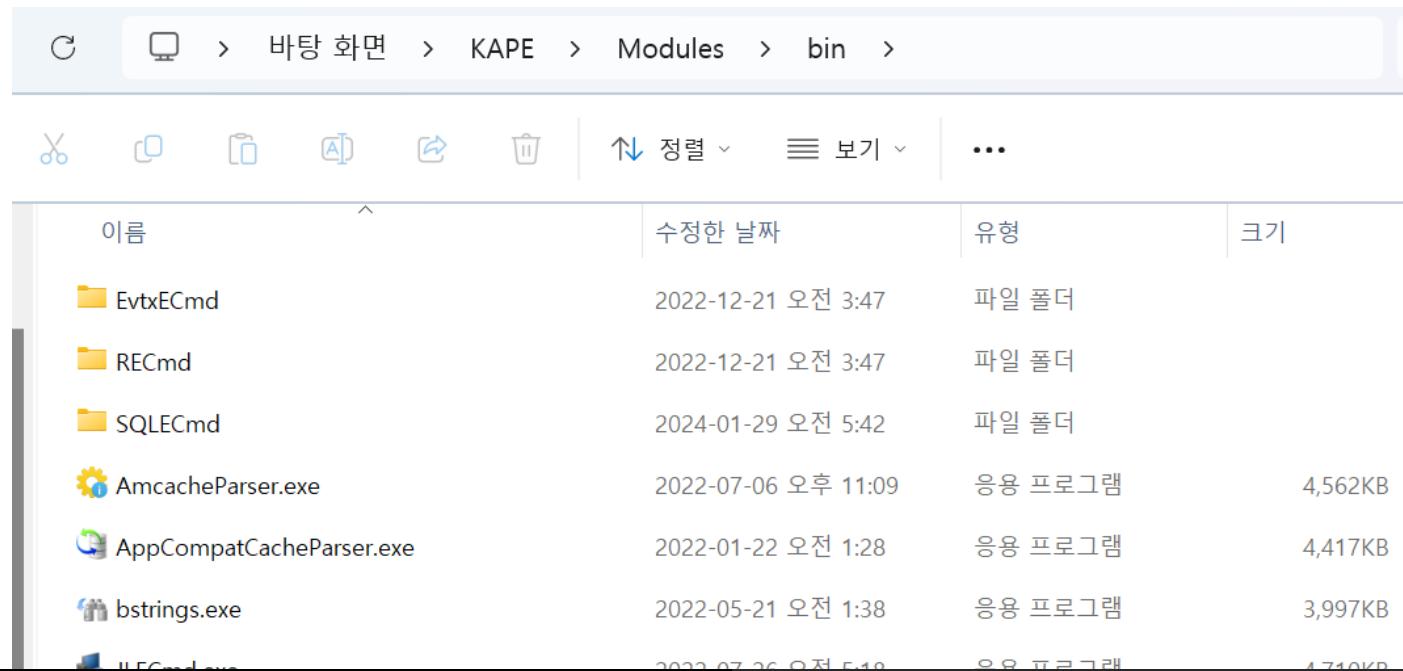
Arsenal Image Mounter



- Mount disk image → E01 파일 열기 → OK 버튼 클릭

KAPE

- Target은 KapeTriage 또는 !SANS_Triage , Module은 !EZParser 를 사용하면 된다.
→ Eric Zimmerman의 도구와 연동이 잘 되어 있다.
다른 도구들도 많이 추가되어 있다. - [NirSoft](#), [hindsight](#), [RegRipper](#) 등등 ([KapeFiles](#) 참고)
- 분석 도구들을 /Modules/bin 폴더에 넣어야 한다.
 - Eric Zimmerman의 도구들은 기본적으로 들어가 있다.



- 생성된 분석 결과들을 Timeline Explorer에 Drag & Drop 하여 분석하면 된다.

The screenshot shows the KAPE tool's user interface. On the left, there is a file browser window titled 'cape_test > out >'. It lists several CSV files categorized by type: EventLogs, FileDeletion, FileFolderAccess, FileSystem, ProgramExecution, Registry, and others. Some specific files like '20240128205208_AutomaticDestinations.csv' and '20240128205209_LeCmd_Output.csv' are highlighted. On the right, the 'Timeline Explorer v2.0.0.1' window is open, showing multiple tabs of event logs. Below the tabs, a table header 'Value Data' is visible with columns for Value and Data. A list of processes is displayed, including 'SnippingTool.exe', 'Calculator.exe', 'mspaint.exe', 'Windows.ShellExperienceHost.exe', 'MSEdge.exe', 'Windows.Explorer.exe', 'OpenWith.exe', 'setup64.exe', 'SearchUI.exe', 'SecHealthUI.exe', 'Apprep.ChxApp.exe', and 'disable-defender.exe'. At the bottom of the Timeline Explorer window, there is a 'Messages' section with log entries from January 28, 2024.

| Value | Data |
|---|------|
| {System32}\SnippingTool.exe | |
| Microsoft.WindowsCalculator_8wekyb3d8bbwe!App | |
| {System32}\mspaint.exe | |
| Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy!App | |
| MSEdge | |
| Microsoft.Windows.Explorer | |
| {System32}\OpenWith.exe | |
| D:\setup64.exe | |
| Microsoft.Windows.Search_cw5n1h2txyewy!CortanaUI | |
| Microsoft.Windows.SecHealthUI_cw5n1h2txyewy!SecHealthUI | |
| Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy!App | |
| C:\Users\User\Downloads\disable-defender (2).exe | |

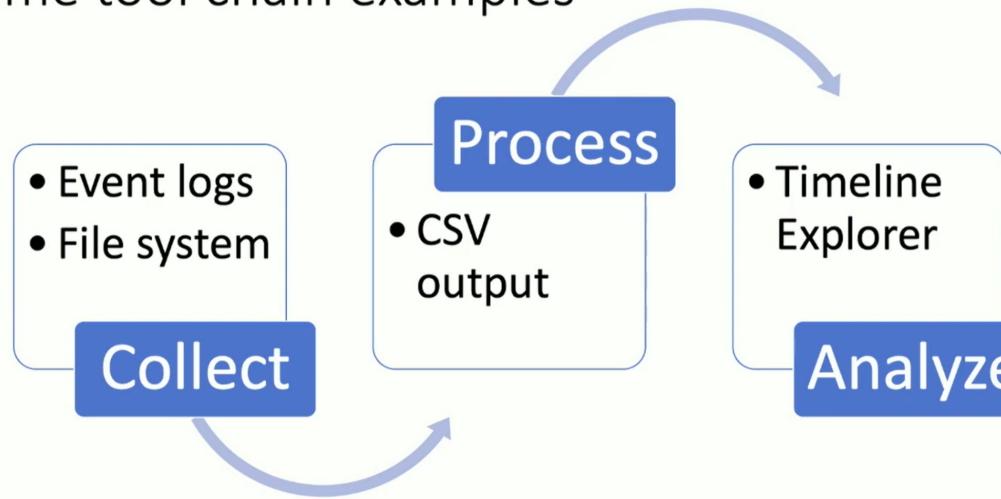
Messages

```

2024-01-28 22:09:56 [Information]: Loading "C:\Users\hyuunnn\Desktop\cape_test\out\ProgramExecution\20240129055150_Amcache_UnassociatedFileEntries.csv"
2024-01-28 22:09:56 [Information]: Found plugin with description "CSV generated from AmcacheParser for new File Entries format"

```

Some tool chain examples



¹ <https://youtu.be/ZCj7cbWwUOs?t=1314>

² <https://ericzimmerman.github.io/KapeDocs/#!index.md#how-kape-works>

참고자료

[Awesome-KAPE](#)

[KapeDocs](#)

[Kroll Artifact Parser and Extractor \(KAPE\) Official Demo](#)

[KAPE + EZ Tools and Beyond - OSDFCon 2019 - Eric Zimmerman](#)

[KAPE - AboutDFIR](#)

[Introduction to KAPE](#)

Plaso

Plaso (Plaso Langar Að Safna Öllu), or *super timeline all the things*, is a Python-based engine used by several tools for automatic creation of timelines. Plaso default behavior is to create super timelines but it also supports creating more targeted timelines.

These timelines support digital forensic investigators/analysts, to correlate the large amount of information found in logs and other files found on an average computer.

- 아티팩트 분석 및 타임라인 생성까지 전체적인 과정을 수행하는 도구¹
- 무료, Python으로 개발되었으며, 포렌식 타임라인 분석 도구인 [Timesketch](#)² 또는 [Timeline Explorer](#)를 활용한다. (개인적으로 [Timeline Explorer](#)가 편하다.)

