

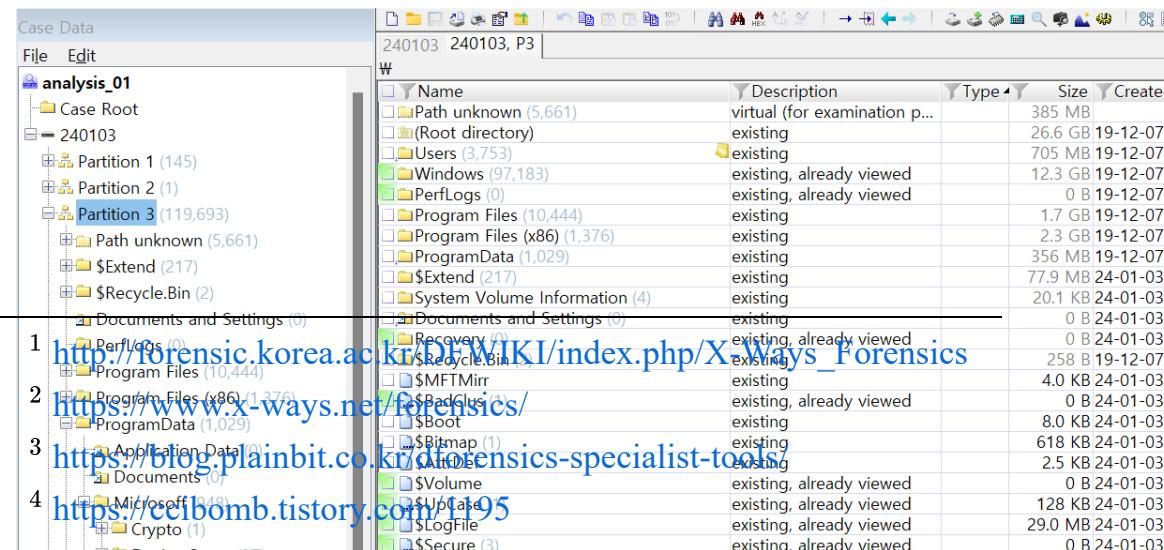
5주차 스터디

X-Ways Forensics 사용법

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

X-Ways Forensics

- 방대한 뷰어 컴포넌트, 파일 복구, 검색, RVS(Refine Volume Snapshot) 기능 등이 있다.¹²
- 그럼에도 타 도구들에 비해 가볍다는 장점이 있다.³
- 다른 포렌식 프로그램보다 적은 요건으로도 마운트를 해준다.⁴ - 최소한의 파티션 복구로 마운트 가능
- 다양한 기능과 옵션으로 인해 숙련도 필요
 - 옵션 설정의 경우 대부분 최적화된 설정이기 때문에 그대로 사용해도 된다.



Case Data	File Explorer	Details												
File Edit	240103 240103, P3	Name	Description	Type	Size	Created	Created2	Modified	Modified2	Record changed	Record changed2	Attr.	1st sector	Comments
analysis_01	Case Root	Path unknown (5,661)	virtual (for examination p...	existing	385 MB	19-12-07d18:03:44	24-01-03d16:28:34	24-01-03d17:20:28		24-01-03d17:20:28		SH	288	
240103	Partition 1 (145)	Path directory		existing	26.6 GB	19-12-07d18:03:44	24-01-03d16:28:38	24-01-03d17:10:05		24-01-03d17:10:05		R	20,280,920	24:pezMxUMLAD/hUFyElx9Z2O
	Partition 2 (1)	Users (3,753)		existing	705 MB	19-12-07d18:03:44	24-01-03d16:28:38	24-01-03d17:20:53		24-01-03d17:20:53			1,232,392	
	Partition 3 (119,693)	Windows (97,183)		existing, already viewed	12.3 GB	19-12-07d18:03:44	24-01-03d16:28:38	24-01-03d17:20:53		24-01-03d17:20:53			6,291,586	
		PerfLogs (0)		existing, already viewed	0 B	19-12-07d18:14:52	24-01-03d16:28:38	19-12-07d18:14:52		24-01-03d16:32:16				
		Program Files (10,444)		existing	1.7 GB	19-12-07d18:14:52	24-01-03d16:28:38	24-01-03d17:20:25		24-01-03d17:20:25		R	1,231,288	
		Program Files (x86) (1,376)		existing	2.3 GB	19-12-07d18:14:52	24-01-03d16:28:38	24-01-03d17:04:13		24-01-03d17:04:13		R	1,232,072	
		ProgramData (1,029)		existing	356 MB	19-12-07d18:14:52	24-01-03d16:28:38	24-01-03d16:53:32		24-01-03d16:53:32		XH	1,232,200	
		\$Extend (217)		existing	77.9 MB	24-01-03d16:28:34		24-01-03d16:28:34		24-01-03d16:28:34		SH	6,291,478	
		System Volume Information (4)		existing	20.1 KB	24-01-03d16:33:11		24-01-03d16:37:25		24-01-03d16:37:25		SH	16,201,408	
		Documents and Settings (0)		existing	0 B	24-01-03d16:35:09		24-01-03d16:35:09		24-01-03d16:35:09		PXSH	6,508,096	
		PerfLogs (0)		existing, already viewed	0 B	24-01-03d16:35:15		24-01-03d16:35:15		24-01-03d16:35:15		XSH	6,508,574	
1	http://forensic.korea.ac.kr/DI/WIKI/index.php/X_Ways_Forensics	Recovery (0)		existing	258 B	19-12-07d18:14:52	24-01-03d16:28:38	24-01-03d16:50:32		24-01-03d16:50:32		SH	6,291,584	
2	https://www.x-ways.net/forensics/	Program Files (x86) (1,376)		existing	4.0 KB	24-01-03d16:28:34		24-01-03d16:28:34		24-01-03d16:28:34		SH	16	
3	https://blog.plainbit.co.kr/forensics-specialist-tools/	ProgramData (1,029)		existing, already viewed	0 B	24-01-03d16:28:34		24-01-03d16:28:34		24-01-03d16:28:34		SH	6,291,472	
4	https://celbomb.tistory.com/1195	Application Data (0)		existing	8.0 KB	24-01-03d16:28:34		24-01-03d16:28:34		24-01-03d16:28:34		SH	0	
		Documents (0)		existing	618 KB	24-01-03d16:28:34		24-01-03d16:28:34		24-01-03d16:28:34		SH	6,290,168	
		\$Bitmap (1)		existing	2.5 KB	24-01-03d16:28:34		24-01-03d16:28:34		24-01-03d16:28:34		SH	280	
		Microsoft (148)		existing, already viewed	0 B	24-01-03d16:28:34		24-01-03d16:28:34		24-01-03d16:28:34		ISH	6,291,462	
		Crypto (1)		existing, already viewed	128 KB	24-01-03d16:28:34		24-01-03d16:28:34		24-01-03d16:28:34		SH	24	
		\$LogFile (1)		existing, already viewed	29.0 MB	24-01-03d16:28:34		24-01-03d16:28:34		24-01-03d16:28:34		SH	6,230,872	
		\$Secure (3)		existing, already viewed	0 B	24-01-03d16:28:34		24-01-03d16:28:34		24-01-03d16:28:34		SH		

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>

X-Ways Forensics

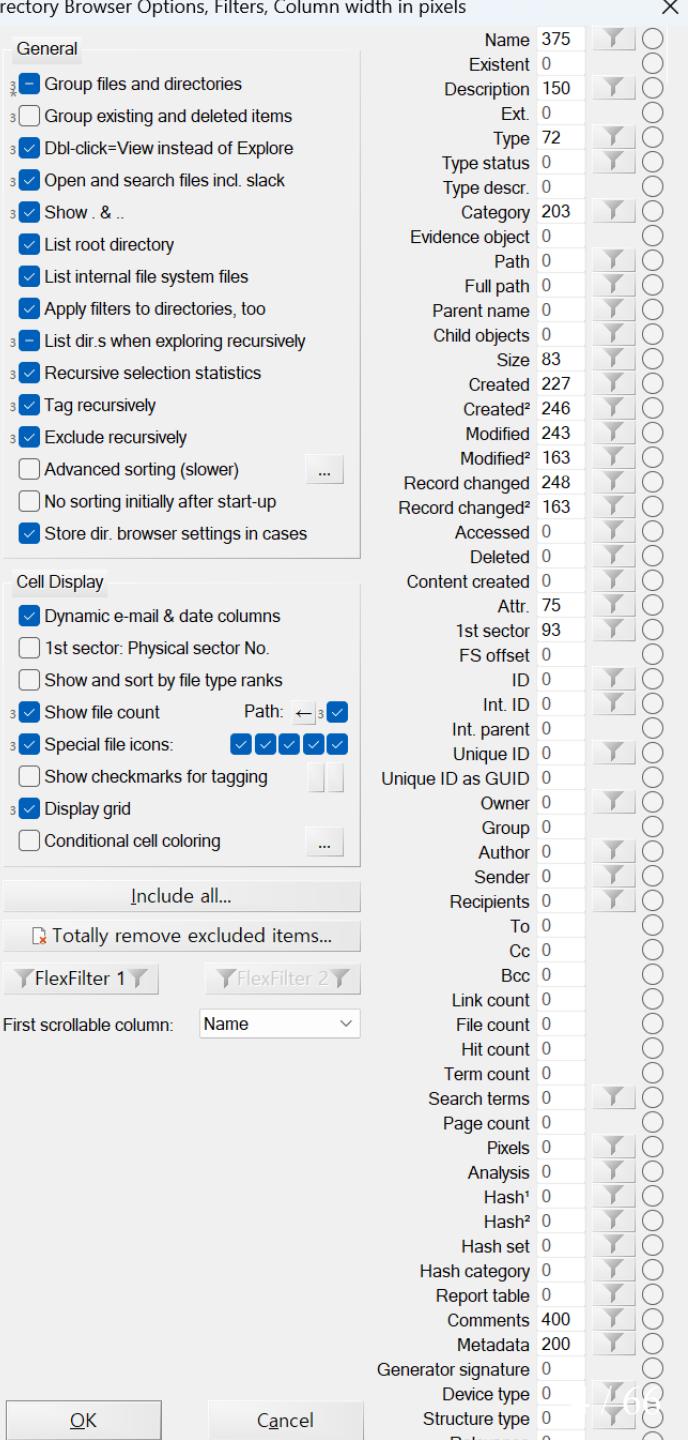
Directory Browser Options (CTRL + F5 or Options -> Directory Browser)¹

- Created² , Modified² , Record changed² 설정 - 숫자 값을 적절히 넣으면 된다.
 - SIA²의 변조 가능성 있음, \$FNA³ 시간 정보도 확인하기 위해 설정
- Type status , Category , Comments , Metadata 등 적절히 설정
 - Catrgory 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>

² SIA (Standard Information Attribute)

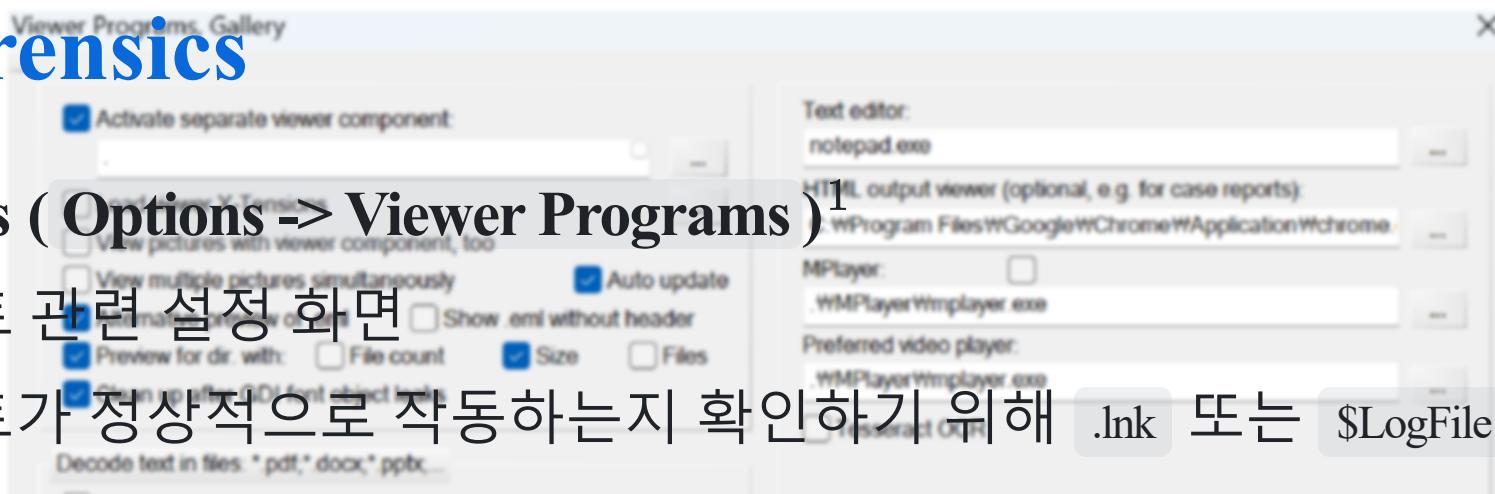
³ \$FNA (\$FILE_NAME - NTFS 속성)



