

5주차 스터디

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

X-Ways Forensics

- TODO

[xways-forensics - forensenellanebbia](#)

[WinHex_Templates](#)

[AutoF](#)

[X-Ways Forensics X-Tensions](#)

참고자료

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

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

컴퓨터\HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\bc\71F23C34			
	이름	종류	데이터
Interface			
Inkfile			
Local Settings			
ImmutableMuiCache			
MrtCache			
MuiCache			
bc			
71F23C34			
Software			
Microsoft			
Windows			
CurrentVersion			
	@C:\Program Files (x86)\Common Files\Microsoft ...	REG_SZ	Visual Studio로 열기(&V)
	@C:\Program Files (x86)\VMware\VMware Worksta...	REG_SZ	This VMware product requires administrator privil...
	@C:\Program Files\Common Files\system\wab32r...	REG_SZ	연락처
	@C:\Program Files\Microsoft Office\Root\VF\SWPr...	REG_SZ	Microsoft Excel 워크시트
	@C:\Program Files\Microsoft Office\Root\VF\SWPr...	REG_SZ	Microsoft Excel 쉼표로 구분된 값 파일
	@C:\Program Files\Microsoft Office\Root\VF\SWPr...	REG_SZ	Microsoft Word 문서
	@C:\Program Files\Microsoft Office\Root\VF\SWPr...	REG_SZ	Microsoft PowerPoint 프레젠테이션
	@C:\Program Files\Microsoft Office\root\VF\SWPr...	REG_SZ	Word
	@C:\Program Files\Microsoft Office\root\VF\SWPr...	REG_SZ	Excel
	@C:\WINDOWS\regedit.exe,-16	REG_SZ	레지스트리 편집기
	@C:\WINDOWS\System32\acppage.dll,-6002	REG_SZ	Windows 배치 파일

참고자료

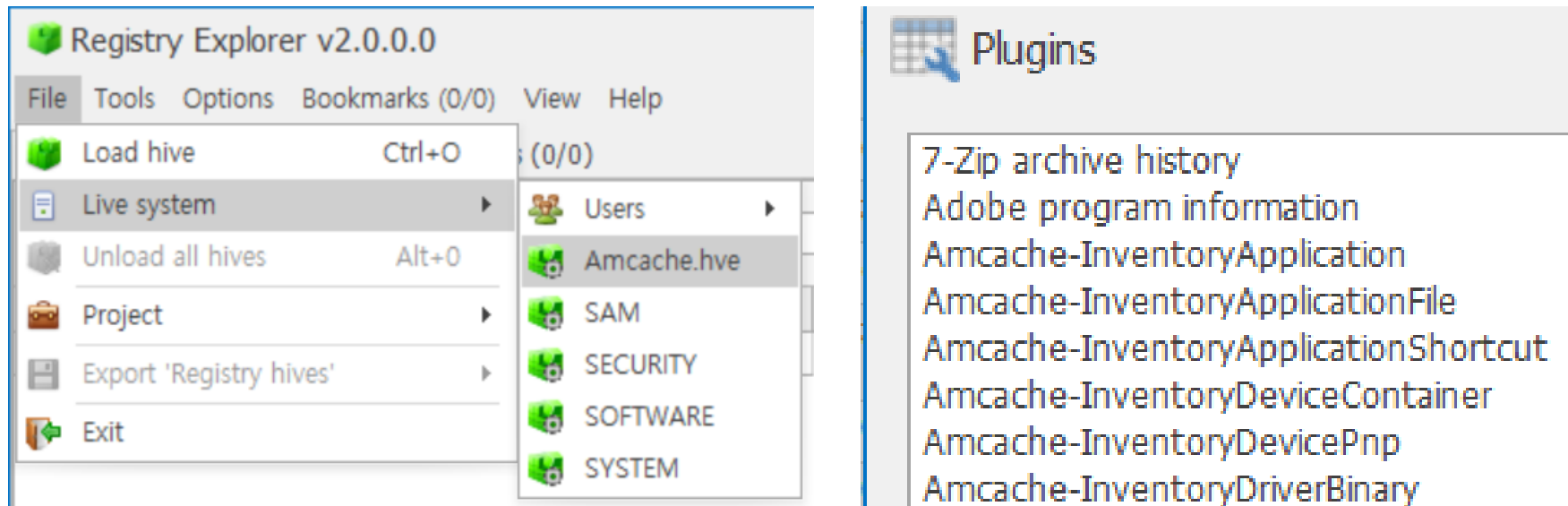
- [MUICache - forensic-artifacts](#)
- [기초부터 따라하는 디지털포렌식](#)
- [Forensic Analysis of MUICache Files in Windows](#)

