

5주차 스터디

X-Ways Forensics 사용법

각종 캐시 파일 분석, Prefetch, Windows Timeline, Windows Search 분석

분석 목표와 분석 계획은 분석이 목표한 방향으로 진행될 수 있게 해준다. 분석 계획은 계획이라는 것을 명심하라.

분석을 진행하다 보면 탐색하고 싶은 뭔가를 발견하거나 또는 탐색할 필요가 있다고 생각되는 것이 있을 수 있다.

일부 아티팩트나 흔적들을 추적하는 것이 분석 목표에 다다르게 할 수도 있지만, 토끼 굴로도 이어질 수도 있다.

목표를 이용해 당신이 당면한 임무를 완수하는 데 집중하게 하고, 다른 관심 있는 사항들은 나중으로 미루게 한다.

이것은 (컨설턴트가 아니더라도) 반드시 기억해야 할 중요한 요소다.

누군가는 여러분의 분석 결과를 애타게 기다리고 있을지도 모른다.

그들은 규정 준수 부서 및 규제 기관에게 민감한 데이터에 접근될 수 있는지(이것은 완전히 새로운 문제로 이어진다) 또는 침해를 통보할 필요가 있는지 등에 따라 사업적으로 중요한 결정을 내려야 하는 상황에 있을 수 있다.

Windows 환경에서 침해 시스템 분석하기 - p134, Eng

¹ 윈도우 환경에서 침해 시스템 분석하기 정리

분석 작업은 대부분 반복 과정이다.

분석을 시작할 때는 몇 가지 발견 사항이나 침해 지표를 갖고 시작하게 된다.

새로운 정보를 찾기 위해 이를 활용하고, 거기서부터 또 다른 정보를 발견하게 되고,
그것을 중심으로 또 다른 분석이 시작된다.

발견된 정보를 좀 더 잘 설명할 수 있도록 계속 진행하며
분석 목표를 달성하기 위해 나아가게 된다.

Windows 환경에서 침해 시스템 분석하기 - p28, Eng

분석을 시작하기 전에 분석가들은 계획을 세워야 한다.

많은 분석가가 분석 시작 전에 문서화 대신 머릿속에 계획이나 절차를 갖고 시작한다.

하지만 분석이 진행되는 동안 뭔가를 빠뜨렸다는 것을 깨닫게 되며,

마지막 단계 직전에 가서야 분석이 누락된 부분에 대해 허겁지겁 분석하기도 한다.

여러분은 시스템에서 데이터가 유출된 징후를 확인하기 위해 찾을 수 있는 모든 위치를 기억할 수 있는가?
아티팩트의 유형과 모음 또는 시스템에 뭔가 발생한 지표 같은 미묘한 힌트들을 기억할 수 있는가?

¹ 윈도우 환경에서 침해 시스템 분석하기 정리

Windows 환경에서 침해 시스템 분석하기 - p31, Eng

데이터를 정확하게 해석하는 것은 매우 중요하다.
침해 6주 전에 발생했는데 분석가의 실수로 3년 전에 침해됐다고 잘못 설명하면
유출된 신용카드 번호의 숫자 산정에 영향을 줄 것이고,
결국 그들이 내야 할 벌금에 막대한 영향을 주게 될 것이다.

Windows 환경에서 침해 시스템 분석하기 - p26, Eng

디지털 포렌식 분석에서 문제 해결 역량과 의사소통 역량은
디지털 포렌식에 대한 탄탄한 기본 지식과 풍부한 실전 감각에서 나온다.

윈도우 포렌식에 있어서 기본 지식은 윈도우 파일시스템에 대한 배경지식과
윈도우 아티팩트에 대한 이해를 토대로 한다.

이러한 배경지식을 발판으로 풍부한 경험에서 나오는 실전 감각을 덧붙일 때
진정한 포렌식 분석관으로 거듭나게 된다.

윈도우 디지털 포렌식 완벽 활용서 - p10

X-Ways Forensics

General Options (F5 or Options -> General Options)¹

- Always run as administrator 체크: 라이브 분석이나 옵션 변경으로 인해 분석 PC의 레지스트리 값이 수정되는 등 작업을 수행할 때 문제가 발생하지 않는다.
- Display time zone → 한국 시간대(UTC +09:00) 설정
- Notation → Seconds: digits after decimal → 3 으로 설정
 - 시간 소수점 3자리까지 확인 가능
- Show file icons → Large Icons 체크
 - 아이콘이 전체적으로 작아서 키우는게 더 좋은 것 같다.
- Hexadecimal offsets 체크: 16진수가 익숙하면 체크, 10진수가 익숙하면 해제하기
- bytes per line : 한 라인에 몇 byte 씩 보여줄지 설정 → 취향대로 설정하기

¹ <https://ccibomb.tistory.com/1182>

² <https://goblinforensics.tistory.com/289>

X-Ways Forensics

Directory Browser Options (CTRL + F5 or Options -> Directory Browser)¹

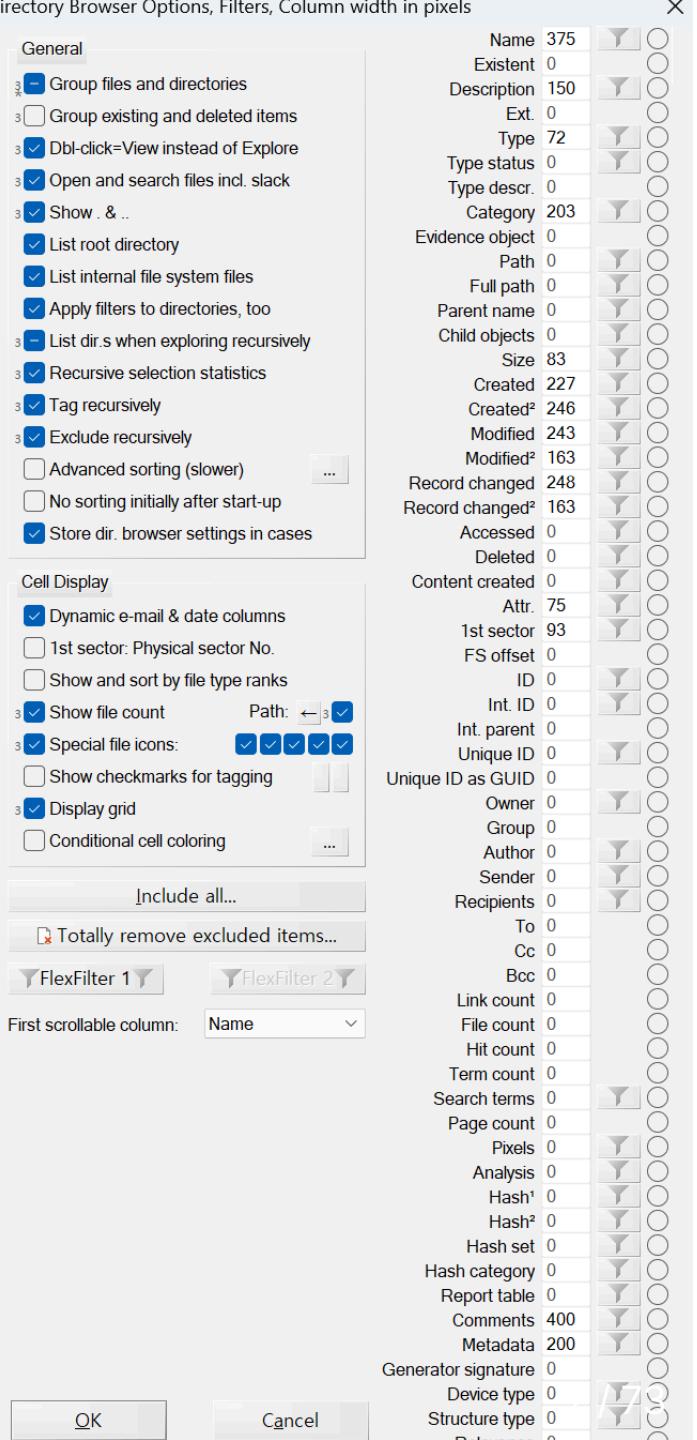
- Created² , Modified² , Record changed² 설정 - 숫자 값을 적절히 넣으면 된다.
 - SIA²의 변조 가능성 있음, \$FNA³ 시간 정보도 확인하기 위해 설정⁴
- Type status , Category , Comments , Metadata 등 적절히 설정
 - Category 는 Type 보다 좀 더 포괄적인 필터링 가능
→ Category 설명 슬라이드 참고
 - Type status 는 변경된 확장자 탐지 가능
→ Type , RVS 설명 슬라이드 참고

¹ <https://ccibomb.tistory.com/1182>, <https://goblinforensics.tistory.com/311>

² SIA (Standard Information Attribute)

³ \$FNA (\$FILE_NAME - NTFS 속성)

⁴ 윈도우 디지털 포렌식 완벽 활용서 - p384, How to Identify Timestamping using KAPE



X-Ways Forensics

- Content created 설정
 - 인터넷에서 파일을 다운로드했을 때 생성 시각은 다운로드 시작 시점, 수정 시각은 다운로드 종료 시점이 저장되는데, 해당 옵션을 설정하면 파일 헤더에 기록된 마지막 생성 및 수정 시간을 확인할 수 있다.¹²
- Analysis , Comments , Metadata 설정
 - RVS 결과, 각종 플러그인의 결과가 저장된다.
 - X-Tensions 플러그인의 결과를 대부분 Comments 에 저장하는 것 같다.

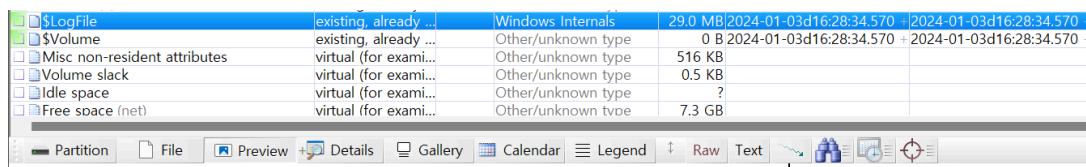
¹ 윈도우 디지털 포렌식 완벽 활용서 - p94

² <https://goblinforensics.tistory.com/311>

X-Ways Forensics

Viewer Programs (Options -> Viewer Programs)¹²³⁴

- 뷰어 컴포넌트 관련 설정 화면
- 뷰어 컴포넌트가 정상적으로 작동하는지 확인하기 위해 .lnk 또는 \$LogFile 파일을 열어보자.

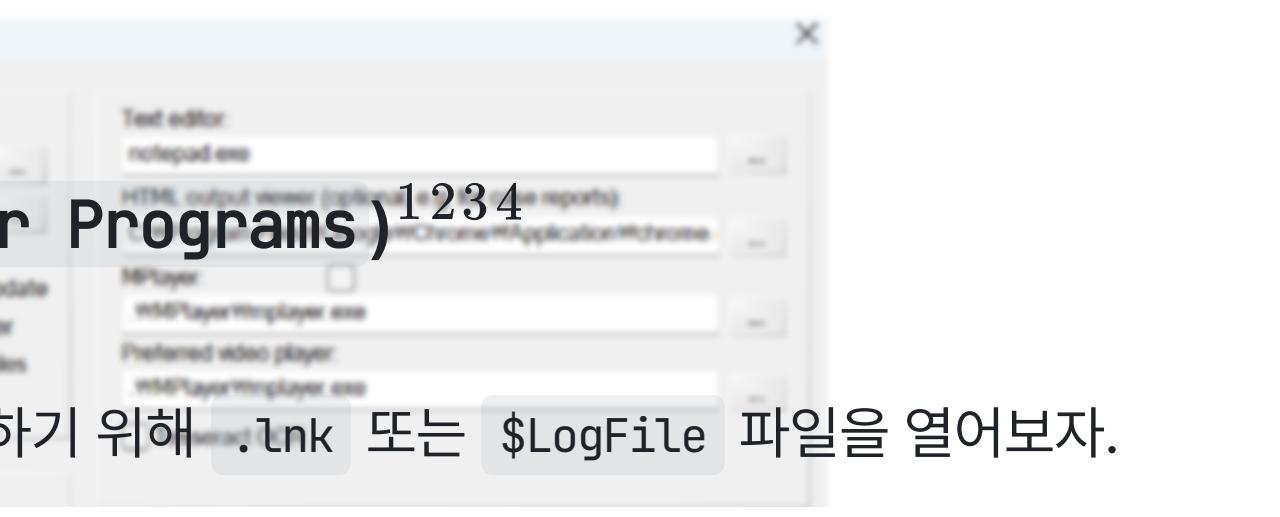


Overview of deleted files. For full analysis click "Raw".

\$LogFile	existing, already ...	Windows Internals	29.0 MB	2024-01-03d16:28:34.570 +	2024-01-03d16:28:34.570 +9
\$Volume	existing, already ...	Other/unknown type	0 B	2024-01-03d16:28:34.570 +	2024-01-03d16:28:34.570 +9
Misc non-resident attributes	virtual (for exami...)	Other/unknown type	516 KB		
Volume slack	virtual (for exami...)	Other/unknown type	0.5 KB		
Idle space	virtual (for exami...)	Other/unknown type	?		
Free space (net)	virtual (for exami...)	Other/unknown type	7.3 GB		

Local State~RF22c94.TMP

Not in volume snapshot	true
Incomplete	true
LogFile Offset	0x11558
File ID	109237
Sequence Number	4
Parent	110515
Flags	A
File Size	37978



¹ <https://ccibomb.tistory.com/1183>

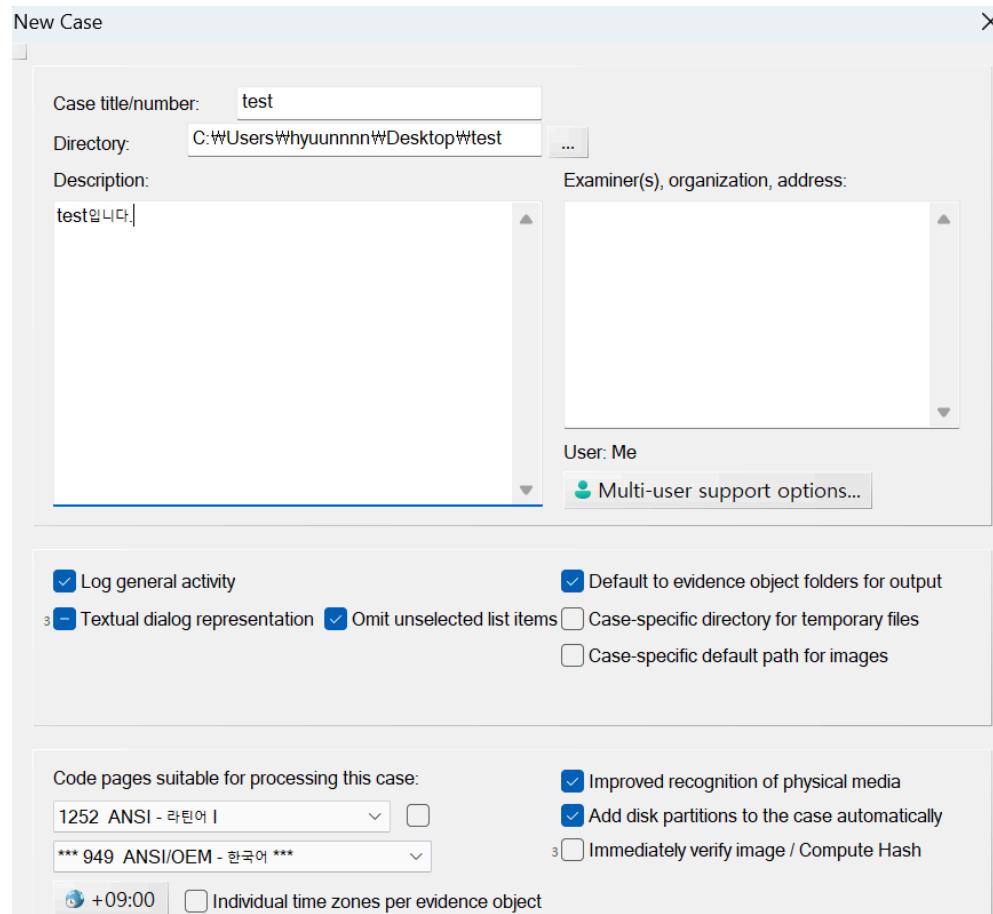
² <https://goblinforensics.tistory.com/313>

³ <https://goblinforensics.tistory.com/330>

⁴ <https://youtu.be/OuT33vh8ZoM>

X-Ways Forensics

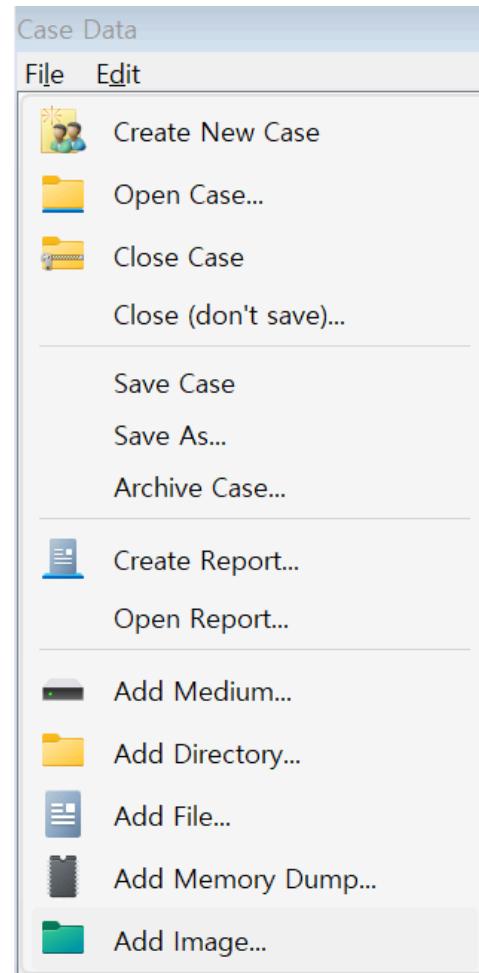
- View → Show → Case Data 활성화
- Case Data → File → Create New Case 클릭