X-Ways Forensics

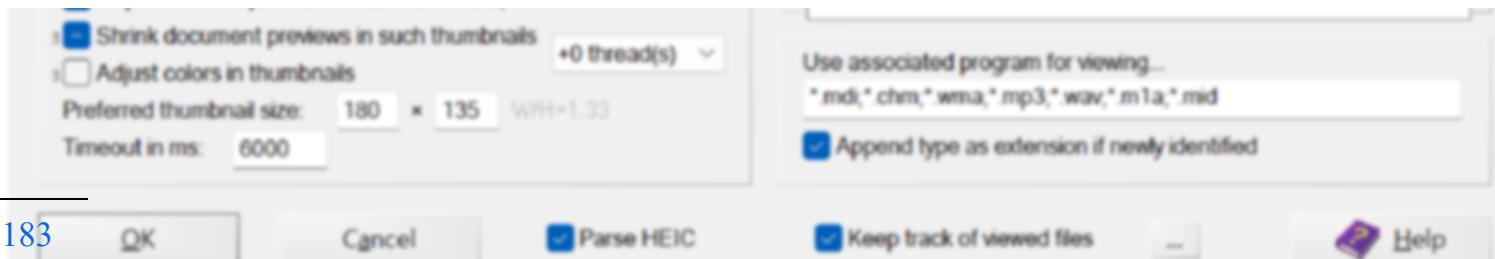
Viewer Programs (Options -> Viewer Programs)¹

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



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

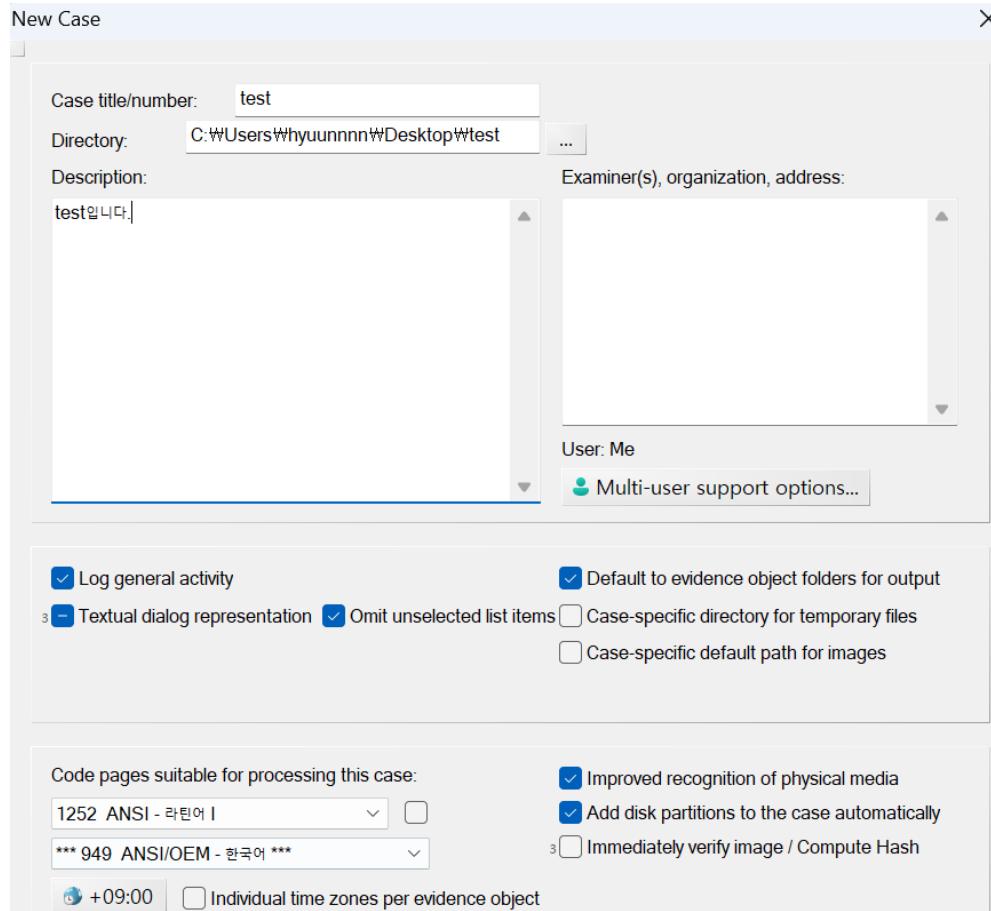
Link target information	
Target attributes	R (Directory)
Target file size	0
Show Window	SW_NORMAL
Target created	2024-01-03d16:48:29 +0900
Last written	2024-01-03d16:49:34 +0900
Last accessed	2024-01-03d16:49:34 +0900



¹ <https://ccibomb.tistory.com/1183>

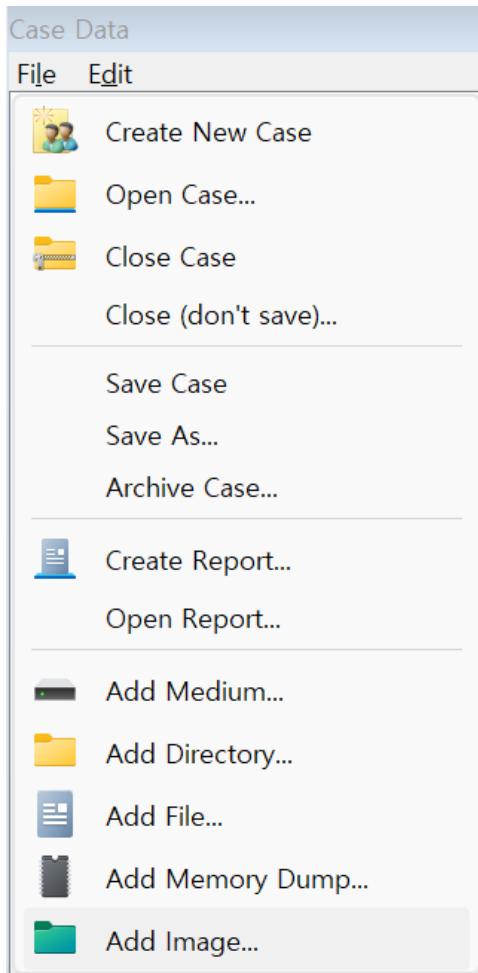
X-Ways Forensics

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

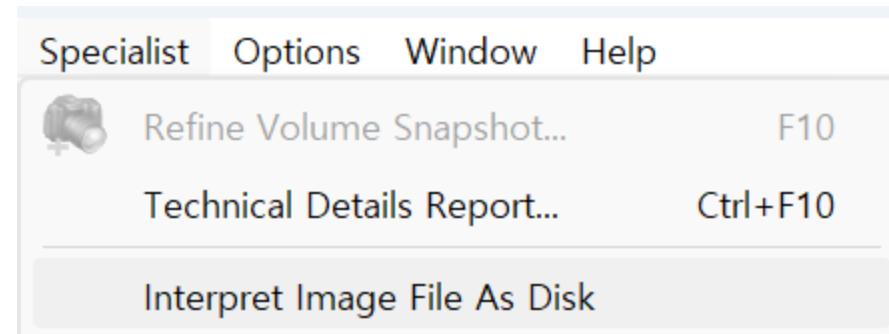


X-Ways Forensics

- 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

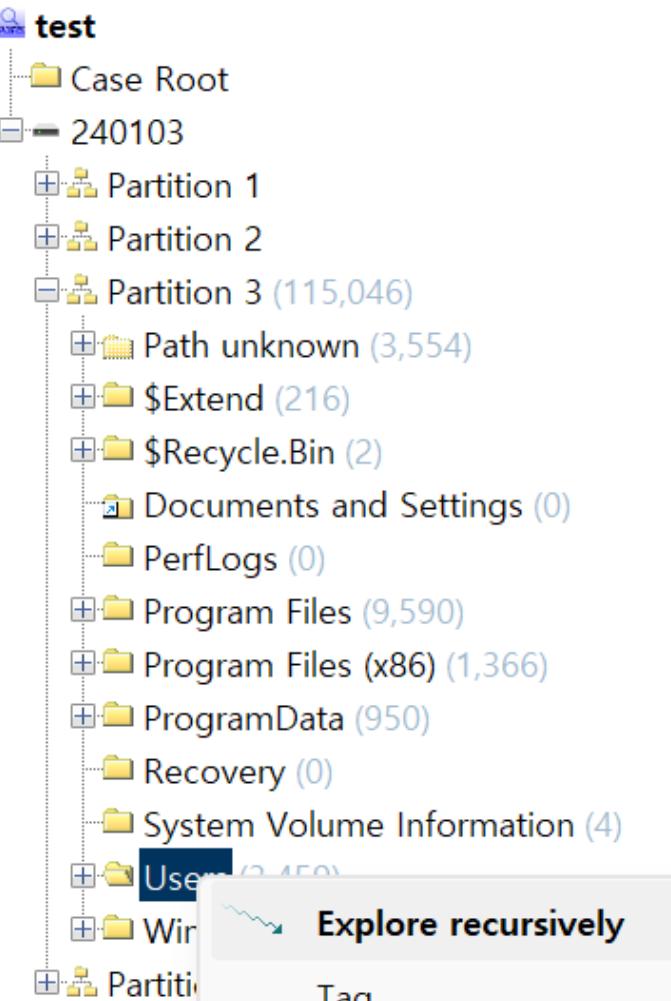
- 그러나 케이스를 만들어서 사용하는 방법이 더 편하고, 이점이 있기 때문에 케이스를 만들어서 사용하자

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

240103 240103, P3										3,418+41=3	
Users and subdirectories											
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	+ 2024-01-03d17:21:30.017 +9	+ 2024-01-03d17:21:30.017 +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	+ 2024-01-03d17:21:30.017 +9	+ 2024-01-03d17:21:30.017 +9		
인터넷.lnk	existing	Ink	Windows Internals	104 B	2024-01-03d17:17:23.011	+ 2024-01-03d17:34:22.424 +9	+ 2024-01-03d17:34:22.424 +9	+ 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	+ 2024-01-03d17:21:29.860 +9	+ 2024-01-03d17:21:29.860 +9	+ 2024-01-03d17:21:29.876 +9		
문서.mydocs	existing, already ...mydocs	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	+ 2024-01-03d16:49:35.022 +9	+ 2024-01-03d16:49:35.022 +9		
다운로드.lnk	existing	Ink	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	+ 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	+ 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	+ 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	+ 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	+ 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	+ 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	+ 2024-01-03d17:11:36.093 +9	+ 2024-01-03d17:11:36.093 +9		
{7C5A40EF-A0FB-4BFC-874A-C0F2E0B...	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	+ 2024-01-03d17:09:56.619 +9	+ 2024-01-03d17:09:56.619 +9		
{6D809377-6AF0-444B-8957-A3773F0...	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	+ 2024-01-03d16:59:00.280 +9	+ 2024-01-03d16:59:00.280 +9		
{6D809377-6AF0-444B-8957-A3773F0...	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	+ 2024-01-03d16:59:00.249 +9	+ 2024-01-03d16:59:00.249 +9		
{6D809377-6AF0-444B-8957-A3773F0...	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	+ 2024-01-03d17:20:51.171 +9	+ 2024-01-03d17:20:51.171 +9		
{3DA71D5A-20CC-432F-A115-DFE9237...	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	+ 2024-01-03d17:34:20.861 +9	+ 2024-01-03d17:34:20.861 +9		
{1AC14E77-02E7-4E5D-B744-2EB1AE51...	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	+ 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	+ 2024-01-03d16:59:03.014 +9	+ 2024-01-03d16:59:03.014 +9		
{1AC14E77-02E7-4E5D-B744-2EB1AE5...	existing		Other/unknown type	36.1 KB	2024-01-03d16:59:00.093	+ 2024-01-03d16:59:00.108 +9	+ 2024-01-03d16:59:00.108 +9	+ 2024-01-03d16:59:00.108 +9	+ 2024-01-03d16:59:00.108 +9		
{1AC14E77-02E7-4E5D-B744-2EB1AE51...	existing		Other/unknown type	36.1 KB	2024-01-03d16:59:00.155	+ 2024-01-03d16:59:00.171 +9	+ 2024-01-03d16:59:00.171 +9	+ 2024-01-03d16:59:00.171 +9	+ 2024-01-03d16:59:00.171 +9		
{1AC14E77-02E7-4E5D-B744-2EB1AE51...	existing		Other/unknown type	36.1 KB	2024-01-03d16:58:59.874	+ 2024-01-03d16:58:59.874 +9	+ 2024-01-03d16:58:59.874 +9	+ 2024-01-03d16:58:59.874 +9	+ 2024-01-03d16:58:59.874 +9		

