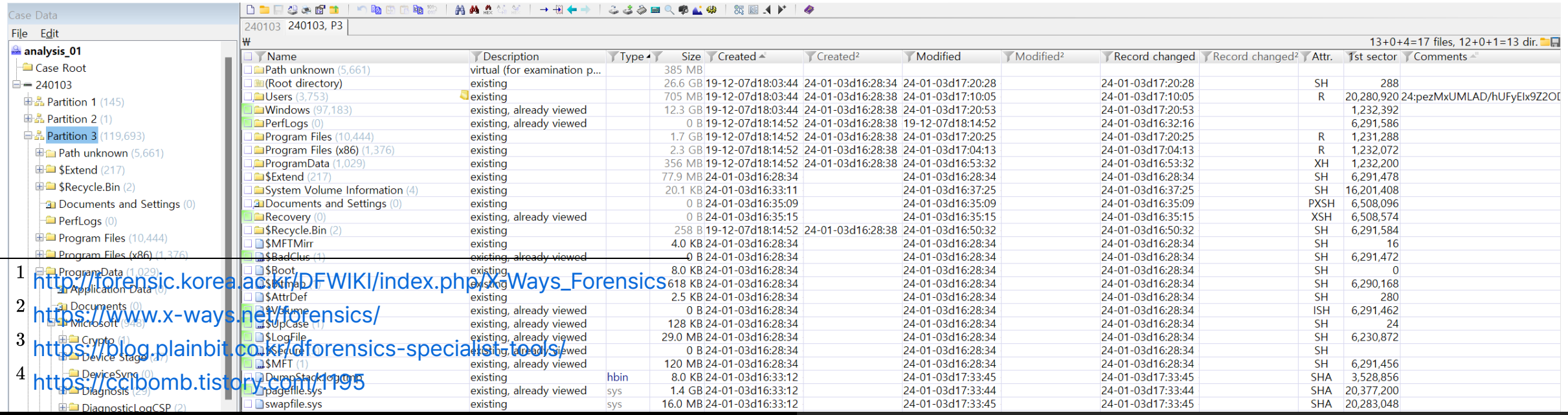
5주차 스터디

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

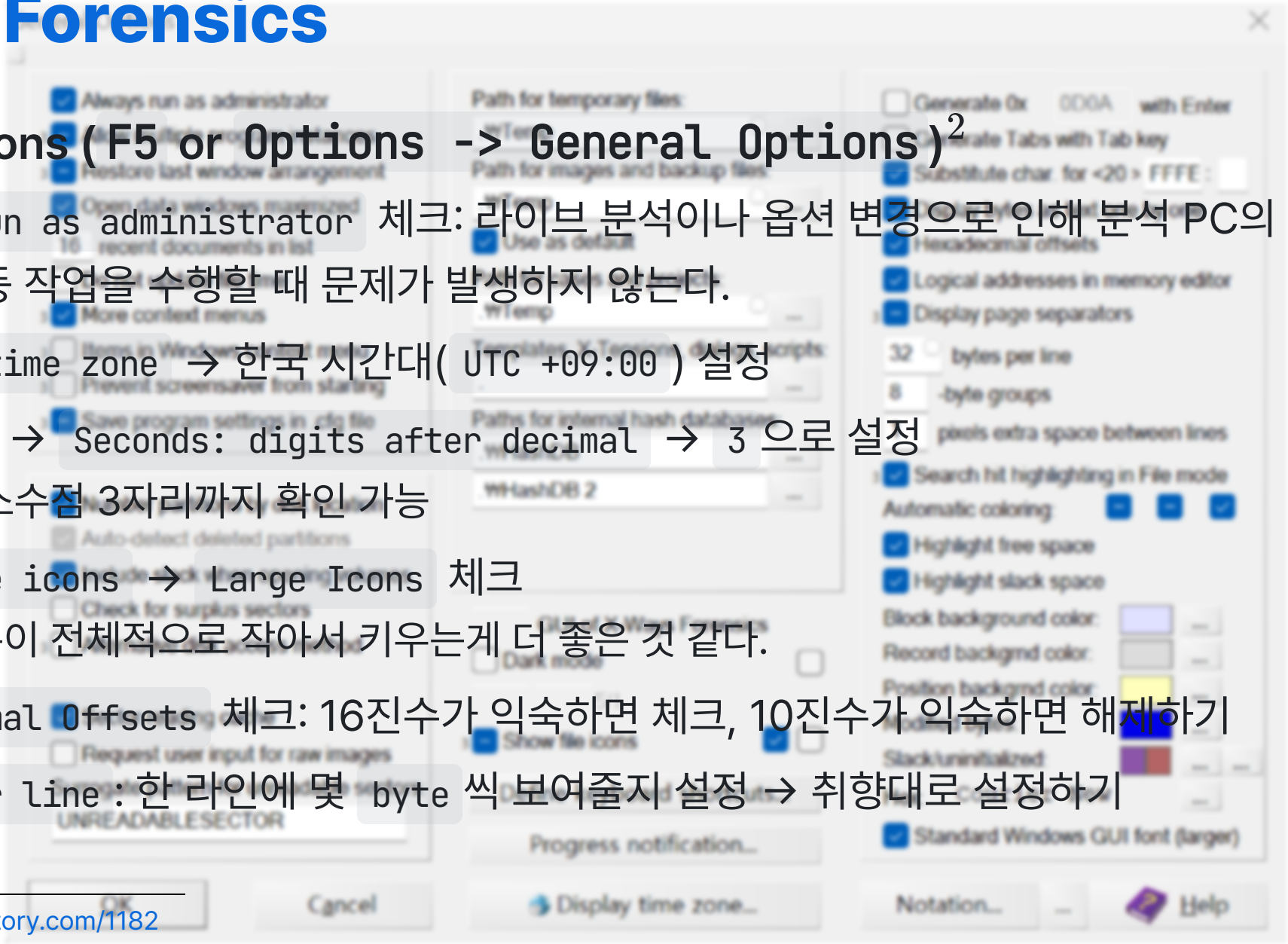
X-Ways Forensics

- 방대한 뷰어 컴포넌트, 파일 복구, 검색, RVS(Refine Volume Snapshot) 기능 등이 있다.[1][2]
- 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.



1 http://forensic.korea.ac.kr/DFWIKI/index.php/X-Ways_Forensics
2 https://www.x-ways.net/forensics/
3 https://blog.plainbit.co.kr/ccforensics-specialist-tools/
4 https://ccibomb.tistory.com/1195

X-Ways Forensics



General Options (F5 or Options -> General Options)[2]

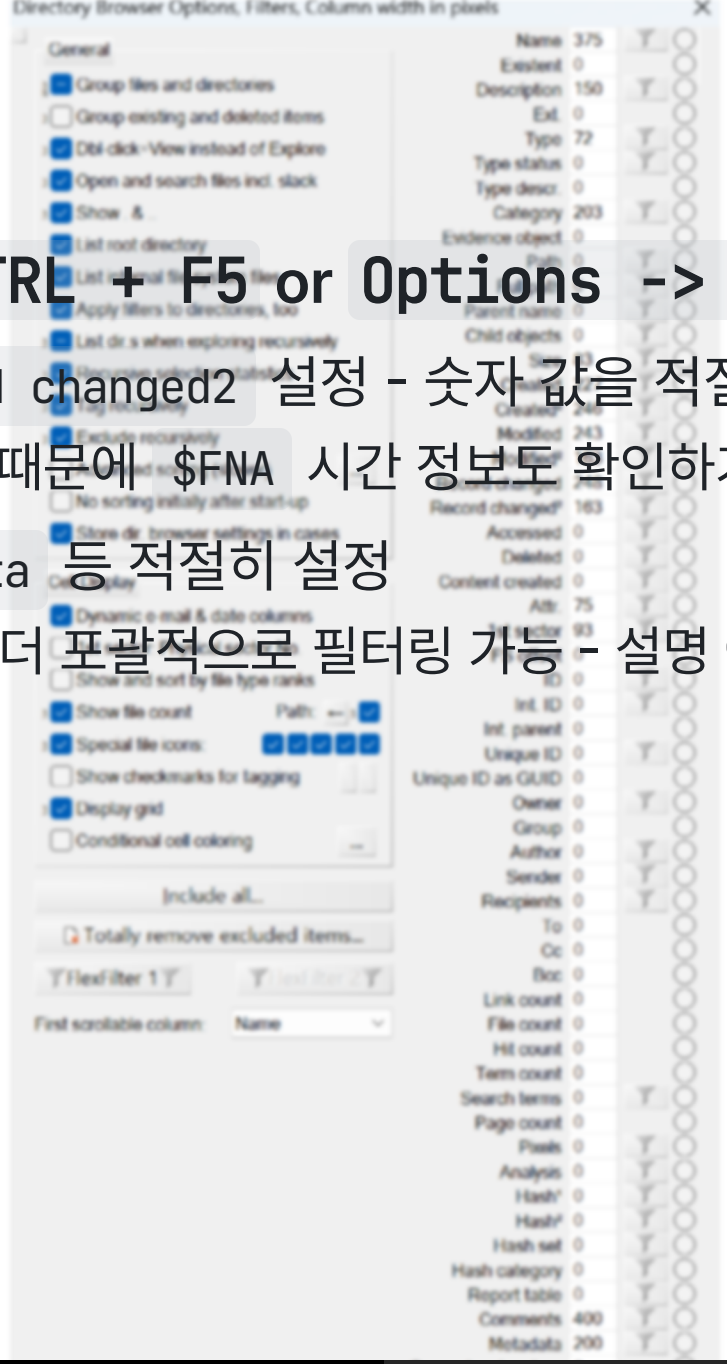
- `Always run as administrator` 체크: 라이브 분석이나 옵션 변경으로 인해 분석 PC의 레지스트리 값이 수정되는 등 작업을 수행할 때 문제가 발생하지 않는다.
- `Display time zone` → 한국 시간대(`UTC +09:00`) 설정
- `Notation` → `Seconds: digits after decimal` → `3` 으로 설정
  - 시간 소수점 3자리까지 확인 가능
- `Show file icons` → `Large Icons` 체크
  - 아이콘이 전체적으로 작아서 키우는게 더 좋은 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`)[3]

- `Created2`, `Modified2`, `Record changed2` 설정 - 숫자 값을 적절히 넣으면 된다.
  - `SIA`[1]의 변조 가능성이 있기 때문에 `$FNA` 시간 정보도 확인하기 위해 설정
- `Category`, `Comments`, `Metadata` 등 적절히 설정
  - `Catrgory`는 `Type` 보다 좀 더 포괄적으로 필터링 가능 - 설명 예정

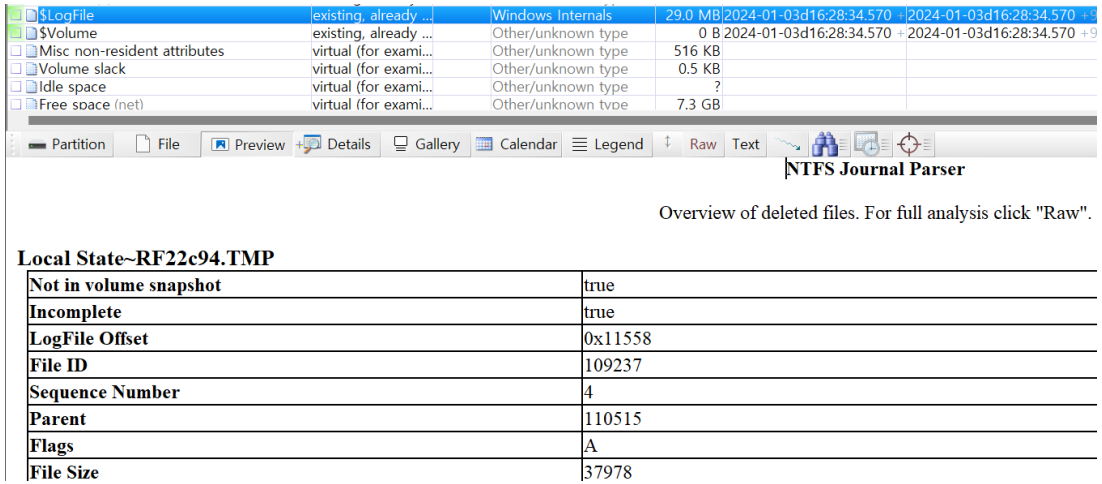


[1] SIA (Standard Information Attribute)
[2] $FNA ($FILE_NAME - NTFS 속성)
[3] https://ccibomb.tistory.com/1182

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.