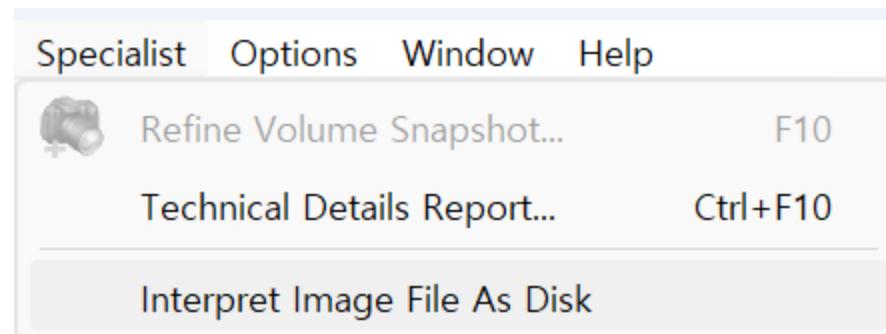
¹ <https://goblinforensics.tistory.com/291>

X-Ways Forensics

- File → Add Image → E01 등 이미지 파일 열기



X-Ways Forensics



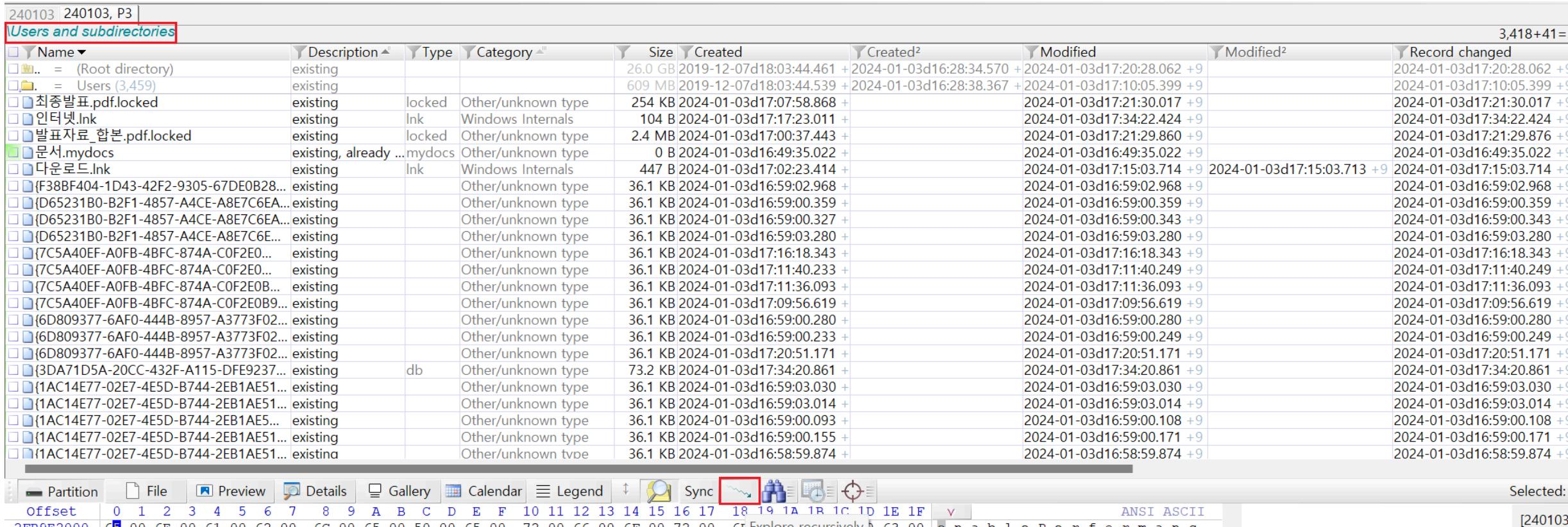
- File → E01 이미지 파일 열기 → Specialist → Interpret Image File As Disk 를 누르면 이미지 파일의 디스크 구조를 보여줘서 분석할 수 있다.

Name	Description	Type	Category	Size
Start sectors	virtual (for exami...)			1.0 MB
Partition 1	partition, existing	FAT32		100 MB
Partition 2	partition, existing	?		16.0 MB
Partition 3	partition, existing	NTFS		19.3 GB
Partition gap	virtual (for exami...)			547 KB
Partition 4	partition, existing	NTFS		573 MB
Unpartitioned space	virtual (for exami...)			2.0 MB

- 그러나 케이스를 만들어서 사용하는 방법이 더 편하고, 이점이 있기 때문에 케이스를 만들어서 사용하자.

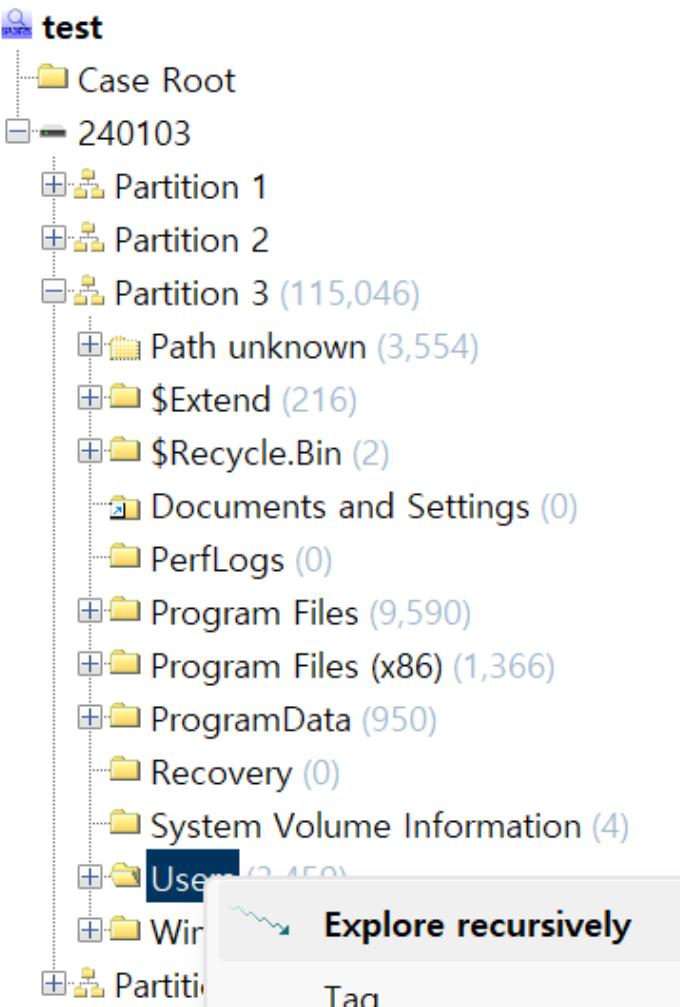
X-Ways Forensics

- Explore Recursively : 재귀 탐색 기능
 - 현재 경로 이후로 존재하는 모든 파일들을 보여준다. - 폴더는 보여주지 않는다.
 - 특정 파일을 찾을 때 필터를 적용하면 수월하게 찾을 수 있다. - 필터 설명 슬라이드 참고



The screenshot displays the X-Ways Forensics interface. The main window shows a list of files under the heading "Users and subdirectories". The columns include Name, Description, Type, Category, Size, Created, Created², Modified, Modified², and Record changed. The list contains numerous files, many of which are locked (indicated by a lock icon) and have various sizes and dates. The "Sync" button in the toolbar is highlighted with a red box. The status bar at the bottom provides details about the current file offset (2FB9E2000) and enables performance settings like "enable performance" and "File cyclic".

X-Ways Forensics



Case Data 창에서 원하는 경로 오른쪽 클릭 → Explore Recursively 도 가능하다.

뒤로가는 Backspace이며, 자주 사용한다. - 재귀 탐색 상태에서 파일을 찾은 후 빠르게 재귀 탐색 기능을 끄고 싶을 때 Backspace를 누르면 된다.

¹ <https://goblinforensics.tistory.com/304>

X-Ways Forensics

- 필터 기능¹²³
 - 상단에 Name, Description, Type, Category 등을 누르면 오름차순, 내림차순 설정이 가능하다.
 - 컬럼 왼쪽의 아이콘을 누르면 각 컬럼에 특화된 필터 기능을 적용할 수 있다.
 - 최대 3개까지 필터를 중첩하여 적용할 수 있다. Shift + 클릭 을 하면 해제된다.
 - 또한 컬럼을 오름차순 정렬 후 타이핑하여 이동할 수 있다.

Name	Description	Type	Category	Size	Created	Created ²	Modified	Modified ²	Record changed
.. = (Root directory)	existing			26.0 GB	2019-12-07d18:03:44.461	+ 2024-01-03d16:28:34.570	+ 2024-01-03d17:20:28.062 +9	+ 2024-01-03d17:20:28.062 +9	+ 2024-01-03d17:20:28.062 +9
.. = Users (3,459)	existing			609 MB	2019-12-07d18:03:44.539	+ 2024-01-03d16:28:38.367	+ 2024-01-03d17:10:05.399 +9	+ 2024-01-03d17:10:05.399 +9	+ 2024-01-03d17:10:05.399 +9
최종발표.pdf.locked	existing	locked	Other/unknown type	254 KB	2024-01-03d17:07:58.868	+ 2024-01-03d17:21:30.017 +9			+ 2024-01-03d17:21:30.017 +9
인터넷.lnk	existing	lnk	Windows Internals	104 B	2024-01-03d17:17:23.011	+ 2024-01-03d17:34:22.424 +9			+ 2024-01-03d17:34:22.424 +9
발표자료_합본.pdf.locked	existing	locked	Other/unknown type	2.4 MB	2024-01-03d17:00:37.443	+ 2024-01-03d17:21:29.860 +9			+ 2024-01-03d17:21:29.876 +9
문서.mydocs	existing, already ...	mydocs	Other/unknown type	0 B	2024-01-03d16:49:35.022	+ 2024-01-03d16:49:35.022 +9			+ 2024-01-03d16:49:35.022 +9
다운로드.lnk	existing	lnk	Windows Internals	447 B	2024-01-03d17:02:23.414	+ 2024-01-03d17:15:03.714 +9	+ 2024-01-03d17:15:03.713 +9	+ 2024-01-03d17:15:03.714 +9	+ 2024-01-03d17:15:03.714 +9
{F38BF404-1D43-42F2-9305-67DE0B28...	existing		Other/unknown type	36.1 KB	2024-01-03d16:59:02.968	+ 2024-01-03d16:59:02.968 +9			+ 2024-01-03d16:59:02.968 +9
{D65231B0-B2F1-4857-A4CE-A8E7C6EA...	existing		Other/unknown type	36.1 KB	2024-01-03d16:59:00.359	+ 2024-01-03d16:59:00.359 +9			+ 2024-01-03d16:59:00.359 +9
{D65231B0-B2F1-4857-A4CE-A8E7C6EA...	existing		Other/unknown type	36.1 KB	2024-01-03d16:59:00.327	+ 2024-01-03d16:59:00.343 +9			+ 2024-01-03d16:59:00.343 +9
{D65231B0-B2F1-4857-A4CE-A8E7C6E...	existing		Other/unknown type	36.1 KB	2024-01-03d16:59:03.280	+ 2024-01-03d16:59:03.280 +9			+ 2024-01-03d16:59:03.280 +9
{7C5A40EF-A0FB-4BFC-874A-C0F2E0...	existing		Other/unknown type	36.1 KB	2024-01-03d17:16:18.343	+ 2024-01-03d17:16:18.343 +9			+ 2024-01-03d17:16:18.343 +9
{7C5A40EF-A0FB-4BFC-874A-C0F2E0...	existing		Other/unknown type	36.1 KB	2024-01-03d17:11:40.233	+ 2024-01-03d17:11:40.249 +9			+ 2024-01-03d17:11:40.249 +9
{7C5A40EF-A0FB-4BFC-874A-C0F2E0B...	existing		Other/unknown type	36.1 KB	2024-01-03d17:11:36.093	+ 2024-01-03d17:11:36.093 +9			+ 2024-01-03d17:11:36.093 +9
{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9...	existing		Other/unknown type	36.1 KB	2024-01-03d17:09:56.619	+ 2024-01-03d17:09:56.619 +9			+ 2024-01-03d17:09:56.619 +9
{680237-6A5D-441B-8957-A3773F02...	existing		Other/unknown type	36.1 KB	2024-01-03d16:59:00.280	+ 2024-01-03d16:59:00.280 +9			+ 2024-01-03d16:59:00.280 +9
{26D809377-6AF0-444B-8957-A3773F02...	existing		Other/unknown type	36.1 KB	2024-01-03d16:59:00.233	+ 2024-01-03d16:59:00.249 +9			+ 2024-01-03d16:59:00.249 +9
{680237-6A5D-441B-8957-A3773F02...	existing		Other/unknown type	36.1 KB	2024-01-03d17:20:51.171	+ 2024-01-03d17:20:51.171 +9			+ 2024-01-03d17:20:51.171 +9
{3DA71D5A-20CC-432F-A115-DFF9237...	existing	db	Other/unknown type	73.2 KB	2024-01-03d17:34:20.861	+ 2024-01-03d17:34:20.861 +9			+ 2024-01-03d17:34:20.861 +9
{11777924-5956-425B-8900-0E501...	existing		Other/unknown type	36.1 KB	2024-01-03d16:59:03.030	+ 2024-01-03d16:59:03.030 +9			+ 2024-01-03d16:59:03.030 +9
{1AC14E77-02E7-4E5D-B744-2EB1AE51...	existing		Other/unknown type	36.1 KB	2024-01-03d16:59:03.014	+ 2024-01-03d16:59:03.014 +9			+ 2024-01-03d16:59:03.014 +9

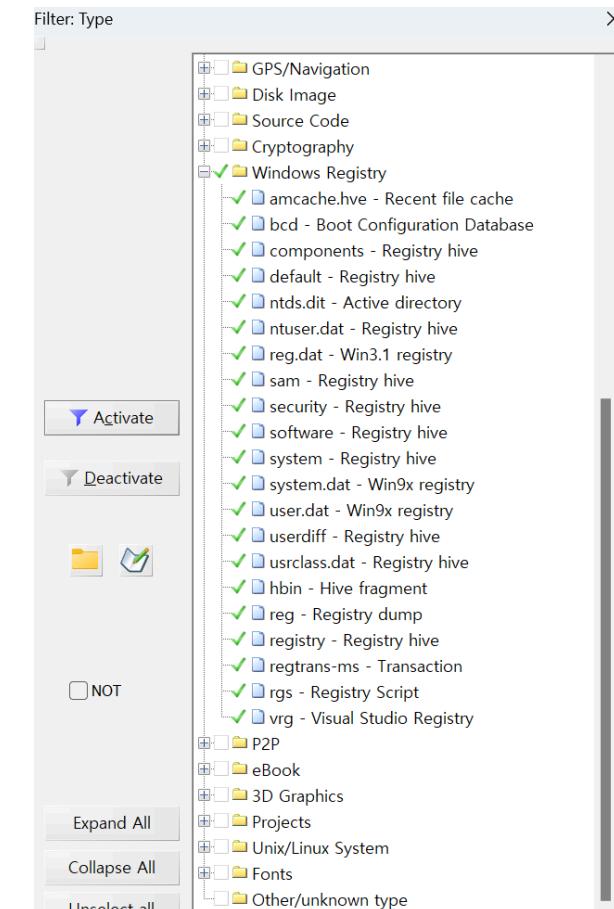
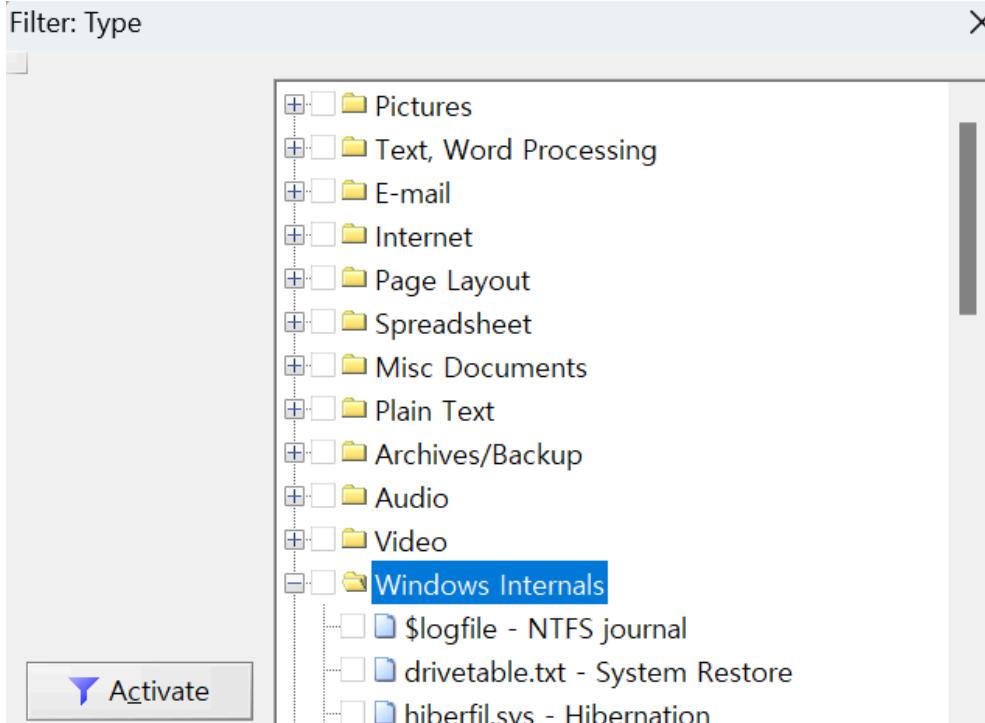
1 <https://scibomb.tistory.com/4193>

2 <https://gobin-forensic.tistory.com/309>

3 <https://youtu.be/dfmokIW7zoc>

X-Ways Forensics

- Type 필터를 사용하면 사진처럼 원하는 확장자, 파일을 선택하여 볼 수 있다.
- Type 들의 그룹은 Category 를 의미한다. - 다음 슬라이드 참고



X-Ways Forensics

- Category 필터 종류를 보면 Type 보다 큰 범주로 묶여있다. - 같은 유형의 파일들을 찾을 수 있다.

