Prefetch

made by 임승연

INDEX

1. 소개

2. 구조와 매커니즘

3. 분석 방법

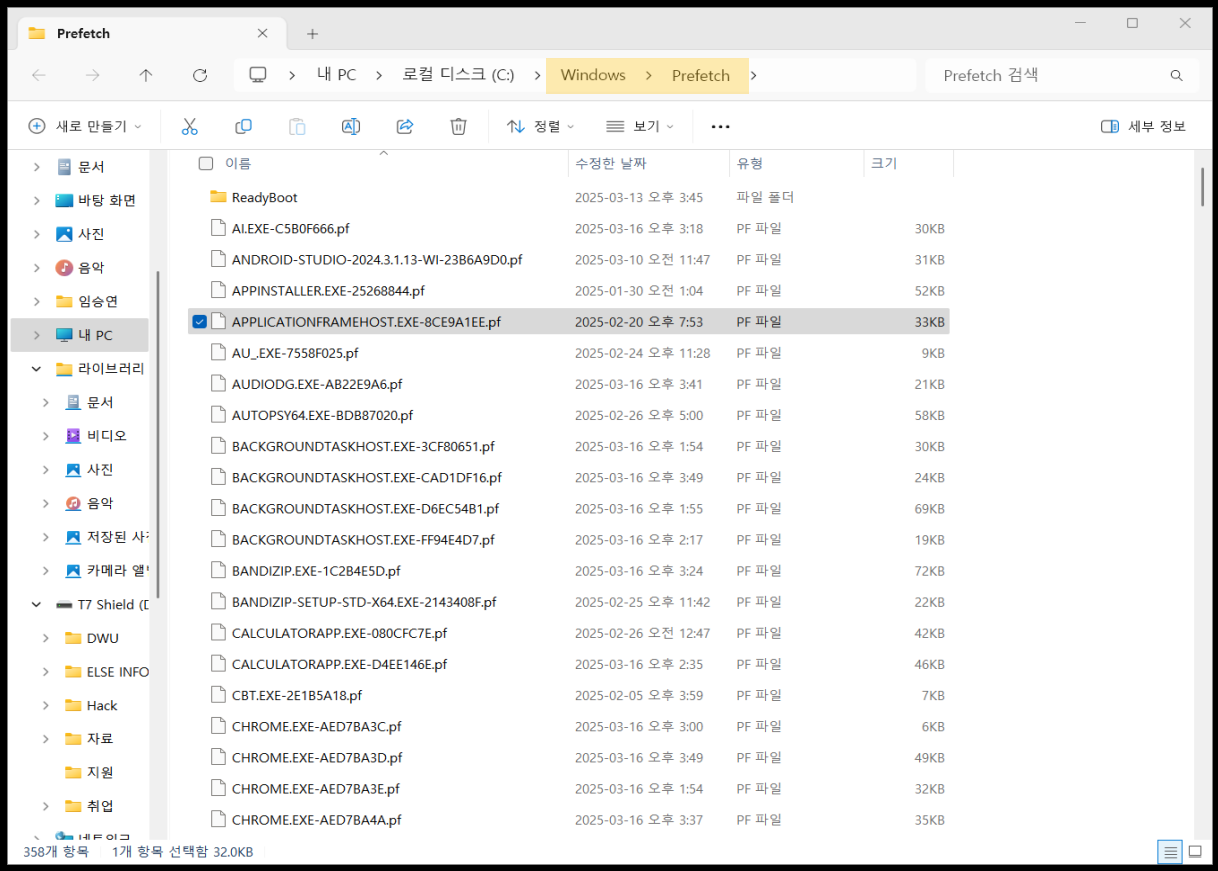
4. 실제 분석 사례 예시

1 Prefetch 소개

Windows Prefetch

- 자주 사용하는 프로그램에 필요한 데이터를 캐싱하여 애플리케이션의 로딩 시간을 단축하기 위해 만들어짐
- Windows 부팅 시 프리패치 파일을 메모리에 로드

- 분류
  - 부트 프리패칭 (Boot Prefetching) : XP, 2003, Vista 2008, 7
  - 응용프로그램 프리패칭 (Application Prefetching): XP, Vista, 7, 8



1 Prefetch 소개

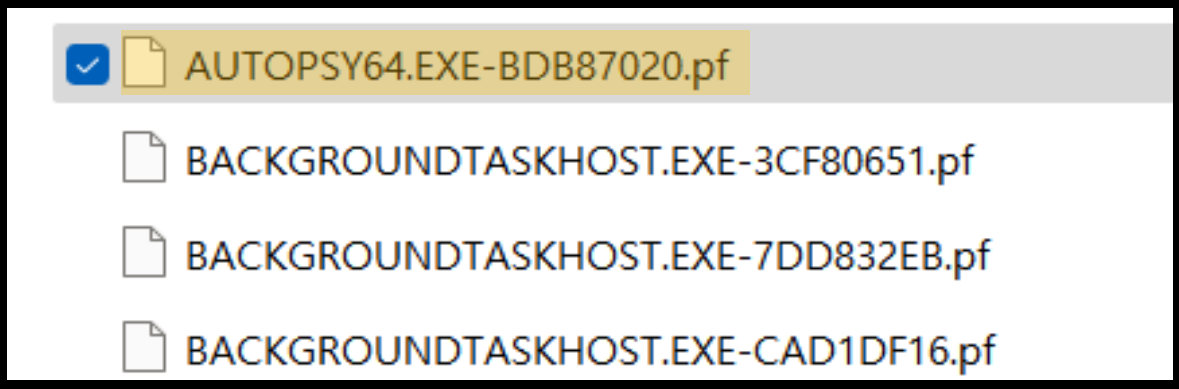
- 프리패치 버전
  - 17 : Windows XP 및 Windows 2003
  - 23 : Windows Vista 및 Windows 7
  - 26 : Windows 8.1
  - 30 : Windows 10
  - 31 : Windows 11
- 프리패치 의 저장 경로
  - %SystemRoot%\Prefetch
- 파일명
  - 부트 프리패치 파일 : NTOSBOOT-B00DFAAD.pf
  - 응용프로그램 프리패치 파일 :[filename]-[filepath_hash].pf

- 부트 프리패칭
  - 부팅 시 사용되는 코드와 데이터를 파일에 저장
  - 부트 프리패칭된 파일을 이용하여 부팅 시 속도 향상

- 응용프로그램 프리패칭
  - 응용 프로그램이 실행되고 10초 지난 후 생성됨
  - 프리패칭된 응용프로그램 실행 시 실행 속도 향상
  - 최대 128개의 파일로, 한계를 넘으면 오래된 순 파일이 자동으로 삭제

1 Prefetch 소개

- 응용프로그램 파일명 :[filename]-[filepath_hash].pf
  - [filename] : 실행 프로그램명
  - [filepath_hash] : 실행 파일 경로 해시값, 경로가 바뀌면 해시값이 바뀜



예시

- AUTOPSY64.EXE-BDB87020.pf 파일에서 `BDB87020` 는 파일이 실행된 경로의 해시로, 이 경로는 다양한 유형의 해싱 함수로 암호화됨

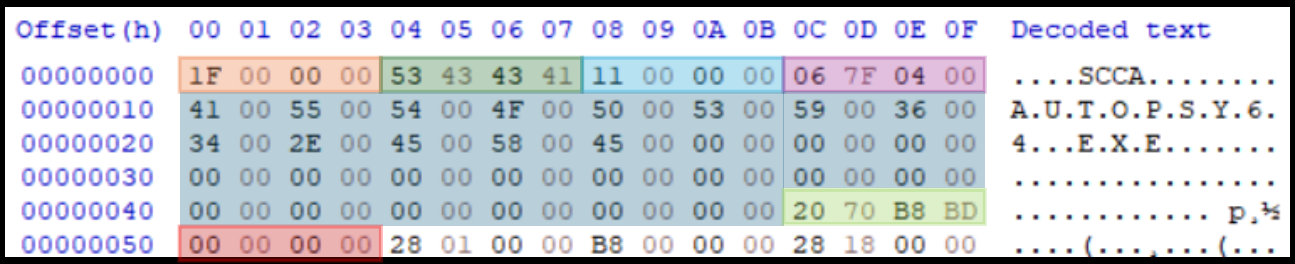
- 프리패치 파일에서 획득 가능한 정보
  - 응용프로그램 이름
  - 응용프로그램의 실행 횟수
  - 응용프로그램 마지막 실행 시간
  - 참조 목록
  - 파일시스템 시간 정보

2 구조와 매커니즘

- Prefetch File information

< File Header Format >

Offset	Length	Notes
0x0000	4	Format Version of the Windows OS
0x0004	4	SCCA signature
0x0008	4	Prefetcher Management Service Version
0x000C	4	Prefetch File Size
0x0010	60	Corresponding name of the executable
0x004C	4	Prefetch Hash Value
0x0050	4	Unknown



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	1F	00	00	00	53	43	43	41	11	00	00	00	06	7F	04	00	....SCCA........
00000010	41	00	55	00	54	00	4F	00	50	00	53	00	59	00	36	00	A.U.T.O.P.S.Y.6.
00000020	34	00	2E	00	45	00	58	00	45	00	00	00	00	00	00	00	4...E.X.E.......
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000040	00	00	00	00	00	00	00	00	00	00	00	00	20	70	B8	BD	.... p¸½
00000050	00	00	00	00	28	01	00	00	B8	00	00	00	28	18	00	00	....(...¸...(...