X-Ways Forensics



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

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

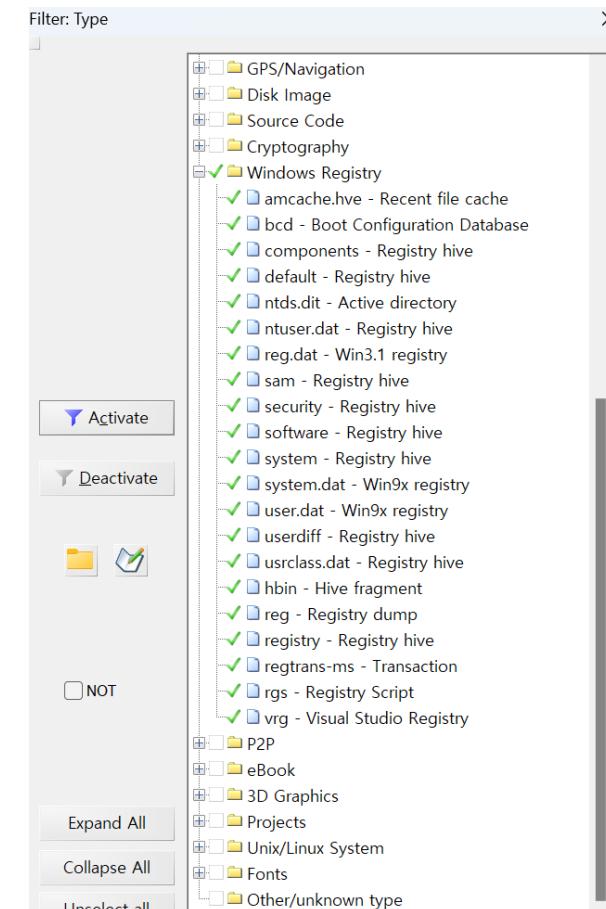
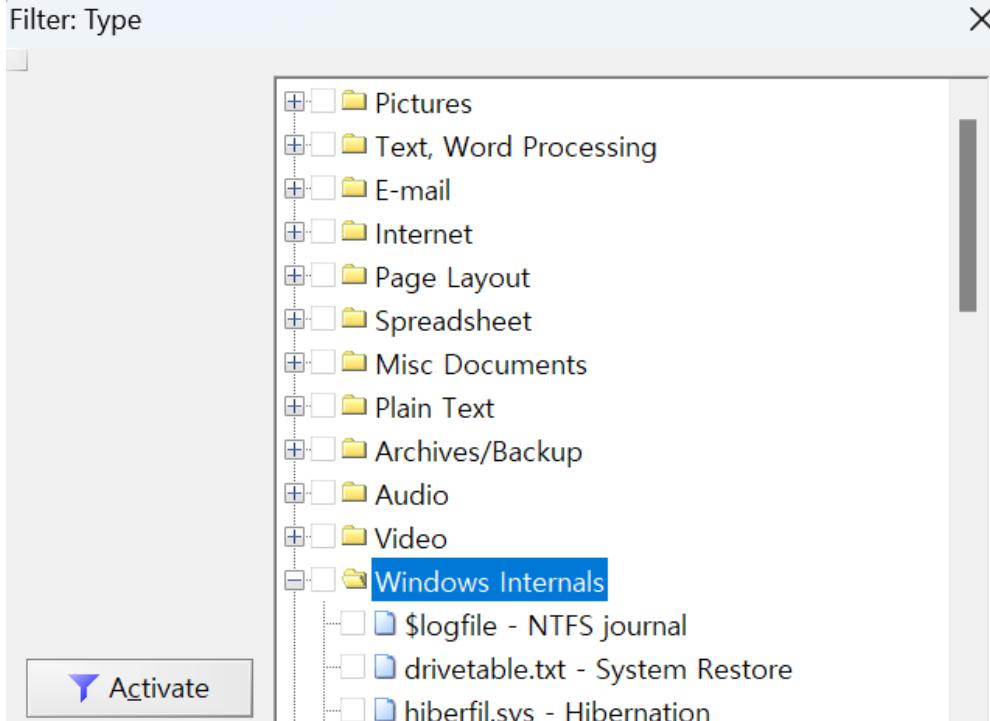
X-Ways Forensics

- 필터 기능¹
 - 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	
.. = 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	
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	Ink	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	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	Ink	Windows Internals	447 B	2024-01-03d17:02:23.414 +		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-C0F2E0B...	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	
{6D809377-6AF0-444B-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	
{6D809377-6AF0-444B-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	
{6D809377-6AF0-444B-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-DFE9237...	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	
{AC14E77-02E7-4E5D-B744-2EB1AE51...	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	

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	6,793	
debuggerDiagRemote.js	existing, har...	js	Other/unknown type	11,496	
debugger.html	existing, har...	html	Pictures	2,613	
debugger.html	existing, har...	html	Text, Word Processing	2,419	
debugger.css	existing, har...	css	E-mail	1	
debugger.css	existing, har...	css	Internet	421	
debugger.bundle.js	existing, har...	js	Page Layout	2,508	
debugger.bundle.js	existing, har...	js	Spreadsheet	28	
DebugAndTrace.aspx	existing	aspx	Misc Documents	240	
DebugAndTrace.aspx	existing	aspx	Plain Text		
DebugAndTrace.aspx	existing	aspx	Archives/Backup		
de-DE.mail.config	existing	config	Audio		
DccpWCpoNzCwM4Qymi_Ji67llso.br[1].js	existing	js			
daytonaOptOut.js	existing, har...	js			
daytonaOptOut.js	existing, har...	js			
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.

240103 240103, P3 WUsers\WUser\WDownloads										14 files, 0 dir.
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		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		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		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		2024-01-03d17:21:28.505 +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		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		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		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		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.

240103 240103 240103, P4 240103, P3 \ and subdirectories										111,233+3,809+4=115,046 files
Name	Description	Type	Category	Size	Created	Created ²	Modified	Modified ²	Record changed	
0IAjDNgXOrFO.exe	existing	exe	Programs	208 KB	2024-01-03d17:18:07.214 +9		2024-01-03d17:18:07.245 +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		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		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		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		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		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		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		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		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		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		2024-01-03d17:18:11.429 +9	

랜섬웨어 의심 파일: 0IAjDNgXOrFO.exe

X-Ways Forensics

기능: 달력에 날짜 별로 정렬하여 보여주며, 클릭하면 사진과 같이 필터가 적용된다.

Name	Description	Type	Category	Size	Created	Created ²	Modified	Modified ²	Record changed
BitLocker.Format.ps1xml	existing, har...	ps1xml	Programs	5.7 KB	2019-12-07d18:10:39.386 +9	2024-01-03d16:31:41.478 +9	2019-12-07d23:59:31.726 +9	2024-01-03d16:31:41.586 +9	2024-01-03d16:31:41.648 +9
BitLocker.Format.ps1xml	existing, har...	ps1xml	Programs	5.7 KB	2019-12-07d18:10:39.386 +9	2024-01-03d16:31:41.478 +9	2019-12-07d23:59:31.726 +9	2024-01-03d16:31:41.648 +9	2024-01-03d16:33:25.365 +9
BitLocker MDM policy Refresh	existing		Other/unknown type	2.3 KB	2024-01-03d16:33:25.350 +9		2024-01-03d16:33:25.365 +9		2024-01-03d16:33:23.725 +9
BitLocker Encrypt All Drives	existing		Other/unknown type	2.4 KB	2024-01-03d16:33:23.725 +9		2024-01-03d16:33:23.725 +9		2024-01-03d16:32:16.586 +9
BitLocker (5)	existing			320 KB	2019-12-07d23:59:36.866 +9	2024-01-03d16:28:39.008 +9	2019-12-07d23:59:37.476 +9	2024-01-03d16:32:16.617 +9	2024-01-03d16:33:25.350 +9
BitLocker (5)	existing			320 KB	2019-12-07d23:59:36.882 +9	2024-01-03d16:28:39.164 +9	2019-12-07d23:59:37.694 +9	2024-01-03d16:33:25.419 +9	2024-01-03d17:35:41.419 +9
BitLocker (2)	existing			4.7 KB	2024-01-03d16:33:23.725 +9		2024-01-03d16:33:25.350 +9		2024-01-03d16:33:25.419 +9
BITE54A.tmp	existing	tmp	Other/unknown type	61.5 KB	2024-01-03d17:35:41.090 +9		2024-01-03d17:35:41.419 +9		2024-01-03d17:35:41.000 +9
BITAC5A.tmp	existing	tmp	Other/unknown type	953 KB	2022-03-08d11:44:10.000 +9	2024-01-03d17:08:26.165 +9	2022-03-08d11:44:10.000 +9	2024-01-03d17:08:26.165 +9	2022-03-08d11:44:10.000 +9
BIT685B.tmp	existing	tmp	Other/unknown type	6.2 KB	2024-01-02d17:17:57.000 +9	2024-01-03d17:31:30.689 +9	2024-01-02d17:17:57.000 +9	2024-01-02d17:17:57.000 +9	2024-01-02d17:17:57.000 +9
BIT3C4C.tmp	existing	tmp	Other/unknown type	22.2 KB	2023-08-18d12:48:12.000 +9	2024-01-03d16:55:56.590 +9	2023-08-18d12:48:12.000 +9	2023-08-18d12:48:12.000 +9	2023-08-18d12:48:12.000 +9
bisrv.dll.mui	existing, har...	mui	Windows Internals	9.0 KB	2019-12-07d23:56:00.006 +9	2024-01-03d16:31:31.946 +9	2019-12-07d23:56:00.006 +9	2024-01-03d16:31:32.258 +9	2024-01-03d16:31:32.351 +9
bisrv.dll.mui	existing, har...	mui	Windows Internals	9.0 KB	2019-12-07d23:56:00.006 +9	2024-01-03d16:31:31.946 +9	2019-12-07d23:56:00.006 +9	2024-01-03d16:31:32.351 +9	2024-01-03d16:32:039 +9
bisrv.dll	existing	dll	Programs	52.0 KB	2023-12-04d11:45:27.970 +9	2024-01-03d16:29:28.055 +9	2023-12-04d11:45:27.970 +9	2024-01-03d16:29:28.055 +9	2024-01-03d16:29:32.039 +9
bisrv.dll	existing	dll	Programs	42.1 KB	2023-12-04d11:45:27.970 +9	2024-01-03d16:29:28.055 +9	2023-12-04d11:45:27.970 +9	2024-01-03d16:29:28.055 +9	2024-01-03d16:29:32.039 +9
bisrv.dll	existing, har...	dll	Programs	834 KB	2023-12-04d11:45:28.595 +9	2024-01-03d16:29:28.055 +9	2023-12-04d11:45:28.595 +9	2024-01-03d16:29:28.055 +9	2024-01-03d16:29:32.039 +9
bisrv.dll	existing, har...	dll	Programs	834 KB	2023-12-04d11:45:28.595 +9	2024-01-03d16:29:28.055 +9	2023-12-04d11:45:28.595 +9	2024-01-03d16:29:28.055 +9	2024-01-03d16:29:32.039 +9
Biometrics.admx	existing	admx	Windows Internals	3.6 KB	2019-12-07d18:10:22.413 +9	2024-01-03d16:29:12.711 +9	2019-12-07d18:10:22.413 +9	2024-01-03d16:29:19.321 +9	2024-01-03d16:29:19.321 +9
Biometrics.adml	existing	adml	Windows Internals	1.7 KB	2019-12-07d23:55:55.881 +9	2024-01-03d16:29:12.523 +9	2023-12-04d11:56:26.627 +9	2024-01-03d16:29:19.273 +9	2024-01-03d16:29:19.273 +9
BioMDL2.ttf	existing	ttf	Fonts	203 B	2023-12-04d11:46:50.521 +9	2024-01-03d16:31:42.789 +9	2023-12-04d11:46:50.521 +9	2024-01-03d16:31:42.789 +9	2024-01-03d16:31:55.945 +9
BioMDL2.ttf	existing	ttf	Fonts	2.3 KB	2023-12-04d11:46:50.521 +9	2024-01-03d16:31:42.789 +9	2023-12-04d11:46:50.521 +9	2024-01-03d16:31:42.789 +9	2024-01-03d16:31:55.945 +9
BioMDL2.ttf	existing, har...	ttf	Fonts	20.7 KB	2023-12-04d11:46:51.474 +9	2024-01-03d16:31:42.789 +9	2023-12-04d11:46:51.474 +9	2024-01-03d16:31:42.789 +9	2024-01-03d16:31:55.945 +9
BioMDL2.ttf	existing, har...	ttf	Fonts	20.7 KB	2023-12-04d11:46:51.474 +9	2024-01-03d16:31:42.789 +9	2023-12-04d11:46:51.474 +9	2024-01-03d16:31:42.789 +9	2024-01-03d16:31:55.945 +9
Biolo.exe	existina	exe	Programs	26.1 KB	2023-12-04d11:46:47.005 +9	2024-01-03d16:31:05.336 +9	2023-12-04d11:46:47.005 +9	2024-01-03d16:31:10.664 +9	2024-01-03d16:31:10.664 +9

2024. 01. 03 클릭 -> 1월 3일 이후 필터 적용

Filter: Timestamps

Created
Created²
Modified
Modified²

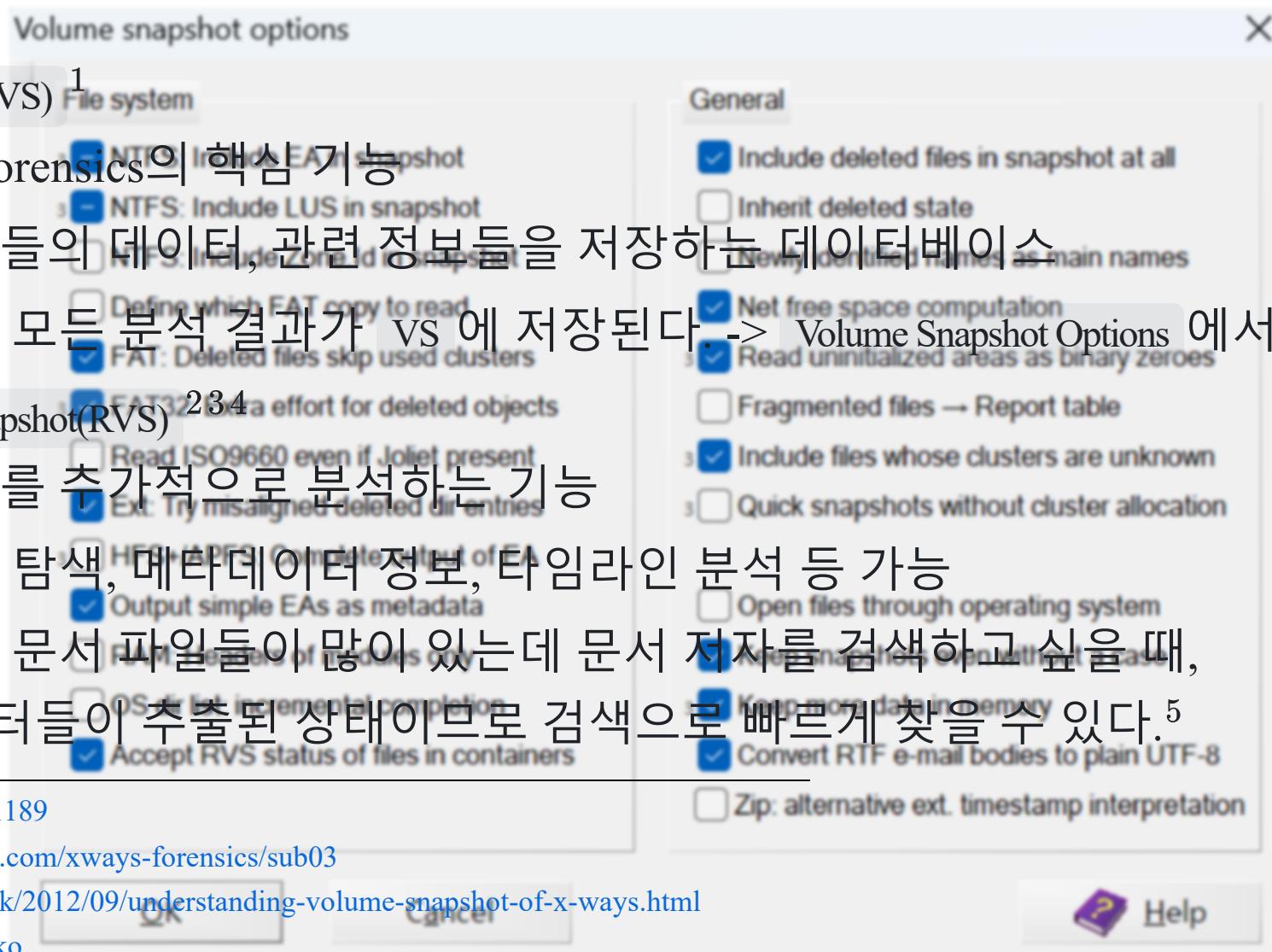
Record changed
Record changed²
Accessed
Deleted