Name	Description	Type	Category	Size	Created
debuggerDiagRemote.js	existing, har...	js	✓ Deactivate this filter		
debuggerDiagRemote.js	existing, har...	js	Other/unknown type	6,793	
debugger.html	existing, har...	html	Pictures	11,496	
debugger.html	existing, har...	html	Text, Word Processing	2,613	
debugger.css	existing, har...	css	E-mail	0	
debugger.css	existing, har...	css	Internet	2,419	
debugger.bundle.js	existing, har...	js	Page Layout	1	
debugger.bundle.js	existing, har...	js	Spreadsheet	4	
DebugAndTrace.aspx	existing	aspx	Misc Documents	2,508	
DebugAndTrace.aspx	existing	aspx	Plain Text	421	
DebugAndTrace.aspx	existing	aspx	Archives/Backup	28	
de-DE.mail.config	existing	config	Audio	240	
DccpWCpoNzCwM4Qymi_Ji67llso.br[1].js	existing	js	Video	22	
daytonaOptOut.js	existing, har...	js			
daytonaOptOut.js	existing, har...	js			
data_3	existing				
data_3	existing				
data_3	existing				
data_3	existing				
data_3	existing				
data_3	existing				
data_3	existing				
data_3	existing				

X-Ways Forensics

- KEEPER CTF IR-1 문제에서 랜섬웨어 찾기
 - 랜섬웨어는 존재했던 파일을 암호화하는 과정에서 파일이 수정된다.

Name	Description	Type	Category	Size	Created	Created ²	Modified	Modified ²	Record changed
= User (3,391)	existing			608 MB	2024-01-03d16:48:28.960 +9				2024-01-03d17:33:51.486 +9
= Downloads (14)	existing			60.1 MB	2024-01-03d16:48:29.085 +9				2024-01-03d17:21:30.017 +9
desktop.ini	existing	ini	Programs	282 B	2024-01-03d16:49:34.866 +9				2024-01-03d16:49:34.866 +9
disable-defender (2).exe.locked	existing	locked	Other/unknown type	295 KB	2024-01-03d16:55:38.536 +9				2024-01-03d17:21:28.557 +9
2023년 10월 회계부.png.locked	existing	locked	Other/unknown type	32.3 KB	2024-01-03d16:58:45.673 +9				2024-01-03d17:18:11.268 +9
2023년 9월 회계부.png.locked	existing	locked	Other/unknown type	53.2 KB	2024-01-03d16:58:54.577 +9				2024-01-03d17:18:11.334 +9
2023년 8월 회계부.png.locked	existing	locked	Other/unknown type	36.4 KB	2024-01-03d16:59:49.702 +9				2024-01-03d17:18:11.317 +9
2023년 5월 회계부.xlsx.locked	existing	locked	Other/unknown type	118 KB	2024-01-03d16:59:55.624 +9				2024-01-03d17:18:11.299 +9

- 암호화된 파일을 찾았다면 Record changed 정렬, Explore Recursively 를 적용하여 찾아낼 수 있다.
 - 파일이 수정됨에 따라서 Record 정보가 변경되었기 때문이다.

Name	Description	Type	Category	Size	Created	Created ²	Modified	Modified ²	Record changed
0IAjDNgXOrF0.exe	existing	exe	Programs	208 KB	2024-01-03d17:18:07.214 +9				2024-01-03d17:18:07.245 +9
Install-2024-01-03.0817.5196.1.odlgz	existing	odlgz	Other/unknown type	2.5 KB	2024-01-03d17:18:07.245 +9				2024-01-03d17:18:07.245 +9
Install-PerUser-2024-01-03.0817.5796.1.odll...	existing	odlgz	Other/unknown type	446 B	2024-01-03d17:18:07.339 +9				2024-01-03d17:18:07.339 +9
Install-PerUser_2024-01-03_081735_16a4-1...	existing	log	Plain Text	124 KB	2024-01-03d17:17:35.792 +9				2024-01-03d17:18:08.604 +9
refcount.ini	existing	ini	Programs	25 B	2024-01-03d16:51:46.453 +9				2024-01-03d17:18:08.807 +9
2023년 10월 회계부.png.locked	existing	locked	Other/unknown type	32.3 KB	2024-01-03d16:58:45.673 +9				2024-01-03d17:18:11.268 +9
2023년 5월 회계부.png.locked	existing	locked	Other/unknown type	118 KB	2024-01-03d16:59:55.624 +9				2024-01-03d17:18:11.299 +9
2023년 8월 회계부.png.locked	existing	locked	Other/unknown type	36.4 KB	2024-01-03d16:59:49.702 +9				2024-01-03d17:18:11.317 +9
2023년 9월 회계부.png.locked	existing	locked	Other/unknown type	53.2 KB	2024-01-03d16:58:54.577 +9				2024-01-03d17:18:11.334 +9
cors(기파발표).pptx.locked	existing	locked	Other/unknown type	1.5 MB	2024-01-03d17:00:22.217 +9				2024-01-03d17:18:11.400 +9
KEEPER 기술문서 최종발표.pptx.locked	existing	locked	Other/unknown type	160 KB	2024-01-03d17:08:39.822 +9				2024-01-03d17:18:11.428 +9

랜섬웨어 의심 파일: 0IAjDNgXOrF0.exe

X-Ways Forensics

필터를 적극 활용하자!

이제 여러분도 분석을 빠르게 하기 위해 필터가 얼마나 유용한지 인지하였을 것이다.

하지만 실제로 필터를 효율적으로 사용하기 위해서는 사건이 어떤 사건인지 그리고 여러분이 얼마나 알고 있는지에 달려있다.

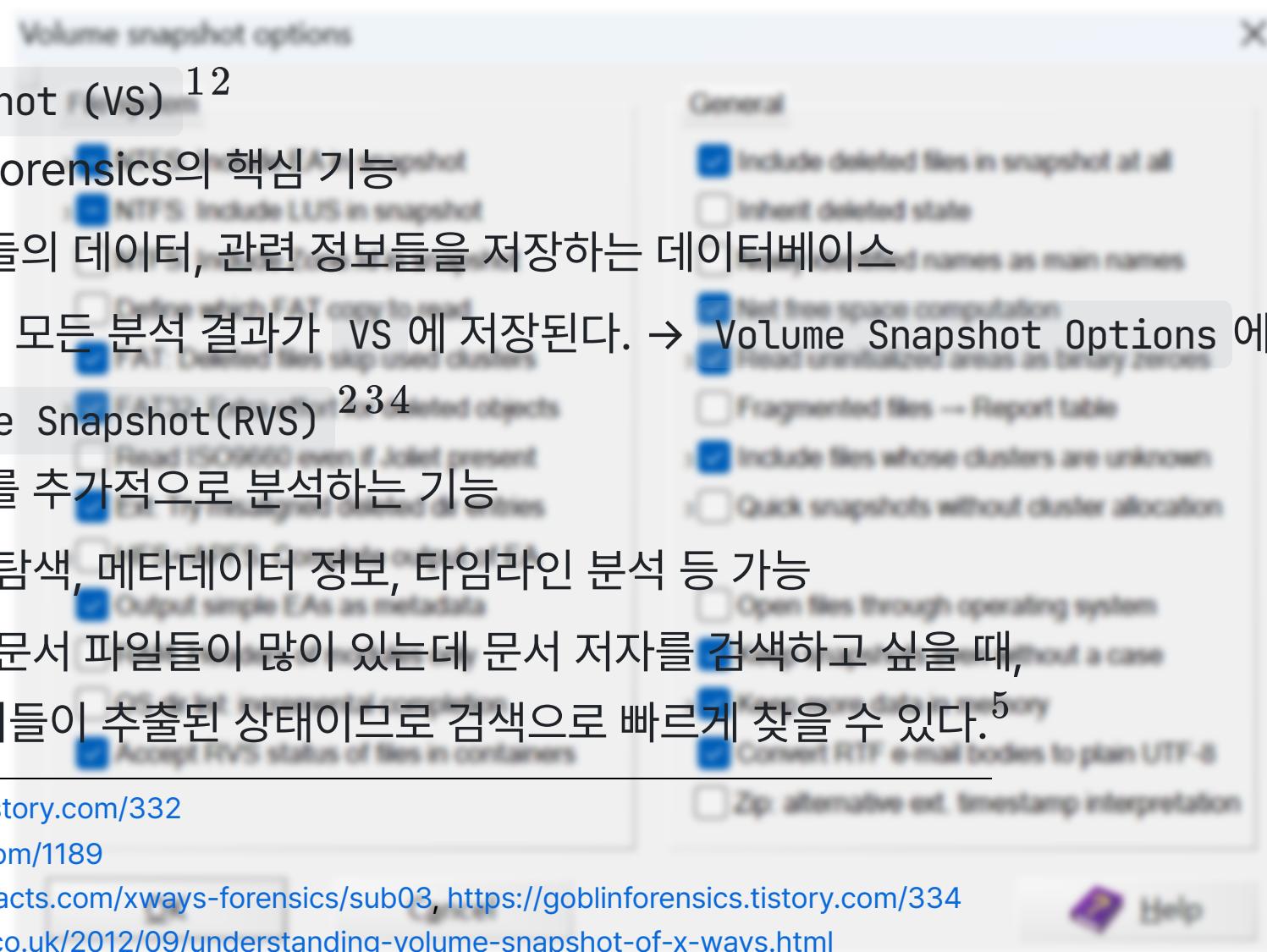
특정 정보를 찾을 때 어떤 종류의 레지스트리 하이브가 필요한지 미리 알고 있다면 Type 컬럼 필터에서 불필요한 파일들은 빠르게 제거할 수 있다.

만약 SYSTEM 하이브가 필요하다면 Name 컬럼 필터를 활용하여 Directory Browser에 있는 파일들에 다시 한번 필터를 적용할 수 있다.

[XWF를 이용한 포렌식 분석 - p140](#)

X-Ways Forensics

- Volume Snapshot (VS)^{1,2}
 - X-Ways Forensics의 핵심 기능
 - 증거 객체들의 데이터, 관련 정보들을 저장하는 데이터베이스
 - X-Ways의 모든 분석 결과가 VS에 저장된다. → Volume Snapshot Options에서 확인 가능
- Refine Volume Snapshot(RVS)^{2,3,4}
 - 증거 객체를 추가적으로 분석하는 기능
 - 압축 파일 탐색, 메타데이터 정보, 타임라인 분석 등 가능
 - 예를 들어 문서 파일들이 많이 있는데 문서 저자를 검색하고 싶을 때, 메타데이터들이 추출된 상태이므로 검색으로 빠르게 찾을 수 있다.⁵



¹ <https://goblinforensics.tistory.com/332>

² <https://ccibomb.tistory.com/1189>

³ <http://www.forensic-artifacts.com/xways-forensics/sub03>, <https://goblinforensics.tistory.com/334>

⁴ <https://www.xwaysclips.co.uk/2012/09/understanding-volume-snapshot-of-x-ways.html>

⁵ <https://www.x-ways.net/forensics/QuickGuide.pdf> - p23 ~ p30, <https://youtu.be/ggSXfAf4Eko>

X-Ways Forensics

- Refine Volume Snapshot(RVS)

- File header signature search^{1,3}

- 파일 카빙을 수행하는 옵션 - File Type Signatures Search.txt⁴ 사용

- Filename prefix 항목에 문자를 지정하면 카빙된 파일명 앞에 추가된다.²

A	B	C	D	E	F	G	
1	Description	Extensions	Header	Offset	Footer	Default size	Flags
2	*** Pictures						
3	JPEG	JPG;jpeg;jpe;thm;mpo	WxFFWxD8WxF[WxC0WxC4WxDBWxDDWxE0-WxE5WxE]	0 ~1	2097152/33554432		e
4	PNG	png	Wx89PNGWx0DWx0AWx1AWx0A	0 ~6			e
5	GIF	gif	GIF8[79]a	0 ~3	2097152/33554432		
6	High Efficiency Image	heic	(ftypheic ftypmif1)	4 ~27	1000000/31457280		
7	Thumbcache fragment	cmmm	CMMM..Wx00Wx00.[^Wx00]	0 ~84	2097152/511705088		GUb
8	TIFF/NEF/CR2/DNG	tif;tiff;nef;cr2;dng;pef;nrw;arw	(Wx49Wx49Wx2AWx00) (Wx4DWx4DWx00Wx2A)	0 ~5	25165824/268435456		
9	Bitmap	bmp;dib	BM.....Wx00.Wx00....[Wx0CWx28Wx38Wx40Wx6CWx7C]Wx	0 ~4			
10	Paint Shop Pro	psp;PsPImage;pfr	(Paint Shop Pro Im)(~BKWx00)	0 ~8		2097152	b
11	Canon Raw	crw	HEAPCCDR	6		8200000	c
12	Adobe Photoshop	PSD;pdd;p3m;p3r;p3l	8BPSWx00Wx01Wx00Wx00Wx00Wx00Wx00Wx00	0 ~9		10485760	b

¹ <https://ccibomb.tistory.com/1186>

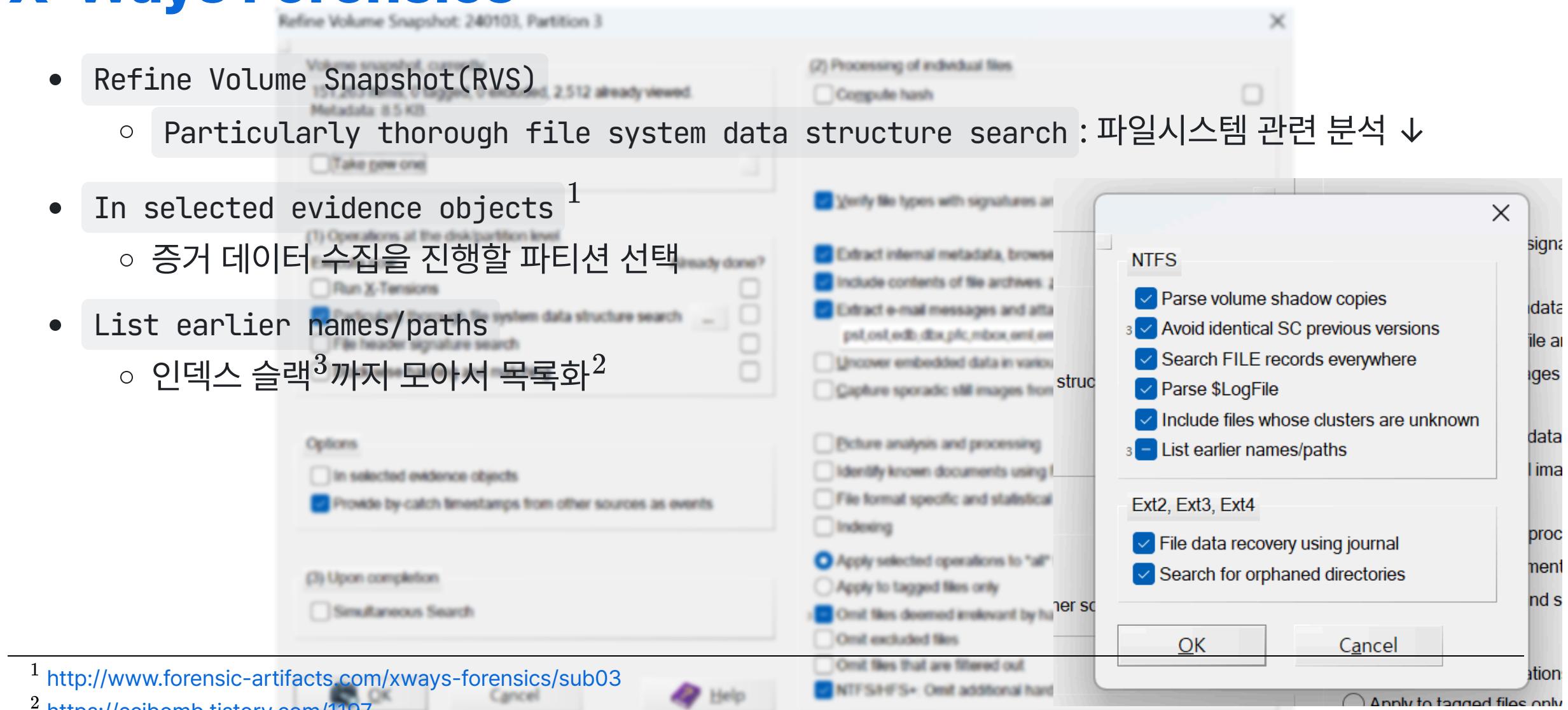
² <http://www.forensic-artifacts.com/xways-forensics/sub03>

³ <http://www.forensic-artifacts.com/xways-forensics/sub13>

⁴ <https://goblinforensics.tistory.com/358>

X-Ways Forensics

- Refine Volume Snapshot(RVS)
 - Particularly thorough file system data structure search : 파일시스템 관련 분석 ↓
- In selected evidence objects¹
 - 증거 데이터 수집을 진행할 파티션 선택
- List earlier names/paths
 - 인덱스 슬랙³까지 모아서 목록화²