$LogFile	existing, already ...		Windows Internals	29.0 MB	2024-01-03d16:28:34.570	2024-01-03d16:28:34.570
$Volume	existing, already ...		Other/unknown type	0 B	2024-01-03d16:28:34.570	2024-01-03d16:28:34.570
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		

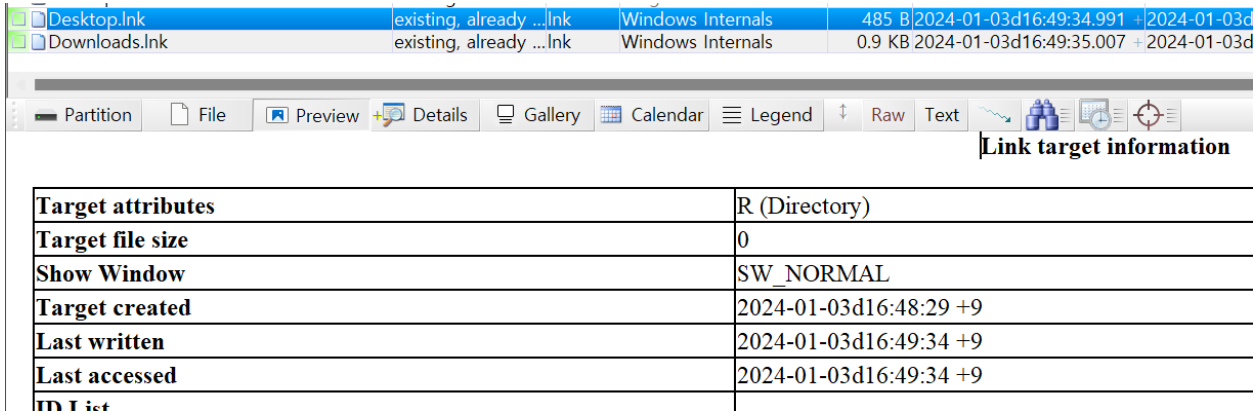
Partition | File | Preview | Details | Gallery | Calendar | Legend | Raw | Text

NTFS Journal Parser

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

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



Desktop.lnk	existing, already ...	lnk	Windows Internals	485 B	2024-01-03d16:49:34.991	2024-01-03d
Downloads.lnk	existing, already ...	lnk	Windows Internals	0.9 KB	2024-01-03d16:49:35.007	2024-01-03d

Partition | File | Preview | Details | Gallery | Calendar | Legend | Raw | Text

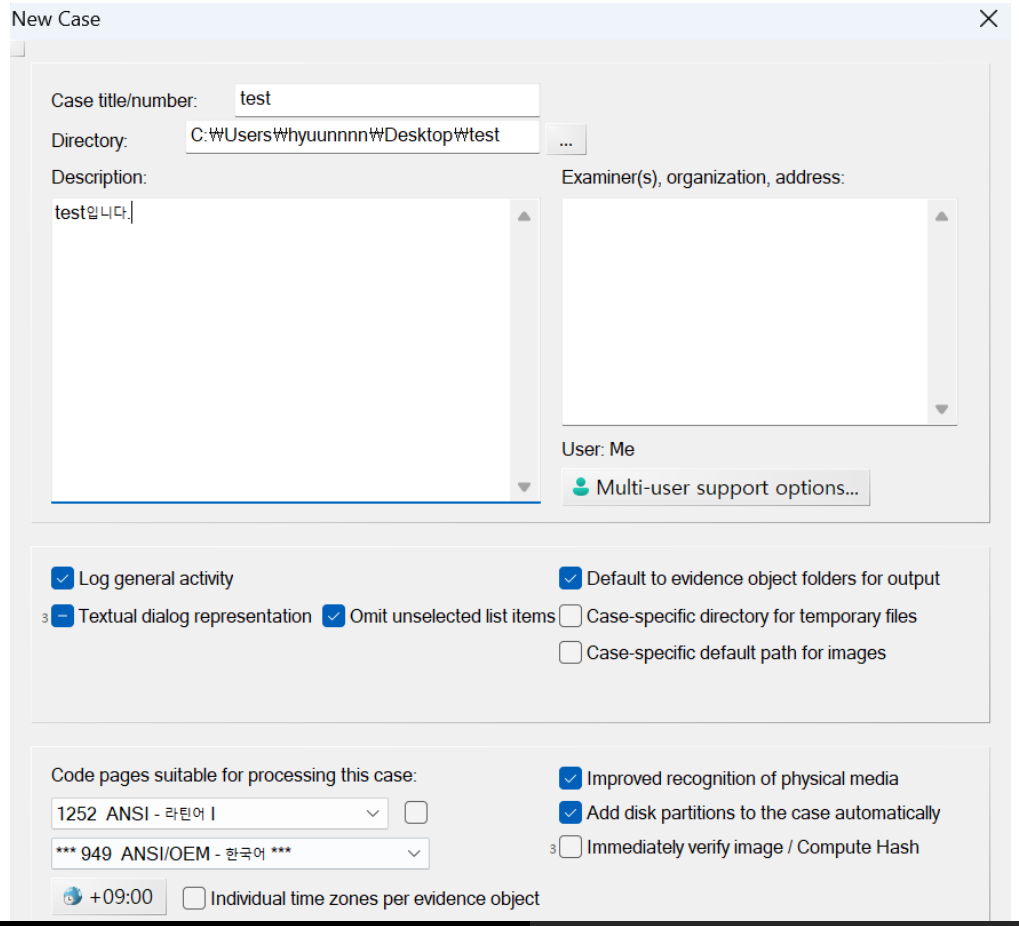
Link target information

Target attributes	R (Directory)
Target file size	0
Show Window	SW_NORMAL
Target created	2024-01-03d16:48:29 +9
Last written	2024-01-03d16:49:34 +9
Last accessed	2024-01-03d16:49:34 +9
ID List	

[1] https://ccibomb.tistory.com/1183

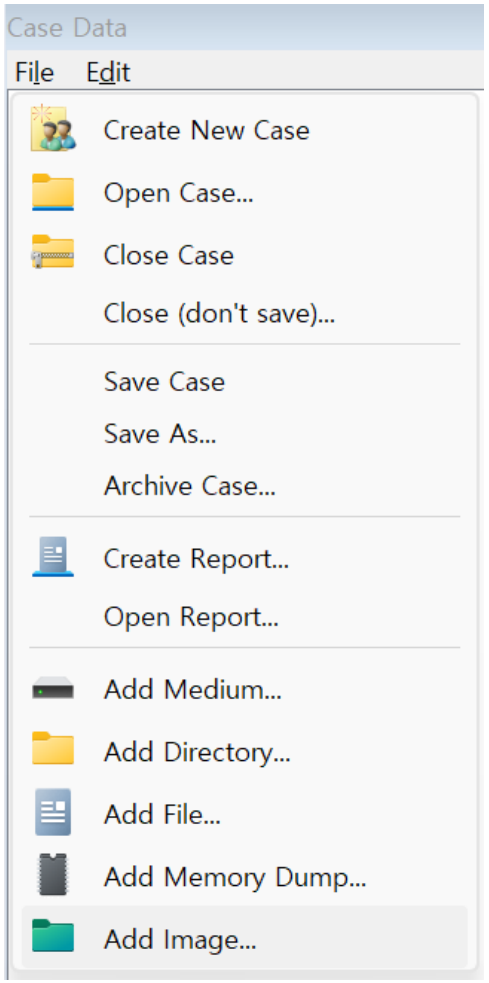
X-Ways Forensics

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

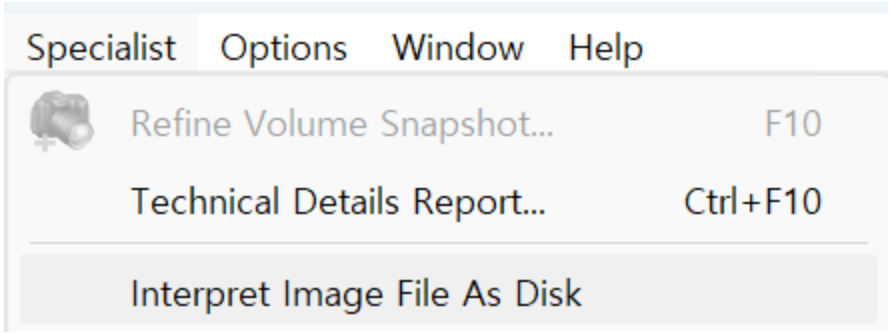


X-Ways Forensics

- `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 분석이 가능하다.

240103 | 240103, P3 | 240103

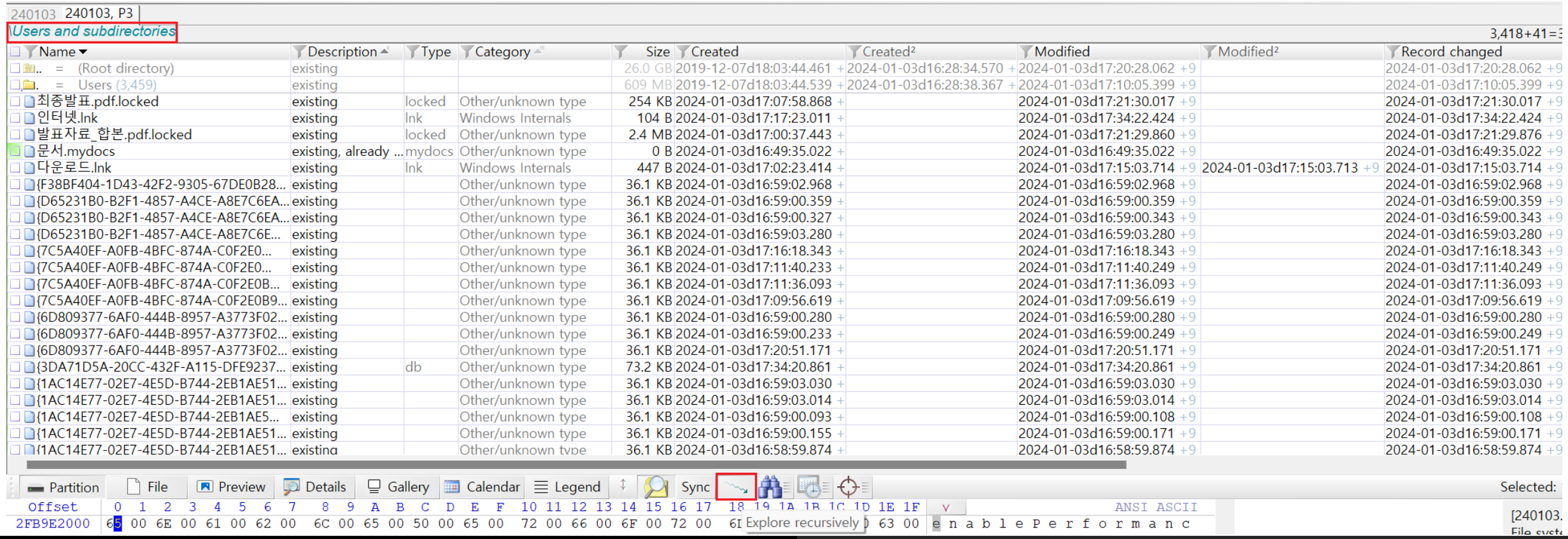
Partitioning style: GPT

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

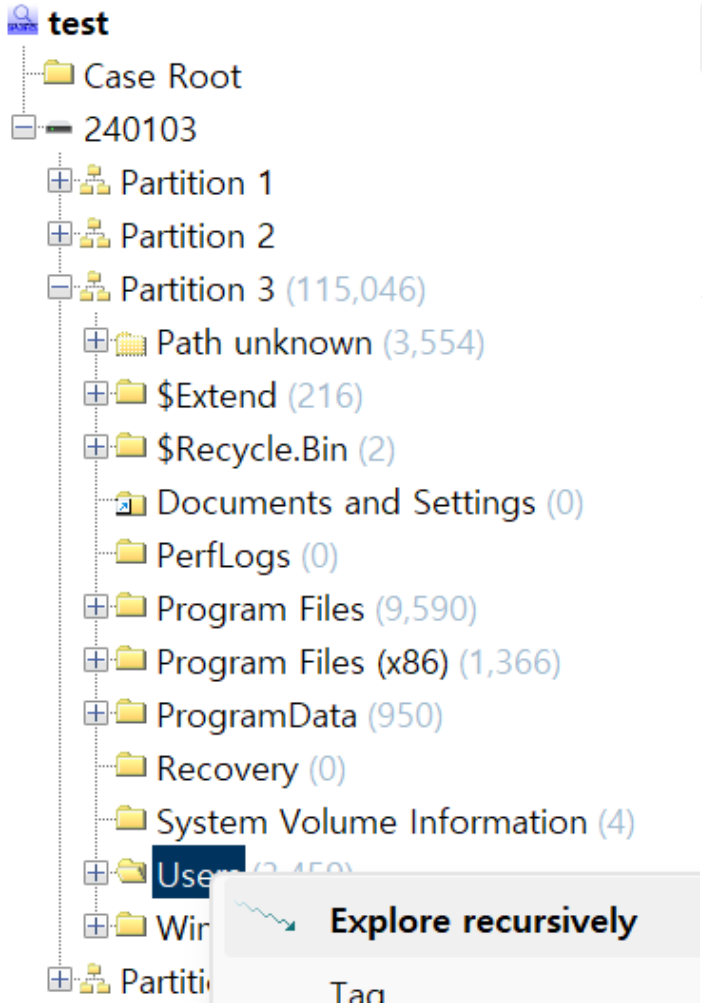
- 그러나 케이스를 만들어서 사용하는 방법이 더 편하고, 이점이 있기 때문에 케이스를 만들어서 사용하자.