(OR)

Before
After
Between ... 2024-01-03d00:00:00 & ... 2099-12-31d00:00:00

X-Ways Forensics

- Volume Snapshot (VS)¹
 - 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)²³⁴
 - 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://ccibomb.tistory.com/1189>

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

³ <https://www.xwaysclips.co.uk/2012/09/understanding-volume-snapshot-of-x-ways.html>

⁴ <https://youtu.be/ggSXfAf4Eko>

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 search¹³

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

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

File Header Search on Partition 3

File type(s): > < Signatures... More...

Filename prefix: Carving_

Intelligent naming, where possible

Name = 1st sector

Opt. subdirectory of WPath unknown\WCarved files:
File Type Signatures Search.txt 사용

Outputs child objects of existing files if suitable

A	B	C	D	E	F	G
Description	Extensions	Header	Offset	Footer	Default size	Flags
*** Pictures						
JPEG	JPG;jpeg;jpe;thm;mpo	FFxD8FF[C0C4DBDDxE0-E5E7]	0 ~1		2097152/33554432	e
PNG	png	89PNGx0Dx0AxA	0 ~6			e
GIF	gif	GIF8[79]a	0 ~3		2097152/33554432	
High Efficiency Image	heic	(ftypheic ftypmif1)	4 ~27		1000000/31457280	
Thumbcache fragment	cmmm	CMM..x00x00.^x00	0 ~84		2097152/511705088	GUB
TIFF/NEF/CR2/DNG	tif;tiff;nef;cr2;dng;pef;nrw;arw	(x49x49x2A)x00)(x4Dx4Dx00x2A)	0 ~5		25165824/268435456	
Bitmap	bmp;dib	BM....x00.x00....[x0Cx28x38x40x6Cx7C]x	0 ~4			
Paint Shop Pro	psp;PsPImage;pfr	(Paint Shop Pro Im) (~BKx00)	0 ~8		2097152	b
Canon Raw	crw	HEAPCCDR	6		8200000	c
Adobe Photoshop	PSD;pdd;p3m;p3r;p3l	8BPSx00x01x00x00x00x00x00x00	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>

X-Ways Forensics

- Verify file types with signatures and algorithms¹²

- 시그니처 분석을 수행하는 옵션 - File Type Signatures Check Only.txt 사용
- 다른 확장자로 위장, 바뀐 파일들을 시그니처 기반으로 탐지 및 검증 가능
 - 예시로 브라우저 캐시 파일을 확인 -> 시그니처를 탐지하여 보여주고 있다.

Name	Description	Type	Type status	Category	Size	Created
= Cache (343)	existing				78.1 MB	2024-01-01 02:16:51,20,662
= Cache_Data (343)	existing				78.1 MB	2024-01-01 02:16:51,20,662
data_0	existing	not verified	Internet	Internet	80.0 KB	2024-01-01 02:16:51,20,662
data_1	existing	not verified	Internet	Internet	776 KB	2024-01-01 02:16:51,20,662
data_2	existing	not verified	Internet	Internet	2.0 MB	2024-01-01 02:16:51,20,662
data_3	existing	not verified	Internet	Internet	16.0 MB	2024-01-01 02:16:51,20,662
f_000001	existing, already viewed	not verified	Other/unkno...	Pictures	707 KB	2024-01-01 02:16:51,20,662
f_000002	existing	not verified	Other/unkno...	Pictures	26.9 KB	2024-01-01 02:16:51,20,662
f_000003	existing	not verified	Other/unkno...	Pictures	44.5 KB	2024-01-01 02:16:51,20,662
f_000004	existing	not verified	Other/unkno...	Pictures	95.0 KB	2024-01-01 02:16:51,20,662
f_000005	existing	not verified	Other/unkno...	Pictures	355 KB	2024-01-01 02:16:51,20,662
f_000006	existing	not verified	Other/unkno...	Pictures	107 KB	2024-01-01 02:16:51,20,662
f_000008	existing	not verified	Other/unkno...	Pictures	270 KB	2024-01-01 02:16:51,20,662
f_000009	existing	not verified	Other/unkno...	Pictures	76.5 KB	2024-01-01 02:16:51,20,662
f_00000a	existing	not verified	Other/unkno...	Pictures	83.7 KB	2024-01-01 02:16:51,20,662
f_00000b	existing	not verified	Other/unkno...	Pictures	40.2 KB	2024-01-01 02:16:51,20,662
f_00000c	existing	not verified	Other/unkno...	Pictures	89.2 KB	2024-01-01 02:16:51,20,662
f_00000d	existing	not verified	Other/unkno...	Pictures	21.2 KB	2024-01-01 02:16:51,20,662
f_00000e	existing, already viewed	not verified	Other/unkno...	Pictures	64.3 KB	2024-01-01 02:16:51,20,662
f_00000f	existing	not verified	Other/unkno...	Pictures	91.5 KB	2024-01-01 02:16:51,20,662
f_000010	existing	not verified	Other/unkno...	Pictures	323 KB	2024-01-01 02:16:51,20,662
f_000011	existing	not verified	Other/unkno...	Pictures	77.3 KB	2024-01-01 02:16:51,20,662
f_000012	existing	not verified	Other/unkno...	Pictures	114 KB	2024-01-01 02:16:51,20,662
f_000013	existing	not verified	Other/unkno...	Pictures	788 KB	2024-01-01 02:16:51,20,662
f_000014	existing	not verified	Other/unkno...	Pictures	39.4 KB	2024-01-01 02:16:51,20,662
f_000016	existing	not verified	Other/unkno...	Pictures	75.3 KB	2024-01-01 02:16:51,20,662
f_000017	existing	not verified	Other/unkno...	Pictures	81.3 KB	2024-01-01 02:16:51,20,662
f_000018	existing	not verified	Other/unkno...	Pictures	314 KB	2024-01-01 02:16:51,20,662
f_000019	existing	not verified	Other/unkno...	Pictures	74.5 KB	2024-01-01 02:16:51,20,662
f_00001a	existing	not verified	Other/unkno...	Pictures	122 KB	2024-01-01 02:16:51,20,662
f_00001b	existing	not verified	Other/unkno...	Pictures	45.4 KB	2024-01-01 02:16:51,20,662
f_00001c	existing	not verified	Other/unkno...	Pictures	98.2 KB	2024-01-01 02:16:51,20,662



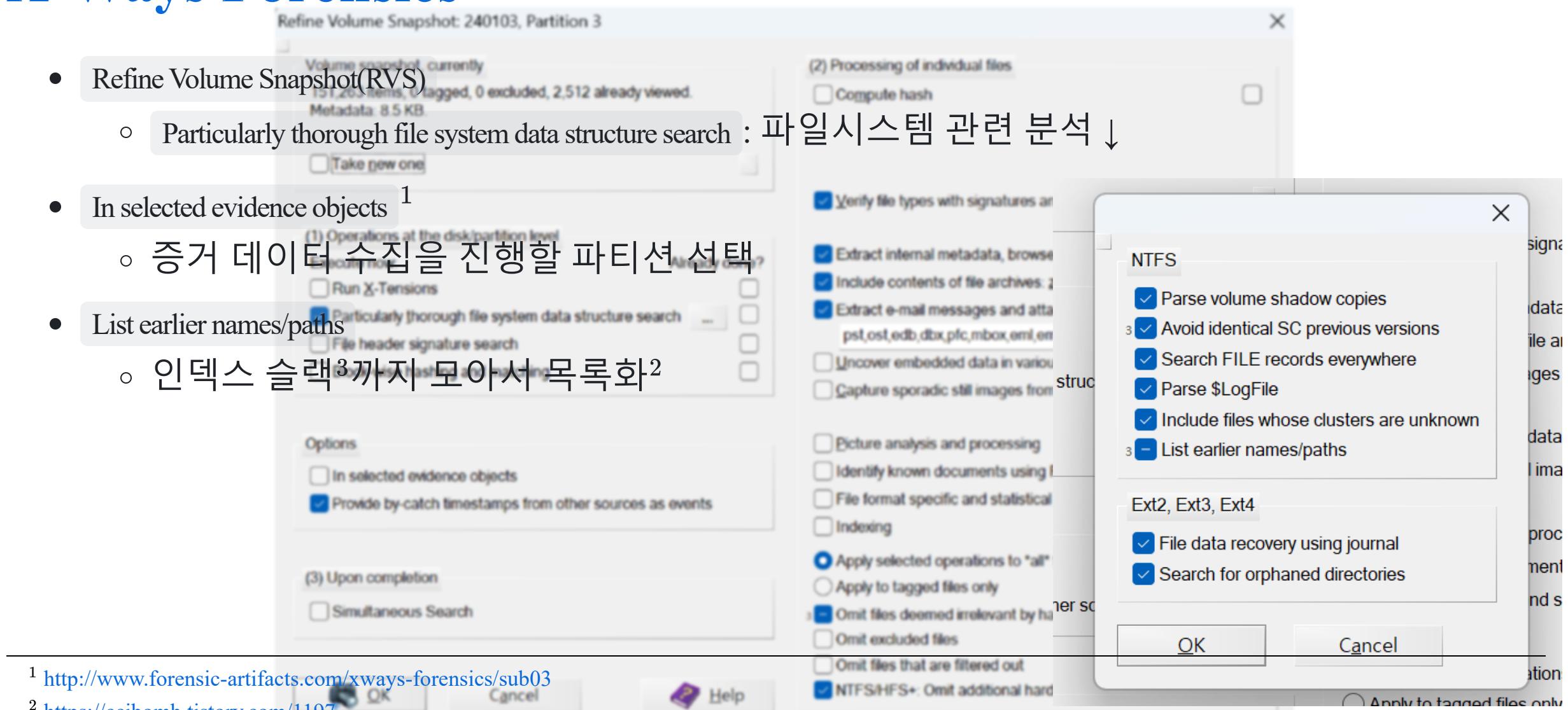
Name	Description	Type	Type status	Category	Size	Created	Modified	Record changed
= Cache (343)	existing							
= Cache_Data (343)	existing							
f_000073	existing, already viewed	jpg	newly identifi...	Pictures				
f_000074	existing, already viewed	jpg	newly identifi...	Pictures				
f_000075	existing, already viewed	jpg	newly identifi...	Pictures				
f_000076	existing, already viewed	jpg	newly identifi...	Pictures				
f_000077	existing, already viewed	jpg	newly identifi...	Pictures				
f_000078	existing, already viewed	jpg	newly identifi...	Pictures				
f_000079	existing, already viewed	png	newly identifi...	Pictures				
f_00007a	existing, already viewed	jpg	newly identifi...	Pictures				
f_00007b	existing, already viewed	png	newly identifi...	Pictures				
f_00007c	existing, already viewed	png	newly identifi...	Pictures				
f_00007d	existing, already viewed	png	newly identifi...	Pictures				
f_00007e	existing, already viewed	gz	newly identifi...	Archives/Bac...				
f_00007f	existing, already viewed	png	newly identifi...	Pictures				
f_000080	existing, already viewed	png	newly identifi...	Pictures				
f_000082	existing							
f_000083	existing, already viewed	png	newly identifi...	Pictures				
f_000084	existing							
f_000085	existing							
f_000086	existing, already viewed	png	newly identifi...	Pictures				
f_000087	existing, already viewed	jpg	newly identifi...	Pictures				
f_000088	existing							
f_000089	existing							
f_00008a	existing							
f_00008b	existing							
f_00008c	existing							
f_00008d	existing							
f_00008e	existing							
f_00008f	existing							
f_000090	existing							
f_000091	existing							
f_000092	existing, already viewed	jpg	newly identifi...	Pictures				
f_000093	existing							



1 <https://ccibombhistory.com/1203>
2 <http://www.forensic-artifacts.com/xways-forensics/ant01/>