¹ <http://www.forensic-artifacts.com/xways-forensics/sub03>

² <https://ccibomb.tistory.com/1197>

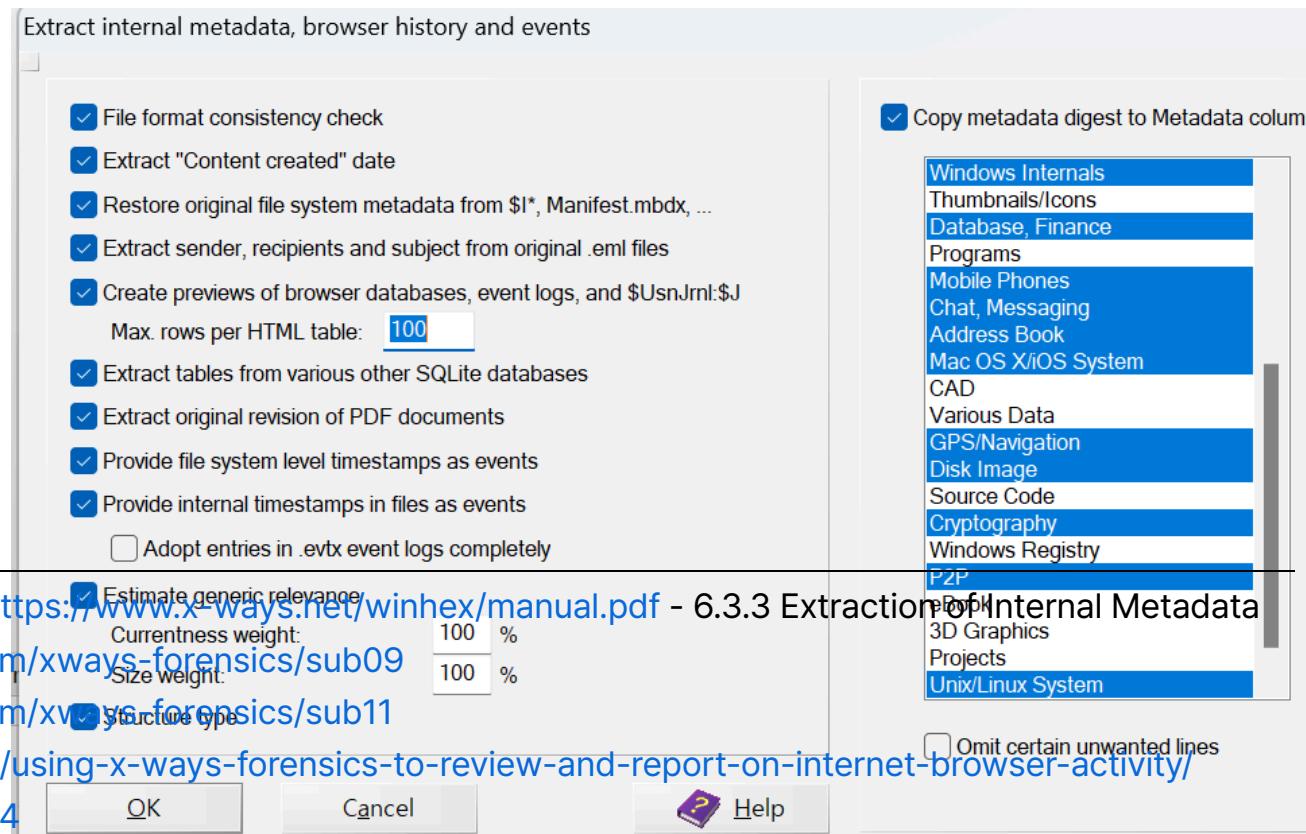
³ 물리적인 구조와 논리적인 구조의 차이로 발생하는 낭비되는 공간 - <http://forensicinsight.org/wp-content/uploads/2012/02/INSIGHT-MFT-INDX-슬랙-분석.pdf>

X-Ways Forensics

- Refine Volume Snapshot(RVS)

- Extract internal metadata, browser history and events²³⁴

→ 일관성 검사¹, 메타데이터 추출, 브라우저 히스토리 분석, 타임라인 분석⁵ - Events 슬라이드 참고



¹ File format consistency check, <https://www.x-ways.net/winhex/manual.pdf> - 6.3.3 Extraction of Internal Metadata

² <http://www.forensic-artifacts.com/xways-forensics/sub09>

³ <http://www.forensic-artifacts.com/xways-forensics/sub11>

⁴ <https://mreerie.com/2022/07/01/using-x-ways-forensics-to-review-and-report-on-internet-browser-activity/>

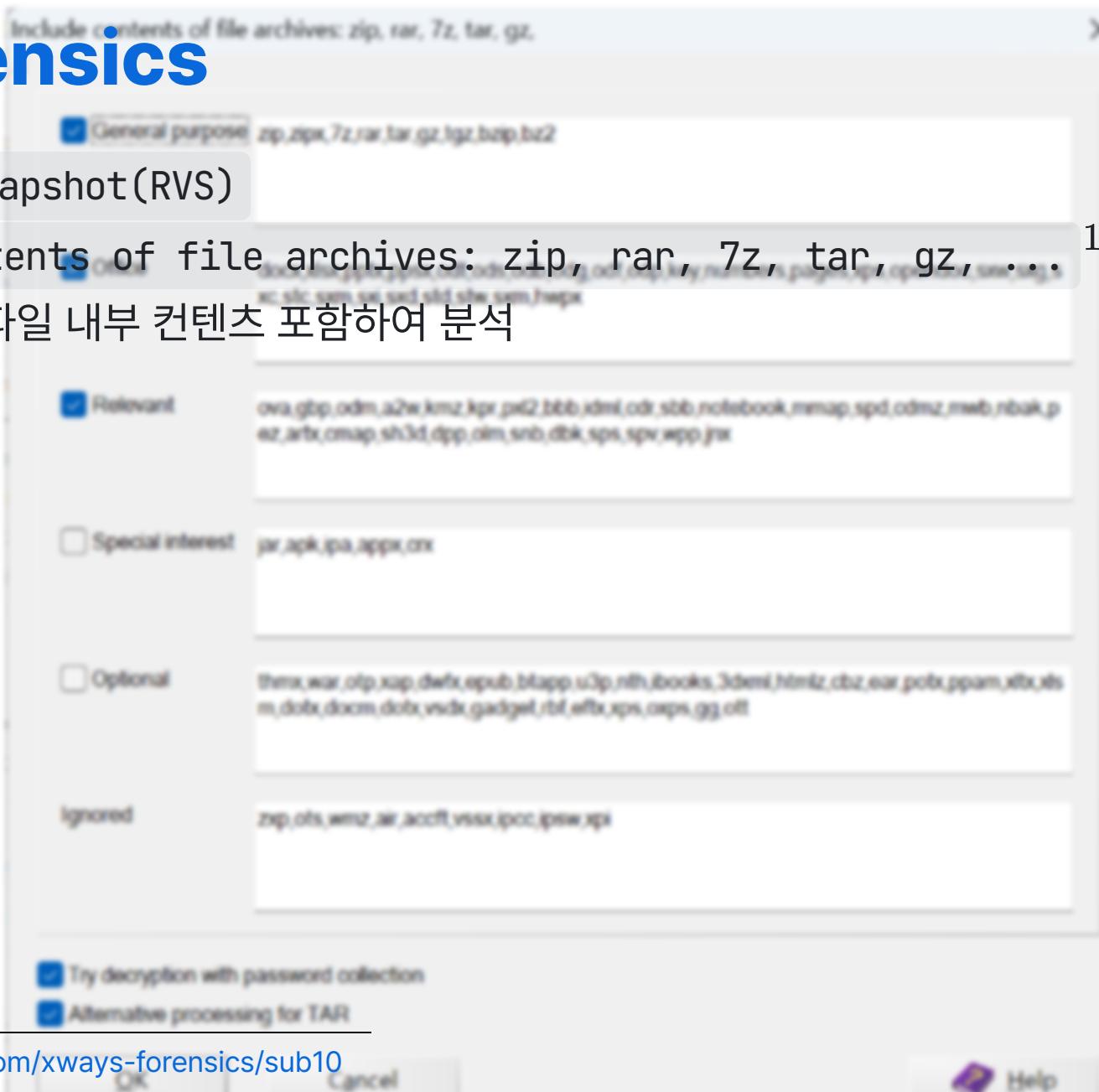
⁵ <https://ccibomb.tistory.com/1204>

X-Ways Forensics

- Refine Volume Snapshot(RVS)

- Include contents of file archives: zip, rar, 7z, tar, gz, ...¹

- 아카이브 파일 내부 컨텐츠 포함하여 분석



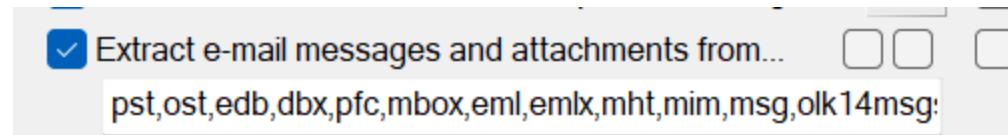
¹ <http://www.forensic-artifacts.com/xways-forensics/sub10>

X-Ways Forensics

- Refine Volume Snapshot(RVS)

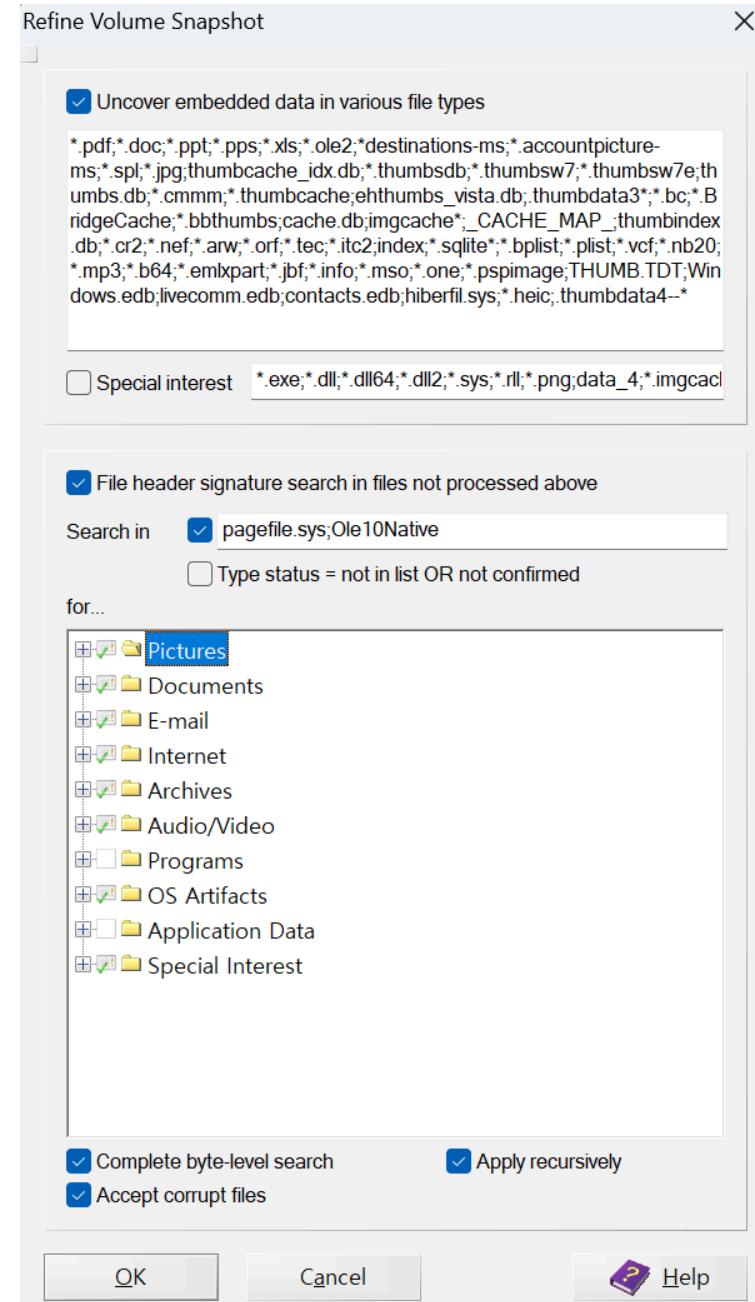
- Extract e-mail messages and attachments from...¹

- pst, ost, edb, eml 등에 존재하는 이메일 메시지 추출



- Uncover embedded data in various file types^{2,3} →

- 파일 내부에 존재하는 다른 파일들을 시그니처 기반으로 추출하는 기능



¹ <http://www.forensic-artifacts.com/xways-forensics/sub07>

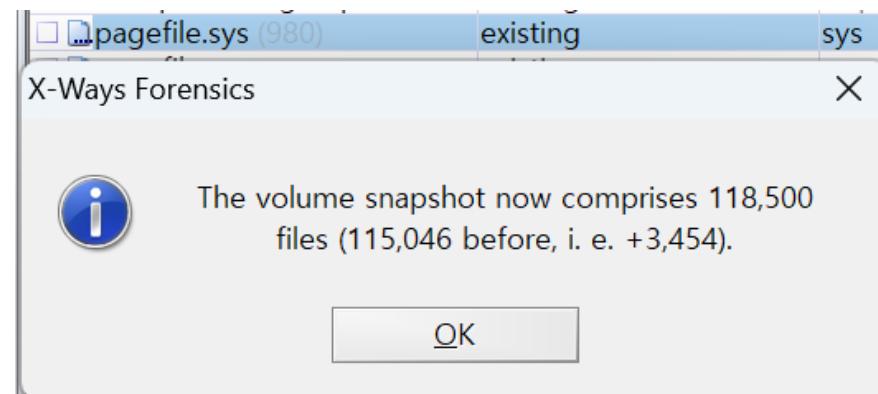
² <https://goblinforensics.tistory.com/340>

³ <http://www.forensic-artifacts.com/xways-forensics/anti02>

X-Ways Forensics

- Refine Volume Snapshot(RVS)
 - Uncover embedded data in various file types
- ex: pagefile.sys → pagefile.sys (980) 변경됨
 - pagefile.sys 내부에 존재하는 파일들을 추출하여 3번 사진의 결과 확인 가능

Name	Type
DumpStack.log.tmp	existing, already viewed
pagefile.sys	existing
swapfile.sys	existing
Free space (net)	virtual (for examination ...)



1

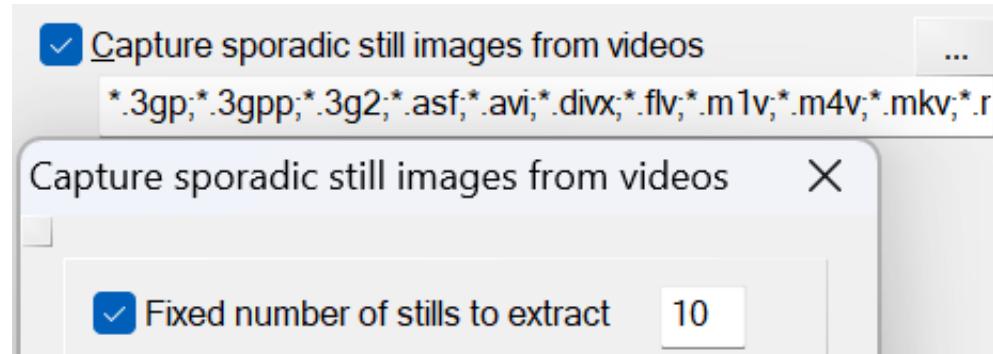
Name	Description
..	(Root directory)
pagefile.sys (980)	existing
Embedded 001.xml	existing
Embedded 0010.jpg	existing
Embedded 002.xml	existing
Embedded 003.png	existing
Embedded 004.png	existing
Embedded 005.png	existing
Embedded 006.png	existing

2

3

X-Ways Forensics

- Refine Volume Snapshot(RVS)
 - Capture sporadic still images from videos
 - 영상 파일을 스틸 사진¹처럼 일정 간격마다 이미지 파일로 생성해주는 기능



- 오른쪽 클릭 → Explore 클릭했을 때 생성된 이미지 파일 확인 가능

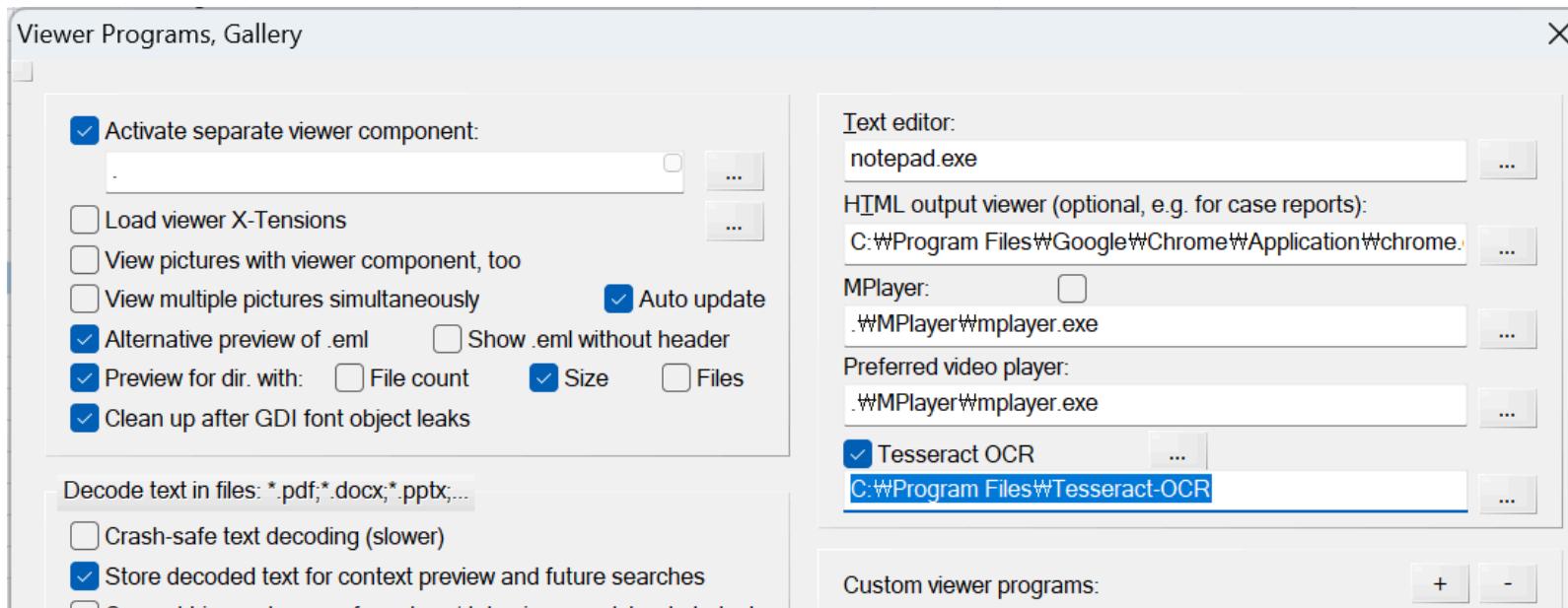
Name	Description	Type	Type status	Category
= SystemSettings (12)	existing			
= Assets (12)	existing			
Fonts (4)	existing			
EdrCalibration.mkv (1)	existing, har... mkv	confirmed		Video
HDRSample.mkv (2)	existing, har... mkv	confirmed		Video
SDRSample.mkv (2)	existing, har... mkv	confirmed		Video