2 구조와 매커니즘

Prefetch File information

- Windows XP, Windows 2003

Format version : 17 (0x11)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x00	Prefetcher version (0x00000011)				Signature (“SCCA”)				Prefetcher Management Service Version (0x0000000F)				File Size			
0x10	Executable File Name (길이가 58byte를 넘을 경우 파일 이름 끝에 0x0000 기록)															
0x20																
0x30																
0x40											파일이름 58일때 0x00		Full Path Hash Value			
0x50	0x00000000				SectionInfoOffset				NumSections				PageInfoOffset			
0x60	NumPages				FileNameInfoOffset				FileNameStringSize				VolumesInfoOffset (디스크 볼륨정보)			
0x70	NumberOfVolumes (디스크 볼륨 개수)				VolumesInfoSize				LastLaunchTime (최종 실행 시각)							
0x80	MinRePrefetchTime								MinReTraceTime							
0x90	NumLaunches (실행 횟수)				Sensitivity											

2 구조와 매커니즘

Prefetch File information

– Windows Vista, Windows 7

Format version : 23 (0x17)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x00	Prefetcher version (0x00000017)				Signature ("SCCA")				Prefetcher Management Service Version (0x00000011)				File Size			
0x10	Executable File Name (길이가 58byte를 넘을 경우 파일 이름 끝에 0x0000 기록)															
0x20																
0x30																
0x40												파일이름 58일때 0x00	Full Path Hash Value			
0x50	0x00000000				SectionInfoOffset				NumSections				PageInfoOffset			
0x60	NumPages				FileNameInfoOffset				FileNameStringSize				VolumesInfoOffset (디스크 볼륨정보)			
0x70	NumberOfVolumes (디스크 볼륨 개수)				VolumesInfoSize				Unknown							
0x80	LastLaunchTime (최종 실행 시각)								Unknown				0x00000000			
0x90	Unknown				0x00000000				NumLaunches (실행 횟수)				Sensitivity			

2 구조와 매커니즘

Prefetch File information

– Windows 8.1

Format version : 26 (0x1A)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x00	Prefetcher version (0x0000001A)				Signature ("SCCA")				Prefetcher Management Service Version				File Size			
0x10	Executable File Name (길이가 58byte를 넘을 경우 파일 이름 끝에 0x0000 기록)															
0x20																
0x30																
0x40													파일이름 58일때 0x00		Full Path Hash Value	
0x50	0x00000000				File metricx array offset (0x130)				NumSections				PageInfoOffset			
0x60	NumPages				FileNameInfoOffset				FileNameStringSize				VolumesInfoOffset (디스크 볼륨정보)			
0x70	NumberOfVolumes (디스크 볼륨 개수)				VolumesInfoSize				Unknown							
0x80	LastLaunchTime (최종 실행 시각)								LastLaunchTime							
0x90	LastLaunchTime								LastLaunchTime							
0xA0	LastLaunchTime								LastLaunchTime							
0xB0	LastLaunchTime								LastLaunchTime							
0xC0	Unknown															
0xD0	NumLaunches (실행 횟수)				Unknown								EmptyValues			
0xE0	EmptyValues															
0xF0																
0x100																
0x110																
0x120																

2 구조와 매커니즘

Prefetch File information

– Windows 10

Format version : 30 (0x1E)

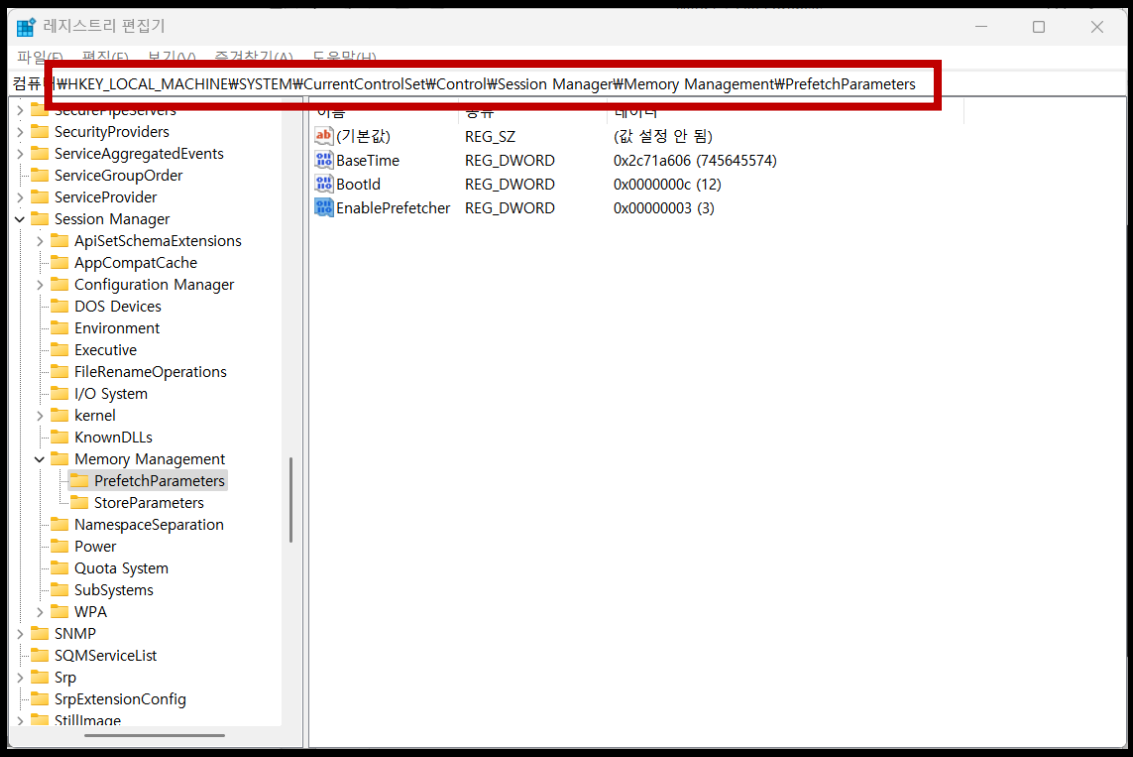
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x00	Prefetcher version (0x0000001E)				Signature (“SCCA”)				Prefetcher Management Service Version				File Size			
0x10	Executable File Name (길이가 58byte를 넘을 경우 파일 이름 끝에 0x0000 기록)															
0x20																
0x30																
0x40											파일이름 58일때 0x00		Full Path Hash Value			
0x50	0x00000000				File metricx array offset (0x128 || 0x130)				NumSections				PageInfoOffset			
0x60	NumPages				FileNameInfoOffset				FileNameStringSize				VolumesInfoOffset (디스크 볼륨정보)			
0x70	NumberOfVolumes (디스크 볼륨 개수)				VolumesInfoSize				Unknown							
0x80	LastLaunchTime (최종 실행 시각)								LastLaunchTime							
0x90	LastLaunchTime								LastLaunchTime							
0xA0	LastLaunchTime								LastLaunchTime							
0xB0	LastLaunchTime								LastLaunchTime							
0xC0	Unknown															
0xD0	NumLaunches (실행 횟수)				Unknown								HashStringOffset			
0xE0	EmptyValues															
0xF0																
0x100																
0x110																
0x120																

2 구조와 매커니즘

- Prefetch 설정 방법

  1. 레지스트리 편집기

  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory\Memory Management\PrefetchParameters`