¹ <https://plaso.readthedocs.io/en/latest/index.html>

² <https://medium.com/@ozan.unal/analysis-of-log-files-using-timesketch-fb68330ea67f>

Plaso

- WSL2에서 진행¹ - 2024. 01. 30 기준

```
sudo add-apt-repository universe
sudo add-apt-repository ppa:gift/stable
sudo apt-get update
sudo apt-get install plaso-tools
```

```
→ ~ log2timeline.py
2024-01-30 05:01:30,439 [INFO] (MainProcess) PID:6008 <data_location> Determined data location: /usr/share/plaso
2024-01-30 05:01:30,446 [INFO] (MainProcess) PID:6008 <artifact_definitions> Determined artifact definitions path: /usr/
share/artifacts
ERROR: Missing source path.

usage: log2timeline.py [-h] [--troubles] [-V] [--artifact_definitions PATH] [--custom_artifact_definitions PATH]
                      [--data PATH] [--archives TYPES] [--artifact_filters ARTIFACT_FILTERS]
                      [--artifact_filters_file PATH] [--extract_winreg_binary] [--preferred_year YEAR]
                      [--skip_compressed_streams] [-f FILE_FILTER] [--hasher_file_size_limit SIZE]
                      [--hashers HASHER_LIST] [--parsers PARSER_FILTER_EXPRESSION] [--yara_rules PATH]
                      [--partitions PARTITIONS] [--volumes VOLUMES] [--codepage CODEPAGE] [--language LANGUAGE_TAG]
                      [--no_extract_winevt_resources] [-z TIME_ZONE] [--no_vss] [--vss_only]
                      [--vss_stores VSS_STORES] [--credential TYPE:DATA] [-d] [-q] [-u] [--info] [--use_markdown]
                      [--no_dependencies_check] [--logfile FILENAME] [--status_view TYPE] [--status_view_file PATH]
                      [--status_view_interval SECONDS] [--buffer_size BUFFER_SIZE] [--queue_size QUEUE_SIZE]
                      [--single_process] [--process_memory_limit SIZE] [--temporary_directory DIRECTORY]
                      [--vfs_back_end TYPE] [--worker_memory_limit SIZE] [--worker_timeout MINUTES]
                      [--workers WORKERS] [--sigsegv_handler] [--profilers PROFILERS_LIST]
                      [--profiling_directory DIRECTORY] [--profiling_sample_rate SAMPLE_RATE] [--storage_file PATH]
                      [--storage_format FORMAT] [--task_storage_format FORMAT]
                      [SOURCE]
```

¹ <https://plaso.readthedocs.io/en/latest/sources/user/Ubuntu-Packaged-Release.html>

Plaso

- 병렬 처리가 되어 있지만 그래도 매우 느리다.
→ 모든 경로를 탐색하기 때문이다. (느린 원인에 Python도 한 몫을 하는 것 같다.)
 - KAPE의 Target 기능으로 선별하여 추출한 후 분석 도구를 사용하면 되겠다.¹
→ 정크 파일들을 제외하고 관심있는 데이터에만 집중

| plaso - log2timeline version 20231224 | | | | | |
|---------------------------------------|--------|---|-----------|------------|------------|
| Source path | | : /mnt/c/Users/hyuuunnn/Desktop/240103.E01 | | | |
| Source type | | : storage media image | | | |
| Processing time | | : 00:44:40 | | | |
| Tasks: | Queued | Processing | Merging | Abandoned | Total |
| | 1 | 1 | 26 | 0 | 41343 |
| Identifier | PID | Status | Memory | Sources | Event Data |
| Main | 5559 | running | 383.1 MiB | 135238 (0) | 47429 (30) |
| 8626 (3) | | NTFS:\Windows\Prefetch\WINLOGON.EXE-DEDDC9B6.pf | | | |
| Worker_01 | 5565 | idle | 293.3 MiB | 4099 (0) | 2400 (0) |
| Worker_02 | 5569 | idle | 281.1 MiB | 35590 (0) | 2469 (0) |
| Worker_03 | 5573 | idle | 249.1 MiB | 4567 (0) | 3695 (0) |
| Worker_04 | 5577 | idle | 271.4 MiB | 9329 (0) | 2431 (0) |
| Worker_05 | 5581 | idle | 273.3 MiB | 4131 (0) | 5712 (3) |
| Worker_06 | 5585 | idle | 297.9 MiB | 7681 (0) | 2556 (0) |
| Worker_07 | 5589 | idle | 279.5 MiB | 4183 (0) | 2653 (0) |
| Worker_08 | 5593 | idle | 291.5 MiB | 5227 (0) | 3108 (3) |
| Worker_09 | 5597 | idle | 273.0 MiB | 4201 (0) | 3103 (3) |
| Worker_10 | 5601 | idle | 273.7 MiB | 4341 (0) | 2446 (0) |
| Worker_11 | 5605 | idle | 276.4 MiB | 4490 (0) | 2641 (3) |
| Worker_12 | 5609 | idle | 274.6 MiB | 7320 (0) | 3689 (3) |
| Worker_13 | 5612 | idle | 264.7 MiB | 6749 (0) | 2427 (3) |
| Worker_14 | 5617 | idle | 267.5 MiB | 4794 (0) | 3898 (3) |
| Worker_15 | 5621 | idle | 295.0 MiB | 10657 (0) | 230254 (0) |
| Worker_16 | 5625 | idle | 276.7 MiB | 5236 (0) | 2890 (0) |
| Worker_17 | 5629 | idle | 281.8 MiB | 4065 (0) | 2772 (3) |
| Worker_18 | 5633 | idle | 278.3 MiB | 4570 (0) | 2457 (3) |

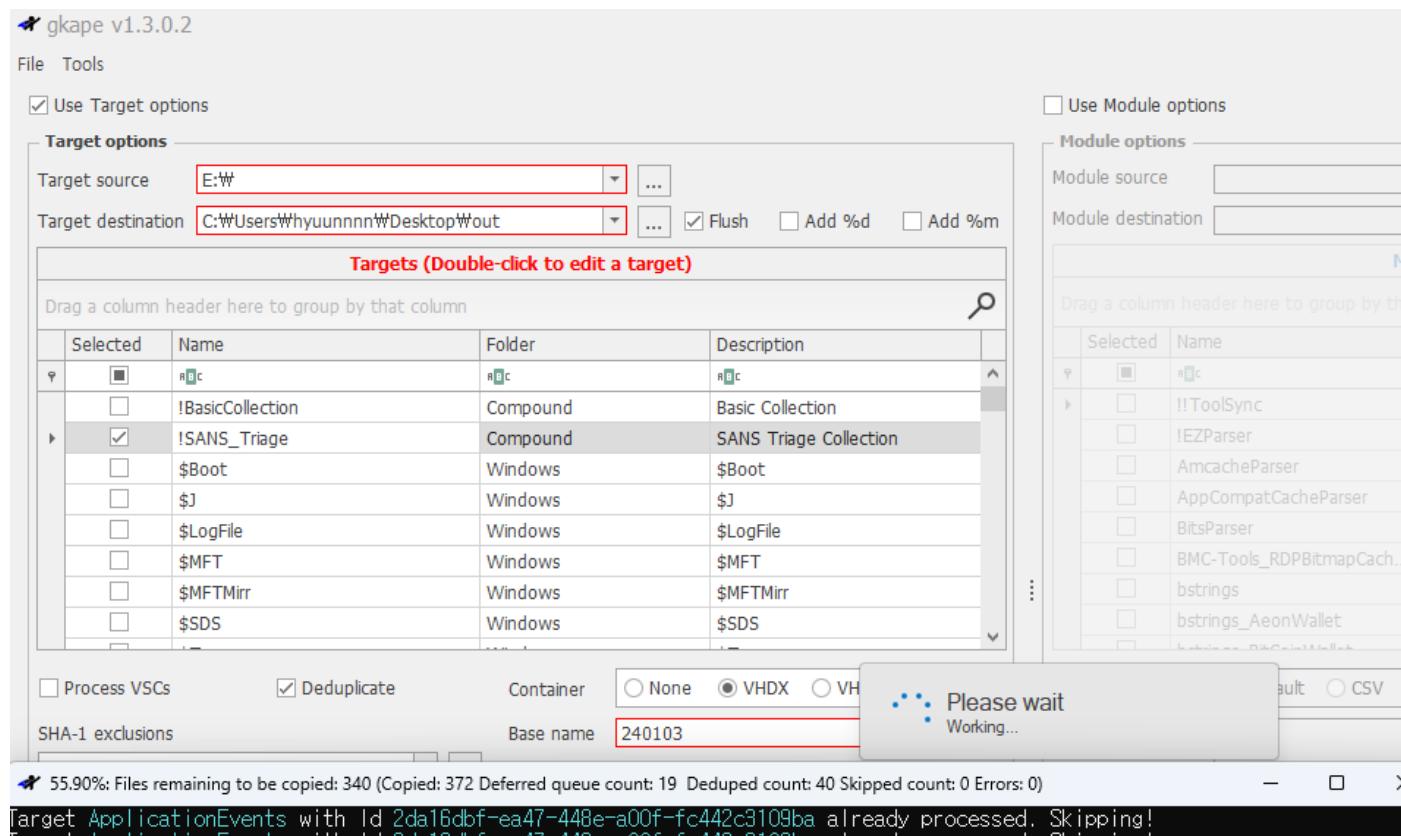
¹ <https://youtu.be/g9V6OUCe12k?t=100>

Plaso

- 도구 정리
 - `image_export.py` : 확장자, 필터 경로, 시그니처, 날짜 등의 필터를 기반으로 파일을 추출하는 도구
 - 개인적으로 KAPE를 사용하는 방법이 더 편한 것 같다.
 - `log2timeline.py` : 마운트 경로, 폴더, 이미지 등을 대상으로 아티팩트를 분석하여 이벤트를 추출하는 도구
 - pinfo, psort 같은 도구로 분석할 수 있는 plaso 덤프 파일이 생성됨
 - 사용 가능한 플러그인 목록은 `log2timeline.py --info` 명령어로 확인 가능
 - `pinfo.py` : 덤프 파일의 정보들을 확인할 수 있다. (어떤 파서를 사용했는지, 분석 대상은 무엇인지 등)
 - `psort.py` : 덤프 파일을 대상으로 필터를 적용하여 `CSV` 파일 등으로 만드는 도구
 - `psteal.py` : `log2timeline.py` → `psort.py` 과정을 한 번에 처리하는 도구

¹ <https://plaso.readthedocs.io/en/latest/sources/user/Users-Guide.html#the-tools>

- Arsenal Image Mounter로 E01 파일 마운트
- KAPE의 Target 기능을 사용하여 분석 파일 추출
 - Target source, destination 지정 → VHDX 선택 → Target 파일 선택 → Execute! 클릭