X-Ways Forensics

- `Explore Recursively` : 재귀 탐색 기능
  - 현재 경로 이후로 존재하는 모든 파일들을 보여준다. - 폴더는 보여주지 않는다.
  - 특정 파일을 찾아야할 때 사진과 같은 상황에서 필터를 적용하면 수월하게 찾을 수 있다.



X-Ways Forensics



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

뒤로가기는 `Backspace` 이며, 매우 유용하다. - 재귀 탐색 상태에서 파일을 찾은 후 빠르게 재귀 탐색 기능을 끄고 싶을 때 `Backspace` 를 누르면 된다.

X-Ways Forensics

- 필터 기능
  - 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.

240103 | 240103, P3

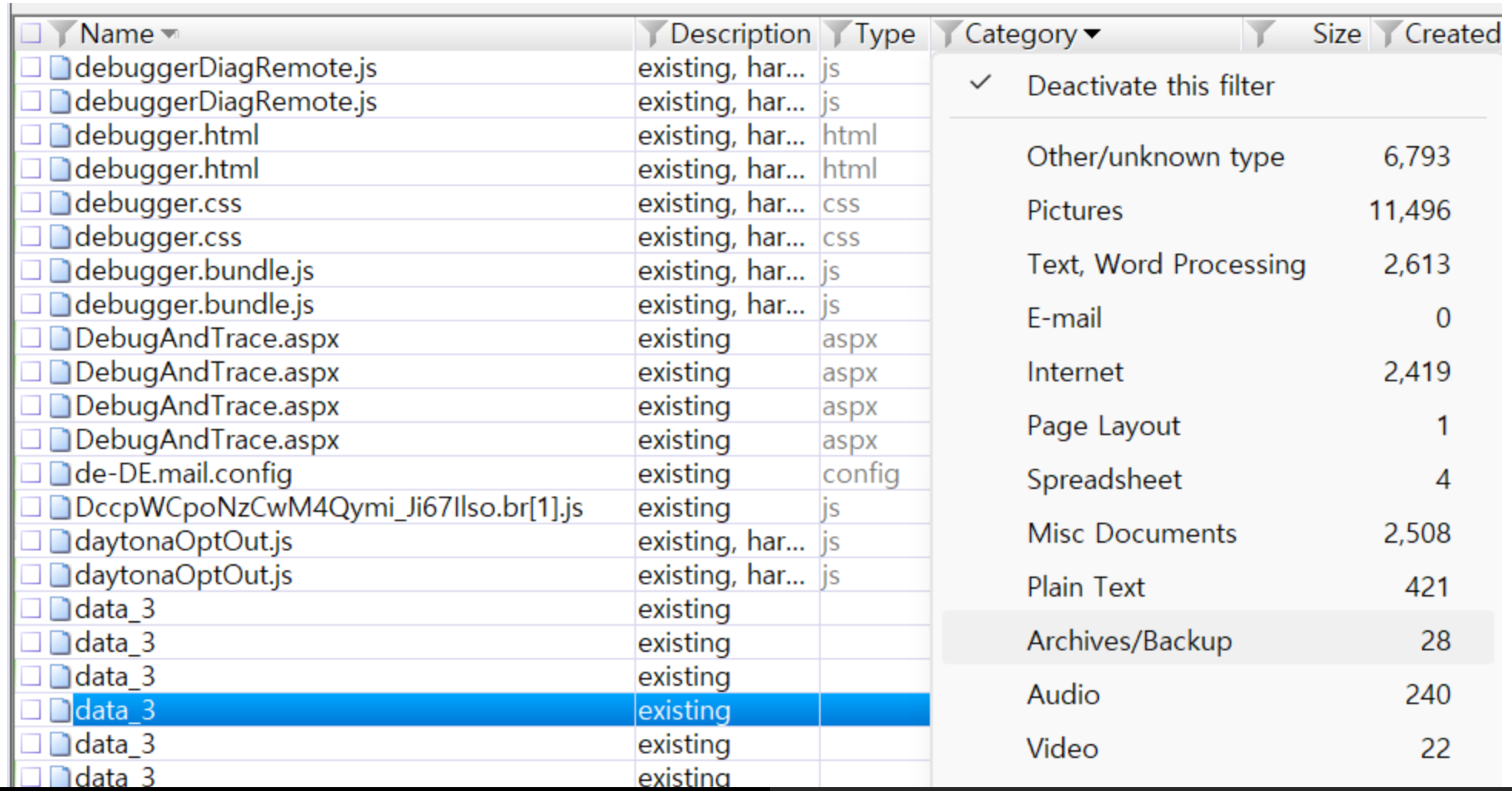
\Users and subdirectories

3,418+41=3

Name	Description	Type	Category	Size	Created	Created²	Modified	Modified²	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	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
{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
{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
{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
{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

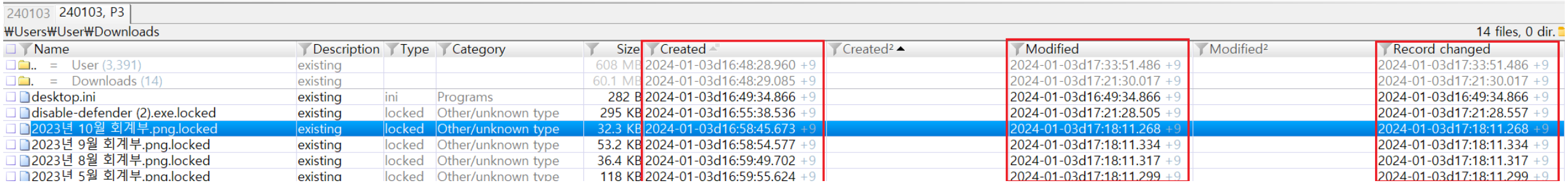
X-Ways Forensics

- `Category` 리스트를 보면 `Type` 보다 큰 범주로 묶어서 보여주는 것을 확인할 수 있다.



X-Ways Forensics

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

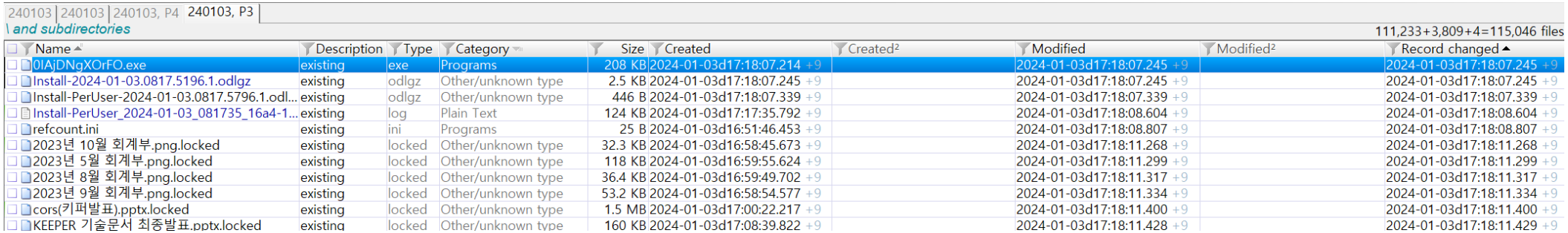


240103 | 240103, P3

₩Users₩User₩Downloads — 14 files, 0 dir.

Name	Description	Type	Category	Size	Created	Created²	Modified	Modified²	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.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

- 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	Created²	Modified	Modified²	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.odl...	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(키퍼발표).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

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

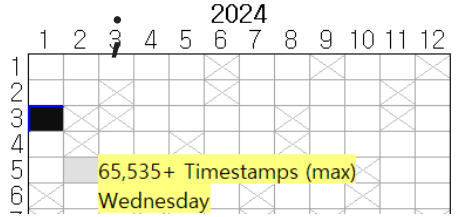
240103 | 240103, P3

1 \ and subdirectories

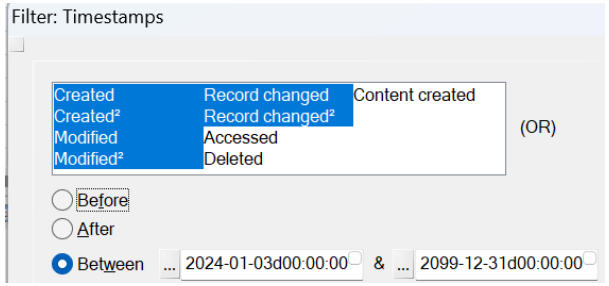
+1,220 +3,309 +119,029 files; 32,475 +1,729 +2 +36,204 dir.; 30 filtered out

Name	Description	Type	Category	Size	Created	Created²	Modified	Modified²	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
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		2024-01-03d16:33:25.365 +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		2024-01-03d16:33:23.725 +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		2024-01-03d16:32:16.586 +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		2024-01-03d16:32:16.617 +9
BitLocker (2)	existing			4.7 KB	2024-01-03d16:33:23.725 +9		2024-01-03d16:33:25.350 +9		2024-01-03d16:33:25.350 +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		2024-01-03d17:35:41.419 +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		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
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
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
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		2024-01-03d16:29:32.039 +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		2024-01-03d16:29:32.039 +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		2024-01-03d16:29:32.039 +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	2024-01-03d16:29:32.039 +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
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
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		2024-01-03d16:31:55.945 +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		2024-01-03d16:31:55.945 +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		2024-01-03d16:31:55.945 +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	2024-01-03d16:31:55.945 +9	2024-01-03d16:31:55.945 +9
BioIso.exe	existing	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

Partition | File | Preview | Details | Gallery | Calendar | Legend | Sync | Selected: 1 file (22.2



2024. 01. 03 클릭 → 1월 3일 이후 필터 적용



X-Ways Forensics

- `Volume Snapshot (VS)`[1]
  - X-Ways Forensics의 핵심 기능
  - 증거 객체들의 데이터, 관련 정보들을 저장하는 데이터베이스
  - 도구상의 모든 분석 결과들이 `VS` 에 저장된다. → `Volume Snapshot Options` 에서 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://ccibomb.tistory.com/1189
[2] http://www.forensic-artifacts.com/xways-forensics/sub03
[3] http://www.forensic-artifacts.com/xways-forensics/sub09
[4] https://www.xwaysclips.co.uk/2012/09/understanding-volume-snapshot-of-x-ways.html
[5] https://www.x-ways.net/forensics/QuickGuide.pdf, https://youtu.be/ggSXfAf4Eko