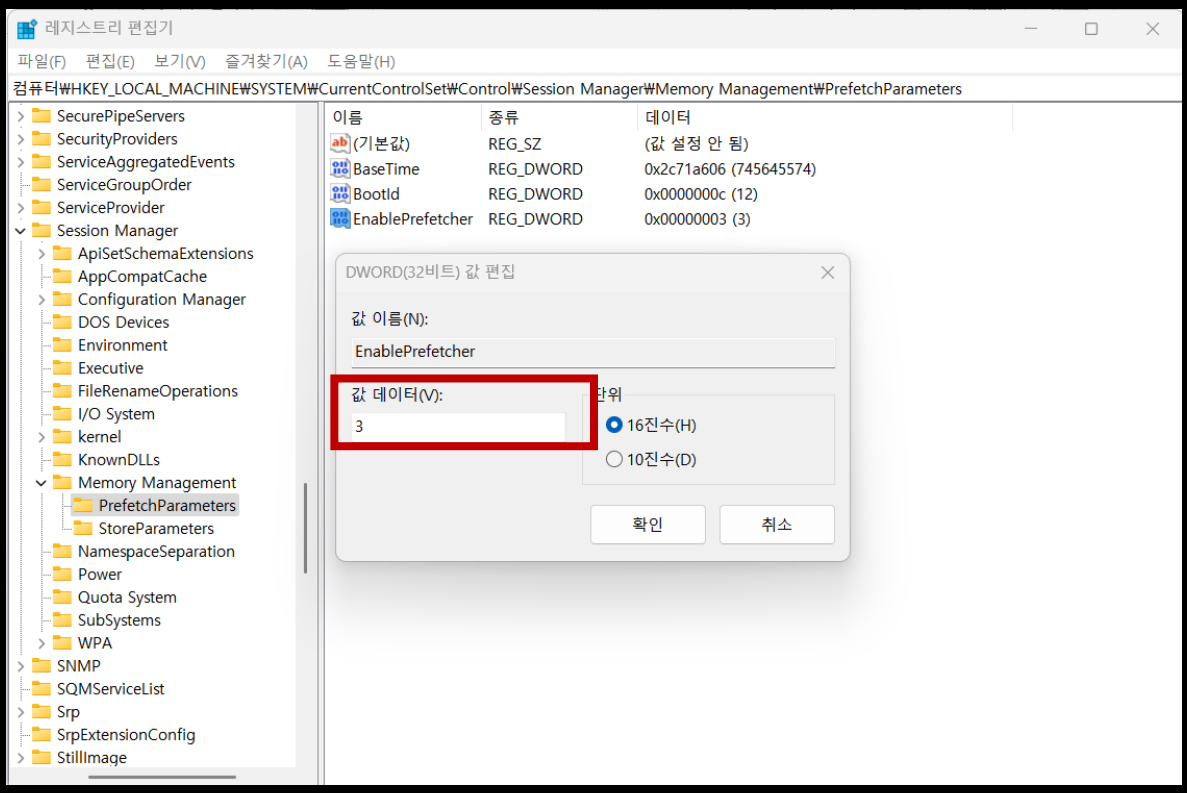


2 구조와 매커니즘

- Prefetch 설정 방법

  2. 레지스트리 편집기

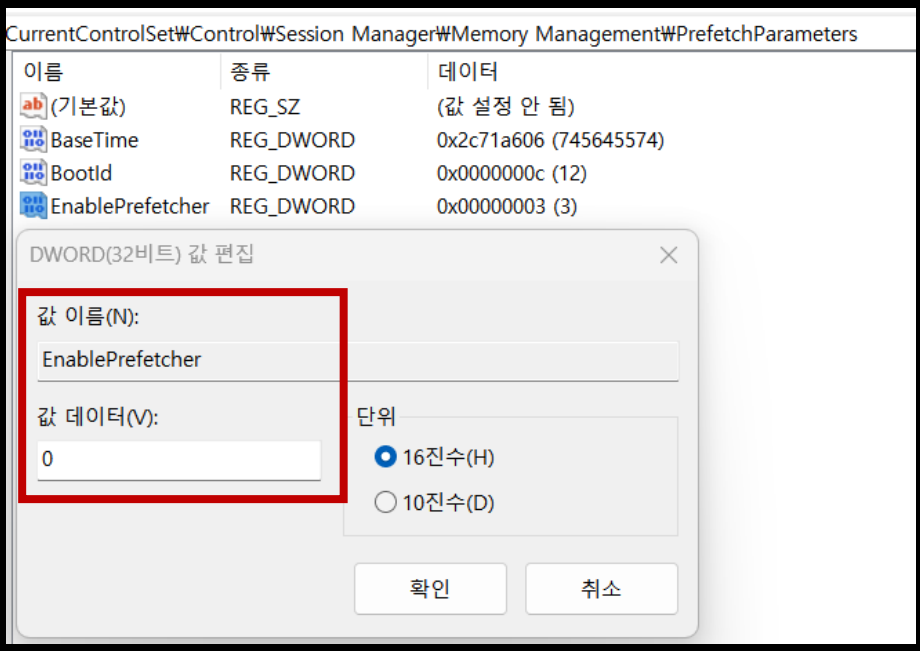
  [EnablePrefetcher] 더블 클릭

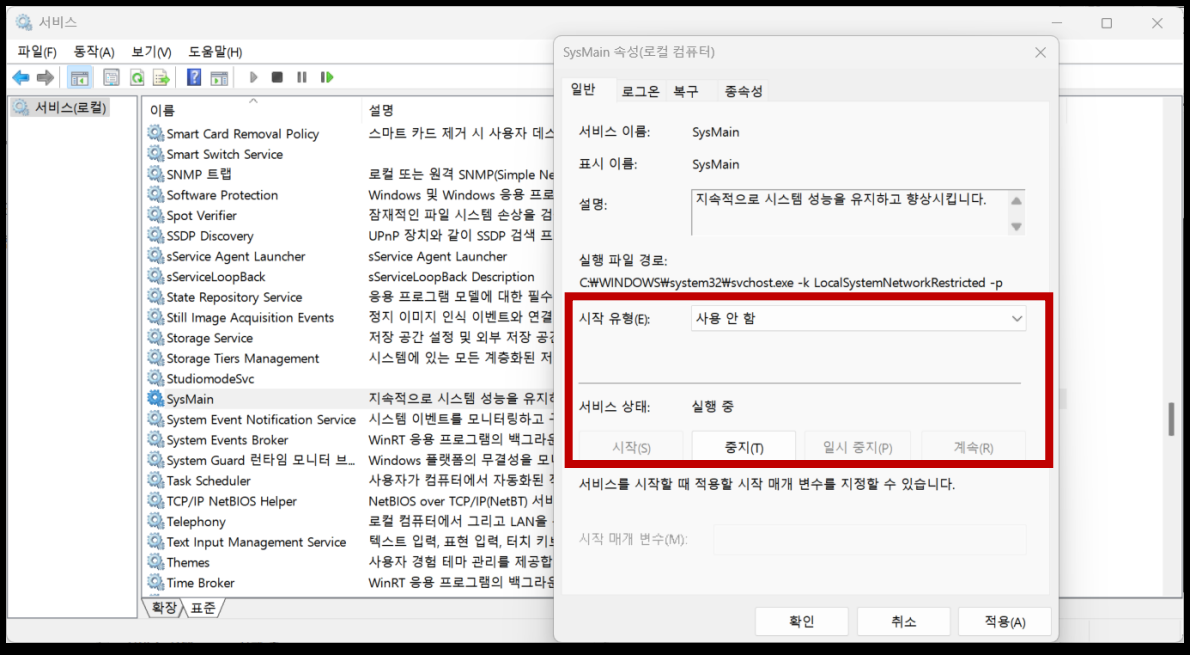


- 값 데이터 별 결과
  - 0 : Prefetch OFF, 사용하지 않음
  - 1 : ALP(Application-Launch Prefetching)만 사용
    - ALP란? 사용자가 자주 사용하는 응용프로그램의 정보를 Prefetch 하는 것. 응용프로그램 실행 속도를 줄여줌
  - 2 : BP(Boot Prefetching)만 사용
    - BP란? 부팅 시 사용되는 파일이나 프로그램의 정보를 Prefetch 하는 것. 부팅 속도를 줄여줌
  - 3 : ALP와 BP 모두 사용

2 구조와 매커니즘

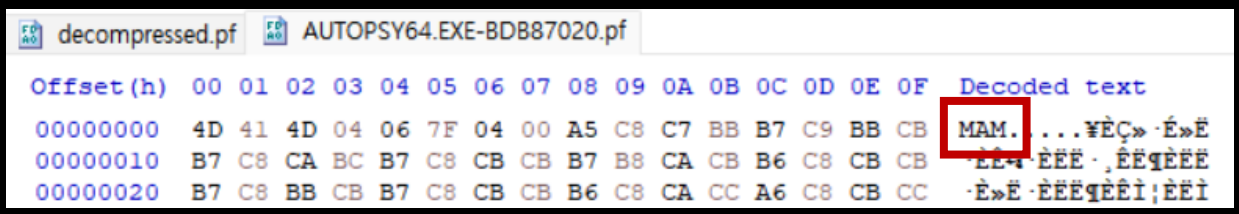
- Prefetch를 완전히 끄는 방법
  1. 레지스트리 에서 EnablePrefetcher 값 데이터를 0으로 바꿈
  2. 서비스 목록에서 Superfetch(SysMain)을 선택
  3. 서비스 상태를 [중지]
  4. 시작 유형을 [사용 안 함] 으로 변경한 후, [적용] – [확인]





3 분석 방법론

- PF 파일 분석
  - Windows 10부터 prefetch 파일 압축
    - MAM 형식(xpress Huffman Algorithm)



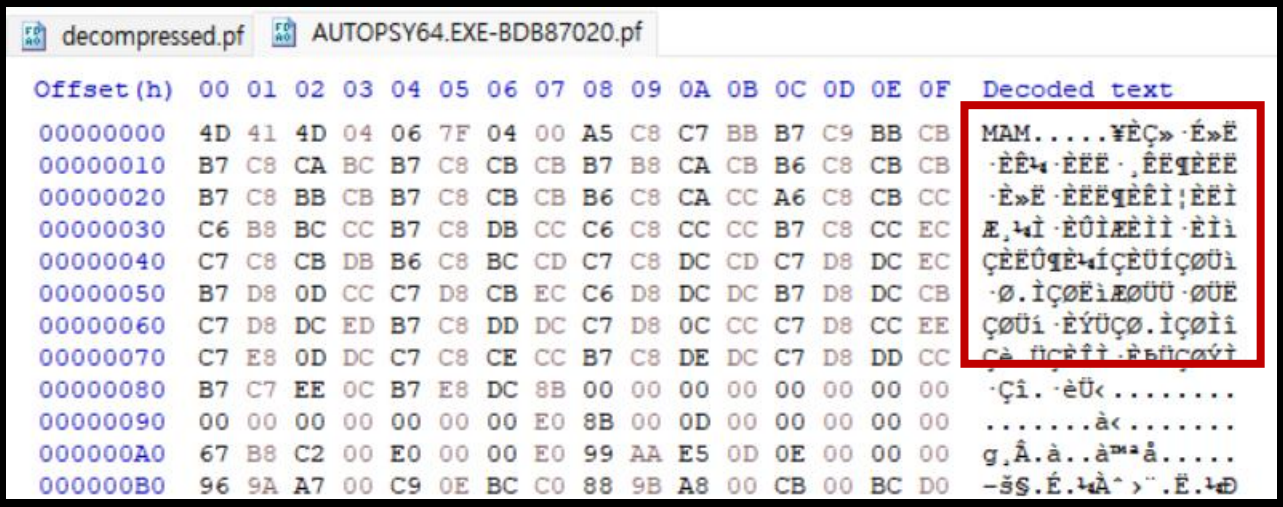
- MAM 압축을 해제해야 내용 확인 가능
- 압축 해제 방법
  - w10pfdecomp.py 이용
  - Prefetchcount.py 스크립트
- MAM 압축을 해제된 파일은 이해 가능한 문자열 형식으로 변환됨

- 압축 방법
  - w10pfdecomp.py 파일 이용

> python w10pfdecomp.py C:\Windows\Prefetch\AUTOPSY64.EXE-BDB87020.pf decompressed.pf
>
> Lucky man, you have your prefetch file ready to be parsed!