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.

Registry Explorer v2.0.0.0
File Tools Options Bookmarks (0/0) View Help

Registry hives (1) Available bookmarks (0/0)

Enter text to search... Find

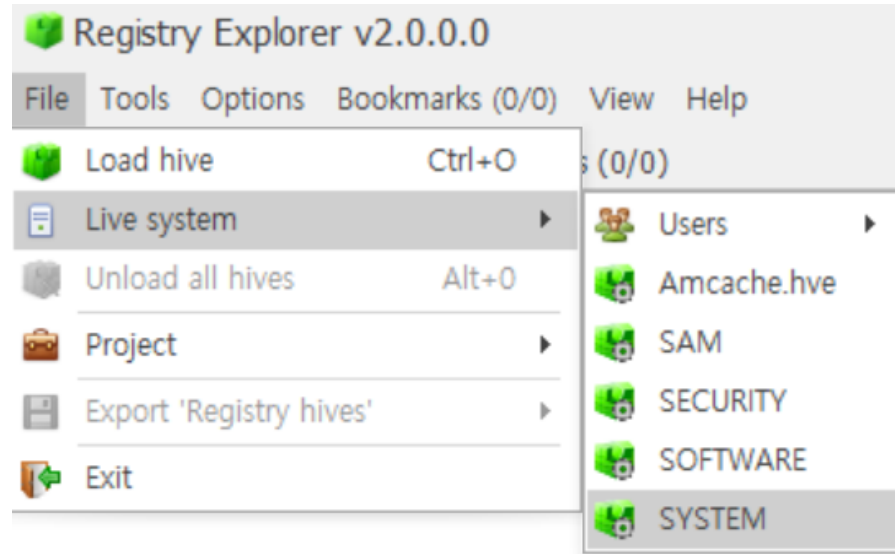
Key name	# values	# subkeys	Last write timestamp
C:\Windows\System32\Wbem\WMI\InventoryApplicationFile	2	2,691	2024-02-01 18:30:22
InventoryApplicationFile	2	198	2024-02-01 16:25:16
InventoryApplicationShortcut	2	0	2024-02-01 17:24:07
InventoryDeviceSensor	2	84	2024-01-28 19:21:29
MareBackupApps	2	6	2024-02-01 00:04:16
DeviceCensus	6	0	2024-02-01 16:25:16
InventoryApplicationFramework	6	33	2024-01-28 19:21:08
InventoryMiscellaneous	6	8	2024-01-22 12:16:34
InventoryMiscellaneousMemorySlotArrayInfo	6	12	2024-01-22 12:16:34
InventoryMiscellaneousUser	6	20	2024-02-01 00:04:18
InventoryMiscellaneousUIPInfo	6	7	2024-02-01 17:24:07
InventoryDeviceContainer	7	1	2024-02-01 17:24:07
InventoryDeviceInterface	7	2	2024-02-01 17:24:07
InventoryDeviceMediaClass	7	1	2024-02-01 17:24:07
InventoryDeviceUsbHubClass	7	446	2024-02-01 17:24:07
InventoryDriverBinary	7	56	2024-02-01 17:24:07
InventoryDriverPackage	7	381	2024-02-01 16:25:22
InventoryApplication	8	185	2024-02-01 17:24:07
InventoryDevicePnp	8		