Plaso

log2timeline.py -z Asia/Seoul --storage-file <plaso 덤프 파일명> <VHDX 파일> - 3분 39초 소요

```
→ Desktop log2timeline.py -z Asia/Seoul --storage-file test.plaso 2024-01-30T054405_240103.vhdx
2024-01-30 05:49:39,117 [INFO] (MainProcess) PID:6820 <data_location> Determined data location: /usr/share/plaso
2024-01-30 05:49:39,122 [INFO] (MainProcess) PID:6820 <artifact_definitions> Determined artifact definitions path: /usr/share/artifacts
Checking availability and versions of dependencies.
[OPTIONAL]      unable to determine version information for: flor
[OK]

Source path          : /mnt/c/Users/hyuunnnn/Desktop/2024-01-30T054405_240103.vhdx
Source type         : storage media image
Processing time     : 00:00:00
```

psteal.py -z Asia/Seoul --source <VHDX 파일> -w <CSV 파일명> - 3분 5초 소요

```
→ Desktop psteal.py -z Asia/Seoul --source 2024-01-30T054405_240103.vhdx -w result.csv
2024-01-30 05:50:45,866 [INFO] (MainProcess) PID:6956 <data_location> Determined data location: /usr/share/plaso
2024-01-30 05:50:45,871 [INFO] (MainProcess) PID:6956 <artifact_definitions> Determined artifact definitions path: /usr/share/artifacts
Checking availability and versions of dependencies.
[OPTIONAL]      unable to determine version information for: flor
[OK]

Source path          : /mnt/c/Users/hyuunnnn/Desktop/2024-01-30T054405_240103.vhdx
Source type         : storage media image
Processing time     : 00:00:00

Processing started.
```

- 추출된 CSV 파일을 Timeline Explorer로 분석 - TLEFilePlugins에 의해 자동으로 색 설정되어 있음
- Color를 기준으로 필터링하면 유의미한 아티팩트 분석 가능

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

result.csv

Drag a column header here to group by that column

Enter text to search... Enter text to search... Find

| Line | Tag | Timestamp | Color | Source | Source Long | Message | Parser |
|---------|-----|---------------------|------------|---------|----------------------|---|-----------|
| 1675231 | | 2024-01-03 08:02:49 | WebHistory | EBHIST | Chrome History | https://google.com/ (Google) [count: 5] Visit from: Visit count: 7 Type: [TYPED - ...] | sqlite/ch |
| 1675232 | | 2024-01-03 08:02:49 | WebHistory | EBHIST | Chrome History | https://www.google.com/ (Google) [count: 0] Visit from: https://google.com/ (Google) | sqlite/ch |
| 1675237 | | 2024-01-03 08:02:50 | WebHistory | EBHIST | Chrome History | https://www.google.com/ (Google) [count: 0] Visit from: Visit count: 11 Type: [LIN... | sqlite/ch |
| 1675257 | | 2024-01-03 08:02:52 | WebHistory | EBHIST | Chrome History | https://www.google.com/search?q=winrar&sca_esv=595303506&source=hp&ei=qRSVZYWFG-Tj2.. | sqlite/ch |
| 1675265 | | 2024-01-03 08:02:54 | WebHistory | EBHIST | Chrome History | https://www.google.com/search?q=winrar&sca_esv=595303506&source=hp&ei=qRSVZYWFG-Tj2.. | sqlite/ch |
| 1675372 | | 2024-01-03 08:02:57 | WebHistory | EBHIST | Chrome History | https://www.win-rar.com/ (WinRAR download free and support: WinRAR) [count: 0] Visi... | sqlite/ch |
| 1675373 | | 2024-01-03 08:02:57 | WebHistory | EBHIST | Chrome History | https://www.win-rar.com/start.html?&L=0 (WinRAR download free and support: WinRAR) ... | sqlite/ch |
| 1675461 | | 2024-01-03 08:03:03 | WebHistory | EBHIST | Chrome History | https://www.google.com/search?q=winrar&sca_esv=595303506&source=hp&ei=qRSVZYWFG-Tj2.. | sqlite/ch |
| 1675462 | | 2024-01-03 08:03:03 | WebHistory | EBHIST | Chrome History | https://www.google.com/ (Google) [count: 0] Visit from: Visit count: 11 Type: [TYP... | sqlite/ch |
| 1675482 | | 2024-01-03 08:03:05 | WebHistory | EBHIST | Chrome History | https://www.google.com/search?q=winrar&sca_esv=595303506&source=hp&ei=qRSVZYWFG-Tj2.. | sqlite/ch |
| 1675521 | | 2024-01-03 08:03:07 | WebHistory | WEBHIST | Chrome History | https://winrar.softonic.kr/download (WinRAR - 무료 - 최신 버전 다운로드) [count: 0] Visi... | sqlite/ch |
| 1675955 | | 2024-01-03 08:03:29 | WebHistory | WEBHIST | Chrome History | https://www.softonic.kr/download/winrar/windows/post-download (Download WinRAR 6.22..) | sqlite/ch |
| 1676637 | | 2024-01-03 08:03:45 | WebHistory | WEBHIST | Chrome History | https://gsf-fl.softonic.com/618/d8b/7679679c5d322bf6eabc7a3a35deb3b31d/winrar-x32-6.. | sqlite/ch |
| 1676638 | | 2024-01-03 08:03:45 | WebHistory | WEBHIST | Chrome History | https://www.softonic.kr/download-launch?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9... | sqlite/ch |
| 1677012 | | 2024-01-03 08:04:02 | Execution | REG | AppCompatCache Re... | [HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] Ca... | winreg/ap |
| 1677013 | | 2024-01-03 08:04:02 | WebHistory | WEBHIST | Chrome History | https://gsf-fl.softonic.com/618/d8b/7679679c5d322bf6eabc7a3a35deb3b31d/winrar-x32-6.. | sqlite/ch |
| 1677014 | | 2024-01-03 08:04:02 | WebHistory | WEBHIST | Chrome History | https://www.softonic.kr/download-launch?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9... | sqlite/ch |
| 1677156 | | 2024-01-03 08:04:09 | Execution | LOG | WinPrefetch | Prefetch [WINRAR-X32-622.EXE] was executed - run count 1 path hints: \USERS\USER\DO... | prefetch |
| 1677482 | | 2024-01-03 08:04:13 | Execution | LOG | WinPrefetch | Prefetch [UNINSTALL.EXE] was executed - run count 1 path hints: \PROGRAM FILES (X86..) | prefetch |
| 1678096 | | 2024-01-03 08:04:29 | Execution | LOG | WinPrefetch | Prefetch [WINRAR.EXE] was executed - run count 1 path hints: \PROGRAM FILES (X86)\W... | prefetch |
| 1678113 | | 2024-01-03 08:04:29 | Execution | LOG | WinPrefetch | Prefetch [TRUSTEDINSTALLER.EXE] was executed - run count 1 path hints: \WINDOWS\SER... | prefetch |
| 1678178 | | 2024-01-03 08:04:29 | Execution | LOG | WinPrefetch | Prefetch [TIWORKER.EXE] was executed - run count 1 path hints: \WINDOWS\WINSXS\AMD6... | prefetch |

Plaso

- plaso 덤프 파일을 [Timesketch](#) 또는 sqlite 뷰어 프로그램으로 분석
- WSL2에서 진행¹ - 2024. 01. 30 기준

```
sudo apt install docker-compose-plugin
```

```
curl -s -O https://raw.githubusercontent.com/google/timesketch/master/contrib/deploy_timesketch.sh  
chmod 755 deploy_timesketch.sh
```

```
cd /opt  
sudo ~/deploy_timesketch.sh
```

```
cd timesketch  
sudo docker compose up -d
```

```
sudo docker compose exec timesketch-web tsctl create-user <USERNAME> # 계정 생성 및 비밀번호 설정  
sudo docker compose ps -> 포트 번호 확인 후 접속
```

¹ <https://timesketch.org/guides/admin/install/>

Plaso

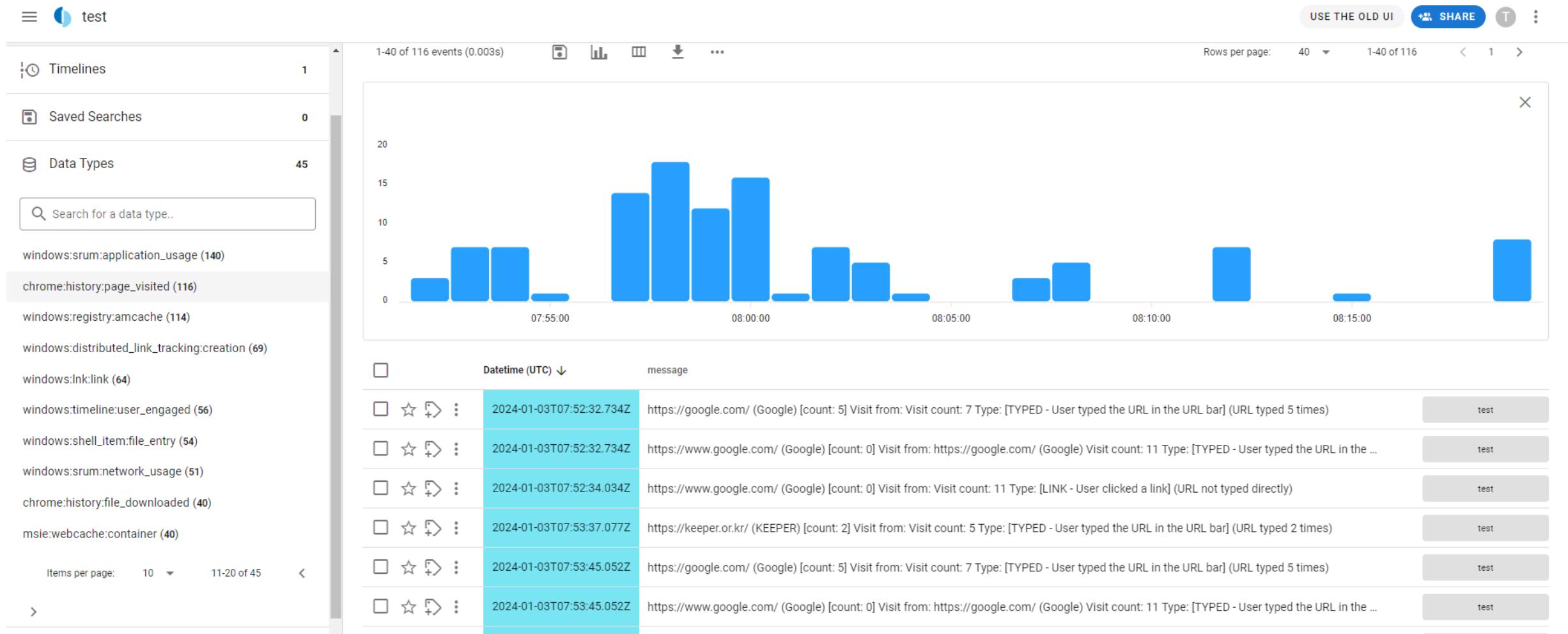
BLANK SKETCH 클릭 → 스케치 파일 생성 → 타임라인 파일 추가

The screenshot shows the Timesketch web application interface. At the top, there is a navigation bar with icons for back, forward, refresh, and search, followed by the URL 'localhost'. To the right of the URL are various browser extension icons. Below the navigation bar, the Timesketch logo ('timesketch') is on the left, and a 'USE THE OLD UI' button is on the right. A user profile icon with the number '1' is also present.