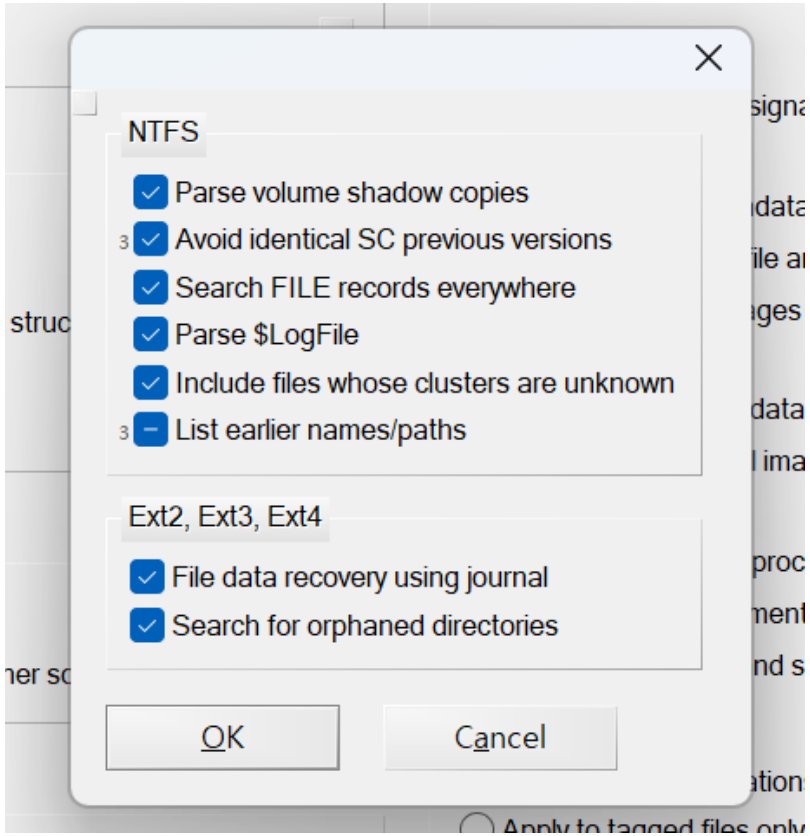
X-Ways Forensics

- `Refine Volume Snapshot(RVS)`
  - `File header signature search`, `Verify file types with signatures and algorithms`
    - 파일 복구, 확장자 검증 등을 수행하는 옵션
    - 다른 확장자로 위장한 파일들을 시그니처 기반으로 탐지 및 검증
    - `File Type Signatures *.txt` 파일 참고

	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	₩xFF₩xD8₩xFF[₩xC0₩xC4₩xDB₩xDD₩xE0-₩xE5₩xE7	0	~1	2097152/33554432	e
4	PNG	png	₩x89PNG₩x0D₩x0A₩x1A₩x0A	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..₩x00₩x00.[^₩x00]	0	~84	2097152/511705088	GUb
8	TIFF/NEF/CR2/DNG	tif;tiff;nef;cr2;dng;pef;nrw;arw	(₩x49₩x49₩x2A₩x00)|(₩x4D₩x4D₩x00₩x2A)	0	~5	25165824/268435456	
9	Bitmap	bmp;dib	BM.....₩x00.₩x00....[₩x0C₩x28₩x38₩x40₩x6C₩x7C]₩›	0	~4		
10	Paint Shop Pro	psp;PspImage;pfr	(Paint Shop Pro Im)|(~BK₩x00)	0	~8	2097152	b
11	Canon Raw	crw	HEAPCCDR	6		8200000	c
12	Adobe Photoshop	PSD;pdd;p3m;p3r;p3l	8BPS₩x00₩x01₩x00₩x00₩x00₩x00₩x00₩x00	0	~9	10485760	b

X-Ways Forensics

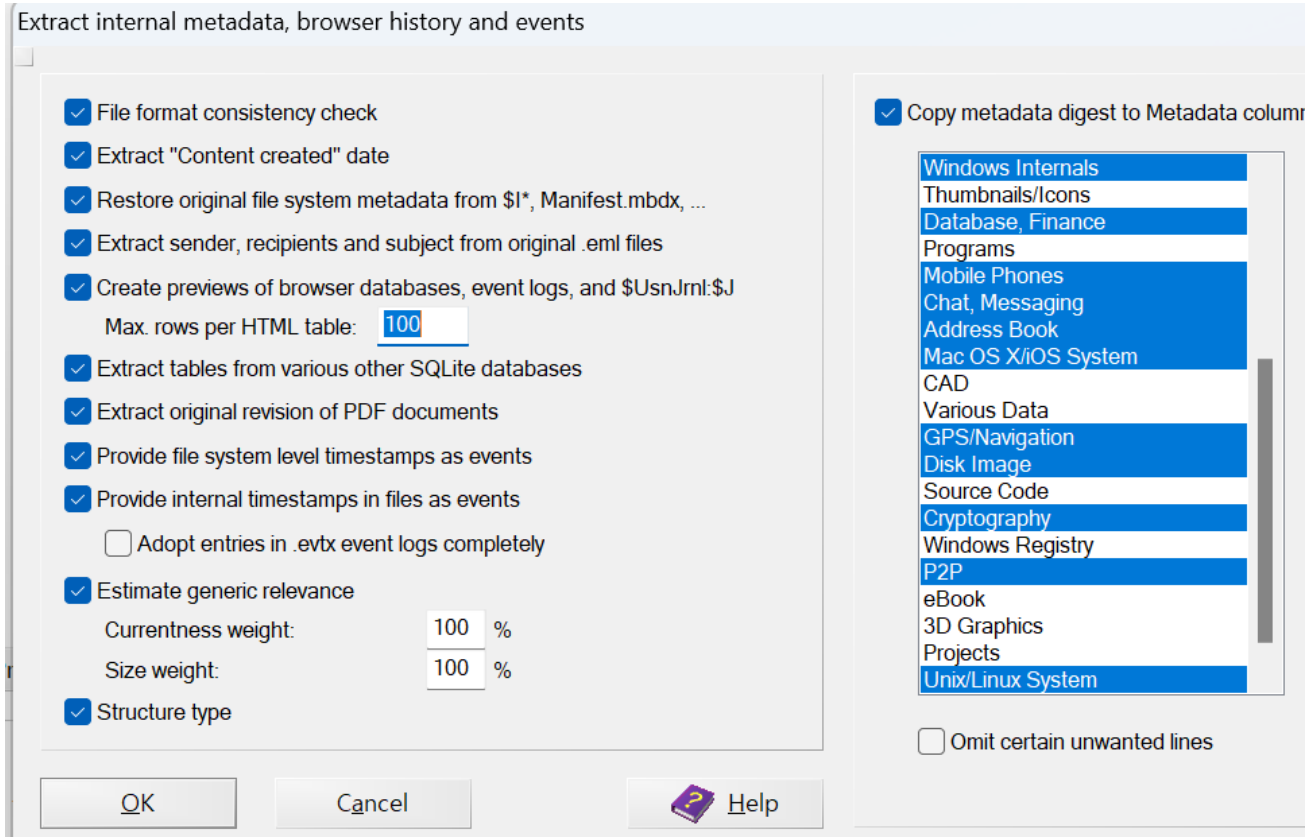
- `Refine Volume Snapshot(RVS)`
  - `Particularly thorough file system data structure search` : 파일시스템 관련 분석



X-Ways Forensics

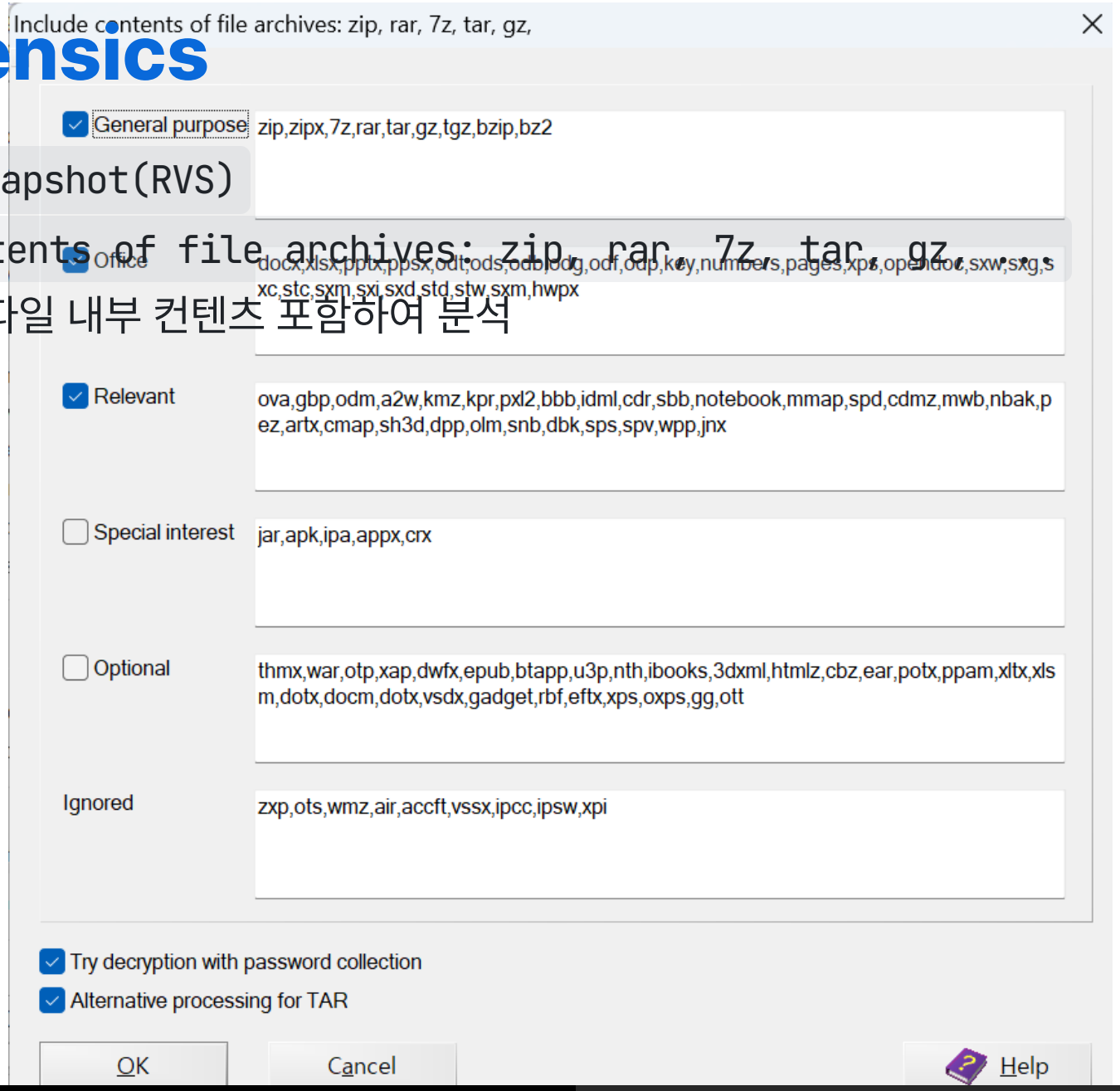
- `Refine Volume Snapshot(RVS)`
  - `External internal metadata, browser history and events`

    → 일관성 검사(consistency check), 메타데이터 추출 및 각종 아티팩트 분석



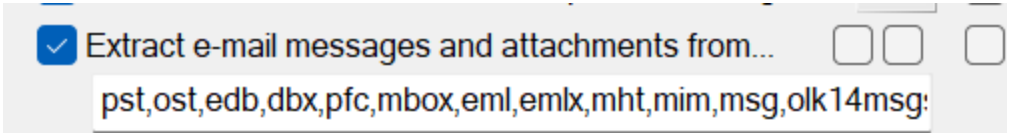
X-Ways Forensics

- Refine Volume Snapshot(RVS)
  - Include contents of file archives: zip, rar, 7z, tar, gz, ...
    - 아카이브 파일 내부 컨텐츠 포함하여 분석