3 분석 방법론

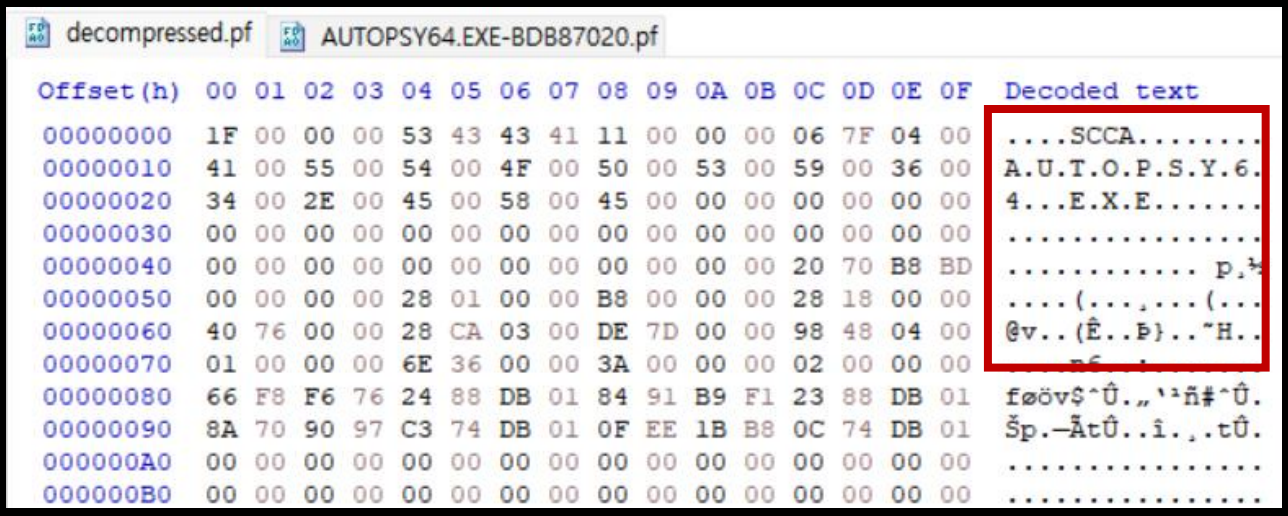
- 압축 해제 전



decompressed.pf AUTOPSY64.EXE-BDB87020.pf

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	4D	41	4D	04	06	7F	04	00	A5	C8	C7	BB	B7	C9	BB	CB	MAM.....¥ÈÇ»·É»Ë
00000010	B7	C8	CA	BC	B7	C8	CB	CB	B7	B8	CA	CB	B6	C8	CB	CB	·ÈÊ¼·ÈËË·¸ÊË¶ÈËË
00000020	B7	C8	BB	CB	B7	C8	CB	CB	B6	C8	CA	CC	A6	C8	CB	CC	·È»Ë·ÈËË¶ÈÊÌ¦ÈËÌ
00000030	C6	B8	BC	CC	B7	C8	DB	CC	C6	C8	CC	CC	B7	C8	CC	EC	Æ¸¼Ì·ÈÛÌÆÈÌÌ·ÈÌì
00000040	C7	C8	CB	DB	B6	C8	BC	CD	C7	C8	DC	CD	C7	D8	DC	EC	ÇÈËÛ¶È¼ÍÇÈÜÍÇØÜì
00000050	B7	D8	0D	CC	C7	D8	CB	EC	C6	D8	DC	DC	B7	D8	DC	CB	·Ø.ÌÇØËìÆØÜÜ·ØÜË
00000060	C7	D8	DC	ED	B7	C8	DD	DC	C7	D8	0C	CC	C7	D8	CC	EE	ÇØÜí·ÈÝÜÇØ.ÌÇØÌî
00000070	C7	E8	0D	DC	C7	C8	CE	CC	B7	C8	DE	DC	C7	D8	DD	CC	Çè.ÜÇÈÎÌ·ÈÞÜÇØÝÌ
00000080	B7	C7	EE	0C	B7	E8	DC	8B	00	00	00	00	00	00	00	00	·Çî.·èÜ‹........
00000090	00	00	00	00	00	00	00	E0	8B	00	0D	00	00	00	00	00	.......à‹.......
000000A0	67	B8	C2	00	E0	00	00	E0	99	AA	E5	0D	0E	00	00	00	g¸Â.à..à™ªå.....
000000B0	96	9A	A7	00	C9	0E	BC	C0	88	9B	A8	00	CB	00	BC	D0	–š§.É.¼À^›¨.Ë.¼Ð

- 압축 해제 후



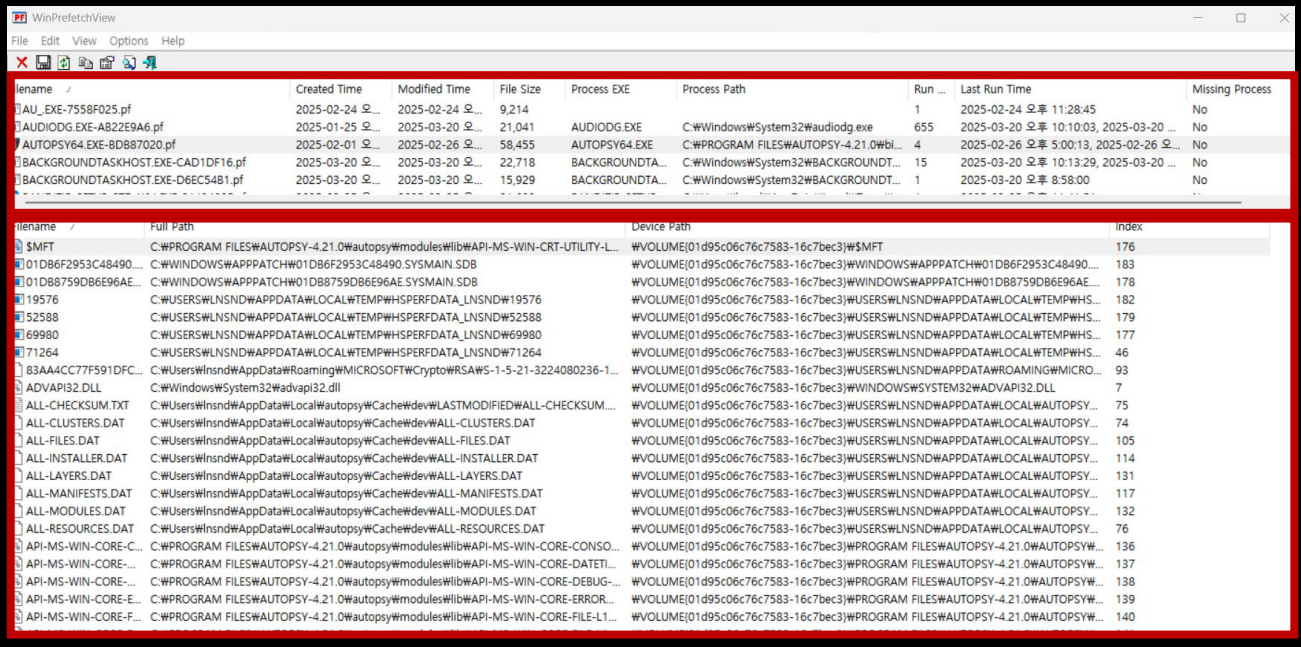
decompressed.pf AUTOPSY64.EXE-BDB87020.pf

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	1F	00	00	00	53	43	43	41	11	00	00	00	06	7F	04	00	....SCCA........
00000010	41	00	55	00	54	00	4F	00	50	00	53	00	59	00	36	00	A.U.T.O.P.S.Y.6.
00000020	34	00	2E	00	45	00	58	00	45	00	00	00	00	00	00	00	4...E.X.E.......
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000040	00	00	00	00	00	00	00	00	00	00	00	00	20	70	B8	BD	.... p¸½
00000050	00	00	00	00	28	01	00	00	B8	00	00	00	28	18	00	00	....(...¸...(...
00000060	40	76	00	00	28	CA	03	00	DE	7D	00	00	98	48	04	00	@v..(Ê..Þ}..˜H..
00000070	01	00	00	00	6E	36	00	00	3A	00	00	00	02	00	00	00	....n6..:.......
00000080	66	F8	F6	76	24	88	DB	01	84	91	B9	F1	23	88	DB	01	føöv$ˆÛ.„‘¹ñ#ˆÛ.
00000090	8A	70	90	97	C3	74	DB	01	0F	EE	1B	B8	0C	74	DB	01	Šp.—ÃtÛ..î.¸.tÛ.
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....