Values Amcache-InventoryApplicationFile

Drag a column header here to group by that column

Timestamp	Path	Name	Product Name	Publisher	Version	SHA1
2024-01-22 12:15:59	c:\Program Files (x86)\Windows Kits\10\WinBin\10.0.22621.0\Wx64\adpcmencode3.exe	adpcmencode3.exe	microsoft® windows® operating system	microsoft corporation	10.0.22621.2428 (winbuild.160101.0800)	f7c943a02d469855aa2e4abe0e429de85a
2024-01-22 12:15:59	c:\Program Files (x86)\Windows Kits\10\WinBin\10.0.22621.0\Wx64\adpcmencode3.exe	adpcmencode3.exe	microsoft® windows® operating system	microsoft corporation	10.0.22621.2428 (winbuild.160101.0800)	1e2edb3b955c64f9233e039958b8f3fe7c6
2024-01-22 12:15:59	c:\Users\Whyuunnnn\AppData\Local\Waffine\Waffine.exe	AFFINE.exe	affine	toeverything	0.11.3	d5520b82f8f487bbf1e1f0cd8ceb4cf2b6d
2024-01-22 12:15:59	c:\Users\Whyuunnnn\AppData\Local\Waffine\Wapp-0.11.0\Waffine.exe	AFFINE.exe	affine	toeverything	0.11.3	07e86888232c723887caf0e3628689c45e
2024-01-25 12:33:40	c:\Windows\System32\Waggregator\host.exe	AggregatorHost.exe	microsoft® windows® operating system	microsoft corporation	10.0.22621.2506 (winbuild.160101.0800)	810101becfeaf16a23e566385644454b7a
2024-01-22 12:15:59	c:\Program Files\Wingw64\Wbin\Wahost.exe	ahost.exe				595ce7d96d1dc0a24f969d09c4c8215ba2
2024-01-22 12:15:59	c:\Program Files\Microsoft Office\Wroot\Wv\ProgramFilesCommonx64\Microsoft Shared\Woffice16\Wai.exe	ai.exe	artificial intelligence	microsoft corporation	0.14.12.0	ec80d3d49a04edd22d5a7820ef36d30783
2024-01-22 12:15:59	c:\Program Files\Microsoft Office\Wroot\Wv\ProgramFilesCommonx86\Microsoft Shared\Woffice16\Wai.exe	ai.exe	artificial intelligence	microsoft corporation	0.14.12.0	5f66ee17a5900e6511d58ff1211a02df397
2024-01-22 12:15:59	c:\Program Files\Microsoft Office\Wroot\Wv\ProgramFilesCommonx86\Microsoft Shared\Woffice16\Waimgr.exe	aimgr.exe	artificial intelligence	microsoft corporation	0.14.12.0	25f27be54803a2e2acc721217f51efe5807
2024-01-22 12:15:59	c:\Program Files\Microsoft Office\Wroot\Wv\ProgramFilesCommonx64\Microsoft Shared\Woffice16\Waimgr.exe	aimgr.exe	artificial intelligence	microsoft corporation	0.14.12.0	d3a7735b54f40b5414e43ab544347ace15
2024-01-22 12:15:59	c:\Users\Whyuunnnn\AppData\Local\Zoom\Wbin\Wairhost.exe	airhost.exe	airhost	zoom video communications, inc.	5.17.2.29988	92e7865336354ea56a5b059dc80ef71eeb
2024-01-22 12:15:59	c:\Program Files (x86)\Windows Kits\10\Wapp certification\Waltstatic.exe	altstatic.exe	microsoft® windows® operating system	microsoft corporation	10.0.22621.2428 (winbuild.160101.0800)	10ee1257ba999eb13f287ba8667d9b54c
2024-01-22 12:15:59	c:\Program Files (x86)\Microsoft SDKs\Windows\10.0a\WinWnetfx 4.8\tools\Wx64\Wai.exe	ai.exe	microsoft® .net framework	microsoft corporation	14.8.3928.0 built by: net48rel1	f10c3293ac5c2c171cd70908f36aa25e583
2024-01-22 12:15:59	c:\Program Files (x86)\Microsoft SDKs\Windows\10.0a\WinWnetfx 4.8\tools\Wai.exe	ai.exe	microsoft® .net framework	microsoft corporation	14.8.3928.0 built by: net48rel1	957ce0fea65f6287f4d08929fa9f947d2
2024-01-22 12:15:59	c:\Program Files\Walcritty\Walcritty.exe	alacritty.exe				6c5448d7513021353f673789a9f922513c