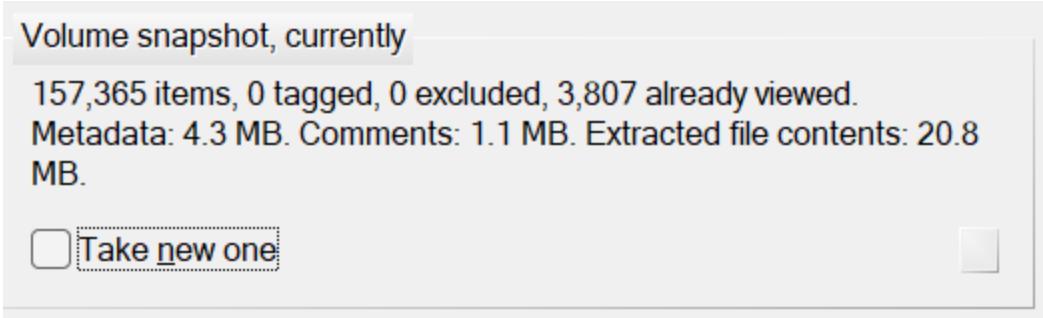


X-Ways Forensics

- `Refine Volume Snapshot(RVS)`
  - `Extract e-mail messages and attachments from...`
    - `pst`, `ost`, `edb`, `eml` 등에 존재하는 이메일 메세지 추출

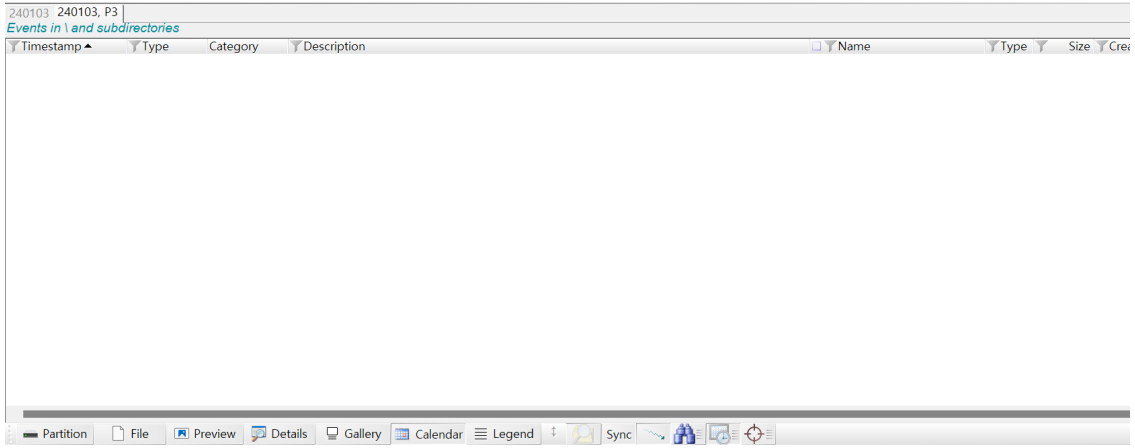


- RVS 완료 후 다시 들어가면 현재까지 수집된 Volume Snapshot 확인 가능

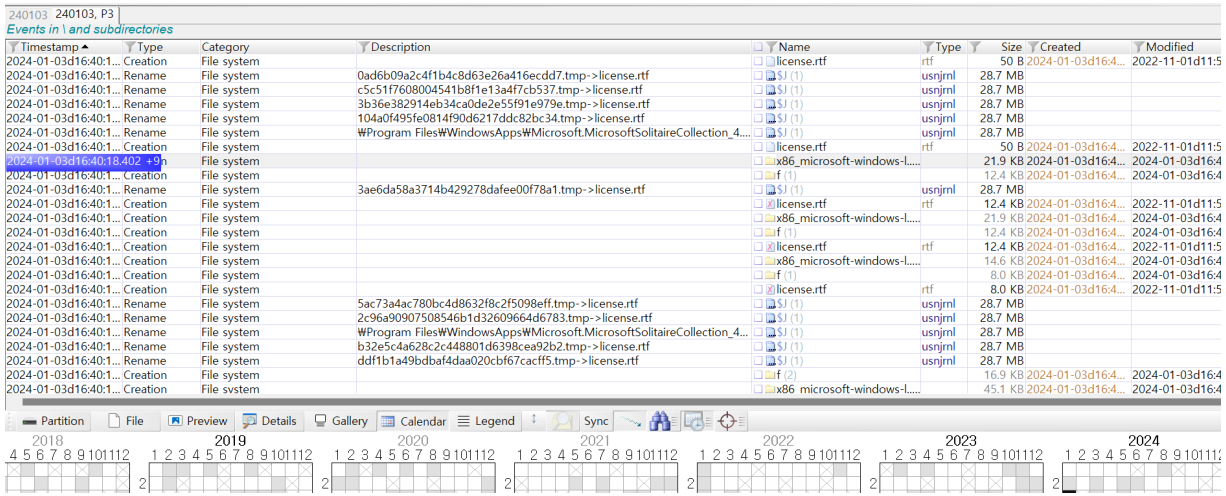


X-Ways Forensics

- `Events` : `RVS` 로 분석된 이벤트 확인 가능



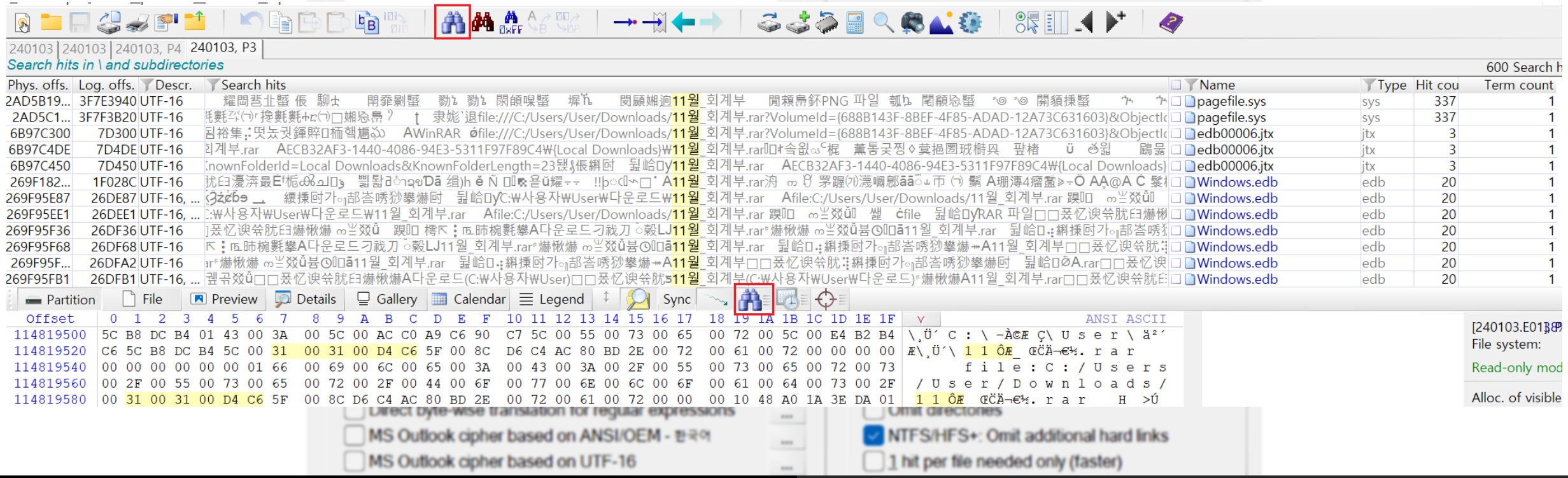
Before



After

X-Ways Forensics

- `Simultaneous Search`
  - 여러 단어들을 검색할 수 있는 기능
  - 상단 아이콘 버튼으로 사용 가능
  - 하단 아이콘 버튼으로 검색 결과 확인



참고자료

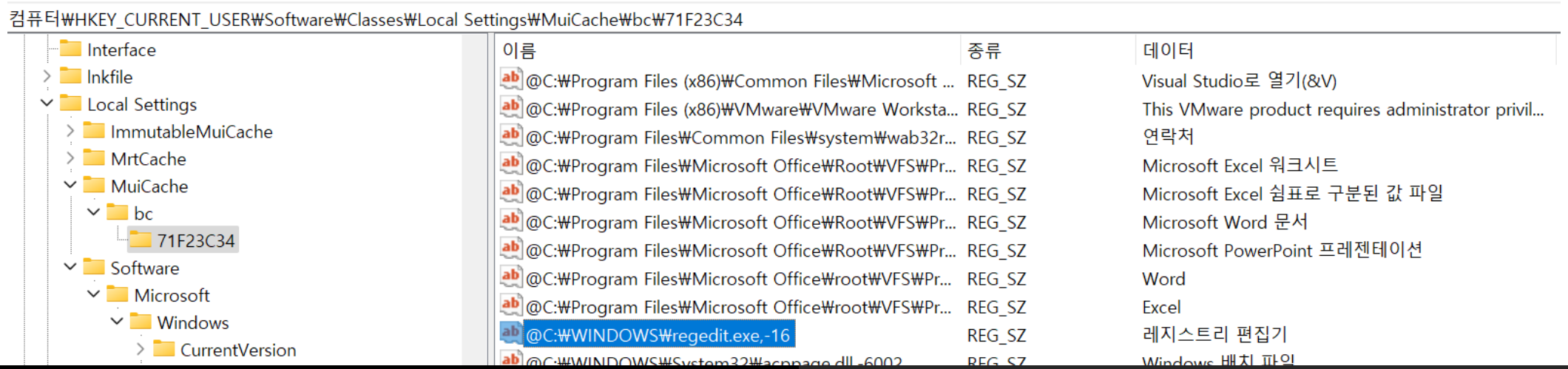
- Youtube - X-Ways Software Technology AG, TED SMITH
- Blog - ccibomb, goblinforensics
- X-Ways 실무 활용 가이드
- X-Ways - XWFQuickStart, QuickGuide, manual
- XWF를 이용한 포렌식 분석

MUICache

- 윈도우 환경에서 다중 언어를 지원하기 위해 존재하는 캐시
- 예를 들어 윈도우 내장 프로그램인 `regedit` 은 `레지스트리 편집기` , `taskmgr` 는 `작업 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`



참고자료

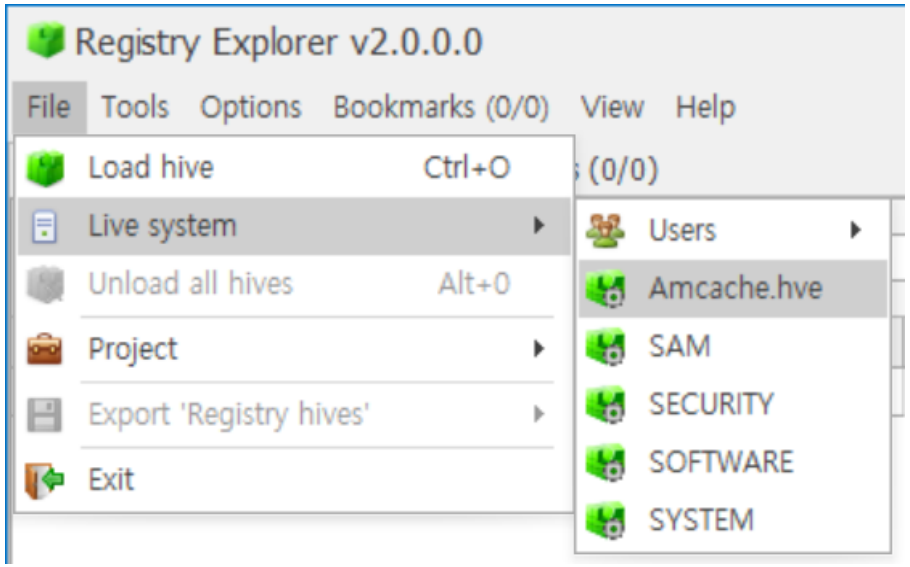
- MUICache - forensic-artifacts
- 기초부터 따라하는 디지털포렌식
- Forensic Analysis of MUICache Files in Windows