Name	Description	Type	Type status	Category	Size
= Assets (12)	existing				5.3 MB
= SDRSample.mkv (2)	existing, har... jpg	mkv	confirmed	Video	1.7 MB
SDRSample.mkv 0m 01s.jpg	existing, alre... jpg	jpg	confirmed	Pictures	149 KB
SDRSample.mkv 0m 10s.jpg	existing, alre... jpg	jpg	confirmed	Pictures	139 KB

¹ https://ko.wikipedia.org/wiki/스틸_사진

X-Ways Forensics - Tesseract OCR¹

- 구글에서 만든 오픈소스 광학 문자 인식 엔진 - [윈도우 설치 파일](#)
- `Additional script data`, `Additional language data`는 상황에 맞게 설치

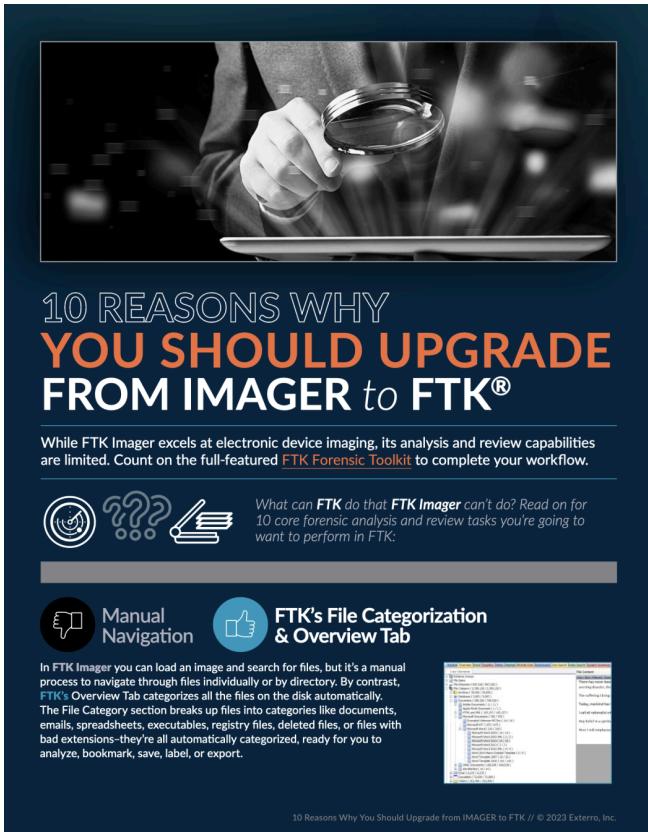


- `Options` → `Viewer Programs` → `Tesseract OCR` 활성화 → 설치한 경로 입력 → ... 버튼 클릭 → 인식할 언어 선택 (최대 2개까지 가능)

¹ <https://ko.wikipedia.org/wiki/테서랙트>

X-Ways Forensics - Tesseract OCR

- tessdata_best에서 최신 학습 모델로 바꿀 수 있다. → 설치할 때 파일들이 포함되기 때문에 pass
 - Capture sporadic still images from videos 을 활용하여 영상을 사진으로 추출 → 활용도 높음¹



The image shows the X-Ways Forensics software interface. The top menu bar includes 'File', 'Preview', 'Details', 'Gallery', 'Calendar', 'Legend', 'VC', 'OCR', and other options. The main area displays a list of files with columns for name, status, type, and size. One file, 'f 000121 ifull-disk-imaging-capabilitie', is selected. The 'Details' tab is active, showing detailed information about the selected file. An 'OCR' button is visible in the top right corner of the interface.

¹ <https://mreerie.com/2022/06/03/exploring-ocr-capability-tesseract-with-xwf/>

X-Ways Forensics

- Refine Volume Snapshot(RVS)
 - File format specific and statistical encryption tests^{1 2}

1. 엔트로피 테스트를 통해 255 바이트보다 큰 파일에 한해서 암호화되어었는지 여부를 확인
 - TrueCrypt, PGP Desktop, BestCrypt, DriveCrypt 등
 - 엔트로피가 특정 임계값을 초과했을 때 e? 플래그가 설정된다.
 - ZIP, RAR, TAR, GZ, BZ, 7Z, ARJ, CAB, JPG, PNG, GIF, TIF, MPG, SWF 등 압축 파일은 제외
 - 압축 파일이라서 엔트로피가 상승하여 암호화된 것인지 압축된 것인지 구별하기 어려움
2. .doc, .xls, .ppt, .pst, .xlsx, .pptx, .pdf 등 암호화 여부를 확인하며 DRM 여부도 확인
 - positive인 경우 e! 플래그가 설정된다.

하단에 있는 Legend 버튼에서 확인 가능 →

E: encrypted at filesystem level
e: encrypted in archive
e!: file type specific encryption/DRM
e?: high entropy, possibly fully encrypted

¹ <https://www.x-ways.net/winhex/manual.pdf> - 6.3.10 Detection of Encryption

² <http://www.forensic-artifacts.com/xways-forensics/sub14>

X-Ways Forensics

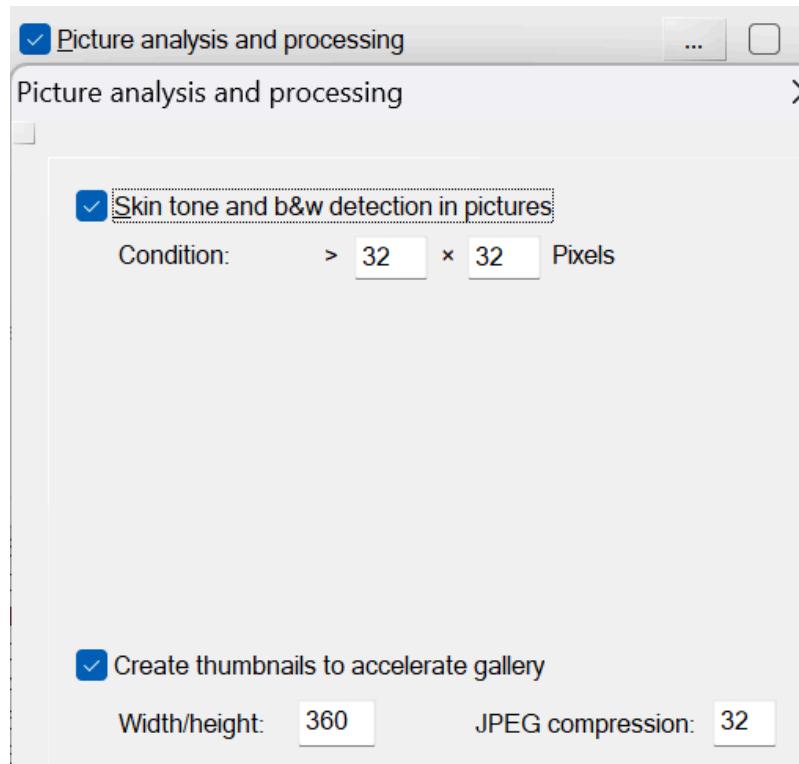
- Refine Volume Snapshot(RVS)
 - File format specific and statistical encryption tests¹

test.xfc 240103 240103, P3											
▼ 1 \ and subdirectories											
Name	Description	Type	C.	C.	Mod	Mod	R	R	Attr.	1st sector	
mpenginedb.db	existing	db	n.....	202...	2024...	2024...	20...	20...	e?XA	116,896	
segoeui_seibold[1].woff2	existing	woff2	n...F...	202...	2024...	2024...	20...	20...	e?XA	23,938,856	
segoeui_regular[1].woff2	existing	woff2	n...F...	202...	2024...	2024...	20...	20...	e?XA	23,102,440	
toptraffic[1]	existing		n.....	202...	2024...	2024...	20...	20...	e?XA	22,999,720	
topTraffic_638004170464094982	existing		n.....	202...	2024...	2024...	20...	20...	e?A	19,722,816	
2023년 10월 회계부.png.locked	existing	locked	n.....	202...	2024...	2024...	20...	20...	e?A	760,704	
2023년 5월 회계부.png.locked	existing	locked	n.....	202...	2024...	2024...	20...	20...	e?IA	19,872,032	
2023년 8월 회계부.png.locked	existing	locked	n.....	202...	2024...	2024...	20...	20...	e?IA	496,432	
2023년 9월 회계부.png.locked	existing	locked	n.....	202...	2024...	2024...	20...	20...	e?IA	766,424	
cors(키퍼발표).pptx.locked	existing	locked	n.....	202...	2024...	2024...	20...	20...	e?A	778,792	
KEEPER 기술문서 최종발표.pptx.locked	existing	locked	n.....	202...	2024...	2024...	20...	20...	e?A	9,052,472	
2024-01-03	existing		n.....	202...	2024...	2024...	20...	20...	e?A	118,856	
2023_하계_기술문서_중간발표.pdf.locked	existing	locked	n.....	202...	2024...	2024...	20...	20...	e?A	504,368	
AccessData_FTK_Imager_4.7.1.exe.locked	existing	locked	n.....	202...	2024...	2024...	20...	20...	e?A	25,022,256	
disable-defender (2).exe.locked	existing	locked	n.....	202...	2024...	2024...	20...	20...	e?A	9,128,928	
winrar-x32-622.exe.locked	existing	locked	n.....	202...	2024...	2024...	20...	20...	e?A	9,062,464	
x86_x86_64 아키텍처 차이.pdf.locked	existing	locked	n.....	202...	2024...	2024...	20...	20...	e?IA	9,105,416	
발표자료_합본.pdf.locked	existing	locked	n.....	202...	2024...	2024...	20...	20...	e?A	23,849,440	
최종발표.pdf.locked	existing	locked	n.....	202...	2024...	2024...	20...	20...	e?A	19,861,856	

- KEEPER CTF IR-1에서 해당 기능을 활용하여 감염 파일을 찾을 수 있다. - Attr.에서 e? 필터 적용

X-Ways Forensics

- Refine Volume Snapshot(RVS)
 - Picture analysis and processing¹
 - 피부톤을 탐지하여 보여주는 기능, PhotoDNA 활용



¹ <https://www.x-ways.net/winhex/manual.pdf> - 6.3.8 Pictures Analysis and Processing

X-Ways Forensics

- Refine Volume Snapshot(RVS)
 - Picture analysis and processing

File Path	Name	Type	Description	Size	Creation Date	Last Modified	Accessed	Owner	Permissions	File Details
f_00006e [c9232d31-8a41-4e2c-a4a8-aa474d]existing	jpg	newly identified	Pictures	52.7 KB	2024-01-03d16:57:35.160 +9	2024-01-03d16:57:43.057 +9	2024-01-03d17:34:43.039 +9	A	9,112,920 46% skin tones	
f_00006b [upload_17041941710246z8W.jpg]existing	jpg	newly identified	Pictures	28.2 KB	2024-01-03d16:57:35.299 +9	2024-01-03d16:57:43.044 +9	2024-01-03d17:34:43.039 +9	A	23,359,536 50% skin tones	
f_000107 [Jv2rS6lQj3UmZuQJ2Uu5uzNzB0.j]existing	jpg	newly identified	Pictures	16.9 KB	2024-01-03d17:12:45.587 +9	2024-01-03d17:12:46.067 +9	2024-01-03d17:34:43.572 +9	A	16,197,472 51% skin tones	
f_000079 [Vibe_SC_076±ºĐÁÀº°¬ÇÉ¼Ó@]existing	png	newly identified	Pictures	83.9 KB	2024-01-03d16:57:45.954 +9	2024-01-03d16:57:47.297 +9	2024-01-03d17:34:43.039 +9	A	23,101,256 52% skin tones	
f_00015b [th]existing, alre... jpg	jpg	newly identified	Pictures	18.1 KB	2024-01-03d17:20:06.298 +9	2024-01-03d17:20:06.324 +9	2024-01-03d17:34:43.929 +9	A	85,056 57% skin tones	
f_000067 [f37997d8-b723-445d-945d-d2293]existing, alre... jpg	jpg	newly identified	Pictures	54.9 KB	2024-01-03d16:57:35.159 +9	2024-01-03d16:57:42.954 +9	2024-01-03d17:34:43.039 +9	A	768,744 68% skin tones	
f_000101 [upload_1704182609838G3XXi.jpg]existing, alre... jpg	jpg	newly identified	Pictures	17.3 KB	2024-01-03d17:12:44.163 +9	2024-01-03d17:12:44.473 +9	2024-01-03d17:34:43.555 +9	A	4,049,720 85% skin tones	

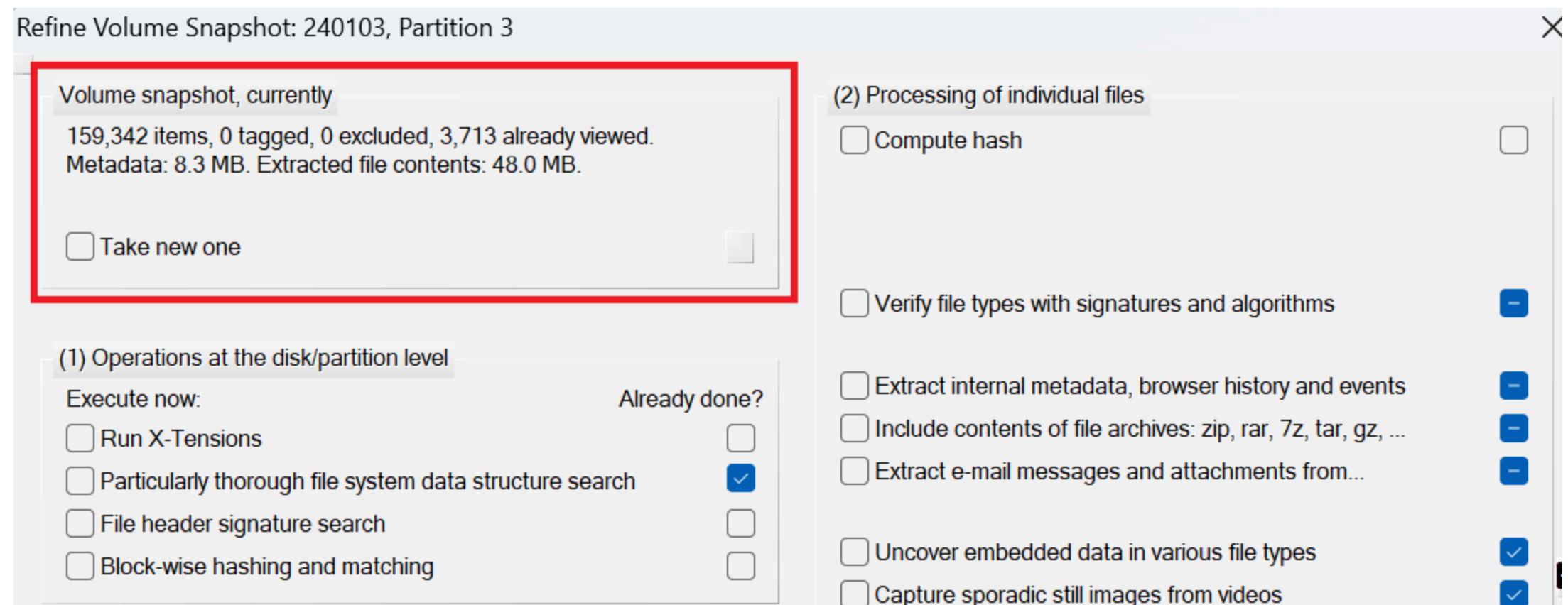


- ..?
- 이미지 분석에서 참고용으로 활용하면 좋을 것 같다.

X-Ways Forensics

- Refine Volume Snapshot(RVS)

- RVS 완료 후 다시 들어가면 현재 수집된 Volume Snapshot 확인 가능



X-Ways Forensics

The following search terms will be searched
(use the 'OR' operator to search multiple lines):



- Match case
- Character adjustment
- Regular expressions

Merge hits for identical search terms

11월

- Simultaneous Search 1234

- 여러 단어들을 검색할 수 있는 기능, 정규식 사용 가능
 - 디스크에 존재하는 파일들을 검색하여 유의미한 데이터 추출 가능
- 상단 아이콘 버튼으로 사용 가능
- 하단 아이콘 버튼으로 검색 결과 확인

The screenshot shows the X-Ways Forensics interface with the following details:

- Search Bar:** The search term "11월" is entered.
- Search Options:** "All objects in volume snapshot (19.2 GB)" is selected.
- Search Results Table:** A table showing search hits across various files and folders. The columns include Physical offset, Logical offset, Description, Name, Type, Hit count, and Term count.
- File Preview:** A preview pane at the bottom shows the content of a file starting with "11월_회계부" containing ANSI ASCII text.
- Toolbar:** Various forensic analysis tools are available in the toolbar, with the search icon highlighted.
- Status Bar:** Shows the file system as "Read-only mod" and the allocation status as "Alloc. of visible".