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>

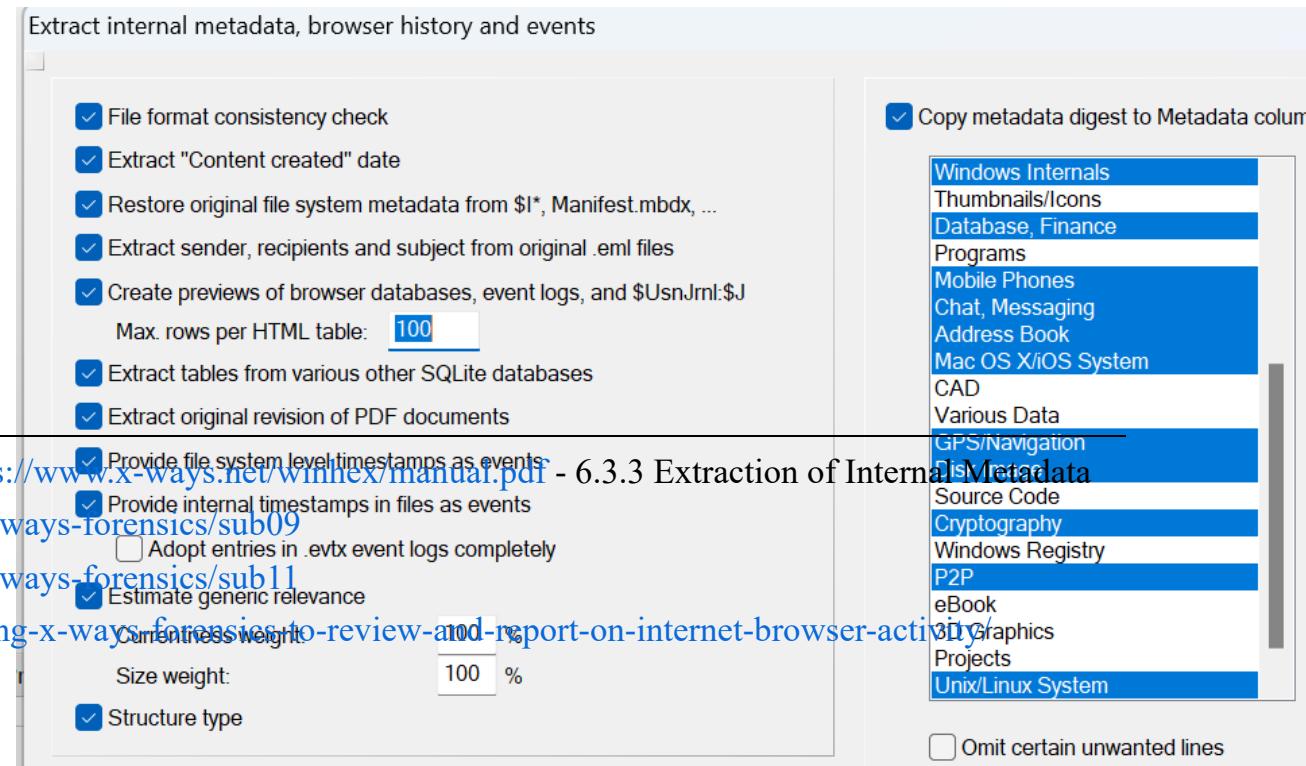
³ 물리적인 구조와 논리적인 구조의 차이로 발생하는 낭비되는 공간 - <http://forensicinsight.org/wp-content/uploads/2012/02/INSIGHT-MFT-INDX-슬랙-분석.pdf>

X-Ways Forensics

- Refine Volume Snapshot(RVS)

- Extract internal metadata, browser history and events²³⁴⁶

-> 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>

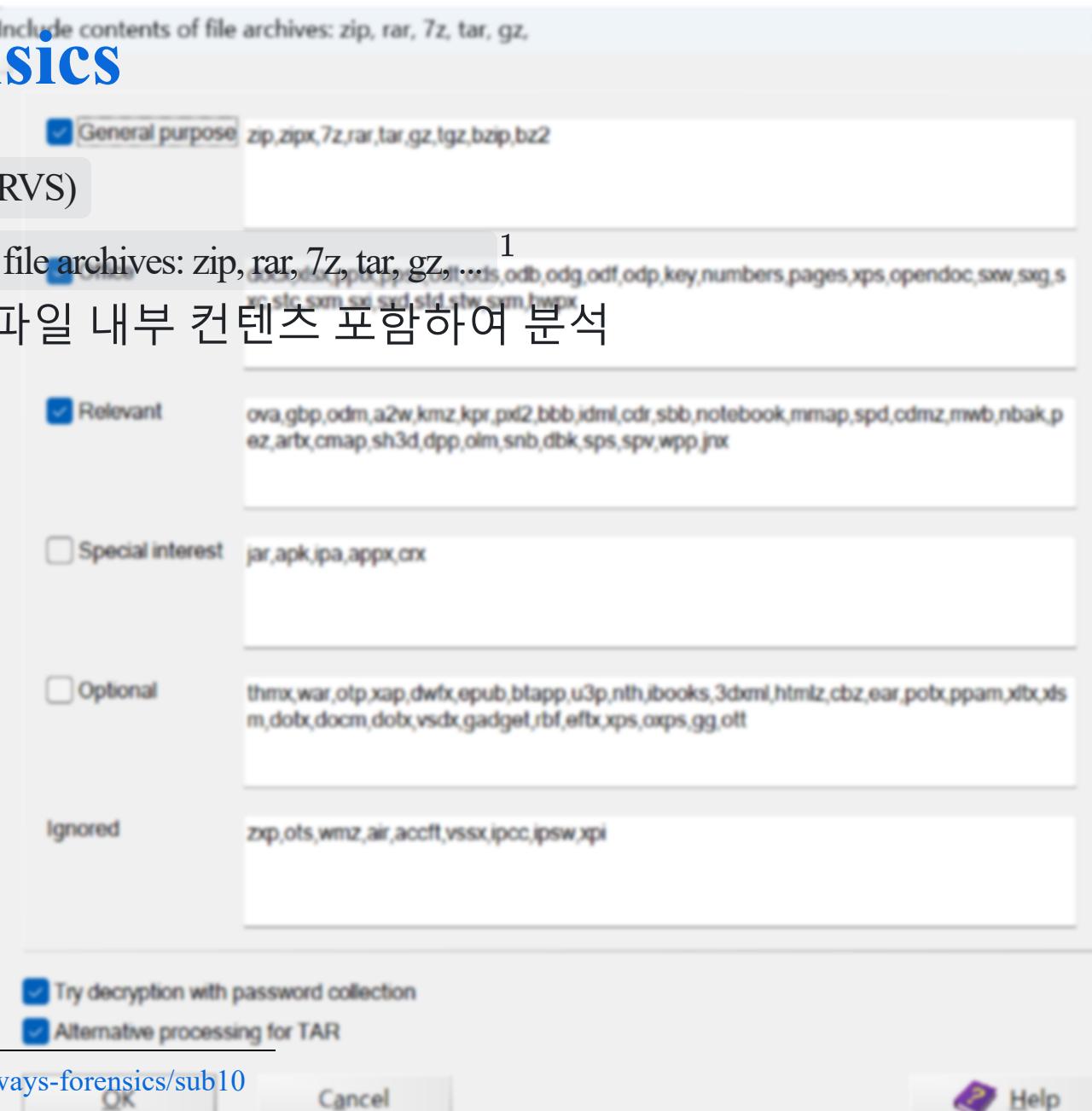
⁶ <https://youtu.be/2KYtZ-ycjWs>

X-Ways Forensics

- Refine Volume Snapshot(RVS)

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

- 아카이브 파일 내부 컨텐츠 포함하여 분석



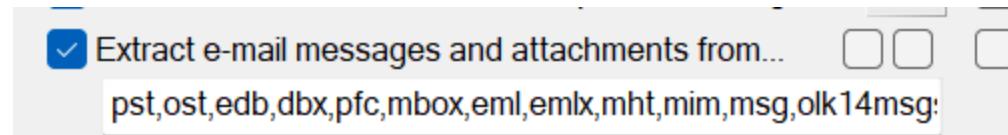
¹ <http://www.forensic-artifacts.com/xways-forensics/sub10>

X-Ways Forensics

- Refine Volume Snapshot(RVS)

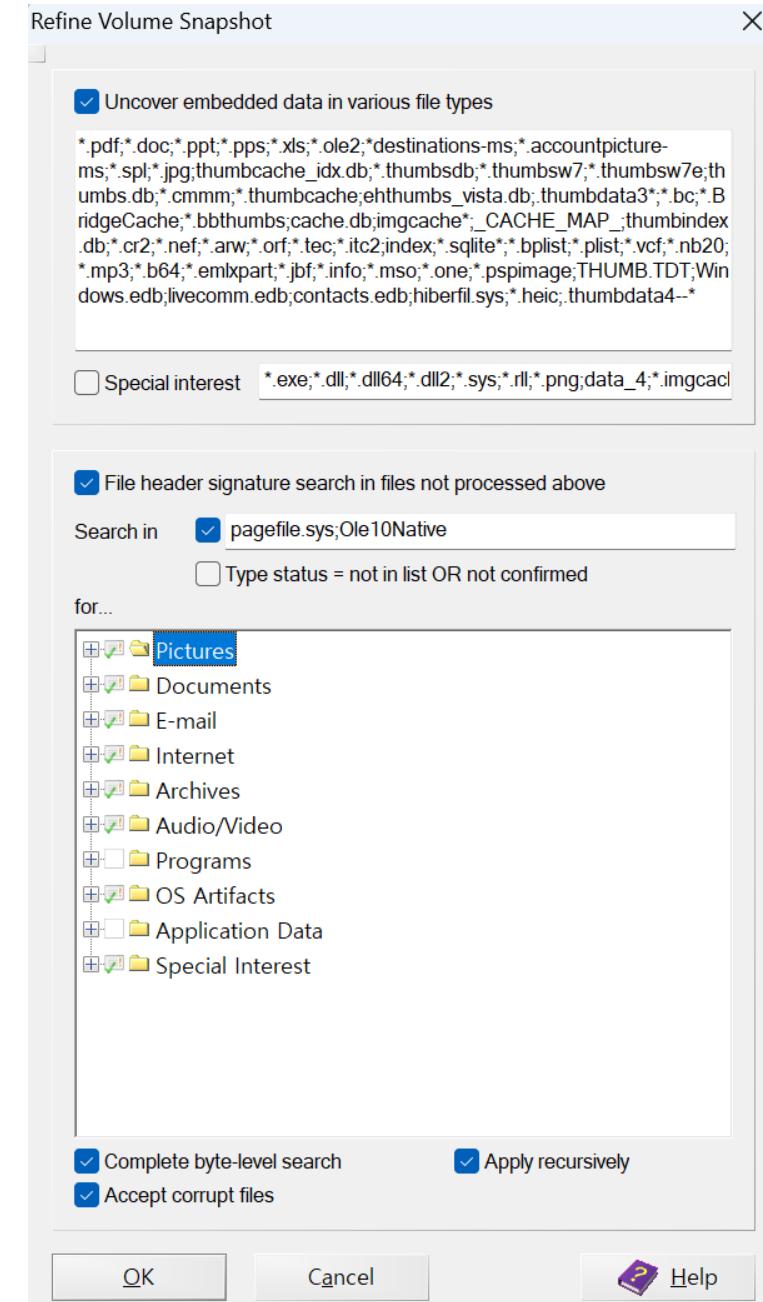
- Extract e-mail messages and attachments from...^{1,2}

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



- Uncover embedded data in various file types^{3,4} →

- 파일 내부에 존재하는 다른 파일들을 시그니처 기반으로 추출하는 기능



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

² https://youtu.be/HiBz_ETu5Kw

³ <https://goblinforensics.tistory.com/340>

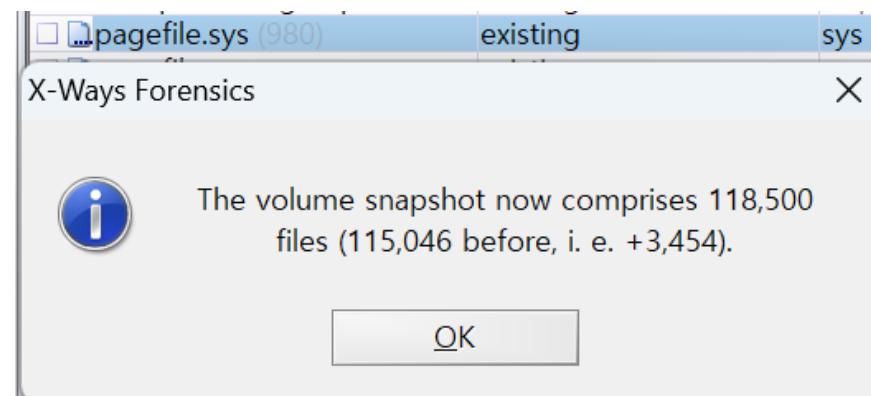
⁴ <http://www.forensic-artifacts.com/xways-forensics/anti02>

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
pagefile.sys	existing
swapfile.sys	existing
Free space (net)	virtual (for examination ...)