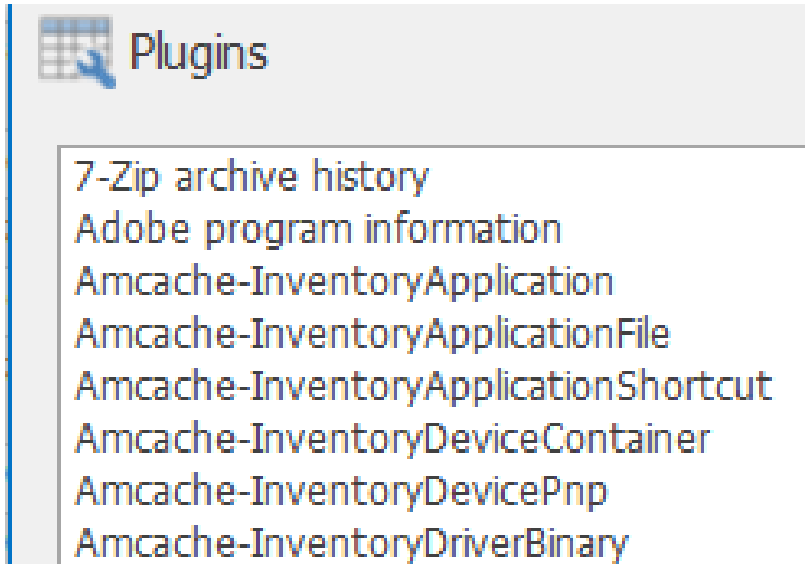
AmCache & ShimCache (AppCompatCache)

- 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 Zimmerman의 `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

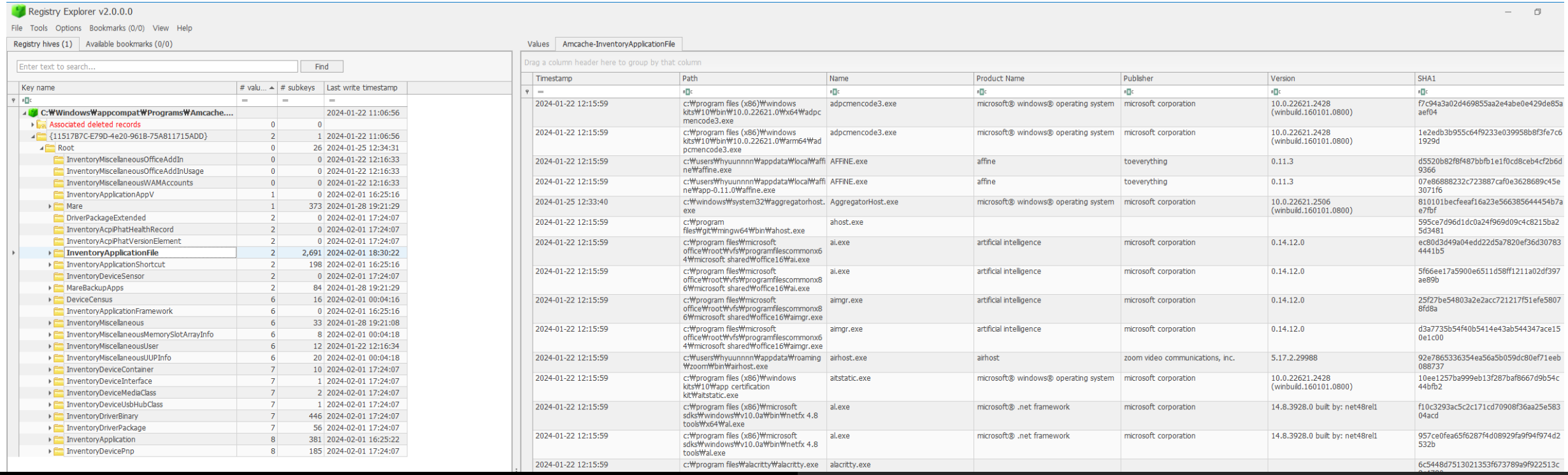




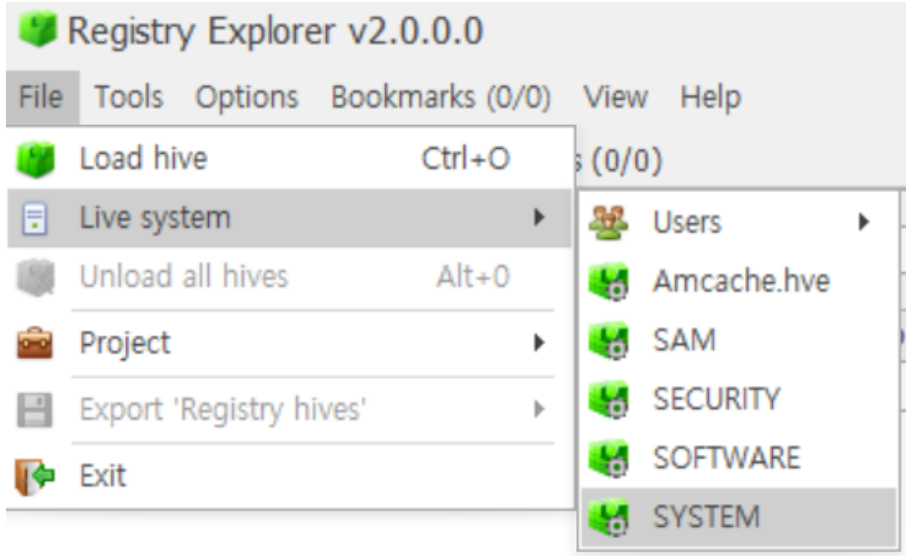
- `InventoryApplicationFile`, `InventoryDeviceContainer` 등 프로그램 실행 정보, 외부 장치 연결 정보, 최초 또는 마지막 연결, 설치 시간 등 확인할 수 있다.

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.



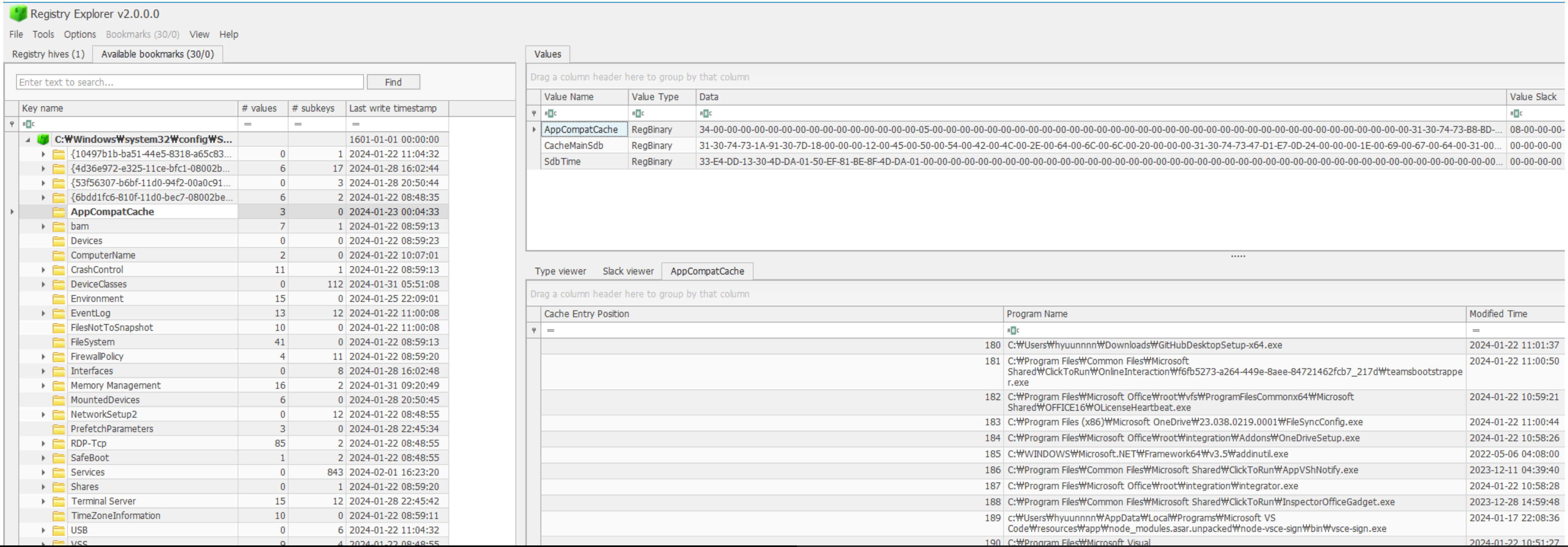
ShimCache (AppCompatCache)



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

ShimCache (AppCompatCache)

- `MUICache`, `Prefetch`, `Amcache`, `ShimCache`, `FeatureUsage`, `AppCompatFlags`, `BAM (Background Activity Moderator)` 등을 활용하여 악성 파일 탐지에 유용한 정보들을 얻을 수 있다.
    - `FeatureUsage` ~ `BAM` 도 실행 파일과 관련된 정보들을 얻을 수 있다. - 1주차 슬라이드에 언급함