X-Ways Forensics

- 그러면 RVS 사용할 때 모든 옵션을 다 체크하고 분석하면 되는건가?

정말 모든 옵션을 선택할 필요가 있을까?

물론 XWF가 매우 효율적이고 빠른 프로그램이기는 하지만 불필요한 옵션을 사용하게 되면 처리 시간이 당연히 증가하게 되고 VS에 더 많은 데이터가 저장되게 된다.

사건이 사진과 전혀 관련이 없는데도 불구하고 피부색이나 흑백사진에 대한 옵션을 사용할 필요가 정말 있는 것일까?

처리 시간을 최소화하기 위해서 필요한 것만 선택하는 것이 좋다.
그리고 필요하다면 나중에 추가적인 RVS 옵션을 선택하면 된다.

[XWF를 이용한 포렌식 분석 - p122](#)

RVS 속도와 관련된 팁

만약에 현재 사용자가 생성한 워드 파일을 복원하는 것이 목적이라면
이 목적에 부합하는 파일 헤더 시그니처 검색 옵션을 선택하는 것이 좋다.

XWF에서는 사용자가 원하는 종류의 워드 파일을 찾을 수 있도록 지원하며
이렇게 진행하면 해당 사건에 관련이 있는 데이터만 복원하여
분석해야 할 데이터를 줄일 수 있게 된다.

[XWF를 이용한 포렌식 분석 - p122](#)

X-Ways Forensics

- 해시 데이터베이스 (Hash Database)^{1,2}
 - TODO
- 블록 해시(Block Hash)³
 - TODO
- 퍼지 해시(FuzZyDoc)⁴
 - RVS → Identify known documents using FuzZyDoc
 - TODO
- 해시 컨테이너 (Hash Container)⁵
 - TODO

¹ <http://www.forensic-artifacts.com/xways-forensics/sub04>

² <https://goblinforensics.tistory.com/342>

³ <https://ccibomb.tistory.com/1201>

⁴ <https://ccibomb.tistory.com/1202>

⁵ <https://mreerie.com/2022/01/26/selectively-hashing-files-in-x-ways-forensics/>

X-Ways Forensics

- 리버스 이미지¹, 라이브 포렌식²
 - TODO
- 컨테이너 파일, 스켈레톤 이미지, 클린즈드 이미지^{3 4 5}
 - TODO

¹ <https://goblinforensics.tistory.com/293>

² <https://goblinforensics.tistory.com/295>

³ https://www.x-ways.net/investigator/containers_vs_skeleton_images.html

⁴ <https://www.x-ways.net/investigator/scheme.png>

⁵ <https://goblinforensics.tistory.com/297>

X-Ways Forensics

- Report
 - X-Ways 실무 활용 가이드 - Report 생성
 - [X-Ways Forensics] 11 Export list
 - 보고서 작성 기능 - 1 2
- X-Tensions
 - 기술문서 발표 자료 참고

ETC

- forensenellanebbia - xways-forensics
- kacos2000 - WinHex_Templates
- Extracting Data from the Event Payload from .evtx Event Logs with X-Ways Forensics

참고자료

- Youtube - [X-Ways Software Technology AG, TED SMITH](#)
- Blog - [ccibomb, goblinforensics, mreerie](#)
- [X-Ways 실무 활용 가이드](#)
- X-Ways - [XWFQuickStart, QuickGuide, manual](#)
- [XWF를 이용한 포렌식 분석 - Second Edition](#)
- [윈도우 디지털 포렌식 완벽 활용서](#)

MUI Cache

- 윈도우 환경에서 다중 언어를 지원하기 위해 존재하는 캐시
- 예를 들어 윈도우 내장 프로그램인 `regedit` 은 레지스트리 편집기 , `taskmgr` 는 작업 관리자 로 저장되어 있다. → 예를 들어 존재하지 않는 파일이 여기에 남아있다면 악의적인 파일로 의심 가능
- 이러한 정보도 결국 프로그램이 실행됨에 따라 기록된 것이기 때문에 포렌식 분석에 활용 가능

HKCU\Software\Classes\Local Settings\MuiCache

HKCU\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache

컴퓨터\HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\bc\71F23C34			
	이름	종류	데이터
> Interface	@C:\Program Files (x86)\Common Files\Microsoft ...	REG_SZ	Visual Studio로 열기(&V)
> Inkfile	@C:\Program Files (x86)\VMware\VMware Worksta...	REG_SZ	This VMware product requires administrator privil...
\ Local Settings	@C:\Common Files\Microsoft Office\Root\WFS\Pr...	REG_SZ	연락처
\ ImmutableMuiCache	@C:\Program Files\Microsoft Office\Root\WFS\Pr...	REG_SZ	Microsoft Excel 워크시트
\ MrtCache	@C:\Program Files\Microsoft Office\Root\WFS\Pr...	REG_SZ	Microsoft Excel 스크립트로 구분된 값 파일
\ MuiCache	@C:\Program Files\Microsoft Office\Root\WFS\Pr...	REG_SZ	Microsoft Word 문서
\ bc	@C:\Program Files\Microsoft Office\Root\WFS\Pr...	REG_SZ	Microsoft PowerPoint 프레젠테이션
\ 71F23C34	@C:\Program Files\Microsoft Office\Root\WFS\Pr...	REG_SZ	Word
\ Software	@C:\Program Files\Microsoft Office\Root\WFS\Pr...	REG_SZ	Excel
\ Microsoft	@C:\Program Files\Microsoft Office\Root\WFS\Pr...	REG_SZ	레지스트리 편집기
\ Windows	@C:\WINDOWS\regedit.exe,-16	REG_SZ	Windows 배치 파일
\ CurrentVersion	@C:\WINDOWS\System32\Acquire.dll,-6002	REG_SZ	

참고자료

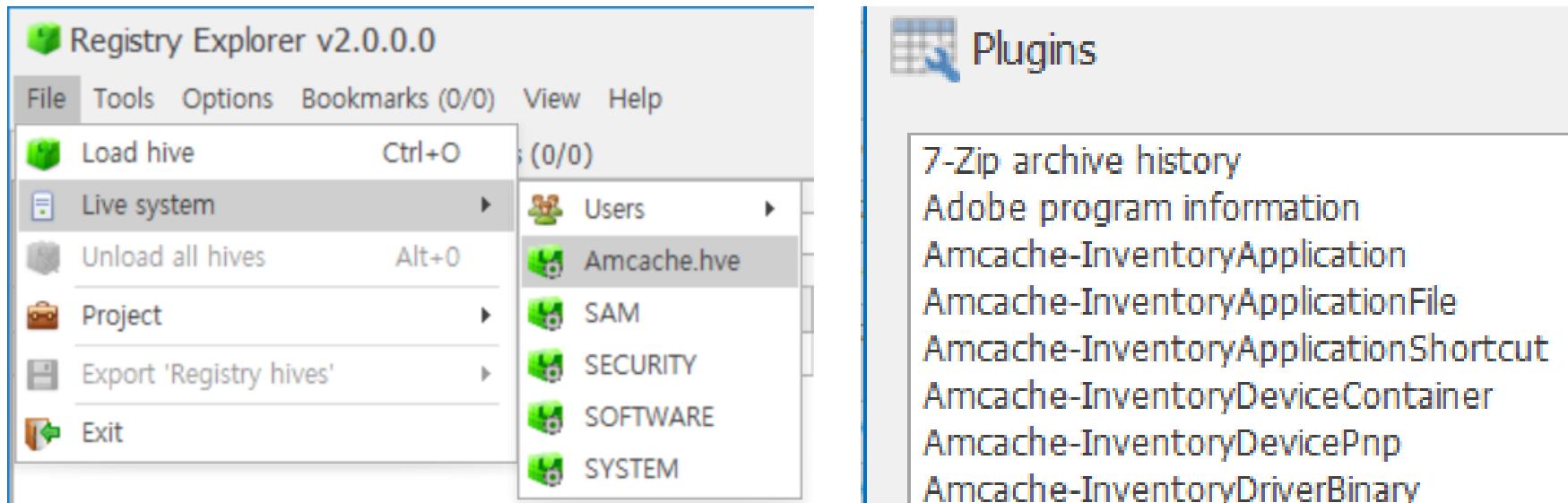
- MUICache - forensic-artifacts
- 기초부터 따라하는 디지털포렌식
- Forensic Analysis of MUICache Files in Windows

AmCache & ShimCache (AppCompatCache)

- 윈도우 운영체제의 버전이 업데이트됨에 따라 일부 기능들이 변경될 수 있는데 이때 해당 기능에 의존하는 프로그램들이 영향을 미칠 수 있다고 한다. → 호환성 관리자 프로그램이 이를 해결해준다.
- 윈도우 7에서는 `RecentFileCache.bcf`라는 파일로 존재했으나, 윈도우 8 이후로 `Amcache.hve`라는 레지스트리 하이브 파일로 대체되었다.
- ShimCache 도 호환성 관련 문제를 해결하기 위한 아티팩트
- AmCache 경로
 - `C:\Windows\appcompat\Programs\AmCache.hve`
- ShimCache (AppCompatCache) 경로
 - `HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache`
- [Eric Zimmerman](#)의 `AmCacheParser`, `AppCompatCacheParser` 또는 `RegistryExplorer`로 분석 가능
 - GUI 프로그램인 `Registry Explorer` 사용할 예정

AmCache

- 추출해서 확인하는 방법도 좋으나, 빠르게 확인하기 위해 현재 사용 중인 PC의 Amcache 파일 분석
- Registry Explorer 관리자 권한으로 실행 → File → Live system → AmCache.hve 클릭



- InventoryApplicationFile, InventoryDeviceContainer 등 프로그램 실행 정보, 외부 장치 연결 정보, 최초 또는 마지막 연결, 설치 시간 등 확인할 수 있다.

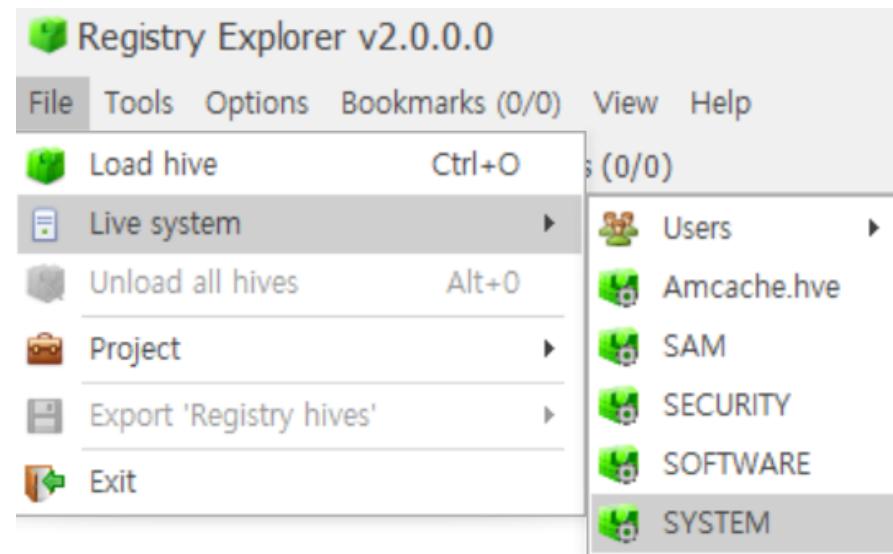
AmCache

- 왼쪽에 키 이름을 누르면 하위 키들을 파싱하여 오른쪽에 결과를 보여준다.
- 현재 `InventoryDriverPackage` 키에 대한 플러그인이 없다.
 - 시간이 된다면 플러그인을 개발하여 기여해보자..! - [RegistryPlugins](#)

The screenshot shows the Registry Explorer interface with the title "Registry Explorer v2.0.0.0". The left pane displays a tree view of registry keys under "Registry hives (1)". The selected key is "C:\Windows\appcompat\Programs\Amcache...", which contains several subkeys like "Associated deleted records", "Root", and "InventoryApplicationFile". The right pane shows a table titled "Values" for the "Amcache-InventoryApplicationFile" key. The table has columns: Timestamp, Path, Name, Product Name, Publisher, Version, and SHA1. It lists numerous entries, mostly from Microsoft, such as "adpcmencode3.exe", "AFFINE.exe", "ahost.exe", and "ai.exe", along with their respective timestamps and file paths.

Timestamp	Path	Name	Product Name	Publisher	Version	SHA1
2024-01-22 12:15:59	c:\Windows\program files (x86)\Windows kits\10\bin\W10.0.22621.0\W64\adpcmencode3.exe	adpcmencode3.exe	microsoft® windows® operating system	microsoft corporation	10.0.22621.2428 (winbuild.160101.0800)	f7c94a3a02d46985aa2e4abe0e429daef04
2024-01-22 12:15:59	c:\Windows\program files (x86)\Windows kits\10\bin\W10.0.22621.0\W64\adpcmencode3.exe	adpcmencode3.exe	microsoft® windows® operating system	microsoft corporation	10.0.22621.2428 (winbuild.160101.0800)	1e2ed3b3b955c64f9233e039958b8f3fe7c1929d
2024-01-22 12:15:59	c:\Users\hyunnnn\AppData\Local\Affine\ne\Affine.exe	AFFINE.exe	affine	toeverything	0.11.3	d5520b82f8f487fb1ef0cd8ceb4cf2b6d9366
2024-01-22 12:15:59	c:\Users\hyunnnn\AppData\Local\Affine\ne\Affine-0.11.0\Affine.exe	AFFINE.exe	affine	toeverything	0.11.3	07e86888232c723887caf0e3628689c45e3071f6
2024-01-25 12:33:40	c:\Windows\system32\AggregatorHost.exe	AggregatorHost.exe	microsoft® windows® operating system	microsoft corporation	10.0.22621.2506 (winbuild.160101.0800)	810101becfeaf16a23e56638564454b7ae7fb7
2024-01-22 12:15:59	c:\Windows\program files\mingw64\bin\ahost.exe	ahost.exe				595ce7d96d1dc0a24f969d09c4c8215ba25d3481
2024-01-22 12:15:59	c:\Windows\program files\microsoft\office\root\Windows\programfilescommon\x64\microsoft shared\Office16\ahost.exe	ai.exe	artificial intelligence	microsoft corporation	0.14.12.0	ec80d3d4904e4dd22d5a7920ef26d30783441b5
2024-01-22 12:15:59	c:\Windows\program files\microsoft\office\root\Windows\programfilescommon\x64\microsoft shared\Office16\ahost.exe	ai.exe	artificial intelligence	microsoft corporation	0.14.12.0	5f66ee17a5900e6511d58ff1211a02df397ae99b
2024-01-22 12:15:59	c:\Windows\program files\microsoft\office\root\Windows\programfilescommon\x64\microsoft shared\Office16\aimgr.exe	aimgr.exe	artificial intelligence	microsoft corporation	0.14.12.0	25f27be54803a2e2acc721217f51efe58078ff8a
2024-01-22 12:15:59	c:\Windows\program files\microsoft\office\root\Windows\programfilescommon\x64\microsoft shared\Office16\aimgr.exe	aimgr.exe	artificial intelligence	microsoft corporation	0.14.12.0	d3a7735b54f40b5414e3ab54437ace150e1c00
2024-01-22 12:15:59	c:\Users\hyunnnn\AppData\roaming\Zoom\bin\airhost.exe	airhost.exe	zoom video communications, inc.	zoom video communications, inc.	5.17.2.29988	92e7865336354ea56a5b059dc80ef71eeb088737
2024-01-22 12:15:59	c:\Windows\program files (x86)\Windows kits\10\app certification kit\alstatic.exe	alstatic.exe	microsoft® windows® operating system	microsoft corporation	10.0.22621.2428 (winbuild.160101.0800)	10ee1257ba999eb13f287bfab667d9b54c44fb2
2024-01-22 12:15:59	c:\Windows\program files (x86)\Microsoft sdks\Windows\10.0.0\bin\WinFx 4.8 tools\Wal.exe	al.exe	microsoft® .net framework	microsoft corporation	14.8.3928.0 built by: net48rel1	f10c3293ac5c2c171cd70908f36aa25e58304acd
2024-01-22 12:15:59	c:\Windows\program files (x86)\Microsoft sdks\Windows\10.0.0\bin\WinFx 4.8 tools\Wal.exe	al.exe	microsoft® .net framework	microsoft corporation	14.8.3928.0 built by: net48rel1	95ce0fea6f6287fd08929fa9f94f974d2532b
2024-01-22 12:15:59	c:\Windows\program files\alacrity\alacrity.exe	alacrity.exe				6c5448d7513021353f673789a9f922513c9c4780
2024-01-28 19:20:52	c:\Windows\program files\autopsy\4.21.0\autopsy\aleapp\aleapp.exe	aleapp.exe				a55be6420a79b2bc03542faa5bdeb25579d3d27

ShimCache (AppCompatCache)



- File → Live system → SYSTEM 클릭 (HKLM\SYSTEM 하위 경로에 존재하기 때문)
- Available Bookmarks에 가면 AppCompatCache 가 있다.