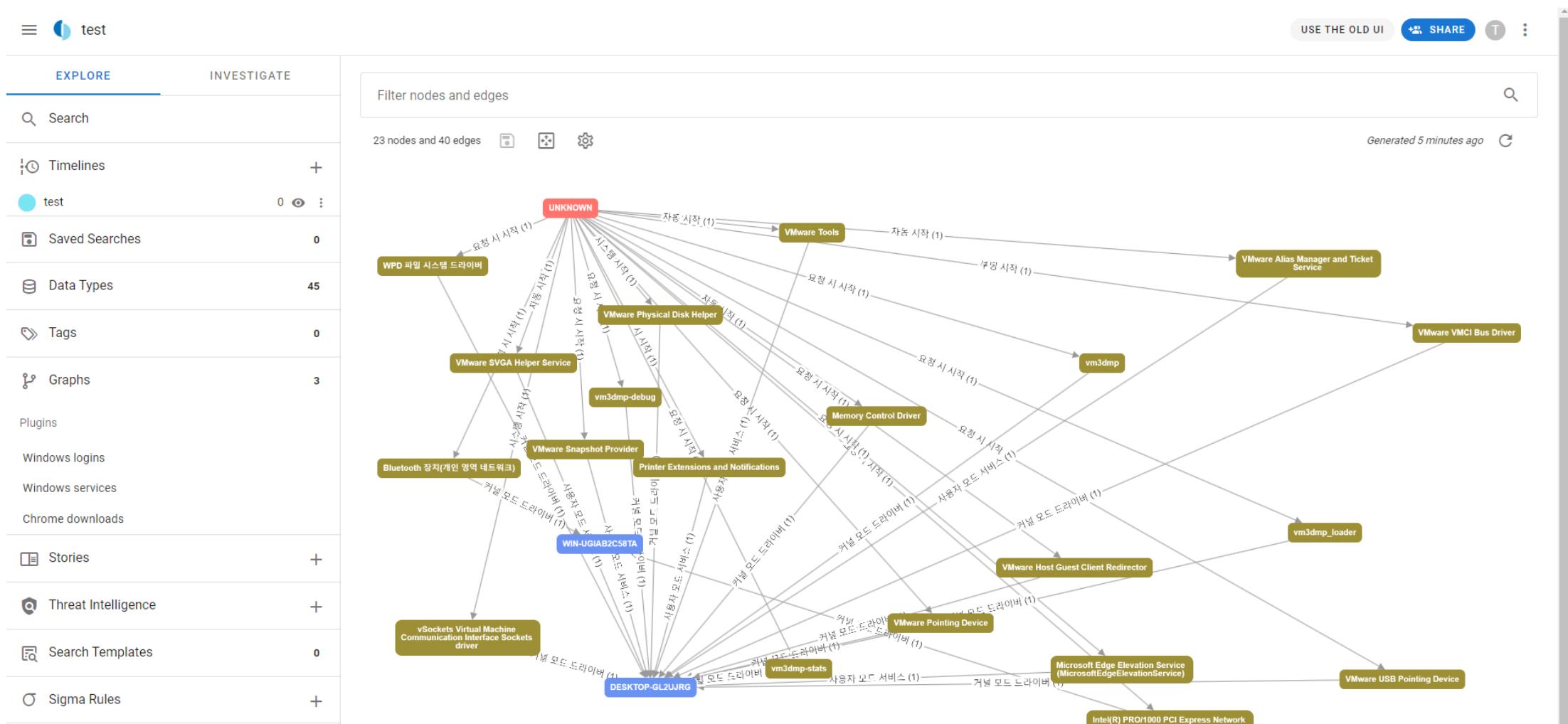
In the center, a large button labeled 'BLANK SKETCH' is highlighted in blue. Above it, the text 'Start new investigation' is displayed. Below this section, the heading 'Your recent work' is shown, followed by tabs for 'RECENT', 'MY SKETCHES', 'SHARED WITH ME', and 'ARCHIVED'. A search bar with a magnifying glass icon and the placeholder 'Search' is located to the right of the tabs.

The main content area displays a table with columns: 'Name', 'Creator', 'Created at', and 'Last active'. The message 'No data available' is centered in the table. At the bottom of the page, there are buttons for 'Rows per page' (set to 15), and navigation arrows for 'Previous' and 'Next' pages.

- Data Type 별 분석 가능, 이벤트 발생 시간을 기준으로 그래프를 생성하여 타임라인 분석에 용이함



- 그래프 분석 가능 - 사용자별 윈도우 서비스 사용 기록 (Windows services)



참고자료

- Getting Started with Plaso and Log2Timeline - Forensic Timeline Creation
- Introduction to Plaso Heimdall
- Plaso and WSL 2 - The WSL Adventures Continue...
- Plaso (log2timeline) docs
- CASE 001 SUPER TIMELINE ANALYSIS
- PLASO – 슈퍼 타임라인 분석 도구 활용 방안
- Working with log2timeline and Timesketch
- Overview of Installing log2timeline and using Timesketch
- 타임라인 분석 도구 - DFRC

X-Ways Forensics

- 다음 주차에 계속
- 짱짱 도구임 - 웬만하면 FTK Imager를 사용하지 않게 된다.

참고자료

- Youtube - [X-Ways Software Technology AG, TED SMITH](#)
- Blog - [ccibomb, goblinforensics](#)
- [X-Ways 실무 활용 가이드](#)
- X-Ways - [XWFQuickStart, manual](#)
- [XWF를 이용한 포렌식 분석](#)

ETC

- Carpe Forensics
- Velociraptor
- grr
- ...

웹 브라우저 분석

- 인터넷에 접속하기 위해 사용되는 프로그램
- 대표적으로 Chrome, Edge, Firefox, Safari 등이 있다.
- 많은 브라우저들이 [크로미움](#) 기반으로 개발되어 Chrome에 존재하는 아티팩트와 매우 유사하다.¹
- 그러나 Firefox, Safari와 같이 자체 개발된 경우 다른 아티팩트 구조로 되어있다.
- 검색 기록, 방문 기록, 다운로드 기록, 즐겨찾기 등 브라우저에서 활동한 모든 기록이 남아있다.

| | | |
|-------------|--|---|
| Web Browser | <u>BrowsingHistoryView</u> | Chrome, IE/Edge, FireFox, Opera의 히스토리를 통합해 보여주는 GUI 도구로 이미지 데이터를 분석하기 위해서는 마운트하거나 히스토리만 별도 풀더로 추출해 입력해야 한다. |
| | <u>Hindsight</u> | 브라우저 데이터 중 대부분 히스토리, 캐시, 쿠키 분석에만 집중하는데 반해 해당 도구는 크롬의 다양한 데이터를 분석해 CSV로 출력해준다. CSV 분석은 엑셀도 좋지만 앞서 소개한 Timeline Explorer를 추천한다. |
| | <u>Cache/CookiesView,...</u> | 히스토리 분석으로 부족하다면 링크에 있는 다양한 캐시, 쿠키 분석 도구를 사용해보자. |

¹ <https://namu.wiki/w/The Chromium Projects#s-4.1>

² <https://blog.plainbit.co.kr/dforensics-specialist-tools/>

웹 브라우저 분석

- 아티팩트 경로
 - Chrome: %LocalAppData%\Google\Chrome\User Data\Default
 - Edge: %LocalAppData%\Microsoft\Edge\User Data\Default ,
%LocalAppData%\Microsoft\Windows\WebCache\WebCacheV01.dat
- 분석 도구는 [hindsight](#), [NirSoft - Web Browser Tools Package](#) 등이 있지만 hindsight를 사용할 예정
- hindsight는 크로미움 기반 브라우저를 타겟으로 하고 있다.
- 크로미움 기반이 아닌 브라우저 분석 또는 캐시 등의 상세한 분석이 필요하다면 NirSoft의 도구를 활용해야 한다. (ex: 방문한 페이지 html 파일 추출 등)
 - NirSoft의 [BrowserHistoryView](#)는 다양한 브라우저들의 History 정보를 분석해준다.

웹 브라우저 분석

- hindsight

The logo consists of three stylized characters composed of brackets and other symbols. The characters have a blocky, geometric appearance. Below the characters, the text "by @_RyanBenson" is on the left and "v2023.03" is on the right, separated by a diagonal slash.

웹 브라우저 분석

- localhost:8080 접속 → Path 입력 → Run 클릭 → Save XLSX 클릭

The screenshot shows the Hindsight web interface. At the top, there's a large stylized 'H' logo and the word 'Hindsight'. To its right is a link to 'Web Artifact Analysis'. Below the header, a descriptive text reads: 'Hindsight is a free tool for analyzing web artifacts. To get started, select the 'Input Type' below and fill out the 'Input Path' field. Review the plugins and options on the right, and hit the 'Run' button at the bottom.' A Chrome browser icon is positioned next to the descriptive text.