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 제공[1]

```
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

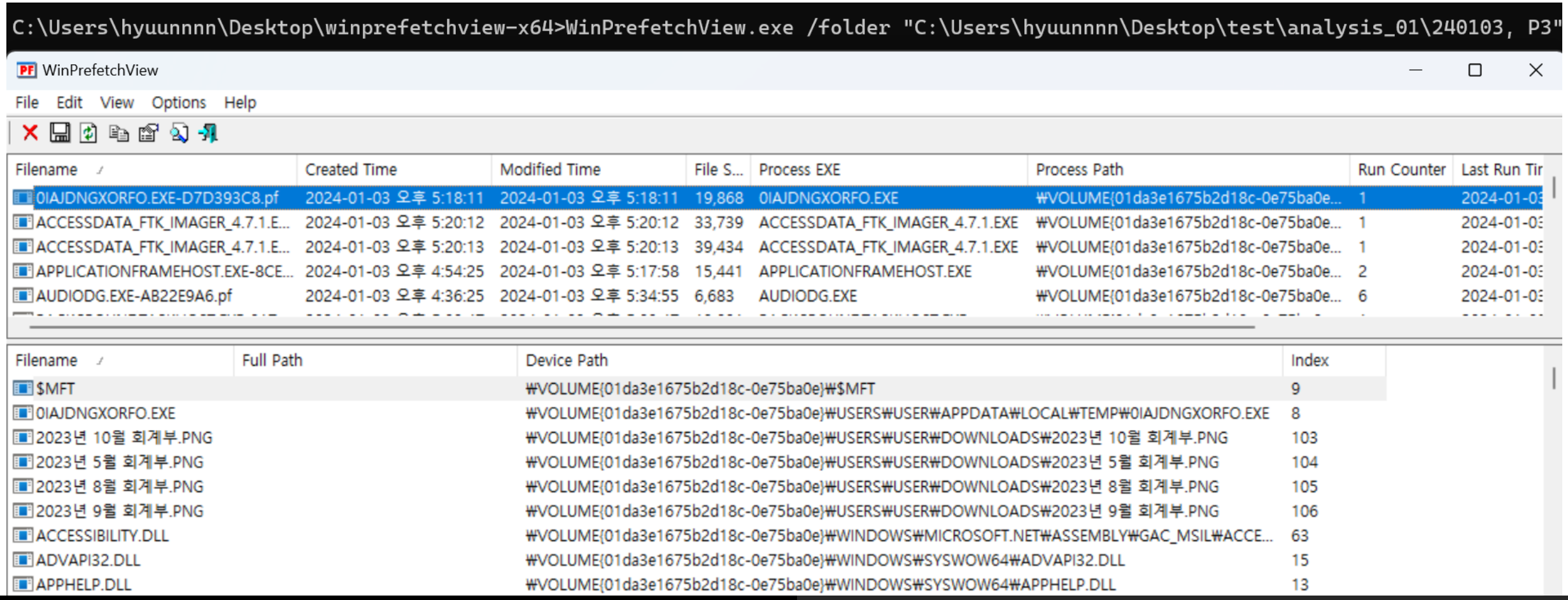
Prefetch (프리패치)

- 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`
- WinPrefetchView를 사용할 예정
  - Eric Zimmerman의 도구를 사용하고 싶다면 PECmd 사용해도 좋다.
    → Costas라는 사람이 만든 Prefetch-Browser도 있다.

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

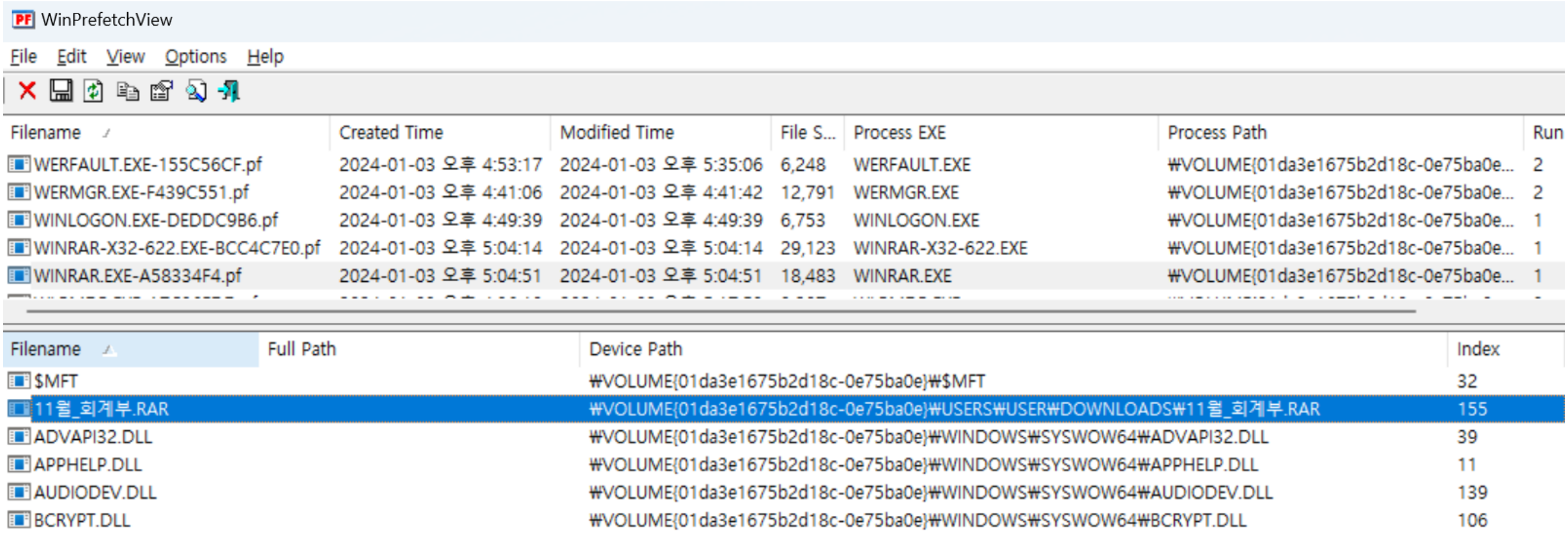
Prefetch (프리패치)

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



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.

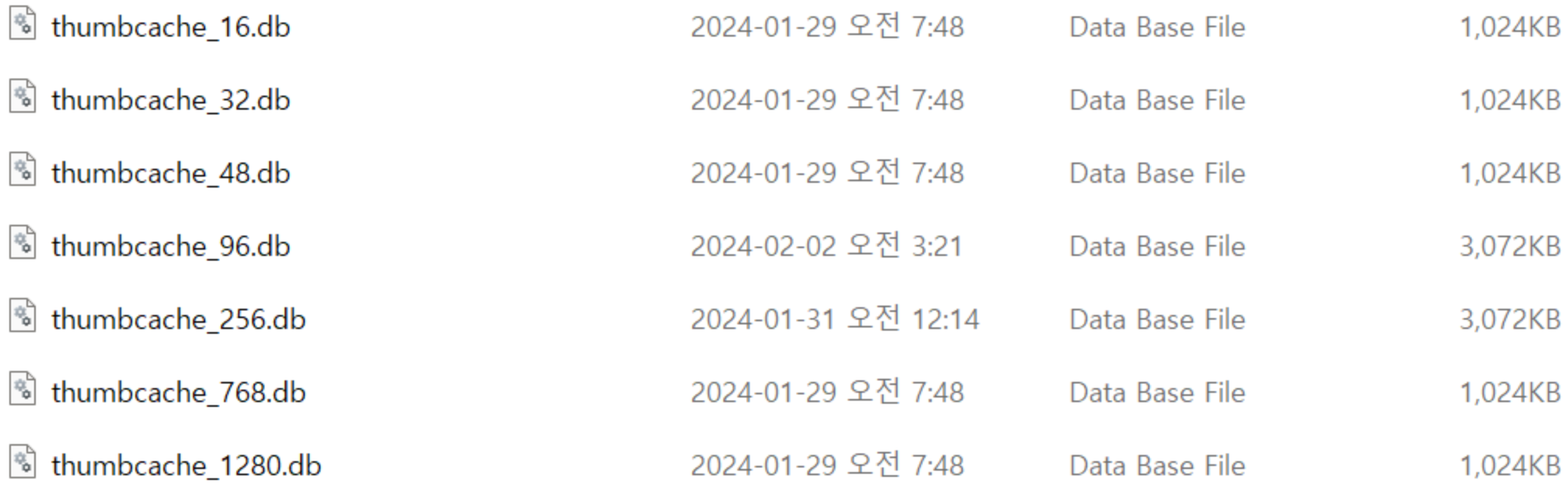


참고자료

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

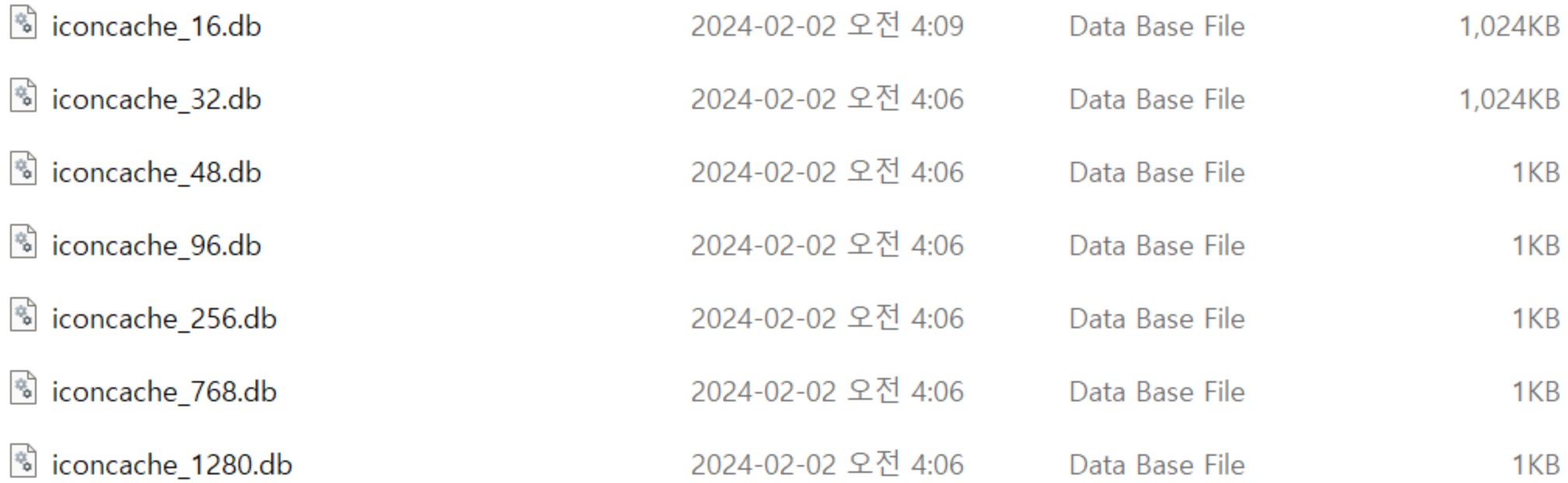
ThumbnailCache & IconCache

- `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.



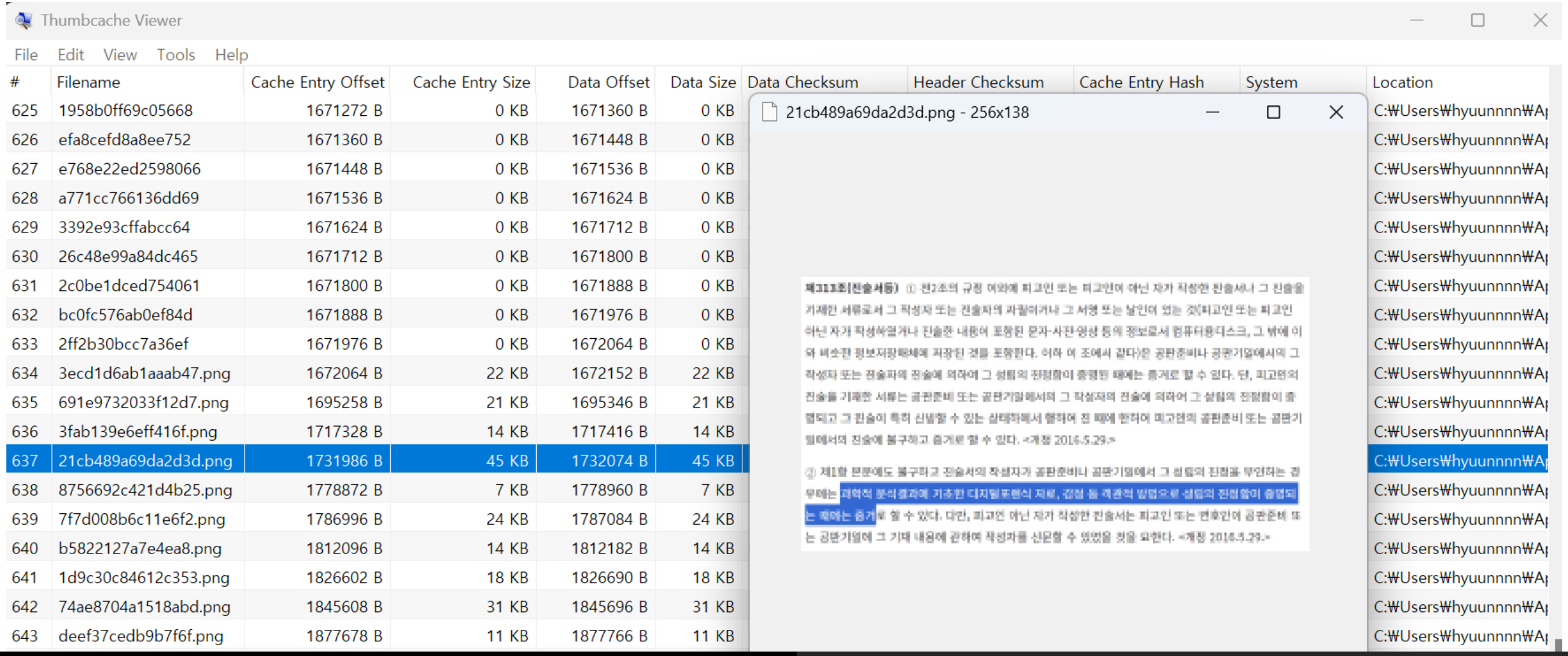
ThumbnailCache & IconCache

- `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.



ThumbnailCache & IconCache

- Thumbcache Viewer 도구를 사용하여 분석 가능



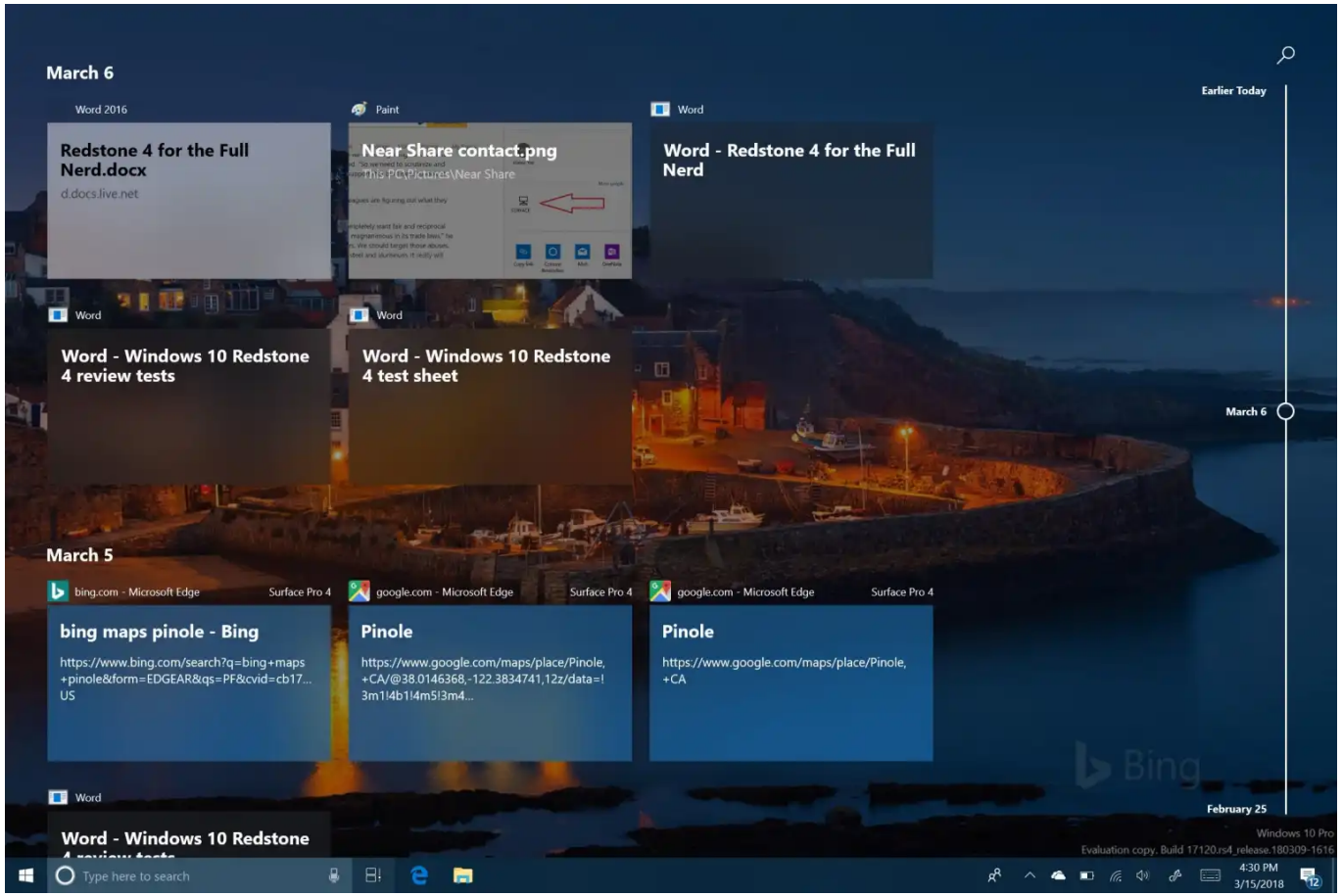
#	Filename	Cache Entry Offset	Cache Entry Size	Data Offset	Data Size	Data Checksum	Header Checksum	Cache Entry Hash	System	Location
625	1958b0ff69c05668	1671272 B	0 KB	1671360 B	0 KB					C:₩Users₩hyuunnnn₩A
626	efa8cefd8a8ee752	1671360 B	0 KB	1671448 B	0 KB					C:₩Users₩hyuunnnn₩A
627	e768e22ed2598066	1671448 B	0 KB	1671536 B	0 KB					C:₩Users₩hyuunnnn₩A
628	a771cc766136dd69	1671536 B	0 KB	1671624 B	0 KB					C:₩Users₩hyuunnnn₩A
629	3392e93cffabcc64	1671624 B	0 KB	1671712 B	0 KB					C:₩Users₩hyuunnnn₩A
630	26c48e99a84dc465	1671712 B	0 KB	1671800 B	0 KB					C:₩Users₩hyuunnnn₩A
631	2c0be1dced754061	1671800 B	0 KB	1671888 B	0 KB					C:₩Users₩hyuunnnn₩A
632	bc0fc576ab0ef84d	1671888 B	0 KB	1671976 B	0 KB					C:₩Users₩hyuunnnn₩A
633	2ff2b30bcc7a36ef	1671976 B	0 KB	1672064 B	0 KB					C:₩Users₩hyuunnnn₩A
634	3ecd1d6ab1aaab47.png	1672064 B	22 KB	1672152 B	22 KB					C:₩Users₩hyuunnnn₩A
635	691e9732033f12d7.png	1695258 B	21 KB	1695346 B	21 KB					C:₩Users₩hyuunnnn₩A
636	3fab139e6eff416f.png	1717328 B	14 KB	1717416 B	14 KB					C:₩Users₩hyuunnnn₩A