AppCompatCache PCA (Windows 11 only)

- 윈도우 11에 새롭게 등장한 아티팩트
- PCA 는 Program Compatibility Assistant 의 약자이며, 해당 파일 또한 호환성 관련 파일임을 알 수 있다.
- 수집 경로: C:\Windows\appcompat\pca
- 실행 시간, 경로, 파일 버전 등이 프로그램 실행 시에 저장된다.
- pcasvc 서비스에 의해 파일이 생성된다. (PcaAppLaunchDic.txt , PcaGeneralDb0-1.txt)

```
C:\Users\hyuunnnn>sc query pcasvc

SERVICE_NAME: pcasvc
    종류               : 30  WIN32
    상태               : 4   RUNNING
                          (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    검사점             : 0x0
    WAIT_HINT          : 0x0
```

AppCompatCache PCA (Windows 11 only)

- PcaAppLaunchDic.txt 출력 결과 - 프로그램의 마지막 실행 시간 제공¹

```
C:\lazarus\lazarus.exe|2024-01-30 11:52:45.205
C:\Users\hyuunnnn\AppData\Local\Programs\Python\Python311\python.exe|2024-01-30 12:26:14.049
C:\Users\hyuunnnn\Downloads\parsec-windows.exe|2024-01-31 05:50:56.197
C:\Program Files\Parsec\parsecd.exe|2024-01-31 06:05:46.726
C:\Users\hyuunnnn\Downloads\hindsight_gui.exe|2024-01-31 06:12:34.705
C:\Users\hyuunnnn\Downloads\PrefetchBrowser.exe|2024-02-01 17:29:33.679
C:\Users\hyuunnnn\Desktop\winprefetchview-x64\WinPrefetchView.exe|2024-02-01 17:38:35.629
C:\Users\hyuunnnn\Desktop\AppCompatCacheParser\AppCompatCacheParser.exe|2024-02-01 18:21:36.017
C:\Users\hyuunnnn\Desktop\AmcacheParser\AmcacheParser.exe|2024-02-01 18:21:40.725
C:\Users\hyuunnnn\Desktop\RegistryExplorer\RegistryExplorer.exe|2024-02-01 19:20:11.892
C:\Program Files (x86)\YES24eBook\YES24eBook.exe|2024-02-01 19:35:33.374
C:\Users\hyuunnnn\Desktop\thumbcache_viewer.exe|2024-02-01 20:17:50.723
C:\Users\hyuunnnn\Downloads\Clippy.exe|2024-02-01 20:56:18.563
C:\Users\hyuunnnn\Downloads\WindowsTimeline.exe|2024-02-01 21:01:52.629
```

- PcaGeneralDb0.txt , PcaGeneralDb1.txt 파일은 아래 블로그 참고

¹ <https://aboutdfir.com/new-windows-11-pro-22h2-evidence-of-execution-artifact/>

참고자료

- 앤캐시(Amcache.hve) 파일을 활용한 응용 프로그램 삭제시간 추정방법
- AmCache - forensic-artifacts, swiftforensics
- ANALYSIS OF THE AMCACHE V2 - slides
- Leveraging the Windows Amcache.hve File in forensic Investigations
- Revealing the RecentFileCache.bcf File
- Caching Out: The Value of Shimcache for Investigators
- ShimCache - forensic-artifacts
- [논문리뷰] Windows 10에서의 심캐시 구조 분석과 안티포렌식 도구 실행 흔적 탐지 도구 제안 - 영상
- New Windows 11 Pro (22H2) Evidence of Execution Artifact! - Video
- 기초부터 따라하는 디지털포렌식

Prefetch (프리패치)

- Windows XP 이후로 도입된 기술이며, 윈도우 부팅 속도 및 프로그램 실행 시간을 단축할 수 있다.
- 프로그램이 사용하는 시스템 자원을 프리패치 파일(*.pf)에 저장하고, 윈도우 부팅 시 해당 파일들을 모두 메모리에 로드한다.¹ → 디스크를 검색하거나 읽는 과정을 줄임으로써 단축할 수 있다.
- 프리패치 파일이 없는 프로그램이 실행되었을 때 10초 동안 모니터링하며, 그동안 메모리에 로드한 코드의 일부 또는 전체를 파일로 생성한다. → 재실행 시 초기 실행 속도 향상
- 수집 경로: C:\Windows\prefetch
- [WinPrefetchView](#)를 사용할 예정
 - Eric Zimmerman의 도구를 사용하고 싶다면 [PECmd](#) 사용해도 좋다.
→ Costas라는 사람이 만든 [Prefetch-Browser](#)도 있다.

¹ [https://github.com/proneer/Slides/blob/master/Windows/\(FP\) 프리%2C슈퍼 패치 포렌식 \(Prefetch %26 Superfetch Forensics\).pdf](https://github.com/proneer/Slides/blob/master/Windows/(FP)%20프리%2C슈퍼%20패치%20포렌식(Prefetch%26Superfetch%20Forensics).pdf)

Prefetch (프리패치)

- WinPrefetchView.exe /folder <추출한 폴더 경로> - 별도의 옵션 없이 exe 파일을 실행하면 현재 사용 중인 PC의 프리패치 파일 분석

The screenshot shows the WinPrefetchView application interface. At the top, there is a command-line input field containing the command: C:\Users\hyuunnnn\Desktop\winprefetchview-x64>WinPrefetchView.exe /folder "C:\Users\hyuunnnn\Desktop\test\analysis_01\240103, P3". Below the input field is the application's title bar and menu bar (File, Edit, View, Options, Help). Underneath the menu is a toolbar with various icons. The main area contains two tables of data.

Filename	Created Time	Modified Time	File S...	Process EXE	Process Path	Run Counter	Last Run Tir
0IAJDNGXORFO.EXE-D7D393C8.pf	2024-01-03 오후 5:18:11	2024-01-03 오후 5:18:11	19,868	0IAJDNGXORFO.EXE	\VOLUME{01da3e1675b2d18c-0e75ba0e...}	1	2024-01-03
ACCESSDATA_FTK_IMAGER_4.7.1.E...	2024-01-03 오후 5:20:12	2024-01-03 오후 5:20:12	33,739	ACCESSDATA_FTK_IMAGER_4.7.1.EXE	\VOLUME{01da3e1675b2d18c-0e75ba0e...}	1	2024-01-03
ACCESSDATA_FTK_IMAGER_4.7.1.E...	2024-01-03 오후 5:20:13	2024-01-03 오후 5:20:13	39,434	ACCESSDATA_FTK_IMAGER_4.7.1.EXE	\VOLUME{01da3e1675b2d18c-0e75ba0e...}	1	2024-01-03
APPLICATIONFRAMEHOST.EXE-8CE...	2024-01-03 오후 4:54:25	2024-01-03 오후 5:17:58	15,441	APPLICATIONFRAMEHOST.EXE	\VOLUME{01da3e1675b2d18c-0e75ba0e...}	2	2024-01-03
AUDIODG.EXE-AB22E9A6.pf	2024-01-03 오후 4:36:25	2024-01-03 오후 5:34:55	6,683	AUDIODG.EXE	\VOLUME{01da3e1675b2d18c-0e75ba0e...}	6	2024-01-03

Filename	Full Path	Device Path	Index
\$MFT		\VOLUME{01da3e1675b2d18c-0e75ba0e}\\$MFT	9
0IAJDNGXORFO.EXE		\VOLUME{01da3e1675b2d18c-0e75ba0e}\USERS\USER\APPDATA\LOCAL\TEMP\0IAJDNGXORFO.EXE	8
2023년 10월 회계부.PNG		\VOLUME{01da3e1675b2d18c-0e75ba0e}\USERS\USER\DOWNLOADS\2023년 10월 회계부.PNG	103
2023년 5월 회계부.PNG		\VOLUME{01da3e1675b2d18c-0e75ba0e}\USERS\USER\DOWNLOADS\2023년 5월 회계부.PNG	104
2023년 8월 회계부.PNG		\VOLUME{01da3e1675b2d18c-0e75ba0e}\USERS\USER\DOWNLOADS\2023년 8월 회계부.PNG	105
2023년 9월 회계부.PNG		\VOLUME{01da3e1675b2d18c-0e75ba0e}\USERS\USER\DOWNLOADS\2023년 9월 회계부.PNG	106
ACCESSIBILITY.DLL		\VOLUME{01da3e1675b2d18c-0e75ba0e}\WINDOWS\MICROSOFT.NET\ASSEMBLY\GAC_MSIL\ACCE...	63
ADVAPI32.DLL		\VOLUME{01da3e1675b2d18c-0e75ba0e}\WINDOWS\SYSWOW64\ADVAPI32.DLL	15
APPHELP.DLL		\VOLUME{01da3e1675b2d18c-0e75ba0e}\WINDOWS\SYSWOW64\APPHELP.DLL	13

Prefetch (프리패치)

- 프리패치 분석을 통해 해당 프로그램이 어떤 프로그램을 건드렸는지 확인할 수 있다.
 - 이전 슬라이드의 사진을 보면 랜섬웨어로 확인된 파일에 의해 png 파일이 감염된 것으로 볼 수 있다.
 - WinRAR 압축 프로그램으로 11월_회계부.rar 파일을 열었다는 증거를 확인할 수 있다.
 - 실행 횟수는 틀린 경우도 있기 때문에 UserAssist, evtx 등 다른 아티팩트에서 교차 검증이 필요하다.¹

The screenshot shows the WinPrefetchView application interface. The main window displays a table of prefetch files with columns for Filename, Created Time, Modified Time, File S..., Process EXE, Process Path, and Run. Below this is another table showing device paths for various files, including the ransomware sample.

Filename	Created Time	Modified Time	File S...	Process EXE	Process Path	Run
WERFAULT.EXE-155C56CF.pf	2024-01-03 오후 4:53:17	2024-01-03 오후 5:35:06	6,248	WERFAULT.EXE	##VOLUME{01da3e1675b2d18c-0e75ba0e...}	2
WERMGR.EXE-F439C551.pf	2024-01-03 오후 4:41:06	2024-01-03 오후 4:41:42	12,791	WERMGR.EXE	##VOLUME{01da3e1675b2d18c-0e75ba0e...}	2
WINLOGON.EXE-DEDDC9B6.pf	2024-01-03 오후 4:49:39	2024-01-03 오후 4:49:39	6,753	WINLOGON.EXE	##VOLUME{01da3e1675b2d18c-0e75ba0e...}	1
WINRAR-X32-622.EXE-BCC4C7E0.pf	2024-01-03 오후 5:04:14	2024-01-03 오후 5:04:14	29,123	WINRAR-X32-622.EXE	##VOLUME{01da3e1675b2d18c-0e75ba0e...}	1
WINRAR.EXE-A58334F4.pf	2024-01-03 오후 5:04:51	2024-01-03 오후 5:04:51	18,483	WINRAR.EXE	##VOLUME{01da3e1675b2d18c-0e75ba0e...}	1

Filename	Full Path	Device Path	Index
\$MFT		##VOLUME{01da3e1675b2d18c-0e75ba0e}##\$MFT	32
11월_회계부.RAR		##VOLUME{01da3e1675b2d18c-0e75ba0e}##USERS##USER##DOWNLOADS##11월_회계부.RAR	155
ADVAPI32.DLL		##VOLUME{01da3e1675b2d18c-0e75ba0e}##WINDOWS##SYSWOW64##ADVAPI32.DLL	39
KEEPER	KEEPER 포렌식 완벽 활용서 - p173	##VOLUME{01da3e1675b2d18c-0e75ba0e}##WINDOWS##SYSWOW64##APPEHELP.DLL	11

참고자료

- [Prefetching - wikipedia](#)
- [Prefetcher- wikipedia](#)
- [\(FP\) 프리,슈퍼 패치 포렌식 \(Prefetch & Superfetch Forensics\).pdf](#)
- [프리패치 고급 분석 \(Advanced Prefetch Analysis\)](#)
- [기초부터 따라하는 디지털포렌식](#)

ThumbnailCache & IconCache

- **ThumbnailCache** : 윈도우 폴더 미리보기에 사용되는 캐시 파일
 - 최초로 생성된 미리보기 이미지 파일을 캐싱한 후 재방문 시 캐시된 이미지를 보여준다.
→ 폴더를 열 때마다 미리보기 이미지 파일을 새롭게 생성하는 것은 비효율적이다.
 - 수집 경로: %UserProfile%\AppData\Local\Microsoft\Windows\Explorer
 - thumbcache_xxx.db (xxx: 사이즈별 크기) 형태로 저장되어 있다.

 thumbcache_16.db	2024-01-29 오전 7:48	Data Base File	1,024KB
 thumbcache_32.db	2024-01-29 오전 7:48	Data Base File	1,024KB
 thumbcache_48.db	2024-01-29 오전 7:48	Data Base File	1,024KB
 thumbcache_96.db	2024-02-02 오전 3:21	Data Base File	3,072KB
 thumbcache_256.db	2024-01-31 오전 12:14	Data Base File	3,072KB
 thumbcache_768.db	2024-01-29 오전 7:48	Data Base File	1,024KB
 thumbcache_1280.db	2024-01-29 오전 7:48	Data Base File	1,024KB

ThumbnailCache & IconCache

- IconCache : 탐색기에서 보여주는 아이콘들을 캐싱한 후 재방문 시 캐시된 아이콘을 보여준다.
- 아이콘은 EXE 파일 구조 내부의 리소스 영역에 저장되어 있다. → 탐색기에서 볼 때마다 내부에 존재하는 아이콘을 꺼내서 보여주는 것은 비효율적이다.
- 수집 경로: %UserProfile%\AppData\Local\Microsoft\Windows\Explorer
 - iconcache_xxx.db (xxx: 사이즈별 크기) 형태로 저장되어 있다.

 iconcache_16.db	2024-02-02 오전 4:09	Data Base File	1,024KB
 iconcache_32.db	2024-02-02 오전 4:06	Data Base File	1,024KB
 iconcache_48.db	2024-02-02 오전 4:06	Data Base File	1KB
 iconcache_96.db	2024-02-02 오전 4:06	Data Base File	1KB
 iconcache_256.db	2024-02-02 오전 4:06	Data Base File	1KB
 iconcache_768.db	2024-02-02 오전 4:06	Data Base File	1KB
 iconcache_1280.db	2024-02-02 오전 4:06	Data Base File	1KB

ThumbnailCache & IconCache

- Thumbcache Viewer 도구를 사용하여 분석 가능

The screenshot shows the Thumbcache Viewer application window. The main table lists cache entries with columns: #, Filename, Cache Entry Offset, Cache Entry Size, Data Offset, Data Size, Data Checksum, Header Checksum, Cache Entry Hash, System, and Location. Entry 637 is selected, showing details: 21cb489a69da2d3d.png - 256x138. A tooltip provides technical information about thumbnail extraction from file headers.

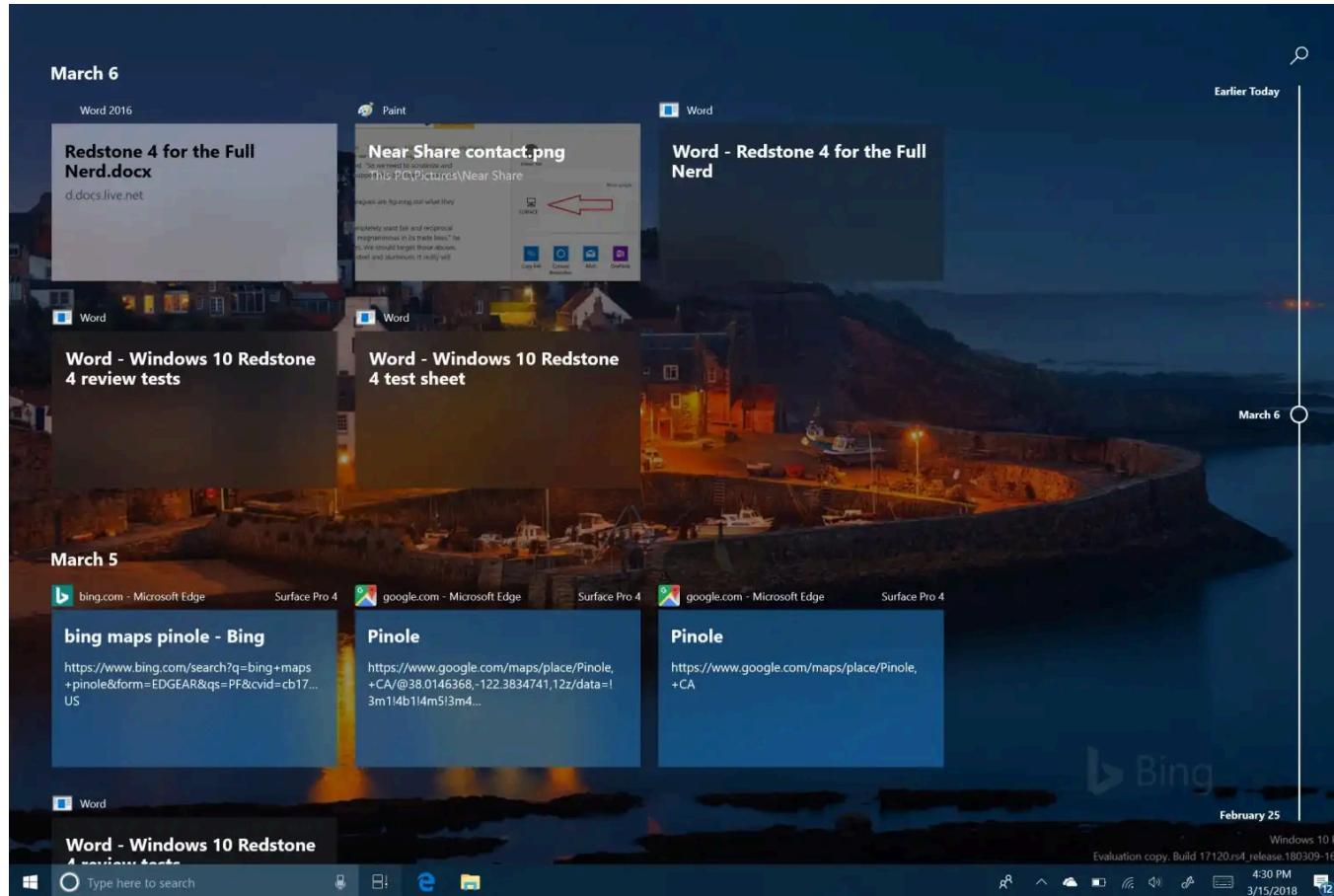
#	Filename	Cache Entry Offset	Cache Entry Size	Data Offset	Data Size	Data Checksum	Header Checksum	Cache Entry Hash	System	Location
625	1958b0ff69c05668	1671272 B	0 KB	1671360 B	0 KB					C:\Users\hyuunnnn\Ap
626	efa8cef8a8ee752	1671360 B	0 KB	1671448 B	0 KB					C:\Users\hyuunnnn\Ap
627	e768e22ed2598066	1671448 B	0 KB	1671536 B	0 KB					C:\Users\hyuunnnn\Ap
628	a771cc766136dd69	1671536 B	0 KB	1671624 B	0 KB					C:\Users\hyuunnnn\Ap
629	3392e93cffabcc64	1671624 B	0 KB	1671712 B	0 KB					C:\Users\hyuunnnn\Ap
630	26c48e99a84dc465	1671712 B	0 KB	1671800 B	0 KB					C:\Users\hyuunnnn\Ap
631	2c0be1dced754061	1671800 B	0 KB	1671888 B	0 KB					C:\Users\hyuunnnn\Ap
632	bc0fc576ab0ef84d	1671888 B	0 KB	1671976 B	0 KB					C:\Users\hyuunnnn\Ap
633	2ff2b30bcc7a36ef	1671976 B	0 KB	1672064 B	0 KB					C:\Users\hyuunnnn\Ap
634	3ecd1d6ab1aab47.png	1672064 B	22 KB	1672152 B	22 KB					C:\Users\hyuunnnn\Ap
635	691e9732033f12d7.png	1695258 B	21 KB	1695346 B	21 KB					C:\Users\hyuunnnn\Ap
636	3fab139e6eff416f.png	1717328 B	14 KB	1717416 B	14 KB					C:\Users\hyuunnnn\Ap
637	21cb489a69da2d3d.png	1731986 B	45 KB	1732074 B	45 KB					C:\Users\hyuunnnn\Ap
638	8756692c421d4b25.png	1778872 B	7 KB	1778960 B	7 KB					C:\Users\hyuunnnn\Ap
639	7f7d008b6c11e6f2.png	1786996 B	24 KB	1787084 B	24 KB					C:\Users\hyuunnnn\Ap
640	b5822127a7e4ea8.png	1812096 B	14 KB	1812182 B	14 KB					C:\Users\hyuunnnn\Ap
641	1d9c30c84612c353.png	1826602 B	18 KB	1826690 B	18 KB					C:\Users\hyuunnnn\Ap
642	74ae8704a1518abd.png	1845608 B	31 KB	1845696 B	31 KB					C:\Users\hyuunnnn\Ap
643	deef37cedb9b7f6f.png	1877678 B	11 KB	1877766 B	11 KB					C:\Users\hyuunnnn\Ap