3 분석 방법론

Prefetch 분석 도구

- WinPrefetchView



- 기본적으로 실행되고 있는 PC의 프리패치를 보여줌
- 분석 결과 화면
  - 위쪽에서 `.pf` 파일을 선택하면, 아래쪽 화면에서 정보 확인 가능

3 분석 방법론

Prefetch 분석 도구

- WinPrefetchView

< 위쪽 화면 >

속성	설명
Filename	프리패치 파일 이름
Created Time	프리패치 생성 시각 (= 응용프로그램 최초 실행 시각)
Modified Time	프리패치 변경 시각 (= 응용프로그램 마지막 실행 시각)
File Size	프리패치 파일 크기
Precess EXE	응용프로그램(exe) 이름
Process Path	응용프로그램 경로 → 응용프로그램이 실행된 볼륨의 정보
Run Counter	응용프로그램 실행 횟수
Last Run Time	응용프로그램 마지막 실행 시각
Missing Process	응용프로그램 삭제 여부 (Yes / No)

< 아래쪽 화면 >

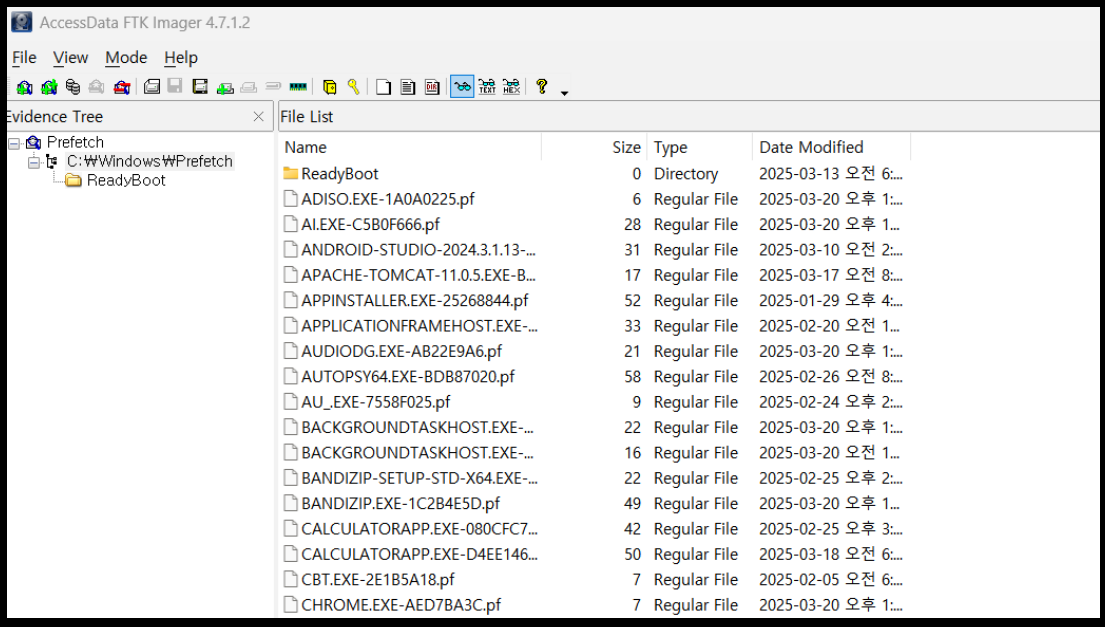
속성	설명
Filename	응용프로그램과 함께 로드된 파일의 이름
Full Path	응용프로그램과 함께 로드된 파일의 경로
Device Path	볼륨 정보를 포함한 경로 → 응용프로그램이 실행된 볼륨 정보
Index	응용프로그램 실행 과정에서 로드된 순서

3 분석 방법론

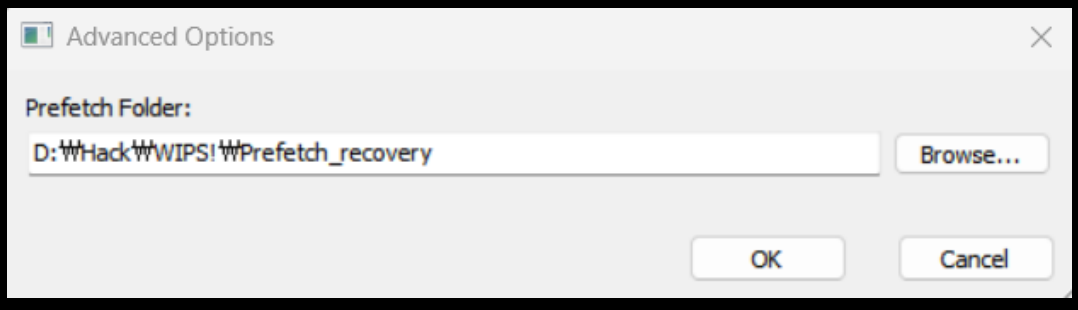
Prefetch 분석 도구

삭제된 프리패치 수집하기

< FTK Imager 활용>



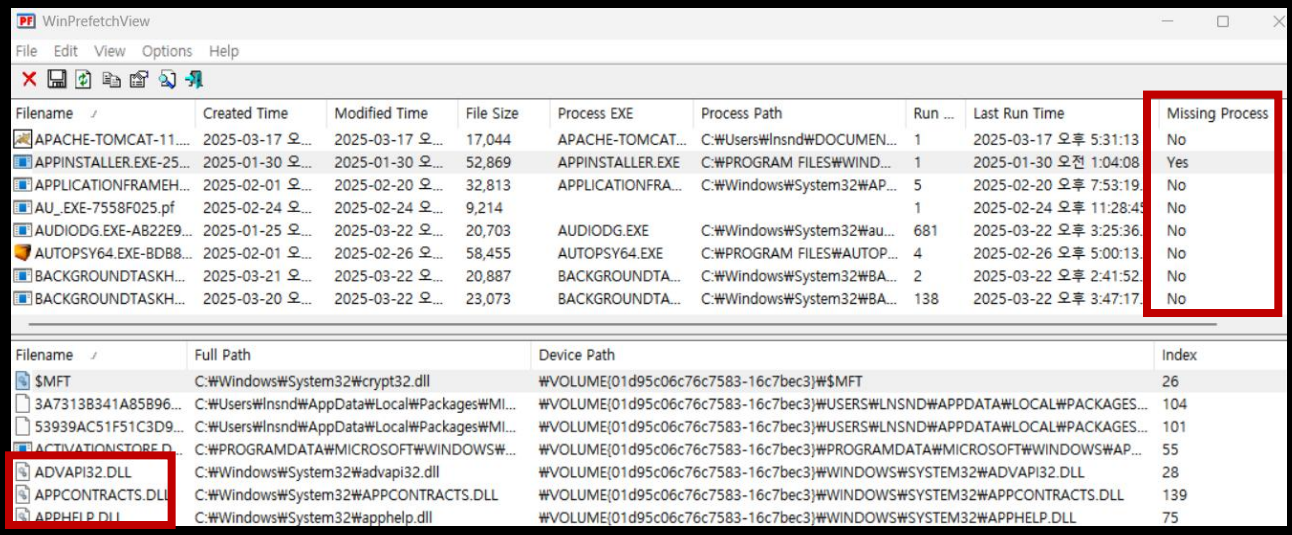
- Prefetch 폴더를 Export Files 하여 추출
- WinPrefetchView의 Options-Advanced Options에서 추출한 Prefetch 경로 설정



3 분석 방법론

Prefetch 분석 도구

삭제된 프리패치 수집하기



1. 외부 저장장치 프로그램 실행

   D 드라이브에서 실행했음을 알 수 있음

2. 응용프로그램이 삭제된 경우

   'Missing Process'가 Yes로 표시된 경우, 응용프로그램이 삭제된 것인데, 악성코드가 실행되는 과정에서 자신을 삭제하는 경우가 많기 때문에 주의 깊게 봐야 함

3. 정상 프로세스에서 의심스러운 동작이 의심되는 경우

   해커가 별도의 응용프로그램이 아닌 DLL Injection 등의 공격을 통해 해당 프로그램에 접근한 경우, 하단에 로드되는 DLL 목록에서 수상한 경로를 확인 가능

4 실제 분석 사례 예시

Prefetch 분석 도구 - PECmd

- prefetch 파일을 압축 해제하지 않아도 분석 가능
- 알 수 있는 정보

Name	Information	Example
Created on	생성 일시	2025-03-16 06:25:03
Modified on	수정 일시	2025-03-22 07:05:36
Last accessed on	마지막으로 접근한 일시	2025-03-22 07:36:25
Executable name	실행 파일 이름	WINPREFETCHVIEW.EXE
Hash	Prefetch 해시값 표시	F70B7212
File size (bytes)	파일 크기 (bytes)	336,662
Version	Windows Version	null
Run count	WINPREFETCH의 총 실행 횟수	6
Last run	가장 최근에 실행한 일시	2025-03-22 07:05:26
Other run times	기타 실행 일시	2025-03-22 06:49:18, 2025-03-21 12:55:27, 2025-03-20 13:13:34 ...
Volume information	볼륨 정보 1. 참조된 디렉토리 목록 2. 참조된 파일	#0: Name: \VOLUME{0000000000000000-02f25557} Serial: 2F25557 Created: 1601-01-01 00:00:00 Directories: 2 File references: 3 #1: Name: \VOLUME{01d95c06c76c7583-16c7bec3} Serial: 16C7BEC3 Created: 2023-03-21 15:06:56 Directories: 210 File references: 1,157