Inputs

Input Type: Chrome **Profile Path:** C:\Users\hyuunnn\Desktop\Default
Cache Path: [empty input field]

Description: Chrome is a free web browser from Google that runs on Windows, macOS, Linux, ChromeOS, iOS, and Android. Each user's web history and configuration information is stored under their user directory, so there may be multiple sets of browser data on the system.

Available Decryption: Windows Mac Linux

Default Locations:

- Windows XP: \[userdir]\Local Settings\Application Data\Google\Chrome\User Data
- Vista/7/8/10/11: \[userdir]\AppData\Local\Google\Chrome\User Data
- Linux: \[userdir]\.config\google-chrome
- OSX/macOS: \[userdir]/Library/Application Support/Google/Chrome/Default
- iOS: \Applications\com.google.chrome.ios\Library\Application Support\Google\Chrome
- Android: /userdata/data/com.android.chrome/app_chrome

Plugin Selector

- Chrome Extension Names [v20210424]
- Generic Timestamp Decoder [v20160907]
- Google Analytics Cookie Parser [v20170130]
- Google Searches [v20160912]
- Load Balancer Cookie Decoder [v20200213]
- Quantcast Cookie Parser [v20160907]
- Query String Parser [v20170225]
- Time Discrepancy Finder [v20170129]

Options Selector

Log Path: hindsight.log
Timezone: Pacific [-8/-7]
Copy files before opening?
Temp Path: hindsight-temp

Run

웹 브라우저 분석

| Hindsight Internet History Forensics (v2023.03) | | | |
|---|-------------------------|---|--|
| Type | Timestamp (US/Pacific) | URL | Title / Name / Status |
| url | 2023-11-28 08:03:46.272 | https://blog.naver.com/munzh/222613672332 | Quartus(쿼터스) ModelSim 설치 .. : 네이버블로그 |
| url | 2023-11-28 08:03:48.052 | https://blog.naver.com/munzh/222613672332 | Quartus(쿼터스) ModelSim 설치 .. : 네이버블로그 |
| url | 2023-11-28 08:04:06.360 | https://www.google.com/search?q=xilinx+%EC%84%A4%EC%B9%98&rlz=xilinx 설치 - Google 검색 | |
| url | 2023-11-28 08:04:09.610 | https://www.google.com/search?q=xilinx+%EB%B2%84%EC%A0%84+%Exilinx 버전 설치 - Google 검색 | |
| url | 2023-11-28 08:04:09.949 | https://www.google.com/search?q=xilinx+%EB%B2%84%EC%A0%84+%Exilinx 버전 설치 - Google 검색 | |
| url | 2023-11-28 08:04:13.107 | https://www.google.com/search?q=xilinx+%EA%B5%AC%EB%B2%84%EC%Exilinx 구버전 설치 - Google 검색 | |
| url | 2023-11-28 08:04:13.508 | https://www.google.com/search?q=xilinx+%EA%B5%AC%EB%B2%84%EC%Exilinx 구버전 설치 - Google 검색 | |
| url | 2023-11-28 08:04:20.233 | https://www.google.com/search?q=xilinx+%EA%B5%AC%EB%B2%84%EC%Exilinx 구버전 설치 - Google 검색 | |
| url | 2023-11-28 08:04:21.723 | https://m.blog.naver.com/iniproinc/221918636801 | Vivado/Vitis 2019.2에서 IPI Navigator와 함께 시작하기 : 네이버 블로그 |
| url | 2023-11-28 08:04:24.050 | https://m.blog.naver.com/iniproinc/221918636801 | Vivado/Vitis 2019.2에서 IPI Navigator와 함께 시작하기 : 네이버 블로그 |
| url | 2023-11-28 08:04:24.269 | https://m.blog.naver.com/iniproinc/221918636801 | Vivado/Vitis 2019.2에서 IPI Navigator와 함께 시작하기 : 네이버 블로그 |
| url | 2023-11-28 08:04:25.088 | https://www.google.com/search?q=xilinx+%EC%B5%9C%EC%8B%A0%EB%Exilinx 최신버전 - Google 검색 | |
| url | 2023-11-28 08:04:25.213 | https://m.blog.naver.com/iniproinc/221918636801 | Vivado/Vitis 2019.2에서 IPI Navigator와 함께 시작하기 : 네이버 블로그 |

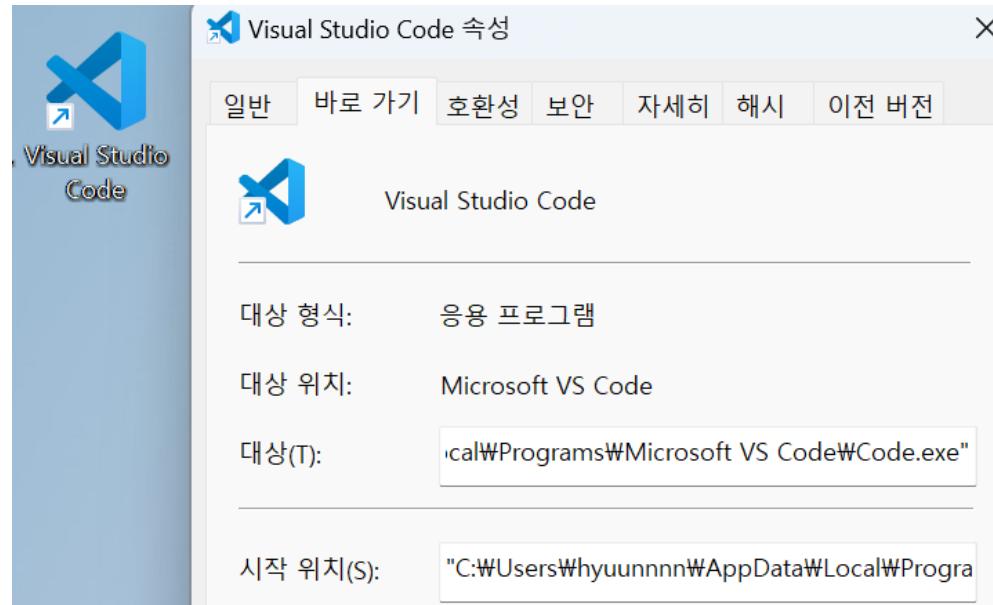
웹 브라우저 분석

- Internet Explorer 10 부터 WebCacheV01.dat 파일에 기록을 저장한다.¹
- IE 지원 종료 후 Edge 브라우저에서도 위 파일에 저장한다.
 - Edge는 Default 경로와 WebCacheV01.dat 파일 분석 필요
- ESE(Extensible Storage Engine) Database 포맷 사용
 - 이를 해석해주는 도구 활용 ([ESEDATABASEVIEW](#), [IE10ANALYZER](#) 등)
- 웹 브라우저 사용 기록 외에 PC에서 사용한 파일 기록들도 존재한다.

| Creation Time | Expiry Time | Modified Time | Accessed Time | PostCheck Time | Url |
|---------------|-------------|----------------|-----------------|----------------|---|
| 0 | 2024-02-... | 2024-01-25 ... | 2024-01-25 2... | 0 | Visited: hyuunnnn@file:///C:/Users/hyuunnnn/Documents/GitHub/forensic-study-2023winter/slides/1.pdf |
| 0 | 2024-02-... | 2024-01-25 ... | 2024-01-25 2... | 0 | Visited: hyuunnnn@https://github.com/EricZimmerman/evtx/tree/master/evtx/Maps |
| 0 | 2024-02-... | 2024-01-25 ... | 2024-01-25 2... | 0 | Visited: hyuunnnn@file:///C:/Users/hyuunnnn/Documents/GitHub/2024-KEEPER-Forensic-Study/2/2.pdf |
| 0 | 2024-02-... | 2024-01-25 ... | 2024-01-25 2... | 0 | Visited: hyuunnnn@file:///C:/Users/hyuunnnn/Documents/GitHub/2024-KEEPER-Forensic-Study/1/1.pdf |
| 0 | 2024-02-... | 2024-01-25 ... | 2024-01-25 2... | 0 | Visited: hyuunnnn@file:///C:/Users/hyuunnnn/Documents/GitHub/2024-KEEPER-Forensic-Study/3/3.pdf |

¹ <https://su0-0su.tistory.com/31>

LNK (바로가기) 분석



- 윈도우 운영체제에서 사용되는 링크 파일이며, 실행했을 때 대상 경로에 지정된 파일, 디렉토리 등이 실행된다.
- 포렌식 관점에서 LNK 파일에 유의미한 데이터들이 존재한다.¹ - 이후에 설명할 내용

² <http://forensic-proof.com/archives/607>

LNK (바로가기) 분석

| 이름 | 경로 |
|------------|--|
| 최근에 실행한 파일 | %AppData%\Microsoft\Windows\Recent |
| 시작 메뉴 | %AppData%\Microsoft\Windows\Start Menu %ProgramData%\Microsoft\Windows\Start Menu |
| 바탕화면 | %UserProfile%\Desktop |
| 빠른 실행 관련 | %AppData%\Microsoft\Internet Explorer\Quick Launch %AppData%\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar |

- 왜 포렌식 관점에서 의미 있을까?
 - 프로그램 설치, 실행 등의 작업을 했을 때 Lnk 파일이 생성된다.
→ 생성되었다는 것은 파일이 실행되었음을 의미한다.