1



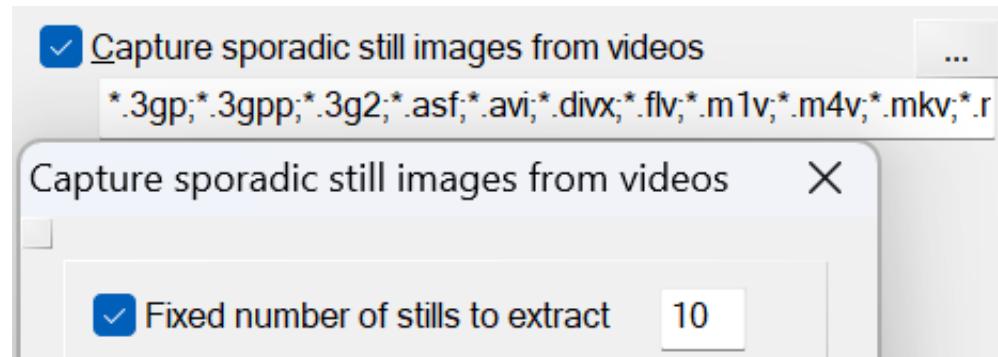
2

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

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

Windows\SystemResources\Windows.UI.SettingsAppThreshold\SystemSettings\Assets				
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	

240103 Case Root 240103 240103, P3					
Windows\SystemResources\Windows.UI.SettingsAppThreshold\SystemSettings\Assets\SDRSample.mkv					
Name	Description	Type	Type status	Category	Size
= Assets (12)	existing				5.3 MB
= SDRSample.mkv (2)	existing, har... jpg	confirmed	Video		1.7 MB
SDRSample.mkv 0m 01s.jpg	existing, alre... jpg	confirmed	Pictures		149 KB
SDRSample.mkv 0m 10s.jpg	existing, alre... jpg	confirmed	Pictures		139 KB

¹ https://ko.wikipedia.org/wiki/스틸_사진

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.

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

² <http://www.forensic-artifacts.com/xways-forensics/sub14> 하단에 있는 Legend 버튼에서 확인 가능 - E: encrypted at filesystem level
e: encrypted in archive

X-Ways Forensics

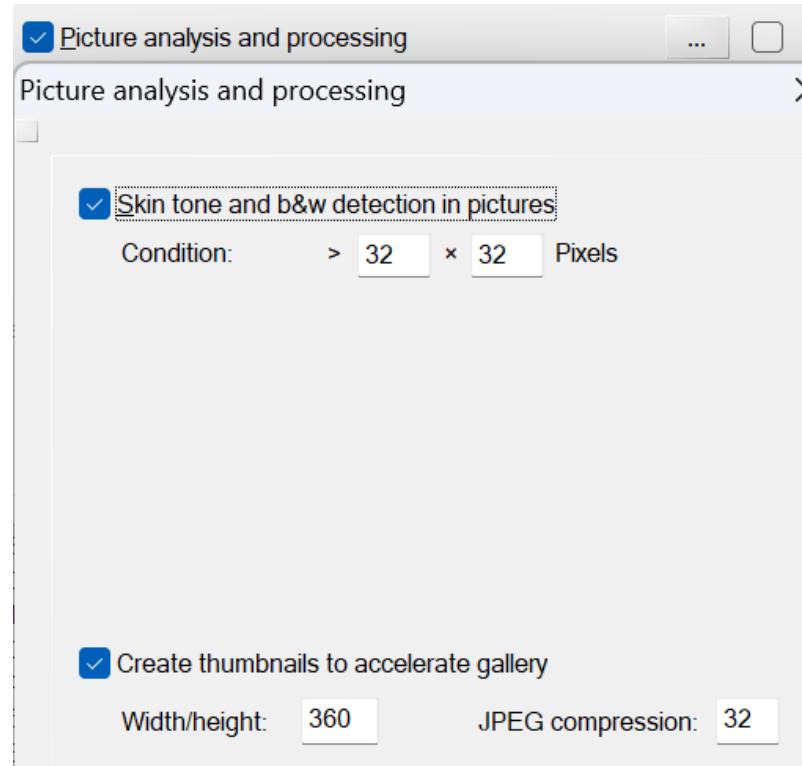
- Refine Volume Snapshot(RVS)
 - File format specific and statistical encryption tests¹

test.xfc 240103 240103, P3											
Y1 \ 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

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

2	f_00006e [c9232d31-8a41-4e2c-a4a8-aa474d]existing	jpg	newly identifi... 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											
2	f_00006b [upload_17041941710246z8W.jpg]existing	jpg	newly identifi... 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											
2	f_000107 [Jv2rS6lQj3UmZuQJ2Uu5uzNzB0.j	existing	jpg	newly identifi... 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										
2	f_000079 [Vibe_SC_076±ºĐÁÀº°¬ÇÉ¼Ô@]existing	png	newly identifi... 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											
2	f_00015b [th]	existing, alre...	jpg	newly identifi... 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										
2	f_000067 [f37997d8-b723-445d-945d-d2293]existing, alre...	jpg	newly identifi... 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											
2	f_000101 [upload_1704182609838G3XXi.jpg]existing, alre...	jpg	newly identifi... 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											

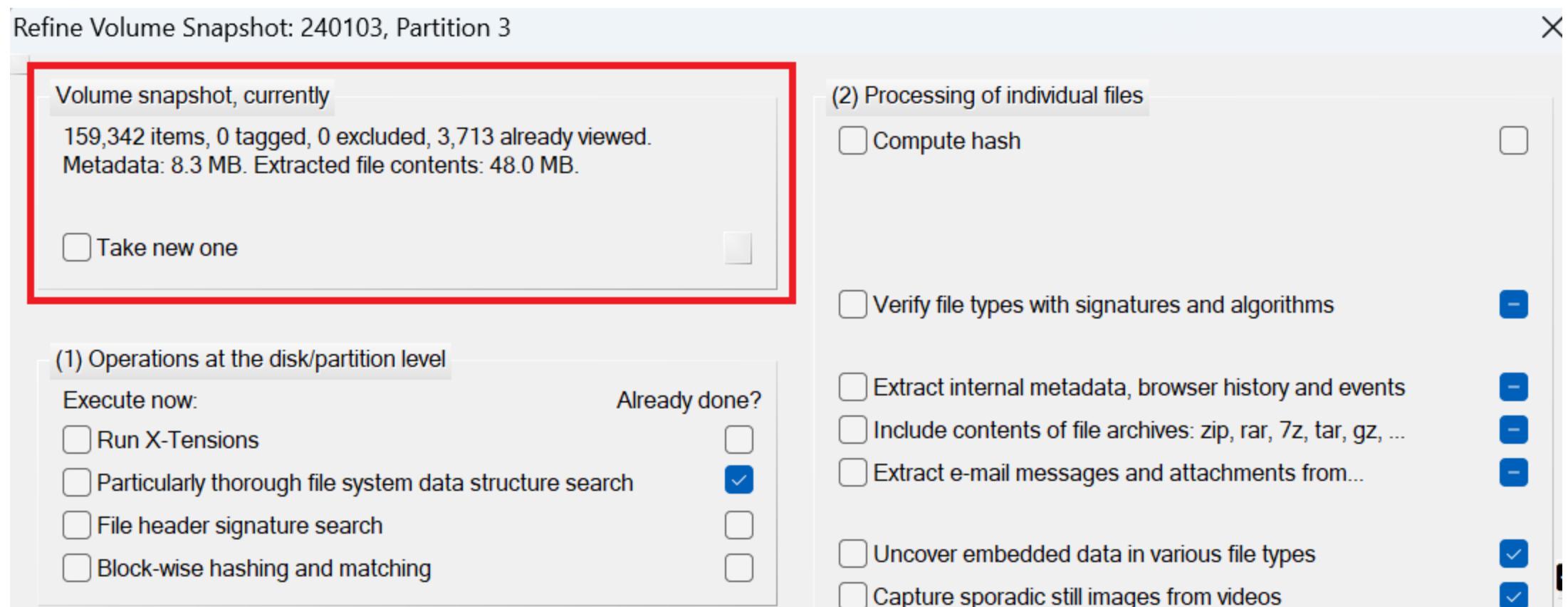


- ..?
- 이미지 분석에서 참고용으로 활용하면 좋을 것 같다.

X-Ways Forensics

- Refine Volume Snapshot(RVS)

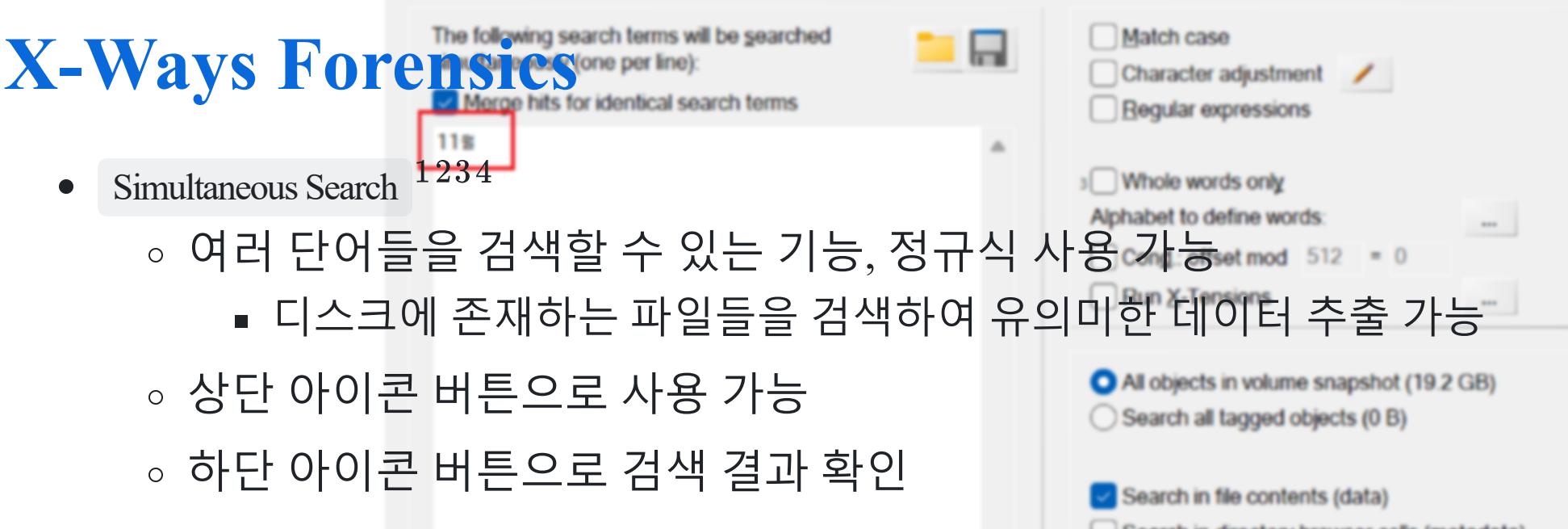
- RVS 완료 후 다시 들어가면 현재 수집된 Volume Snapshot 확인 가능



X-Ways Forensics

- Simultaneous Search

- 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 main X-Ways Forensics interface with a toolbar at the top and a search results table below. The table has columns for Physical offset, Logical offset, Description, Search hits, Name, Type, Hit count, and Term count. The search results table lists numerous files found in the volume snapshot, including various log files, system files like pagefile.sys, and application files like Aedb00006.jtx. The bottom part of the interface shows a hex dump of a file with several URLs highlighted in blue, indicating they are search results. The URLs include <https://goblinforensics.tistory.com/346>, <https://goblinforensics.tistory.com/348>, <https://goblinforensics.tistory.com/350>, and <https://youtube/Gh19E2dzh4>.

X-Ways Forensics

- 블록 해시(Block Hash)^{1 2}
 - TODO
- 퍼지 해시(FuzzYDoc)³
 - RVS -> Identify known documents using FuzzYDoc
 - TODO

¹ <https://ccibomb.tistory.com/1201>

² <http://www.forensic-artifacts.com/xways-forensics/sub04>

³ <https://ccibomb.tistory.com/1202>

⁴ <https://mreerie.com/2022/01/26/selectively-hashing-files-in-x-ways-forensics/>

X-Ways Forensics

- 라이브 포렌식, 컨테이너 파일, 스켈레톤 이미지, 클린즈드 이미지
 - TODO

¹ https://www.x-ways.net/investigator/containers_vs_skeleton_images.html

² <https://www.x-ways.net/investigator/scheme.png>

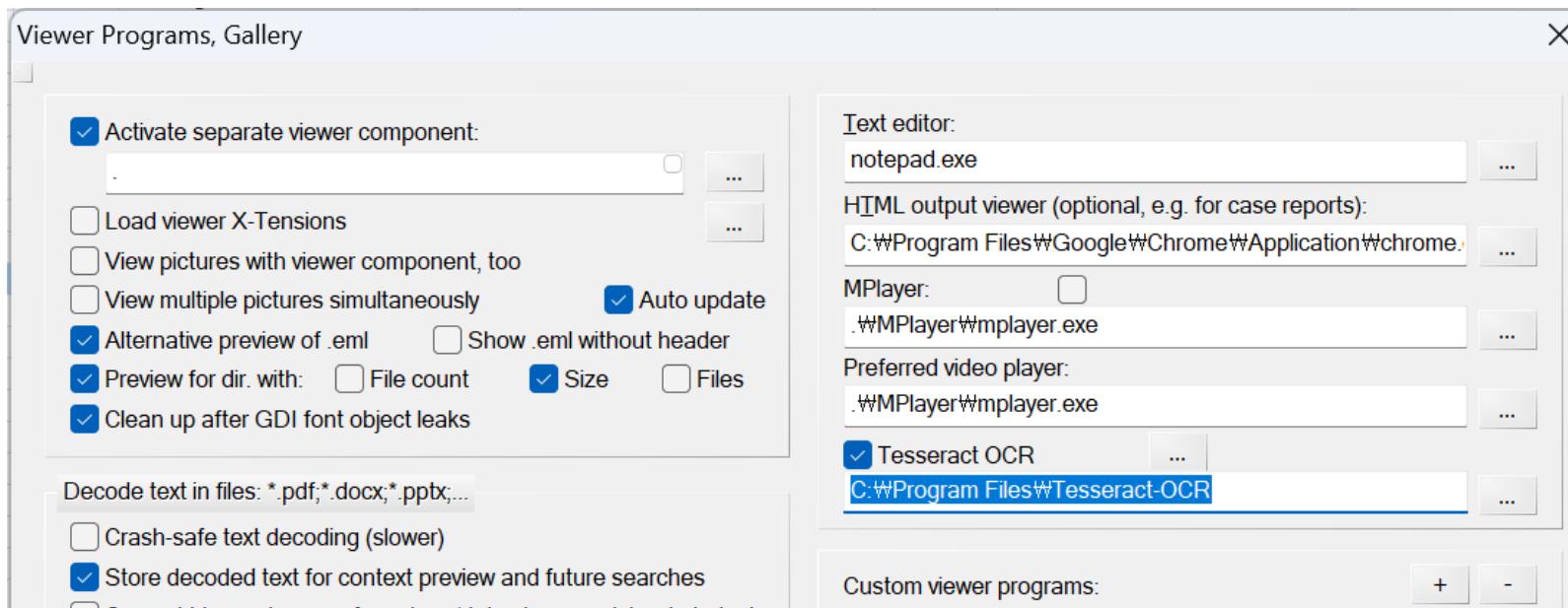
³ <https://goblinforensics.tistory.com/295>

⁴ <https://goblinforensics.tistory.com/297>

⁵ <https://youtu.be/JWA-xrXsXJA>

X-Ways Forensics - Tesseract OCR¹

- 구글에서 만든 오픈소스 광학 문자 인식 엔진 - 윈도우 설치 파일
- Additional script data, Additional language data는 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

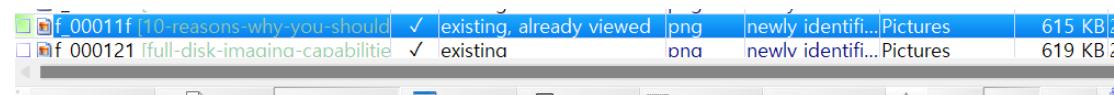
- [tessdata_best](#)에서 최신 학습 모델로 바꿀 수 있다. -> 설치할 때 파일들이 포함되기 때문에 pass
 - Capture sporadic still images from videos 을 활용하여 영상을 사진으로 추출 -> 활용도 높음¹

10 REASONS WHY
YOU SHOULD UPGRADE
FROM IMAGER to FTK®

While FTK Imager excels at electronic device imaging, its analysis and review capabilities are limited. Count on the full-featured FTK Forensic Toolkit to complete your workflow.