4 실제 분석 사례 예시

Prefetch 분석 도구 - PECmd

- PECmd.exe 로 AUTOPSY64.EXE-BDB87020.pf 파일을 파싱하기 위해 –f 옵션을 사용

< ./PECmd.exe –f "C:\Windows\Prefetch\WINPREFETCHVIEW.EXE-F70B7212.pf" 실행 결과 >

```
PS C:\Users\lnsnd\Documents\PECmd> ./PECmd.exe -f "C:\Windows\Prefetch\WINPREFETCHVIEW.EXE-F70B7212.pf"
PECmd version 1.5.0.0

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

Command line: -f C:\Windows\Prefetch\WINPREFETCHVIEW.EXE-F70B7212.pf

Warning: Administrator privileges not found!

Keywords: temp, tmp

Processing C:\Windows\Prefetch\WINPREFETCHVIEW.EXE-F70B7212.pf

Created on: 2025-03-16 06:25:03
Modified on: 2025-03-22 07:05:36
Last accessed on: 2025-03-22 12:23:25

Executable name: WINPREFETCHVIEW.EXE
Hash: F70B7212
File size (bytes): 336,662
Version: null

Run count: 6
Last run: 2025-03-22 07:05:26
Other run times: 2025-03-22 06:49:18, 2025-03-21 12:55:27, 2025-03-20 13:13:34, 2025-03-17 02:56:39, 2025-03-16 06:24:53

Volume information:

#0: Name: \VOLUME{0000000000000000-02f25557} Serial: 2F25557 Created: 1601-01-01 00:00:00 Directories: 2 File references: 3
#1: Name: \VOLUME{01d95c06c76c7583-16c7bec3} Serial: 16C7BEC3 Created: 2023-03-21 15:06:56 Directories: 210 File references: 1,157

Directories referenced: 212

00: \VOLUME{0000000000000000-02f25557}\HACK
01: \VOLUME{0000000000000000-02f25557}\HACK\자료
02: \VOLUME{01d95c06c76c7583-16c7bec3}\JDK_ECLIPSE
03: \VOLUME{01d95c06c76c7583-16c7bec3}\JDK_ECLIPSE\ECLIPSE
04: \VOLUME{01d95c06c76c7583-16c7bec3}\JDK_ECLIPSE\ECLIPSE\PLUGINS
05: \VOLUME{01d95c06c76c7583-16c7bec3}\JDK_ECLIPSE\ECLIPSE\PLUGINS\ORG.ECLIPSE.JUSTJ.OPENJDK.HOTSPOT.JRE.FULL.WIN32.X86_64_17.0.8.V20230831-1047

Files referenced: 789

00: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSTEM32\C_949.NLS
02: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSTEM32\L_INTL.NLS
03: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSTEM32\KERNEL32.DLL
04: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSTEM32\KERNELBASE.DLL
05: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSTEM32\LOCALE.NLS

783: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSTEM32\USOCLIENT.EXE
784: \VOLUME{01d95c06c76c7583-16c7bec3}\PROGRAM FILES\WINDOWSAPPS\SAMSUNGELECTRONICSCOLTD.SAMSUNGCONTINUITYSERVICE_1.13.6.0_X64__WYX1VJ98G3ASY\WINDOWSMCFCORE\WINDOWSMCFCORE.EXE
785: \VOLUME{01d95c06c76c7583-16c7bec3}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.DESKTOPAPPINSTALLER_1.25.340.0_X64__8WEKYB3D8BBWE\WINDOWSPACKAGEMANAGERSERVER.EXE
786: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSTEM32\WINLOGON.EXE
787: \VOLUME{01d95c06c76c7583-16c7bec3}\PROGRAM FILES\MICROSOFT OFFICE\ROOT\OFFICE16\WINWORD.EXE
788: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSTEM32\WUDFHOST.EXE


---------- Processed C:\Windows\Prefetch\WINPREFETCHVIEW.EXE-F70B7212.pf in 0.51315080 seconds ----------
```

4 실제 분석 사례 예시

Prefetch 분석 도구 - PECmd

- -d 옵션을 통해 Prefetch directory를 분석한 결과의 일부

< ./PECmd.exe –d C:/Windows/Prefetch 실행 결과 일부 >

```
Processing C:\Windows\Prefetch\WINPREFETCHVIEW.EXE-F70B7212.pf

Created on: 2025-03-16 06:25:03
Modified on: 2025-03-22 07:05:36
Last accessed on: 2025-03-22 07:36:25

Executable name: WINPREFETCHVIEW.EXE
Hash: F70B7212
File size (bytes): 336,662
Version: null

Run count: 6
Last run: 2025-03-22 07:05:26
Other run times: 2025-03-22 06:49:18, 2025-03-21 12:55:27, 2025-03-20 13:13:34, 2025-03-17 02:56:39, 2025-03-16 06:24:53

Volume information:

#0: Name: \VOLUME{0000000000000000-02f25557} Serial: 2F25557 Created: 1601-01-01 00:00:00 Directories: 2 File references: 3
#1: Name: \VOLUME{01d95c06c76c7583-16c7bec3} Serial: 16C7BEC3 Created: 2023-03-21 15:06:56 Directories: 210 File references: 1,157

Directories referenced: 212

00: \VOLUME{0000000000000000-02f25557}\HACK
01: \VOLUME{0000000000000000-02f25557}\HACK\자료
02: \VOLUME{01d95c06c76c7583-16c7bec3}\JDK_ECLIPSE
03: \VOLUME{01d95c06c76c7583-16c7bec3}\JDK_ECLIPSE\ECLIPSE
04: \VOLUME{01d95c06c76c7583-16c7bec3}\JDK_ECLIPSE\ECLIPSE\PLUGINS
05: \VOLUME{01d95c06c76c7583-16c7bec3}\JDK_ECLIPSE\ECLIPSE\PLUGINS\ORG.ECLIPSE.JUSTJ.OPENJDK.HOTSPOT.JRE.FULL.WIN32.X86_64_17.0.8.V20230831-1047
06: \VOLUME{01d95c06c76c7583-16c7bec3}\JDK_ECLIPSE\ECLIPSE\PLUGINS\ORG.ECLIPSE.JUSTJ.OPENJDK.HOTSPOT.JRE.FULL.WIN32.X86_64_17.0.8.V20230831-1047\JRE
07: \VOLUME{01d95c06c76c7583-16c7bec3}\PROGRAM FILES
08: \VOLUME{01d95c06c76c7583-16c7bec3}\PROGRAM FILES\COMMON FILES
09: \VOLUME{01d95c06c76c7583-16c7bec3}\PROGRAM FILES\COMMON FILES\MICROSOFT SHARED
10: \VOLUME{01d95c06c76c7583-16c7bec3}\PROGRAM FILES\MICROSOFT VISUAL STUDIO
11: \VOLUME{01d95c06c76c7583-16c7bec3}\PROGRAM FILES\MICROSOFT VISUAL STUDIO\2022
12: \VOLUME{01d95c06c76c7583-16c7bec3}\PROGRAM FILES\MICROSOFT VISUAL STUDIO\2022\COMMUNITY
13: \VOLUME{01d95c06c76c7583-16c7bec3}\PROGRAM FILES\MICROSOFT VISUAL STUDIO\2022\COMMUNITY\COMMON7
14: \VOLUME{01d95c06c76c7583-16c7bec3}\PROGRAM FILES\MICROSOFT VISUAL STUDIO\2022\COMMUNITY\COMMON7\IDE
15: \VOLUME{01d95c06c76c7583-16c7bec3}\USERS
16: \VOLUME{01d95c06c76c7583-16c7bec3}\USERS\LNSND
17: \VOLUME{01d95c06c76c7583-16c7bec3}\USERS\LNSND\APPDATA
18: \VOLUME{01d95c06c76c7583-16c7bec3}\USERS\LNSND\APPDATA\LOCAL
19: \VOLUME{01d95c06c76c7583-16c7bec3}\USERS\LNSND\APPDATA\LOCAL\PROGRAMS
20: \VOLUME{01d95c06c76c7583-16c7bec3}\USERS\LNSND\APPDATA\LOCAL\PROGRAMS\MICROSOFT VS CODE
21: \VOLUME{01d95c06c76c7583-16c7bec3}\USERS\LNSND\APPDATA\LOCAL\PROGRAMS\MICROSOFT VS CODE\RESOURCES
22: \VOLUME{01d95c06c76c7583-16c7bec3}\USERS\LNSND\APPDATA\LOCAL\PROGRAMS\MICROSOFT VS CODE\RESOURCES\APP
23: \VOLUME{01d95c06c76c7583-16c7bec3}\USERS\LNSND\APPDATA\LOCAL\PROGRAMS\MICROSOFT VS CODE\RESOURCES\APP\NODE_MODULES
```

```
74: \VOLUME{0000000000000000-02f25557}\HACK\CTF\BUNKER\DLL\00082B86.DLL
75: \VOLUME{01d95c06c76c7583-16c7bec3}\USERS\LNSND\DOWNLOADS\SNAPSHOT_2024-02-19_03-16\RELEASE\X32\X32DBG.EXE
76: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\APPPATCH\01DB6F2953C48490.SYSMAIN.SDB
77: \VOLUME{0000000000000000-02f25557}\HACK\CTF\BUNKER\DLL\00042790.DLL
78: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\FONTS\STATICCACHE.DAT
79: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSWOW64\TEXTSHAPING.DLL
80: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSWOW64\MSCTF.DLL
81: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSTEM32\IMAGERES.DLL
82: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSTEMRESOURCES\IMAGERES.DLL.MUN
83: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSWOW64\TEXTINPUTFRAMEWORK.DLL
84: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSWOW64\OLEACC.DLL
85: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSTEM32\OLEACCRC.DLL
86: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSTEM32\KO-KR\KERNELBASE.DLL.MUI
87: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSWOW64\COREMESSAGING.DLL
88: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSWOW64\COREUICOMPONENTS.DLL
89: \VOLUME{01d95c06c76c7583-16c7bec3}\WINDOWS\SYSWOW64\CRYPTBASE.DLL
90: \VOLUME{0000000000000000-02f25557}\HACK\CTF\BUNKER\DLL\00043614.DLL


---------- Processed C:\Windows\Prefetch\X96DBG.EXE-FAE95824.pf in 0.08630210 seconds ----------
Processed 401 out of 404 files in 48.3602 seconds

Failed files
  C:\Windows\Prefetch\FONTDRVHOST.EXE-8152304A.pf ==> (Invalid signature! Should be 'SCCA')
  C:\Windows\Prefetch\LOGONUI.EXE-F639BD7E.pf ==> (Invalid signature! Should be 'SCCA')
  C:\Windows\Prefetch\SVCHOST.EXE-3CF81F86.pf ==> (Invalid signature! Should be 'SCCA')
```