LNK (바로가기) 분석

- LECmd

- LECmd.exe -d "%AppData%\Microsoft\Windows\Start Menu\Programs" --csv .
- LECmd.exe -d "%AppData%\Microsoft\Windows\Recent" --html .

```
C:\Users\hyuunnnn\Desktop\LECmd>LECmd.exe -d "%AppData%\Microsoft\Windows\Start Menu\Programs" --csv .
LECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd

Command line: -d C:\Users\hyuunnnn\AppData\Roaming\Microsoft\Windows\Start Menu\Programs --csv .

Warning: Administrator privileges not found!

Looking for lnk files in C:\Users\hyuunnnn\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
Found 39 files

Processing C:\Users\hyuunnnn\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools.lnk

Source file: C:\Users\hyuunnnn\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools.lnk
Source created: 2024-01-22 10:14:00
Source modified: 2022-05-07 05:19:10
Source accessed: 2024-01-28 16:36:27

--- Header ---
Target created: null
Target modified: null
```

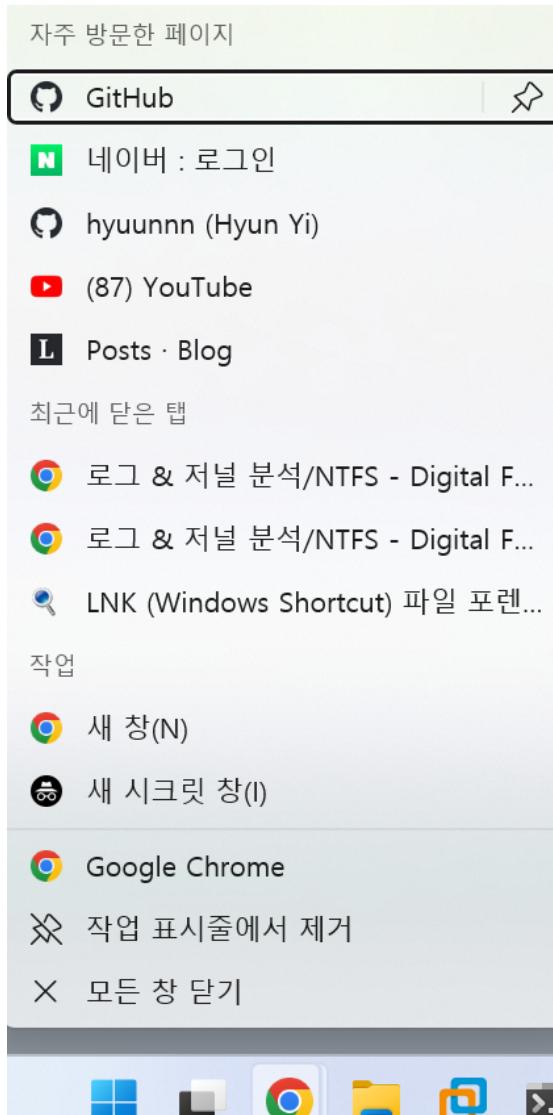
LNK (바로가기) 분석

C:\Users\hyuunnnn\AppData\Roaming\Microsoft\Windows\Recent\학부교과과정변경현황(99-2021).xls.lnk

Source Created: 2024-01-24 08:03:47
Source Modified: 2024-01-24 08:03:47
Source Accessed: 2024-01-28 16:57:11
Target Created: 2024-01-24 08:03:43
Target Modified: 2024-01-24 08:03:44
Target Accessed: 2024-01-24 08:03:47
File Size: 52224 (bytes)
Relative Path: ..\..\..\..\Downloads\학부교과과정변경현황(99-2021).xls
Working Directory: C:\Users\hyuunnnn\Downloads
File Attributes: FileAttributeArchive
Header Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasWorkingDir,IsUnicode, DisableKnownFolderTracking
Drive Type: Fixed storage media (Hard drive)
Volume Serial Number: FA9185E2
Volume Label:
Local Path: C:\Users\hyuunnnn\Downloads\학부교과과정변경현황(99-2021).xls
Network Path:
Common Path:
Arguments:
TargetID Absolute Path: Downloads\학부교과과정변경현황(99-2021).xls
Target \$MFT Entry Number: 0x3EF24
Target \$MFT Sequence Number: 0xF
MachineID: hyuunnn
Machine MAC Address: 3c:e9:f7:bc:51:4d
MAC Vendor: (Unknown vendor) (vendor not included in source .lnk file, auto-resolved by LECmd for end-user upon parsing)
Tracker Created On: 2024-01-22 11:22:12
Extra Blocks Present: TrackerDataBaseBlock, PropertyStoreDataBlock

- Target 은 링크된 파일, Source 는 lNK 파일을 의미한다.
- 예를 들어 기밀 문서를 열고 나서 삭제했더라도 lNK 파일을 통해 PC에 존재했음을 입증할 수 있다.

Jumplist 분석



Jumplist 분석

- 응용 프로그램별로 그룹화되어 최근에 사용한 문서, 프로그램 등을 기록 → LNK 파일들의 모음
- %AppData%\Microsoft\Windows\Recent
 - AutomaticDestinations : 운영체제가 자동으로 남기는 항목
 - CustomDestinations : 응용 프로그램이 자체적으로 관리하는 항목

| 이름 | 수정한 날짜 | 유형 | 크기 |
|---|---------------------|--------------------|-------|
| 1c7a9be1b15a03ba.automaticDestinations-ms | 2024-01-29 오전 1:52 | AUTOMATICDESTIN... | 8KB |
| 1ced32d74a95c7bc.automaticDestinations-ms | 2024-01-26 오전 9:22 | AUTOMATICDESTIN... | 6KB |
| 2fc6fa630bb56a94.automaticDestinations-ms | 2024-01-28 오후 11:33 | AUTOMATICDESTIN... | 3KB |
| 3d3d35cb4b4bd7dc.automaticDestinations-ms | 2024-01-24 오후 3:49 | AUTOMATICDESTIN... | 2KB |
| 4d283783afece743.automaticDestinations-ms | 2024-01-28 오후 11:33 | AUTOMATICDESTIN... | 3KB |
| 5a2098e080cf7ac4.automaticDestinations-ms | 2024-01-29 오전 1:55 | AUTOMATICDESTIN... | 33KB |
| 5b60ff9d777810f7.automaticDestinations-ms | 2024-01-22 오후 8:05 | AUTOMATICDESTIN... | 3KB |
| 5d696d521de238c3.automaticDestinations-ms | 2024-01-29 오전 1:52 | AUTOMATICDESTIN... | 25KB |
| 5f7b5f1e01b83767.automaticDestinations-ms | 2024-01-29 오전 1:57 | AUTOMATICDESTIN... | 140KB |

- 프로그램마다 고유한 AppID 값이 존재하는데, 정리된 AppID 목록을 통해 어떤 프로그램인지 확인 가능

¹ <http://www.forensic-artifact.com/windows-forensics/jumplist>

Jumplist 분석

- JumplistExplorer - GUI 또는 Jumplist-Browser 도구를 사용하여 실습 가능

The screenshot shows the interface of JumpList Explorer v2.0.0.0. It has two main panes displaying jump list data.

Left Pane: Shows a list of applications and their details. The columns are: Source File Name, Jump List Type, App ID, App ID Description, Lnk File Count, and File Size.

| Source File Name | Jump List Type | App ID | App ID Description | Lnk File Count | File Size |
|--|----------------|------------------|--|----------------|-----------|
| C:\Users\hyuunnnn\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\OneDrive ?? (ClassicMru) | Automatic | 4d283783afece743 | | 0 | 2,560 |
| C:\Users\hyuunnnn\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Google Chrome 9.0.597.84 / 12.0.742.100 / 1... | Automatic | 5a2098e080cf7ac4 | OneDrive ?? (ClassicMru) | 5 | 33,792 |
| C:\Users\hyuunnnn\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Google Chrome 9.0.597.84 / 12.0.742.100 / 1... | Automatic | 5b60ff9d777810f7 | | 0 | 2,560 |
| C:\Users\hyuunnnn\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Google Chrome 9.0.597.84 / 12.0.742.100 / 1... | Automatic | 5d696d521de238c3 | Google Chrome 9.0.597.84 / 12.0.742.100 / 1... | 13 | 25,088 |
| C:\Users\hyuunnnn\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Quick Access | Automatic | 5f7b5f1e01b83767 | Quick Access | 99 | 143,360 |
| C:\Users\hyuunnnn\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Microsoft.Windows.ShellExperienceHost | Automatic | 6dc04f5cc522861 | Microsoft.Windows.ShellExperienceHost | 1 | 3,584 |

Right Pane: Shows a detailed view of the Google Chrome jump list entries. The columns are: Entry Number, Target Created On, Target Modified On, Target Accessed On, Absolute Path, Extra ..., and Interact... .

| Entry Number | Target Created On | Target Modified On | Target Accessed On | Absolute Path | Extra ... | Interact... |
|--------------|---------------------|---------------------|---------------------|--|-----------|-------------|
| 13 | 2024-01-28 16:51:43 | 2024-01-28 16:51:43 | 2024-01-28 16:52:16 | My Computer\%C:\%Users\hyuunnnn\Desktop\LECmd\Output_for_Wind... | 2 | 1 |
| 12 | | | | My Computer\%C:\%Users\hyuunnnn\Downloads\%X-Tensions 툴리그인 개발 (1).pdf | 1 | 1 |
| 11 | | | | My Computer\%C:\%Users\hyuunnnn\Downloads\%X-Tensions 툴리그인 개발 (1).pdf | 1 | 1 |
| 5 | 2024-01-25 14:14:15 | 2024-01-25 14:14:15 | 2024-01-25 14:14:17 | My Computer\%C:\%Users\hyuunnnn\Documents\GitHub\forensic-study-2023winter\slides\3.pdf | 2 | 3 |
| 10 | 2024-01-25 20:24:19 | 2024-01-25 20:24:23 | 2024-01-25 20:24:32 | My Computer\%C:\%Users\hyuunnnn\Desktop\wasdf.pdf | 2 | 1 |
| 9 | 2024-01-25 18:28:28 | 2024-01-25 18:28:28 | 2024-01-25 18:28:45 | My Computer\%C:\%temp\%240103_Partition 3-CaseSummary.html | 2 | 1 |
| 8 | | | | My Computer\%C:\%Users\hyuunnnn\Downloads\%X-Tensions 툴리그인 개발 (1).pdf | 1 | 1 |
| 7 | | | | Internet Explorer (Homepage)\%https://github.com/EricZimmerman/evtx/tree/master/evtx/Maps | 1 | 1 |
| 6 | 2024-01-22 11:02:26 | 2024-01-22 11:02:26 | 2024-01-25 14:14:15 | My Computer\%C:\%Users\hyuunnnn\Documents\GitHub\forensic-study-2023winter\slides\1.pdf | 2 | 1 |
| 4 | 2024-01-22 11:02:26 | 2024-01-22 11:02:26 | 2024-01-25 14:14:15 | My Computer\%C:\%Users\hyuunnnn\Documents\GitHub\forensic-study-2023winter\slides\2.pdf | 2 | 1 |
| 3 | 2024-01-24 12:28:34 | 2024-01-24 12:28:34 | 2024-01-24 12:28:43 | My Computer\%C:\%shell32.dll,-21813\%hyuunnnn\shell32.dll,-21798\report (1).pdf | 2 | 1 |
| 2 | | | | My Computer\%C:\%Users\hyuunnnn\Downloads\%3주차.pdf | 1 | 1 |
| 1 | | | | Internet Explorer (Homepage)\%https://accounts.google.com/o/oauth2/v2/auth?access_type=offline&... | 1 | 1 |

Jumplist 분석

The screenshot shows a list of jump items on the left and a detailed view of one item's properties on the right.