참고자료

- (FP) 썸네일, 아이콘 캐시 포렌식 (Thumbnail, Icon Cache Forensics).pdf
- Windows thumbnail cache - wikipedia
- 기초부터 따라하는 디지털포렌식

Windows Timeline

- 윈도우 10에 추가된 타임라인 기능이며, 유저가 실행하고 있거나 실행했던 프로그램들을 확인 가능



¹ <https://www.pcworld.com/article/401705/windows-10-how-to-use-timeline.html>

Windows Timeline

- 윈도우 11에 제거된 기능¹이지만 같은 경로에 db 파일이 존재하며, 데이터도 남아 있음
- %UserProfile%\AppData\Local\ConnectedDevicesPlatform\폴더\ActivitiesCache.db



¹ <https://www.zdnet.com/article/windows-11-microsoft-deletes-these-windows-10-features-and-apps/>

Windows Timeline

- WindowsTimeline 또는 WxCmd 사용하여 분석 가능 - 아래 사진은 WindowsTimeline 사용

WindowsTimeline parser - C:\Users\hyuunnnn\Desktop\test\analysis_01\240103, P3\ActivitiesCache.db

The screenshot shows the WindowsTimeline parser interface. The title bar reads "WindowsTimeline parser - C:\Users\hyuunnnn\Desktop\test\analysis_01\240103, P3\ActivitiesCache.db". The menu bar includes "File", "Run" (which is selected), and "Tools". Below the menu is a toolbar with icons for opening files, running queries, and exiting. The main window displays a table of system activities. The columns are labeled: ETag, Application, Display Name, File Opened, Description, and Content. The table contains numerous rows of activity logs, such as file openings, process executions, and system events. Some entries include file paths like "C:\Users\hyuunnnn\Desktop\test\analysis_01\240103\11월_회계부.rar" and "C:\Users\hyuunnnn\Desktop\test\analysis_01\240103\11월_회계부.pdf".

ETag	Application	Display Name	File Opened	Description	Content
266	*PID00001bc4 (7108)				
263	*PID00001bc4 (7108)				
262	{System}\msiexec.exe	msiexec.exe	msiexec.exe		
259	*PID00001bc4 (7108)				
256	*PID00001bc4 (7108)				
255	*PID00001bc4 (7108)		*PID00001bc4	*PID00001bc4	
254	Microsoft.Windows.WindowsInstaller		Microsoft.Wind...	Microsoft.Windows.WindowsInstaller	
251	C:\Users\hyuunnnn\Desktop\test\analysis_01\240103\11월_회계부.rar				
250	C:\Users\hyuunnnn\Desktop\test\analysis_01\240103\11월_회계부.pdf	AccessData_F...	AccessData_FTK_Imager_4.7.1.exe		
244	MSEdge				
235	Microsoft.Windows.Explorer				
232	Microsoft.Windows.SecHealthUI_cw5n1h2txyewy!SecHealthUI				
229	Microsoft.Windows.Explorer				
223	MSEdge				
210	MSEdge	Microsoft Edge	x86 x86_64 아카데미 차이.pdf	C:\Users\hyuunnnn\Desktop\test\analysis_01\240103\11월_회계부.pdf	file:///C:/Users/User/Downloads/x86 x86_64 아카데미 차이.pdf
204	MSEdge				
168	{ProgramFilesX86}\WinRAR\WinRAR.exe				
159	{SystemX86}\cmd.exe				
158	{SystemX86}\cmd.exe	cmd.exe	cmd.exe		
152	{ProgramFilesX86}\WinRAR\WinRAR.exe				
151	{ProgramFilesX86}\WinRAR\WinRAR.exe	WinRAR	WinRAR		
141	{ProgramFilesX86}\WinRAR\WinRAR.exe	WinRAR	11월_회계부.rar	C:\Users\hyuunnnn\Desktop\test\analysis_01\240103\11월_회계부.pdf	file:///C:/Users/User/Downloads/11월_회계부.rar
132	*PID000017fc (6140)				

참고자료

- [기초부터 따라하는 디지털포렌식](#)
- [Timeline - forensic-artifacts](#)
- [Digital Forensics: Windows 10 Timeline — activitiescache.db](#)
- [WindowsTimeline.pdf - kacos2000](#)
- [Windows 10 Activity Timeline: An Investigator's Gold Mine](#)
- [Exploring the Windows Activity Timeline, Part 1: The High Points](#)
- [Exploring the Windows Activity Timeline, Part 2: Syncing Across Devices](#)
- [Exploring the Windows Activity Timeline, Part 3: The Value of Clipboard Content](#)

Windows Search

- 윈도우에서 파일, 이메일 등의 검색을 빠르게 할 수 있도록 인덱싱 기능을 제공한다.¹
- 인덱싱된 데이터들은 포렌식 분석에 의미있는 정보를 제공한다.



¹ https://www.aon.com/cyber-solutions/aon_cyber_labs/windows-search-index-the-forensic-artifact-youve-been-searching-for/

Windows Search

- %ProgramData%\Microsoft\Search\Data\Applications\Windows
- 윈도우 10은 ESEDB 구조인 Windows.edb 파일이 존재했으나, 윈도우 11은 SQLITE 구조인 Windows.db 파일이 존재한다.
 - 윈도우 10이라면 [WinSearchDBAnalyzer](#) 또는 [WinEDB](#), 윈도우 11은 [SIDR](#) 사용

GatherLogs	2024-01-22 오후 6:01	파일 폴더
Projects	2024-01-22 오후 6:01	파일 폴더
Windows.db	2024-02-02 오전 5:56	Data Base File 168,188KB
Windows.db-shm	2024-02-02 오전 1:25	DB-SHM 파일 320KB
Windows.db-wal	2024-02-02 오전 6:25	DB-WAL 파일 351KB
Windows-gather.db	2024-02-02 오전 6:13	Data Base File 3,816KB
Windows-gather.db-shm	2024-01-29 오전 7:45	DB-SHM 파일 32KB
Windows-gather.db-wal	2024-02-02 오전 6:25	DB-WAL 파일 4,056KB
Windows-usn.db	2024-02-02 오전 3:55	Data Base File 152KB
Windows-usn.db-shm	2024-01-29 오전 7:45	DB-SHM 파일 32KB
Windows-usn.db-wal	2024-02-02 오전 5:58	DB-WAL 파일 4,036KB

Windows Search

SIDR (Search Index DB Reporter) is a Rust-based tool designed to parse Windows search artifacts from Windows 10 (and prior) and Windows 11 systems. The tool handles both ESE databases (Windows.edb) and SQLite databases (Windows.db) as input and generates three detailed reports as output.

- SIDR는 Windows.edb, Windows.db 모두 분석해준다고 한다.
 - sidr.exe <폴더 경로> -f csv

```
C:\Users\hyuunnnn\Downloads>sidr.exe C:\ProgramData\Microsoft\Search\Data\Applications\Windows -f csv
Processing sqlite: C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db
sqlite_get_hostname() failed: Empty field System_ComputerName. Will use 'Unknown' as a hostname.
C:\Users\hyuunnnn\Downloads\Unknown_File_Report_20240201_230758.386590.csv
C:\Users\hyuunnnn\Downloads\Unknown_Internet_History_Report_20240201_230758.386868100.csv
C:\Users\hyuunnnn\Downloads\Unknown_Activity_History_Report_20240201_230758.387023600.csv
```

Windows Search

System_ItemPathDisplay	System_DateCreated	System_DateAccessed	System_Search_AutoSummary	System_Search_GatherTime
file:C:/Users/hyuunnnn/Desktop/240125.txt	2024-01-25T12:22:02.000000Z	2024-01-25T12:24:51.6800367Z	https://www.youtube.com/results?search_query=x-ways https://www.youtube.com/watch?v=mwalgzEfvw&list=PLfZw_tZWahjxJl81b1S-vYQwHs_9ZT77f&index=3 https://www.youtube.com/watch?v=Miydkti_QVE&t=17s https://www.youtube.com/@XWaysSoftwareTechnologyAG/videos https://www.youtube.com/@tedsmith28/videos https://www.youtube.com/watch?v=rEoBox5Izko http://www.forensic-artifacts.com/xways-forensics/sub02	2024-01-25T12:24:52.3689950Z
file:C:/Users/hyuunnnn/Desktop/240103.E01	2024-01-24T06:07:58.000000Z	2024-01-24T06:14:38.8106936Z		2024-01-25T13:18:53.3678643Z
file:C:/Users/hyuunnnn/AppData/Local/Package	2024-01-25T13:23:02.2216580Z	2024-01-25T13:23:02.2216580Z		2024-01-25T13:23:04.3204090Z
file:C:/Users/hyuunnnn/AppData/Local/Package	2024-01-25T13:23:02.2216580Z	2024-01-25T13:23:02.2216580Z		2024-01-25T13:23:04.3361260Z
file:C:/Users/hyuunnnn/.vscode/extensions/.74:2024-01-22T12:34:24.2020642Z	2024-01-22T12:34:24.2020642Z	2024-01-22T12:34:24.2020642Z		2024-01-22T12:34:25.0282762Z
file:C:/Users/hyuunnnn/AppData/Local/Package	2024-01-25T13:23:02.2216580Z	2024-01-25T13:23:02.2216580Z		2024-01-25T13:23:04.3361260Z
file:C:/Users/hyuunnnn/.vscode/extensions/.74:2024-01-22T12:34:24.2020642Z	2024-01-22T12:34:24.2020642Z	2024-01-22T12:34:24.2020642Z		2024-01-22T12:34:25.0232760Z

- 파일과 폴더 경로, 생성, 접근, 인덱싱된 시간 정보, Summary 정보 등 확인 가능

System_UserName	System_Lt	System_Li	System_ItemDate	SS	System_Search_GatherTime
https://www.microsoft.com/ko-kr/edge/welcome?form=MA13FJ	winrt://{S-1-5-21-44 2024-01-28T16:58:01.7464130Z}				2024-01-28T16:58:01.7508640Z
https://www.office.com/	winrt://{S-1-5-21-44 2024-01-28T16:58:01.7486360Z}				2024-01-28T16:58:01.7643372Z
https://www.bing.com/search?q=hxd&form=WSBEDG&qs=CT&	winrt://{S-1-5-21-44 2024-01-28T16:58:01.7464510Z}				2024-01-28T16:58:01.8119503Z
https://www.bing.com/search?q=aint&form=WSBEDG&qs=SW&	winrt://{S-1-5-21-44 2024-01-28T16:58:01.7464620Z}				2024-01-28T16:58:01.8255005Z

- PC에 hxd 가 설치되어 있지 않은 상태에서 엔터를 눌러 브라우저로 검색된 기록 존재

참고자료

- [기초부터 따라하는 디지털포렌식](#)
- [Windows Search Index: The Forensic Artifact You've Been Searching For - Video](#)
- [Windows Search 분석 프로그램 \(Windows.edb\)](#)

마치며..

- 지금까지 설명한 윈도우 아티팩트들 외에도 설명하지 못한 내용들이 있다. ([Mac](#), [Linux](#), [Mobile](#) 등)
 - [Plainbit - Blog](#), [proneer - Slides](#), [forensic-proof](#), [forensic-artifacts](#), [forensic-cheatsheet](#), [Forensics Wiki](#), [ArtifactParsers](#), [awesome](#) 시리즈 - [1](#) [2](#) [3](#) [4](#), [DFIRQuestions](#), [thisweekin4n6](#), [The Hitchhikers Guide to DFIR](#), [Windows Forensics Cheatsheet](#), [DFIR Training cheats](#), [DFIRMindMaps](#), [DFIR Cheat Sheet](#), [dfirdiva](#), [Infosec Reference](#), [DFIR Cheatsheet](#)
 - [13Cubed](#), [DFIRScience](#), [SANSForensics](#), [Ali Hadi](#), [dfrc_KU](#), [DFRWS](#), [OSDFCon](#), [PWF](#), [digital-forensics-lab](#), [Digital-Forensics-Guide](#), [디지털포렌식학회 논문](#), [윈도우 레지스트리 포렌식](#), [윈도우 디지털 포렌식 완벽 활용서](#), [윈도우 환경에서 침해 시스템 분석하기](#) 등 공부 자료는 많이 있다.
 - 새로운 정보를 주기적으로 찾고자 하는 마인드 필요 - 컴퓨터 모든 분야 해당
- 아직 발견되지 않은 새로운 아티팩트도 존재할 수 있다. → 블로그, 도구 개발 등의 방법으로 기여해보자.

¹ [NIST의 디지털 포렌식 도구 검증 체계 소개](#)

포렌식 문제 관련 사이트 정리

CyberDefenders, dfir.training, AboutDFIR, CFReDS¹, Digital Corpora, Ali Hadi, dfirmadness, MemLabs, MemoryForensicSamples, DEFCON DFIR - 2018 2019, Magnet, Cellebrite, belkasoft 등

과제

- Windows Timeline 분석 도구 만들어보기

- ActivitesCache.db 파일은 sqlite 파일이다.
- 파이썬 표준 라이브러리인 sqlite3 모듈을 사용하면 데이터를 읽어올 수 있다. - [docs](#)
- [DB Browser for SQLite](#)와 같은 도구를 사용하여 테이블 구조 및 데이터 확인해보기

Executable	Activity Type	Display Text	Content Info	Last Modified Time	Expiration Time	Start Time	End Time	Duration
D:\setup64.exe	ExecuteOpen	setup64.exe		2024-01-03 07:53:...	2024-02-02 07:5... 2024-01-03 ...			
D:\setup64.exe	InFocus			2024-01-03 07:53:...	2024-02-02 07:5... 2024-01-03 ... 2024-01-03 07... 00:00:02			
D:\setup64.exe	InFocus			2024-01-03 07:53:...	2024-02-02 07:5... 2024-01-03 ... 2024-01-03 07... 00:01:40			
Microsoft.Windows.SecHealthUI_cw5n1h2txyewy!SecHealthUI	ExecuteOpen	Windows ??????		2024-01-03 07:54:...	2024-02-02 07:5... 2024-01-03 ...			
Microsoft.Windows.SecHealthUI_cw5n1h2txyewy!SecHealthUI	InFocus			2024-01-03 07:55:...	2024-02-02 07:5... 2024-01-03 ... 2024-01-03 07... 00:01:42			
MSEdge	InFocus			2024-01-03 07:56:...	2024-02-02 07:5... 2024-01-03 ... 2024-01-03 07... 00:00:04			
Microsoft.Windows.Explorer	InFocus			2024-01-03 07:56:...	2024-02-02 07:5... 2024-01-03 ... 2024-01-03 07... 00:00:48			
*PID00001850	ExecuteOpen	*PID00001850		2024-01-03 07:56:...	2024-02-02 07:5... 2024-01-03 ...			
*PID00001850	InFocus			2024-01-03 07:56:...	2024-02-02 07:5... 2024-01-03 ... 2024-01-03 07... 00:00:04			