637	21cb489a69da2d3d.png	1731986 B	45 KB	1732074 B	45 KB					C:₩Users₩hyuunnnn₩A
638	8756692c421d4b25.png	1778872 B	7 KB	1778960 B	7 KB					C:₩Users₩hyuunnnn₩A
639	7f7d008b6c11e6f2.png	1786996 B	24 KB	1787084 B	24 KB					C:₩Users₩hyuunnnn₩A
640	b5822127a7e4ea8.png	1812096 B	14 KB	1812182 B	14 KB					C:₩Users₩hyuunnnn₩A
641	1d9c30c84612c353.png	1826602 B	18 KB	1826690 B	18 KB					C:₩Users₩hyuunnnn₩A
642	74ae8704a1518abd.png	1845608 B	31 KB	1845696 B	31 KB					C:₩Users₩hyuunnnn₩A
643	deef37cedb9b7f6f.png	1877678 B	11 KB	1877766 B	11 KB					C:₩Users₩hyuunnnn₩A

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

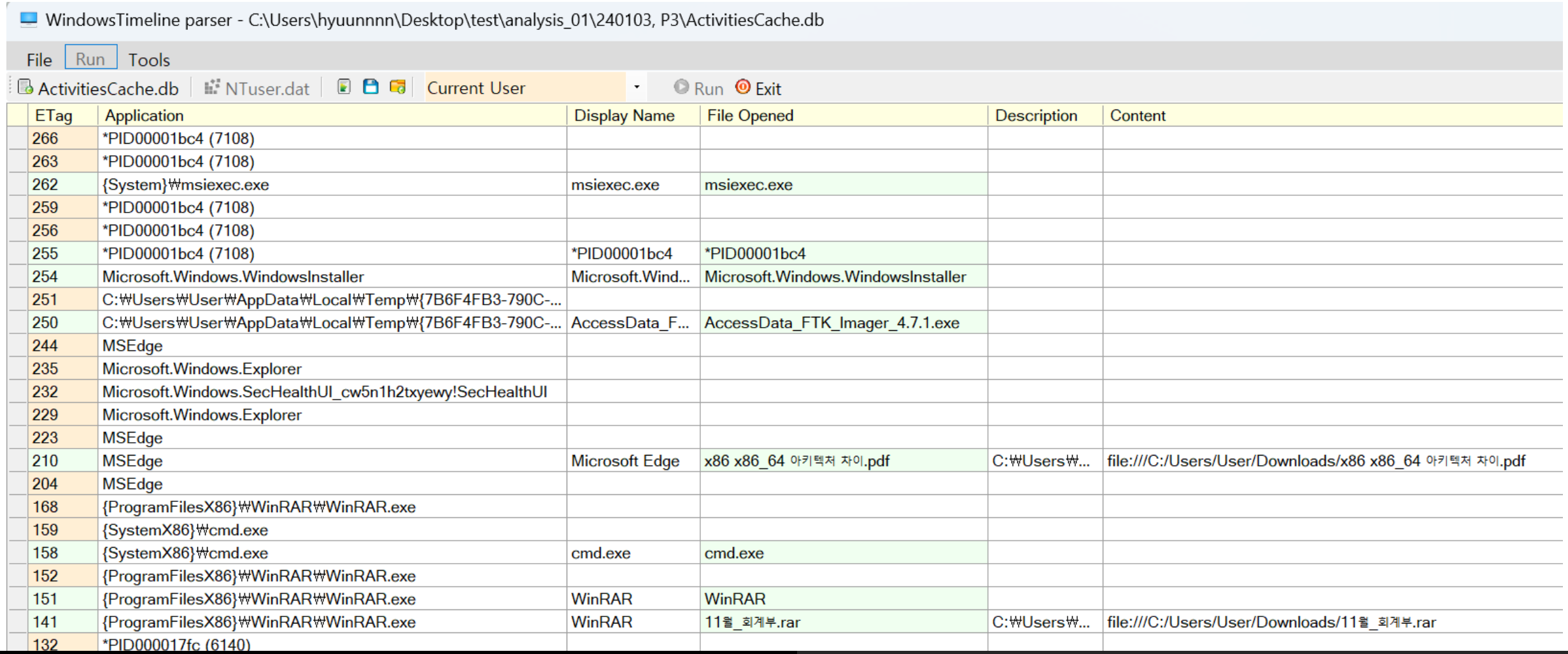
Windows Timeline

- 윈도우 11에 제거된 기능[1]이지만 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



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 아키텍처 차이.pdf	C:₩Users₩...	file:///C:/Users/User/Downloads/x86 x86_64 아키텍처 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

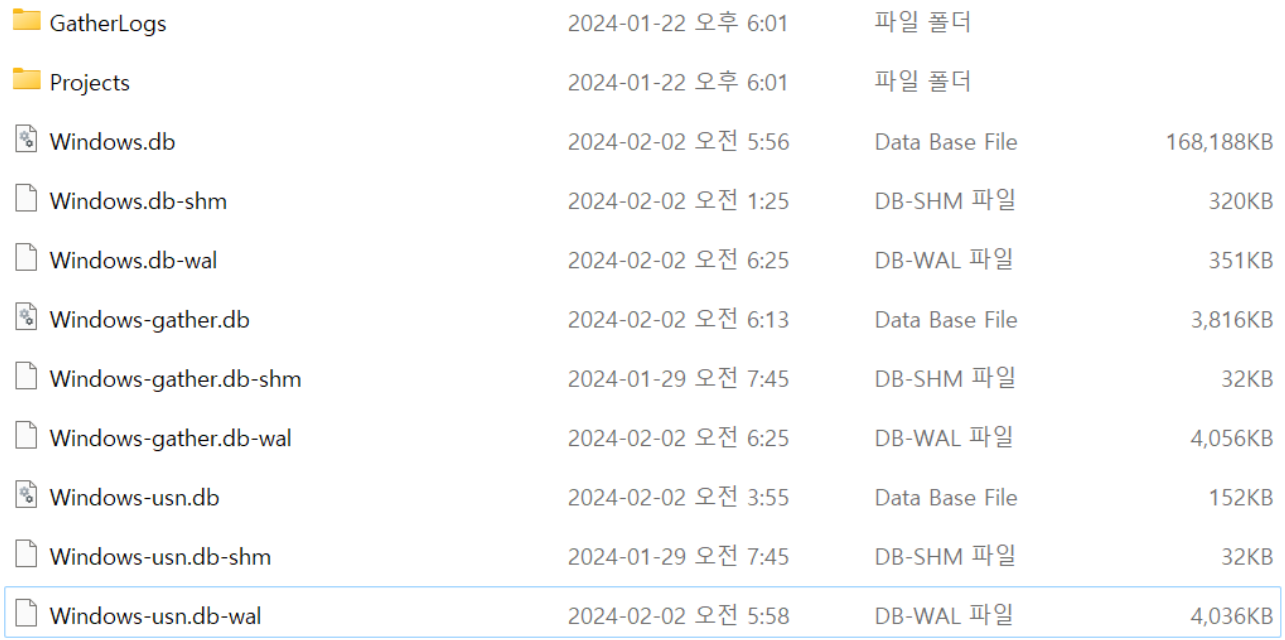
Windows Search

- 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



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	2024-01-25T12:22:02.0000000Z	2024-01-25T12:24:51.6800367Z	https://www.youtube.com/results?search_query=x-ways https://www.youtube.com/watch?v=mwalgzuEfvw&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	2024-01-24T06:07:58.0000000Z	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_ItemName	System_Ite	System_Li	System_ItemDate	S	S	S	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=SW8	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.
  - 또한 운영체제, 기종에 따라서 Mac 포렌식, Linux 포렌식, 모바일 포렌식 등 분야가 광범위하게 있다.
  - Plainbit - Blog, proneer - 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, PWF, digital-forensics-lab, Digital-Forensics-Guide, exploitation-course, 레드팀 플레이북 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.

포렌식 문제 관련 사이트 정리

CyberDefenders, AboutDFIR - Challenges & CTFs, CFReDS, Digital Corpora, Ali Hadi Datasets, dfirmadness, MemLabs, MemoryForensicSamples

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
ABC	ABC	ABC	ABC	=	=	=	=	=
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