Jump Items List:

- Entry #: 0013 - My Computer\\C:\\Users\\hyuunnnn\\Desktop\\LECmd\\20240128165142_LECmd_Output_for_Windex.xhtml
- Entry #: 0012 - My Computer\\C:\\Users\\hyuunnnn\\Downloads\\X-Tensions 풀리그인 개발 (1).pdf
- Entry #: 0011 - My Computer\\C:\\Users\\hyuunnnn\\Downloads\\기술문서 중간발표.pdf
- Entry #: 0005 - My Computer\\C:\\Users\\hyuunnnn\\Documents\\GitHub\\forensic-study-2023winter\\slides\\3.pdf
- Entry #: 0010 - My Computer\\C:\\Users\\hyuunnnn\\Desktop\\asdf.pdf
- Entry #: 0009 - My Computer\\C:\\temp\\240103_Partition 3-CaseSummary.html
- Entry #: 0008 - My Computer\\C:\\Users\\hyuunnnn\\Downloads\\X-Tensions 풀리그인 개발.pdf
- Entry #: 0007 - Internet Explorer (Homepage)\\https://github.com/EricZimmerman/evb/tree/master/evtx/Maps
- Entry #: 0006 - My Computer\\C:\\Users\\hyuunnnn\\Documents\\GitHub\\forensic-study-2023winter\\slides\\1.pdf
- Entry #: 0004 - My Computer\\C:\\Users\\hyuunnnn\\Documents\\GitHub\\forensic-study-2023winter\\slides\\2.pdf
- Entry #: 0003 - My Computer\\C:\\shell32.dll,-21813\\hyuunnnn\\shell32.dll,-21798\\report (1).pdf
- Entry #: 0002 - My Computer\\C:\\Users\\hyuunnnn\\Downloads\\3주차.pdf
- Entry #: 0001 - Internet Explorer (Homepage)\\https://accounts.google.com/o/oauth2/v2/auth?access_type=offline&scope=p...

Properties View:

| Name | Value |
|------------------------|--|
| Icon | File |
| TargetCreationDate | 2024-01-28 16:51:43 |
| TargetModificationDate | 2024-01-28 16:51:43 |
| TargetLastAccessedDate | 2024-01-28 16:52:16 |
| Header.DataFlags | HasTargetIdList, HasLinkInfo,IsUnicode, DisableKnownFolderTracking, AllowLi... |
| Header.FileAttributes | FileAttributeArchive |
| Header.FileSize | 67,564 |
| Header.IconIndex | 0 |
| Header.ShowWindow | SwNormal |
| Absolute path | My Computer\\C:\\Users\\hyuunnnn\\Desktop\\LECmd\\20240128165142_L... |
| LocalPath | C:\\Users\\hyuunnnn\\Desktop\\LECmd\\20240128165142_LECmd_Output... |
| LocationFlags | VolumeIdAndLocalBasePath |

- LNK 파일 분석에서 봤던 Target , 링크 파일과 관련된 정보들이 보인다.
- 실행된 파일의 경로도 확인 가능하다. (Absolute path , LocalPath)

KEEPER CTF IR-2 풀이

피해자는 윈도우 PC를 사용할 때 잦은 알림이 번거롭다고 느껴, 디펜더를 비활성화하는 프로그램을 항상 사용한다고 한다.

또한 피해자에게 들은 바로는 랜섬웨어가 감염되기 전에 컴퓨터가 이상한 행위를 했었다고 한다.

원인을 찾아내고, 어떤 경로로 유입되었는지 분석하라.

다운로드 유입 URL, 다운로드 받은 악성 파일, 다운로드 받은 악성 파일이 실행된 시간을 답으로 입력해야 한다.

파일명은 소문자로 입력, 띄어쓰기는 언더바(_) 처리, 타임스탬프는 한국 시간인 UTC+9를 따르며, ISO 8601 표준에 의해 날짜와 시간 사이에 T 문자를 입력한다.

ex: KEEPER{https://www.example.com/_asdf.asd_2024-12-23T12:34:56}

KEEPER CTF IR-2 풀이

| | | | | |
|-----|-------------------------|-------------------------|---|--|
| 41 | url | 2024-01-02 23:54:28.504 | https://github.com/qtkite/defender-control/releases/tag/v1.5 | Release Defender Control v1.5 · qtkite/defender-control · GitHub |
| 42 | download | 2024-01-02 23:54:34.893 | blob:https://github.com/qtkite/defender-control/releases/download/v1.5/disabled-windows-defender.exe | Cancelled - 0% [0/301568] C:\Users\USER\Downloads\disabled-windows-defender.exe |
| 43 | download | 2024-01-02 23:54:34.893 | https://objects.githubusercontent.com/github-production-release-asset-0/-/blob/RSppokZ1kANM3UybtnoVWNJQxnIIIPFCb7DNQe5+/HSTS_observed | Cancelled - 0% [0/301568] C:\Users\USER\Downloads\disabled-windows-defender.exe |
| 44 | url | 2024-01-02 23:55:09.998 | https://github.com/topics/disable-windows-defender | disable-windows-defender · GitHub Topics · GitHub |
| 45 | site setting (modified) | 2024-01-02 23:55:10.079 | https://[*].github.com/* | cookie_controls_metadata [in F{'last_modified': '13348742110079631', 'setting': {}} |
| 46 | site setting (hsts) | 2024-01-02 23:55:12.966 | Encoded domain: RSppokZ1kANM3UybtnoVWNJQxnIIIPFCb7DNQe5+/HSTS_observed | {'expiry': 1735804512.966468, 'host': 'RSppokZ1kANM3UybtnoVWNJQxnIIIPFCb7DNQe5+/HSTS_observed'} |
| 47 | download | 2024-01-02 23:55:19.690 | https://github.com/qtkite/defender-control/releases/download/v1.5/disabled-windows-defender.exe | Cancelled - 0% [0/301568] C:\Users\USER\Downloads\disabled-windows-defender (1).exe |
| 48 | download | 2024-01-02 23:55:19.690 | https://objects.githubusercontent.com/github-production-release-asset-0/-/blob/RSppokZ1kANM3UybtnoVWNJQxnIIIPFCb7DNQe5+/HSTS_observed | Cancelled - 0% [0/301568] C:\Users\USER\Downloads\disabled-windows-defender (1).exe |
| 49 | download | 2024-01-02 23:55:38.528 | https://github.com/qtkite/defender-control/releases/download/v1.5/disabled-windows-defender.exe | Complete - 100% [301568/30] C:\Users\USER\Downloads\disabled-windows-defender (2).exe |
| 50 | download | 2024-01-02 23:55:38.528 | https://objects.githubusercontent.com/github-production-release-asset-0/-/blob/RSppokZ1kANM3UybtnoVWNJQxnIIIPFCb7DNQe5+/HSTS_observed | Complete - 100% [301568/30] C:\Users\USER\Downloads\disabled-windows-defender (2).exe |
| 94 | url | 2024-01-02 23:58:19.468 | https://keeper.or.kr/board/view/172731 | KEEPER |
| 95 | download | 2024-01-02 23:58:22.209 | blob:https://keeper.or.kr/33feaa89-fa2a-4c65-abe2-3e7b07e73350 | Complete - 100% [1243505/1] C:\Users\USER\Downloads\11월_회계부.rar |
| 96 | url | 2024-01-02 23:58:27.589 | https://github.com/qtkite/defender-control | GitHub - qtkite/defender-control: An open-source windows defender manager. Now you can easily manage your windows defender settings. |
| 97 | url | 2024-01-02 23:58:34.809 | https://keeper.or.kr/board/%EA%B8%EC%88%A0%EB%AC%88%EC% | KEEPER |
| 98 | url | 2024-01-02 23:58:35.188 | https://keeper.or.kr/board/%EA%B8%EC%88%A0%EB%AC%88%EC% | KEEPER |
| 99 | url | 2024-01-02 23:58:35.235 | https://keeper.or.kr/board/%EA%B8%EC%88%A0%EB%AC%88%EC% | KEEPER |
| 100 | login (never save) | 2024-01-02 23:58:36.693 | https://keeper.or.kr/ | |
| 101 | url | 2024-01-02 23:58:41.550 | https://github.com/qtkite/defender-control | GitHub - qtkite/defender-control: An open-source windows defender manager. Now you can easily manage your windows defender settings. |
| 102 | url | 2024-01-02 23:58:41.713 | https://github.com/qtkite/defender-control | GitHub - qtkite/defender-control: An open-source windows defender manager. Now you can easily manage your windows defender settings. |
| 103 | url | 2024-01-02 23:58:42.172 | https://keeper.or.kr/board/%ED%9A%8C%EA%B3%84%EB%B6%80 | KEEPER |
| 104 | site setting (hsts) | 2024-01-02 23:58:42.436 | Encoded domain: by3HYgXFJoQvTPIDd2zzpjW2gj+L2+egy4ezZdihpTo= | HSTS observed |
| 105 | url | 2024-01-02 23:58:42.932 | https://keeper.or.kr/board/view/172699 | KEEPER |
| 106 | download | 2024-01-02 23:58:45.668 | blob:https://keeper.or.kr/d1748001-a21b-4fc8-a31f-3c27e8b6815e | Complete - 100% [33042/330] C:\Users\USER\Downloads\2023년 10월 회계부.png |
| 107 | url | 2024-01-02 23:58:51.332 | https://keeper.or.kr/board/%ED%9A%8C%EA%B3%84%EB%B6%80 | KEEPER |
| 108 | url | 2024-01-02 23:58:51.494 | https://keeper.or.kr/board/%ED%9A%8C%EA%B3%84%EB%B6%80?page= | KEEPER |
| 109 | url | 2024-01-02 23:58:51.531 | https://keeper.or.kr/board/%ED%9A%8C%EA%B3%84%EB%B6%80?page= | KEEPER |
| 110 | url | 2024-01-02 23:58:52.630 | https://keeper.or.kr/board/view/172659 | KEEPER |
| 111 | download | 2024-01-02 23:58:54.577 | blob:https://keeper.or.kr/e5395e36-5d78-471d-bdf7-4d15478fbe78 | Complete - 100% [54504/545] C:\Users\USER\Downloads\2023년 9월 회계부.png |