Manual Navigation

FTK's File Categorization & Overview Tab



10 REASONS WHY

YOU SHOULD UPGRADE
FROM IMAGER to FTK®

While FTK Imager excels at electronic device imaging, its analysis and review capabilities are limited. Count on the full-featured FTK Forensic Toolkit to complete your workflow.

What can FTK do that FTK Imager can't do? Read on for
10 core forensic analysis and review tasks you're going to
want to perform in FTK:

Manual FTK's File Categorization
Navigation & Overview Tab

In FTK Imager you can load an image and search for files, but it's a manual process to navigate through files individually or by directory. By contrast, FTK's Overview Tab categorizes all the files on the disk automatically. The File Category section breaks up files into categories like documents, emails, spreadsheets, executables, registry files, deleted files, or files with bad extensions—they're all automatically categorized, ready for you to analyze, bookmark, save, label, or export.

The File Category section breaks up files into categories like documents, emails, spreadsheets, executables, registry files, deleted files, or files with bad extensions—they're all automatically categorized, ready for you to analyze, bookmark, save, label, or export.

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

10 Reasons Why You Should Upgrade from IMAGER to FTK // © 2023 Exterro, Inc.

X-Ways Forensics

- Report
 - X-Ways 실무 활용 가이드 - Report 생성
 - [X-Ways Forensics] 11 Export list
 - Report Noteworthy Files
- X-Tensions
 - 중간발표 기술문서 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](#)

MUICache

- 윈도우 환경에서 다중 언어를 지원하기 위해 존재하는 캐시
- 예를 들어 윈도우 내장 프로그램인 `regedit` 은 레지스트리 편집기, `taskmgr` 는 작업 관리자로 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:\Program Files\Common Files\system\wab32r...	REG_SZ	연락처
> ImmutableMuiCache	@C:\Program Files\Microsoft Office\Root\VFSS\Pr...	REG_SZ	Microsoft Excel 워크시트
> MrtCache	@C:\Program Files\Microsoft Office\Root\VFSS\Pr...	REG_SZ	Microsoft Excel 쉼표로 구분된 값 파일
> MuiCache	@C:\Program Files\Microsoft Office\Root\VFSS\Pr...	REG_SZ	Microsoft Word 문서
> bc			

참고자료

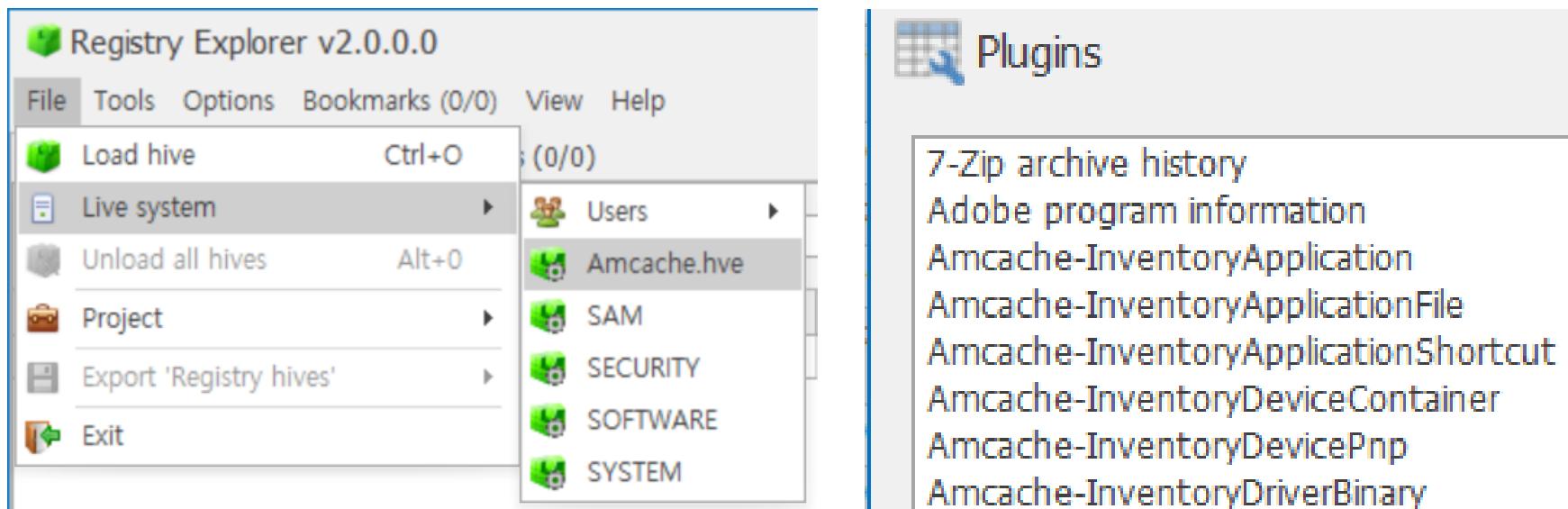
- MUICache - forensic-artifacts
- 기초부터 따라하는 디지털포렌식
- Forensic Analysis of MUICache Files in Windows

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

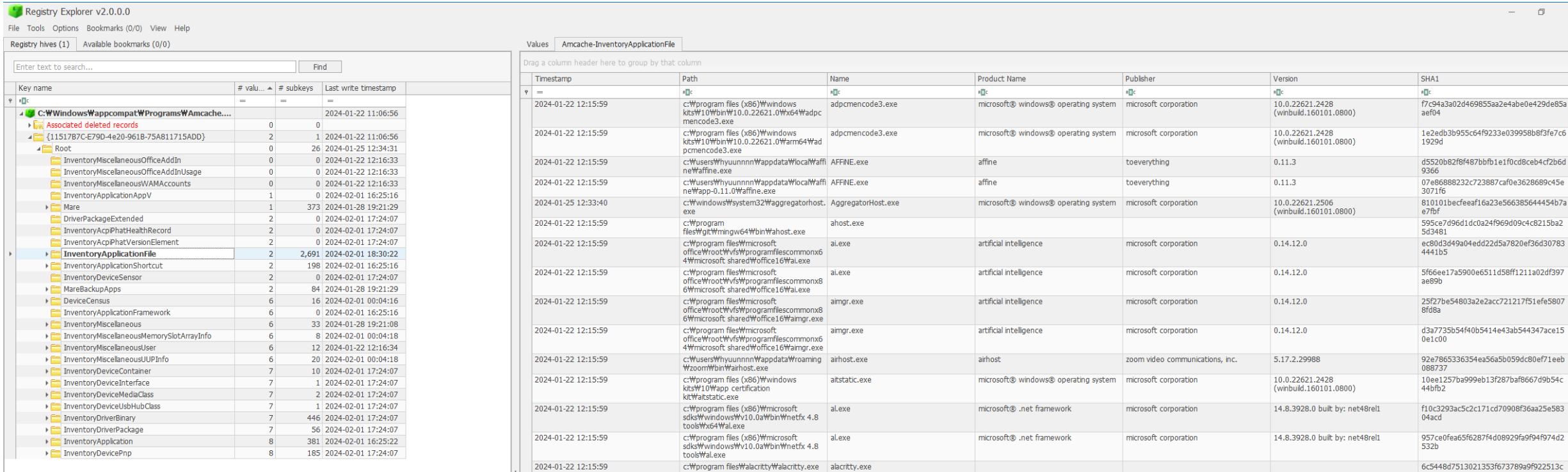
- 추출해서 확인하는 방법도 좋으나, 빠르게 확인하기 위해 현재 사용 중인 PC의 Amcache 파일 분석
- Registry Explorer 관리자 권한으로 실행 -> File -> Live system -> AmCache.hve 클릭



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

AmCache

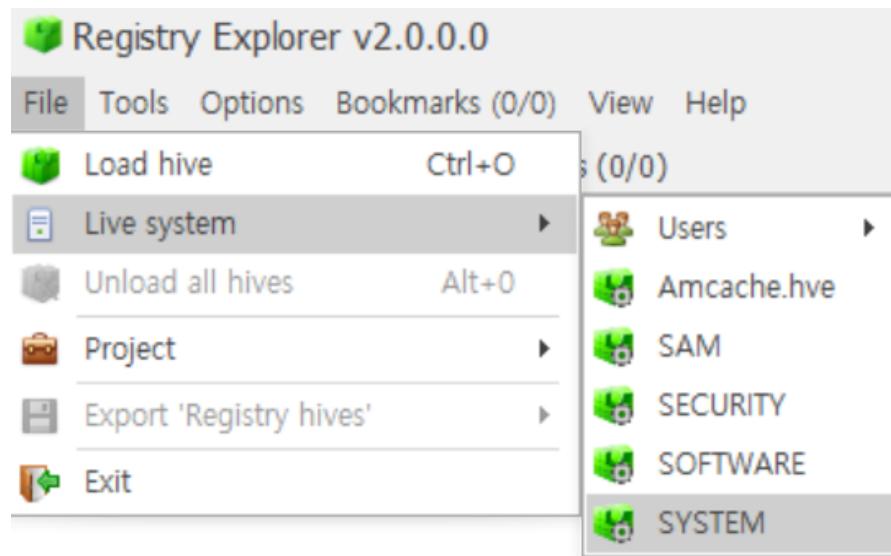
- 왼쪽에 키 이름을 누르면 하위 키들을 파싱하여 오른쪽에 결과를 보여준다.
- 현재 `InventoryDriverPackage`, `Mare` 키에 대한 플러그인이 없다.
 - 시간이 된다면 플러그인을 개발하여 기여해보자..! - [RegistryPlugins](#)
 - `Mare` 는 윈도우 11 최신버전에 새롭게 추가된 것 같다.



The screenshot shows the Registry Explorer interface with the title bar "Registry Explorer v2.0.0.0". The left pane displays the registry tree under "Registry hives (1)". The main pane shows the contents of the "Amcache" key. A secondary pane on the right displays a detailed list of entries from the "Amcache-InventoryApplicationFile" hive, grouped by timestamp. The table has columns for Timestamp, Path, Name, Product Name, Publisher, Version, and SHA1.