4 실제 분석 사례 예시

WINPREFETCHVIEW Prefetch 파일 분석

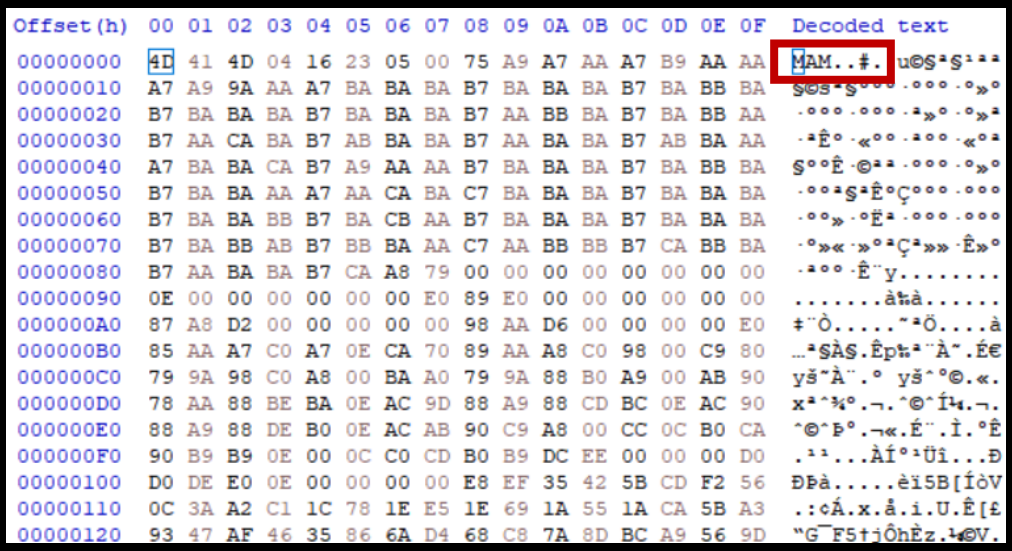
1. 압축을 해제하기 위한 w10pfdecomp.py 파일과 압축을 해제하기 위한 sourceFile인 "C:\Windows\Prefetch\WINPREFETCHVIEW.EXE-F70B7212.pf"과 압축이 풀린 파일을 저장할 경로를 지정해준다.

   python w10pfdecomp.py [sourceFile] [destinationFile]

```
PS C:\Users\lnsnd\Documents> python .\w10pfdecomp.py "C:\Windows\Prefetch\WINPREFETCHVIEW.EXE-F70B7212.pf"
 ./WINPREFETCHVIEW_decompress
Lucky man, you have your prefetch file ready to be parsed!
```

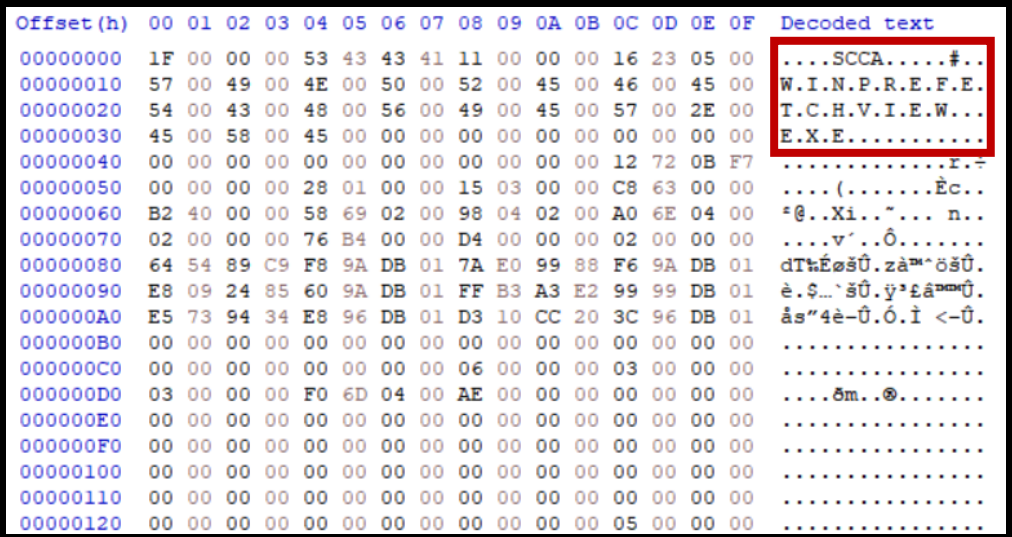
2. 압축 해제가 된 WINPREFETCHVIEW_decompress 파일을 HxD에서 연다.

< 압축 해제 전 >



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	4D	41	4D	04	16	23	05	00	75	A9	A7	AA	A7	B9	AA	AA	MAM..#..u©§ª§¹ªª
00000010	A7	A9	9A	AA	A7	BA	BA	BA	B7	BA	BA	BA	B7	BA	BB	BA	§©šª§ººº·ººº·º»º
00000020	B7	BA	BA	BA	B7	BA	BA	BA	B7	AA	BB	BA	B7	BA	BB	AA	·ººº·ººº·ª»º·º»ª
00000030	B7	AA	CA	BA	B7	AB	BA	BA	B7	AA	BA	BA	B7	AB	BA	AA	·ªÊº·«º·ªºº·«ºª
00000040	A7	BA	BA	CA	B7	A9	AA	AA	B7	BA	BA	BA	B7	BA	BB	BA	§ººÊ·©ªª·ººº·º»º
00000050	B7	BA	BA	AA	A7	AA	CA	BA	C7	BA	BA	BA	B7	BA	BA	BA	·ººª§ªÊºÇººº·ººº
00000060	B7	BA	BA	BB	B7	BA	CB	AA	B7	BA	BA	BA	B7	BA	BA	BA	·ºº»·ºËª·ººº·ººº
00000070	B7	BA	BB	AB	B7	BB	BA	AA	C7	AA	BB	BB	B7	CA	BB	BA	·º»«·»ºªÇª»»·Ê»º
00000080	B7	AA	BA	BA	B7	CA	A8	79	00	00	00	00	00	00	00	00	·ªºº·Ê¨y........
00000090	0E	00	00	00	00	00	00	E0	89	E0	00	00	00	00	00	00	.......à‰à......
000000A0	87	A8	D2	00	00	00	00	00	98	AA	D6	00	00	00	00	E0	‡¨Ò.....˜ªÖ....à
000000B0	85	AA	A7	C0	A7	0E	CA	70	89	AA	A8	C0	98	00	C9	80	…ª§À§.Êp‰ª¨À˜.É€
000000C0	79	9A	98	C0	A8	00	BA	A0	79	9A	88	B0	A9	00	AB	90	yš˜À¨.º yš^°©.«.
000000D0	78	AA	88	BE	BA	0E	AC	9D	88	A9	88	CD	BC	0E	AC	90	xª^¾º.¬.^©^Í¼.¬.
000000E0	88	A9	88	DE	B0	0E	AC	AB	90	C9	A8	00	CC	0C	B0	CA	^©^Þ°.¬«.É¨.Ì.°Ê
000000F0	90	B9	B9	0E	00	0C	C0	CD	B0	B9	DC	EE	00	00	00	D0	.¹¹...ÀÍ°¹Üî...Ð
00000100	D0	DE	E0	0E	00	00	00	00	E8	EF	35	42	5B	CD	F2	56	ÐÞà.....èï5B[Íòv
00000110	0C	3A	A2	C1	1C	78	1E	E5	1E	69	1A	55	1A	CA	5B	A3	.:¢Á.x.å.i.U.Ê[£
00000120	93	47	AF	46	35	86	6A	D4	68	C8	7A	8D	BC	A9	56	9D	"G¯F5†jÔhÈz.¼©V.

< 압축 해제 후 >



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	1F	00	00	00	53	43	43	41	11	00	00	00	16	23	05	00	....SCCA.....#..
00000010	57	00	49	00	4E	00	50	00	52	00	45	00	46	00	45	00	W.I.N.P.R.E.F.E.
00000020	54	00	43	00	48	00	56	00	49	00	45	00	57	00	2E	00	T.C.H.V.I.E.W...
00000030	45	00	58	00	45	00	00	00	00	00	00	00	00	00	00	00	E.X.E...........
00000040	00	00	00	00	00	00	00	00	00	00	00	00	12	72	0B	F7	.............r.÷
00000050	00	00	00	00	28	01	00	00	15	03	00	00	C8	63	00	00	....(.......Èc..
00000060	B2	40	00	00	58	69	02	00	98	04	02	00	A0	6E	04	00	²@..Xi..˜... n..
00000070	02	00	00	00	76	B4	00	00	D4	00	00	00	02	00	00	00	....v´..Ô.......
00000080	64	54	89	C9	F8	9A	DB	01	7A	E0	99	88	F6	9A	DB	01	dT‰Éøš Û.zà™^öš Û.
00000090	E8	09	24	85	60	9A	DB	01	FF	B3	A3	E2	99	99	DB	01	è.$…`š Û.ÿ³£â™™Û.
000000A0	E5	73	94	34	E8	96	DB	01	D3	10	CC	20	3C	96	DB	01	å s"4è–Û.Ó.Ì <–Û.
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000000C0	00	00	00	00	00	00	00	00	06	00	00	00	03	00	00	00	....
000000D0	03	00	00	00	F0	6D	04	00	AE	00	00	00	00	00	00	00	....ðm..®.......
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000120	00	00	00	00	00	00	00	00	00	00	00	00	05	00	00	00	....