hindsight 도구를 활용하여 Edge 브라우저 분석

다운로드 유입 URL: <https://keeper.or.kr/board/view/172731>

다운로드 받은 악성 파일: 11월_회계부.rar

KEEPER CTF IR-2 풀이

- 11월_회계부 검색 → Jumplist 아티팩트를 확인하여 WinRar x64 가 11월_회계부.rar 열었음을 확인 할 수 있다. (2024-01-03 08:04:29 → UTC+9 계산 → 2024-01-03 17:04:29)

The screenshot shows a forensic analysis interface with several windows. At the top is a table of system artifacts:

| App Id | Description | Creation Time | Last Modified | Hostname | Path |
|--------------|--------------|-----------------------------|-----------------------------|-----------------|-------------------------------------|
| WinRAR | WinRAR x64 | 2024-01-03 07:34:56.5001167 | 2024-01-03 08:04:29.4284634 | desktop-gl2ujrg | C:\Users\User\Downloads\11월_회계부.rar |
| Quick Access | Quick Access | 2024-01-03 07:34:56.5001167 | 2024-01-03 08:04:29.5221957 | desktop-gl2ujrg | C:\Users\User\Downloads\11월_회계부.rar |

Below this is a 'Find' dialog box with the term '11월_회계부' entered.

The main pane displays search results for '11월_회계부' in various CSV files:

| File Name | Term | Hits |
|--|---------|------|
| 20240128205208_AutomaticDestinations.csv | 11월_회계부 | 2 |
| 20240128205209_LECmd_Output.csv | 11월_회계부 | 1 |
| 20240128205155_MFTECmd_\$MFT_Output.csv | 11월_회계부 | 1 |
| 20240128205200_MFTECmd_\$J_Output.csv | 11월_회계부 | 13 |
| 20240128205210_PECmd_Output.csv | 11월_회계부 | 1 |
| 20240128205211_RECcmd_Batch_Kroll_Batch_Output.csv | 11월_회계부 | 4 |

KEEPER CTF IR-2 풀이

| 20240128205225_SrumECmd_NetworkConnections_Output.csv | | | 20240128205225_SrumECmd_NetworkUsages_Output.csv | | | 20240128205225_SrumECmd_PushNotifications_Output.csv | | | 20240128205225_SrumECmd_vfupro... | | |
|---|-----|---|--|---------------------|-----|--|-----|------------|--------------------------------------|-------------------|---------------------------------------|
| 20240128205208_AutomaticDestinations.csv | | | 20240128205208_CustomDestinations.csv | | | 20240128205209_LECmd_Output.csv | | | x | User_UsrClass.csv | 20240128205152_MFTECmd_\$Boot_Outo... |
| Drag a column header here to group by that column | | | | | | | | | | | |
| Line | Tag | Source File | Source Created | Source Modified | ... | ... | ... | File Si... | Relative Path | | |
| ▼ = | □ | ■ | = | = | | | | = | ■ | | |
| ▶ 8 | □ | C:\Users\hyuunnnn\Desktop\cape_test\... | 2024-01-03 08:04:29 | 2024-01-03 08:04:29 | ... | ... | ... | 1243505 | ..\..\..\..\..\Downloads\11월_회계부.rar | | |

C:\Users\hyuunnnn\Desktop\cape_test\...\Users\...\AppData\Roaming\Microsoft\Windows\Recent\11월_회계부.lnk

- LNK 파일을 통해서도 확인 가능 - **11월_회계부.lnk** 파일이 **Recent** 폴더에 생성되어 있음
- 종합 분석 도구를 활용한다면 전체적인 악티브트들을 모두 분석하여 보여주기 때문에 더욱 빠른 분석이 가능하다.

과제

LNK 파일 분석 도구 만들어보기

- LNK 파일 내부 구조를 파싱하여 PATH 정보, 시간 정보, 파일명 등을 출력하는 프로그램 개발

The screenshot shows a Windows application window titled "LNK Parser". At the top, there is a search bar containing the path "C:\Users\hyuunnnn\Desktop\testtest" and two buttons: "File" and "Folder". Below the search bar is a table with 14 columns, each representing a different field or timestamp from the LNK file structure. The table contains 10 rows of data. At the bottom right of the application window are three buttons: "Start", "Export CSV", and "Exit".

| LnkFileName | MachineID | FileName | FilePath | FileSize(Byte) | LnkCreationTime | LnkAccessTime | LnkWriteTime | TargetCreationTi... | TargetAccessTime | TargetWriteTime | DriveType | VolumeLabel | DriveSerialNumber |
|--------------|------------|------------|--|----------------|--------------------|--------------------|--------------------|---------------------|--------------------|--------------------|-------------|--------------|-------------------|
| 11월_회계... | desktop... | 11월_회... | C:\Users\#\User#\Downloads\#11월_회계부.rar | 1243505 | 2024/01/03 17:0... | 2024/01/30 16:4... | 2024/01/03 17:0... | 2024/01/03 16:5... | 2024/01/03 17:0... | 2024/01/03 16:5... | DRIVE FIXED | e75ba0e | |
| 2023년 5월... | desktop... | 2023년 ... | C:\Users\#\User#\Downloads\#2023년 5월 회계부.png | 120377 | 2024/01/03 17:0... | 2024/01/30 16:4... | 2024/01/03 17:0... | 2024/01/03 16:5... | 2024/01/03 17:0... | 2024/01/03 16:5... | DRIVE FIXED | e75ba0e | |
| 2023년 8월... | desktop... | 2023년 ... | C:\Users\#\User#\Downloads\#2023년 8월 회계부.png | 37241 | 2024/01/03 17:0... | 2024/01/30 16:4... | 2024/01/03 17:0... | 2024/01/03 16:5... | 2024/01/03 17:0... | 2024/01/03 16:5... | DRIVE FIXED | e75ba0e | |
| 2023년 9월... | desktop... | 2023년 ... | C:\Users\#\User#\Downloads\#2023년 9월 회계부.png | 54504 | 2024/01/03 17:0... | 2024/01/30 16:4... | 2024/01/03 17:0... | 2024/01/03 16:5... | 2024/01/03 17:0... | 2024/01/03 16:5... | DRIVE FIXED | e75ba0e | |
| autorun.lnk | desktop... | autorun... | D:\#\autorun.ico | 55802 | 2024/01/03 16:5... | 2024/01/30 16:4... | 2024/01/03 16:5... | 2023/08/10 22:5... | 1601/01/01 09:0... | 2023/08/10 22:5... | DRIVE CDROM | VMware Tools | 64619155 |
| CD 드라이브... | desktop... | | D:\#\ | 0 | 2024/01/03 16:5... | 2024/01/30 16:4... | 2024/01/03 16:5... | 2023/08/10 22:5... | 1601/01/01 09:0... | 2023/08/10 22:5... | DRIVE CDROM | VMware Tools | 64619155 |
| ms-gaming... | desktop... | | D:\#\ | 0 | 2024/01/03 17:1... | 2024/01/30 16:4... | 2024/01/03 17:3... | 1601/01/01 09:0... | 1601/01/01 09:0... | 1601/01/01 09:0... | DRIVE CDROM | VMware Tools | 64619155 |
| x86_x86_... | desktop... | x86 x86... | C:\#\Users\#\User#\Downloads\#x86 x86_64 아카이브... | 1092574 | 2024/01/03 17:1... | 2024/01/30 16:4... | 2024/01/03 17:1... | 2024/01/03 17:0... | 2024/01/03 17:1... | 2024/01/03 17:0... | DRIVE FIXED | e75ba0e | |
| 다운로드.lnk | desktop... | Downlo... | C:\#\Users\#\User#\Downloads | 4096 | 2024/01/03 17:0... | 2024/01/30 16:4... | 2024/01/03 17:1... | 2024/01/03 16:4... | 2024/01/03 17:1... | 2024/01/03 17:0... | DRIVE FIXED | e75ba0e | |
| 인터넷.lnk | desktop... | Downlo... | C:\#\Users\#\User#\Downloads | 0 | 2024/01/03 17:1... | 2024/01/30 16:4... | 2024/01/03 17:3... | 1601/01/01 09:0... | 1601/01/01 09:0... | 1601/01/01 09:0... | DRIVE FIXED | e75ba0e | |

¹ <http://forensic.korea.ac.kr/tools.html>

참고자료

- What are the forensic analysis tools used by experts? - PLAINBIT
- Magnet AXIOM, 한글화 안 되어도 사용되는 이유 - 보안 뉴스 (2016. 07. 14)
 - 한글화 관련 이슈는 2016년 기준
- 기초부터 따라하는 디지털포렌식
- 웹 브라우저의 포렌식 분석 기법 비교 연구 - 논문 리뷰