Timestamp	Path	Name	Product Name	Publisher	Version	SHA1
2024-01-22 12:15:59	c:\program files (x86)\windows kits\10\bin\10.0.22621.0\w64\adpcmenicode3.exe	adpcmenicode3.exe	microsoft® windows® operating system	microsoft corporation	10.0.22621.2428 (winbuild.160101.0800)	f7c94a3a02d46985aa2e4abe0e429de85aaef04
2024-01-22 12:15:59	c:\program files (x86)\windows kits\10\bin\10.0.22621.0\w64\adpcmenicode3.exe	adpcmenicode3.exe	microsoft® windows® operating system	microsoft corporation	10.0.22621.2428 (winbuild.160101.0800)	1e2edb3b955c64f9233e039958b8f3fe7c61929d
2024-01-22 12:15:59	c:\users\hyunmin\appdata\local\affine\affine\affine.exe	AFFINE.exe	affine	toeverything	0.11.3	d5520b2f8f487bbfb1e1f0cd8ceb4cf2b6d9366
2024-01-22 12:15:59	c:\users\hyunmin\appdata\local\affine\affine\affine.exe	AFFINE.exe	affine	toeverything	0.11.3	07e8688232c723887ca0e362868945e3071f6
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)	810101b8ecfeaf16a23e566385644454b7ae7bf
2024-01-22 12:15:59	c:\program files\mingw64\bin\ahost.exe	ahost.exe				595ce7d96d1dc0a24f96d9094c8215ba2d3481
2024-01-22 12:15:59	c:\program files\microsoft\office\root\fs\programfilescommon\x64\microsoft.shared\office16\aimgr.exe	ai.exe	artificial intelligence	microsoft corporation	0.14.12.0	ec80d3d4904edd22d5a7820ef63d307834441b5
2024-01-22 12:15:59	c:\program files\microsoft\office\root\fs\programfilescommon\x86\microsoft.shared\office16\airhost.exe	ai.exe	artificial intelligence	microsoft corporation	0.14.12.0	5f66e17a5900e6511d58ff1211a02df397ae99b
2024-01-22 12:15:59	c:\program files\microsoft\office\root\fs\programfilescommon\x86\microsoft.shared\office16\aimgr.exe	aimgr.exe	artificial intelligence	microsoft corporation	0.14.12.0	25f27be54803a2eacc721217f51efe58078ffd8a
2024-01-22 12:15:59	c:\program files\microsoft\office\root\fs\programfilescommon\x64\microsoft.shared\office16\aimgr.exe	aimgr.exe	artificial intelligence	microsoft corporation	0.14.12.0	d3a7735b54f40b5414e3ab544347ace150e1c0
2024-01-22 12:15:59	c:\users\hyunmin\appdata\roaming\zoom\win\airhost.exe	airhost.exe	zoom video communications, inc.	5.17.2.29988		92e7865336354ea56a5b059dc80ef1e0b88737
2024-01-22 12:15:59	c:\program files (x86)\windows kits\10\app certification kit\walstatic.exe	alstatic.exe	microsoft® windows® operating system	microsoft corporation	10.0.22621.2428 (winbuild.160101.0800)	10e1e257ba999eb13f287ba8667d9b54c44fbf2
2024-01-22 12:15:59	c:\program files (x86)\microsoft sdk\windows\v10.0\arm\whetfx 4.8 tools\wal.exe	al.exe	microsoft® .net framework	microsoft corporation	14.8.3928.0 built by: net4rel1	f10c329ac5c2c171cd70908f36aa25e58304acd
2024-01-22 12:15:59	c:\program files (x86)\microsoft sdk\windows\v10.0\arm\whetfx 4.8 tools\wal.exe	al.exe	microsoft® .net framework	microsoft corporation	14.8.3928.0 built by: net4rel1	957ce0fea6f62874d08929fa9f4f974d2532b
2024-01-22 12:15:59	c:\program files\walcratty\walcratty.exe	alacrity.exe				6c5448d7513021353f673789a9f22513c

ShimCache (AppCompatCache)



- File -> Live system -> SYSTEM 클릭 (HKLM\SYSTEM 하위 경로에 존재하기 때문)
- Available Bookmarks 에 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

- 앰캐시(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

C:\Users\hyuunnnn\Desktop\winprefetchview-x64>WinPrefetchView.exe /folder "C:\Users\hyuunnnn\Desktop\test\analysis_01\240103, P3"

The screenshot shows the WinPrefetchView application interface. At the top, there's a command-line prompt with the path and file name. Below it is the application window with a menu bar (File, Edit, View, Options, Help) and 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.

The screenshot shows the WinPrefetchView application window. The top menu bar includes File, Edit, View, Options, and Help. Below the menu is a toolbar with icons for opening, saving, and filtering files. The main area contains two tables of data.

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
APPHHELP.DLL		\VOLUME{01da3e1675b2d18c-0e75ba0e}\WINDOWS\SYSWOW64\APPHHELP.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

ThumbnailCache & IconCache

- Thumbnails Viewer 도구를 사용하여 분석 가능

#	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	21cb489a69da2d3d.png - 256x138				C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\1958b0ff69c05668
626	efa8cef8a8ee752	1671360 B	0 KB	1671448 B	0 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\efa8cef8a8ee752
627	e768e22ed2598066	1671448 B	0 KB	1671536 B	0 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\627
628	a771cc766136dd69	1671536 B	0 KB	1671624 B	0 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\628
629	3392e93cffabcc64	1671624 B	0 KB	1671712 B	0 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\629
630	26c48e99a84dc465	1671712 B	0 KB	1671800 B	0 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\630
631	2c0be1dced754061	1671800 B	0 KB	1671888 B	0 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\631
632	bc0fc576ab0ef84d	1671888 B	0 KB	1671976 B	0 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\632
633	2ff2b30bcc7a36ef	1671976 B	0 KB	1672064 B	0 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\633
634	3ecd1d6ab1aab47.png	1672064 B	22 KB	1672152 B	22 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\634
635	691e9732033f12d7.png	1695258 B	21 KB	1695346 B	21 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\635
636	3fab139e6eff416f.png	1717328 B	14 KB	1717416 B	14 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\636
637	21cb489a69da2d3d.png	1731986 B	45 KB	1732074 B	45 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\637
638	8756692c421d4b25.png	1778872 B	7 KB	1778960 B	7 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\638
639	7f7d008b6c11e6f2.png	1786996 B	24 KB	1787084 B	24 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\639
640	b5822127a7e4ea8.png	1812096 B	14 KB	1812182 B	14 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\640
641	1d9c30c84612c353.png	1826602 B	18 KB	1826690 B	18 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\641
642	74ae8704a1518abd.png	1845608 B	31 KB	1845696 B	31 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\642
643	deef37cedb9b7f6f.png	1877678 B	11 KB	1877766 B	11 KB					C:\Users\hyuunnnn\AppData\Local\Temp\IconCache\643

제31회(전승서 등) ① 천3호의 규정 이외에 피고인 또는 피고인이 아닌 자가 작성한 판술서나 그 판술을 기재한 서류로서 그 작성자 또는 판술자의 자필여부나 그 서명 또는 날인에 있는 것(피고인 또는 피고인 아닌 자가 작성하였거나 판술한 내용에 포함된 문자·사진·영상 등에 정보로서 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체에 저장된 것을 포함한다. 하하 이 조에서 같다)은 공판준비나 공판기밀에서 그 작성자 또는 판술자에 진술에 의하여 그 성립의 진정성이 증명된 때에는 증거로 할 수 있다. 단, 피고인의 판술을 기재한 서류는 공판준비 또는 공판기밀에서 그 작성자와 판술에 의하여 그 성립의 진정성이 증명되고 그 판술이 특히 신뢰할 수 있는 상태에서 행하여 질 때에 한하여 피고인의 공판준비 또는 공판기밀에서 그 판술에 불구하고 증거로 할 수 있다. <개정 2016.5.29.>

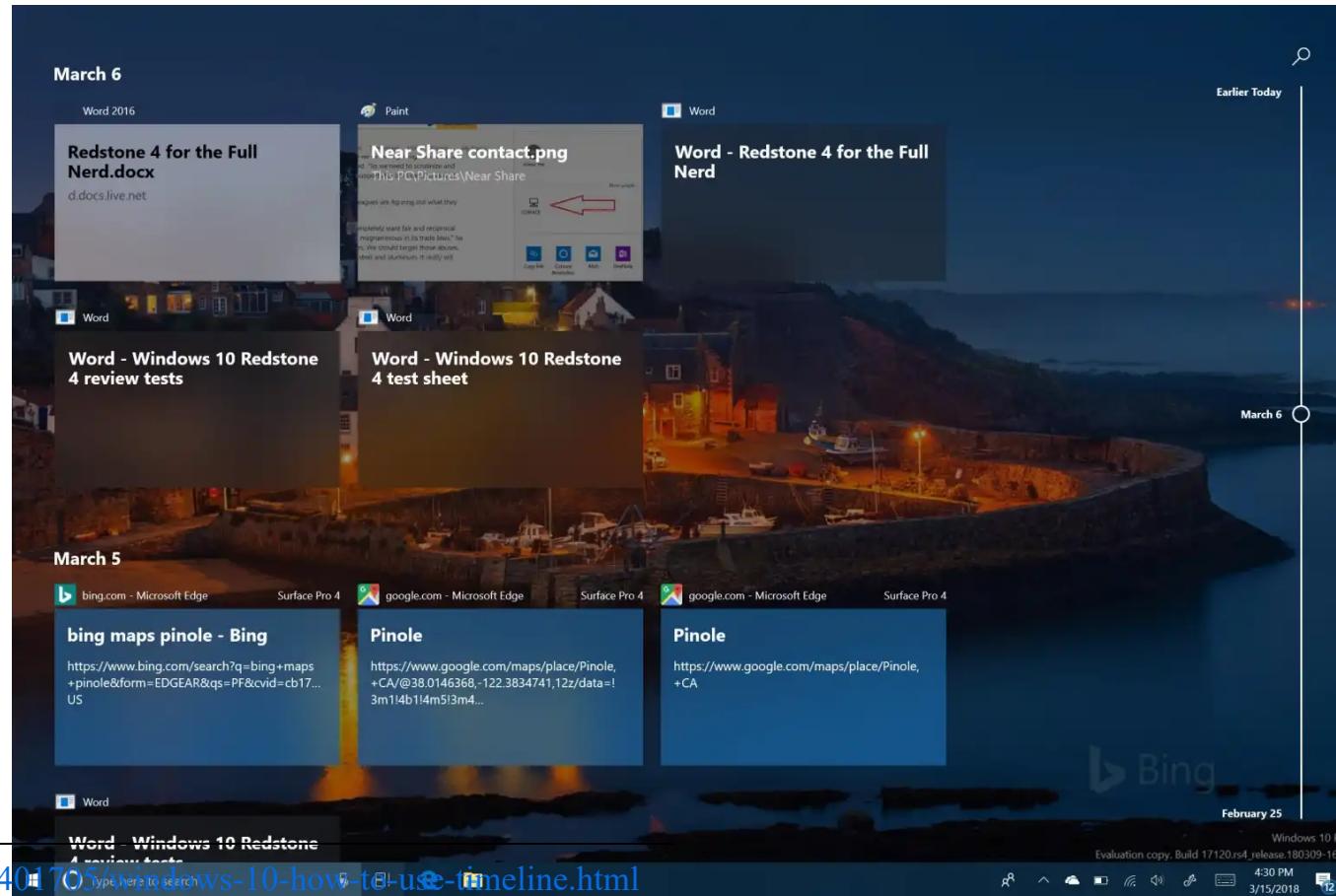
② 제1항 본문에도 불구하고 판술서의 작성자가 공판준비나 공판기밀에서 그 성립의 진정을 부인하는 경우에는 과학적 분석결과에 기초한 디지털표현식 저작, 감정 등 객관적 방법으로 성립의 진정성이 증명되는 때에는 증거로 할 수 있다. 다만, 피고인 아닌 자가 작성한 판술서는 피고인 또는 변호인이 공판준비 또는 공판기밀에 그 기대 내용에 관하여 작성자를 신문할 수 있었을 것을 보한다. <개정 2016.5.29.>

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 WxTCmd 사용하여 분석 가능 - 아래 사진은 WindowsTimeline 사용

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

File	Run	Tools			
ActivitiesCache.db	NTUser.dat	Current User			
Run	Exit				
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##User##AppData##Local##Temp##7B6F4FB3-790C-...				
250	C:\##Users##User##AppData##Local##Temp##7B6F4FB3-790C-...	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 아카텍처 차이.pdf	C:\##Users##...	file:///C:/Users/User/Downloads/x86 x86_64 아카텍처 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##...	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=mwalgzufvw&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		2024-01-22T12:34:25.0282762Z
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		2024-01-22T12:34:25.0232760Z

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

System_UserName	System_ItemName	System_ItemDate	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 hxd가 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, pioneer - Slides, forensic-proof, forensic-artifacts, forensic-cheatsheet, Forensics Wiki, ArtifactParsers, awesome 시리즈 - 1 2 3 4, FrequentlyAskedDFIRQuestions, The Hitchhikers Guide to DFIR: Experiences From Beginners and Experts, thisweekin4n6
 - 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.

과제

- Windows Timeline 분석 도구 만들어보기

- ActivitesCache.db 파일은 sqlite 파일이다.
- 파이썬 표준 라이브러리인 sqlite3 모듈을 사용하면 데이터를 읽어올 수 있다. - [docs](#)

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
C:\Users\User\Downloads\disable-defender (2).exe	ExecuteOpen	disable-defender (2).exe		2024-01-03 07:56:...	2024-02-02 07:5...	2024-01-03 ...		
MSEdge	InFocus			2024-01-03 08:01:...	2024-02-02 08:1...	2024-01-03 ...	2024-01-03 08...	00:16:12
Microsoft.Windows.Explorer	InFocus			2024-01-03 08:02:...	2024-02-02 08:1...	2024-01-03 ...	2024-01-03 08...	00:14:35
Microsoft.Windows.Photos_8wekyb3d8bbwe!App	ExecuteOpen	??????		2024-01-03 08:02:...	2024-02-02 08:0...	2024-01-03 ...		
Microsoft.Windows.Photos_8wekyb3d8bbwe!App	InFocus			2024-01-03 08:02:...	2024-02-02 08:0...	2024-01-03 ...	2024-01-03 08...	00:00:08
Microsoft.Windows.Photos_8wekyb3d8bbwe!App	InFocus			2024-01-03 08:02:...	2024-02-02 08:0...	2024-01-03 ...	2024-01-03 08...	00:00:03
Microsoft.Windows.Photos_8wekyb3d8bbwe!App	InFocus			2024-01-03 08:02:...	2024-02-02 08:0...	2024-01-03 ...	2024-01-03 08...	00:00:03
C:\Users\User\Downloads\winrar-x32-622.exe	ExecuteOpen	winrar-x32-622.exe		2024-01-03 08:04:...	2024-02-02 08:0...	2024-01-03 ...		
C:\Users\User\Downloads\winrar-x32-622.exe	InFocus			2024-01-03 08:04:...	2024-02-02 08:0...	2024-01-03 ...	2024-01-03 08...	00:00:02
*PID000017fc	ExecuteOpen	*PID000017fc		2024-01-03 08:04:...	2024-02-02 08:0...	2024-01-03 ...		
*PID000017fc	InFocus			2024-01-03 08:04:...	2024-02-02 08:0...	2024-01-03 ...	2024-01-03 08...	00:00:02