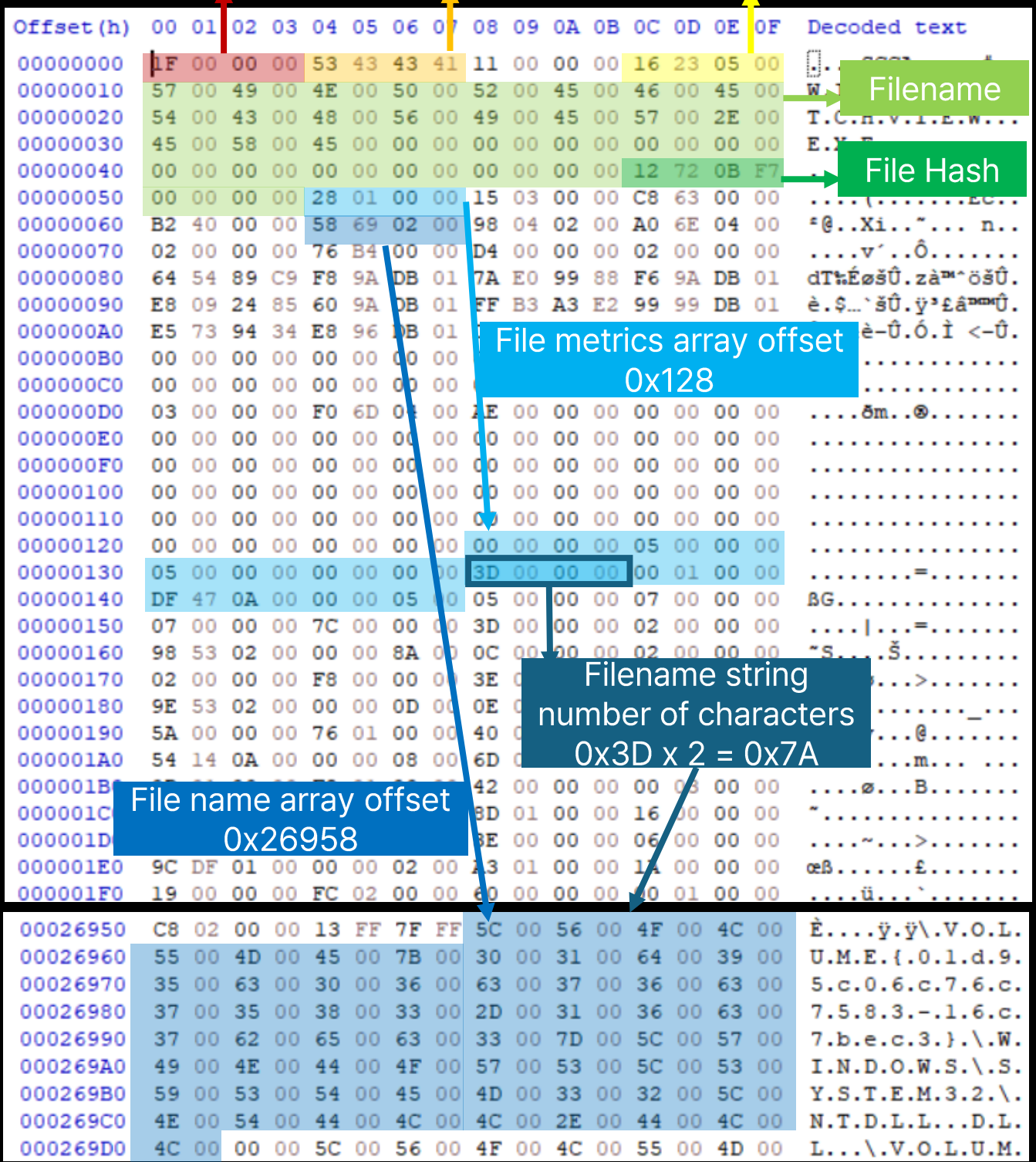
4 실제 분석 사례 예시

WINPREFETCHVIEW Prefetch 파일 분석

Format Version
Windows 11 - 30 version

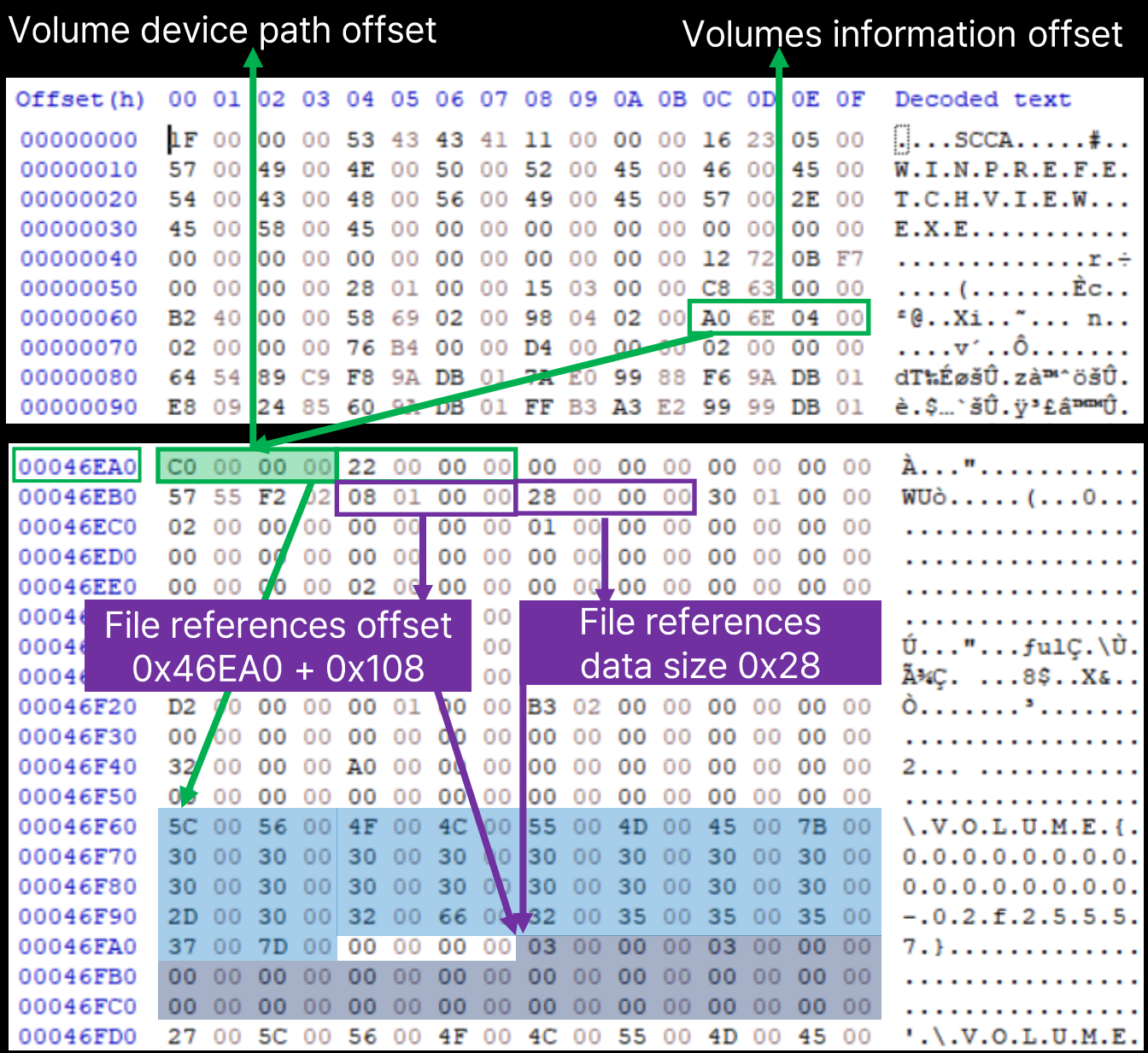
File Signature

파일 크기 336662 byte



4 실제 분석 사례 예시

WINPREFETCHVIEW Prefetch 파일 분석



References

- Shashidhar, Narasimha, and Dylan Novak. "Digital forensic analysis on prefetch files." International Journal of Information Security Science 4.2 (2015): 39-49.
- https://gist.github.com/dfirfpi/113ff71274a97b489dfd
- https://learn.microsoft.com/en-us/previous-versions/technet-magazine/cc162480(v=msdn.10)?redirectedfrom=MSDN#s5
- https://github.com/proneer/Slides – (FP) 프리, 슈퍼 패치 포렌식.PDF
- https://github.com/libyal/libscca/blob/main/documentation/Windows%20Prefetch%20File%20(PF)%20format.asciidoc
- https://forensics.wiki/windows_prefetch_file_format/#file-metrics-entry-record-version-26
- https://www.forensic-cheatsheet.com/KR/Artifact/Prefetch+%26+Superfetch