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

[illegible]

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
        종 류               : 30  WIN32
        상 태               : 4   RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE      : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        검 사 점            : 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
- 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](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

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

WinPrefetchView

File Edit View Options Help

Filename	Created Time	Modified Time	File S...	Process EXE	Process Path	Run Counter	Last Run Tir
OIAJDNGXORFO.EXE-D7D393C8.pf	2024-01-03 오후 5:18:11	2024-01-03 오후 5:18:11	19,868	OIAJDNGXORFO.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
OIAJDNGXORFO.EXE		\\VOLUME{01da3e1675b2d18c-0e75ba0e}#USERS#USER#APPDATA#LOCAL#TEMP#OIAJDNGXORFO.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.

WinPrefetchView

File Edit View Options Help

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
APPHELP.DLL		#VOLUME{01da3e1675b2d18c-0e75ba0e}#WINDOWS#SYSWOW64#APPHELP.DLL	11
AUDIODEV.DLL		#VOLUME{01da3e1675b2d18c-0e75ba0e}#WINDOWS#SYSWOW64#AUDIODEV.DLL	139
BCRYPT.DLL		#VOLUME{01da3e1675b2d18c-0e75ba0e}#WINDOWS#SYSWOW64#BCRYPT.DLL	106

참고자료

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








ThumbnailCache & IconCache

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

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

ThumbnailCache & IconCache

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

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

ThumbnailCache & IconCache

- Thumbcache Viewer 도구를 사용하여 분석 가능

Thumbcache Viewer

File Edit View Tools Help

#	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\Whyuunnnn\A...
626	efa8cefd8a8ee752	1671360 B	0 KB	1671448 B	0 KB					C:\Users\Whyuunnnn\A...
627	e768e22ed2598066	1671448 B	0 KB	1671536 B	0 KB					C:\Users\Whyuunnnn\A...
628	a771cc766136dd69	1671536 B	0 KB	1671624 B	0 KB					C:\Users\Whyuunnnn\A...
629	3392e93cffabcc64	1671624 B	0 KB	1671712 B	0 KB					C:\Users\Whyuunnnn\A...
630	26c48e99a84dc465	1671712 B	0 KB	1671800 B	0 KB					C:\Users\Whyuunnnn\A...
631	2c0be1dced754061	1671800 B	0 KB	1671888 B	0 KB					C:\Users\Whyuunnnn\A...
632	bc0fc576ab0ef84d	1671888 B	0 KB	1671976 B	0 KB					C:\Users\Whyuunnnn\A...
633	2ff2b30bcc7a36ef	1671976 B	0 KB	1672064 B	0 KB					C:\Users\Whyuunnnn\A...
634	3ecd1d6ab1aabb47.png	1672064 B	22 KB	1672152 B	22 KB					C:\Users\Whyuunnnn\A...
635	691e9732033f12d7.png	1695258 B	21 KB	1695346 B	21 KB					C:\Users\Whyuunnnn\A...
636	3fab139e6eff416f.png	1717328 B	14 KB	1717416 B	14 KB					C:\Users\Whyuunnnn\A...
637	21cb489a69da2d3d.png	1731986 B	45 KB	1732074 B	45 KB					C:\Users\Whyuunnnn\A...
638	8756692c421d4b25.png	1778872 B	7 KB	1778960 B	7 KB					C:\Users\Whyuunnnn\A...
639	7f7d008b6c11e6f2.png	1786996 B	24 KB	1787084 B	24 KB					C:\Users\Whyuunnnn\A...
640	b5822127a7e4ea8.png	1812096 B	14 KB	1812182 B	14 KB					C:\Users\Whyuunnnn\A...
641	1d9c30c84612c353.png	1826602 B	18 KB	1826690 B	18 KB					C:\Users\Whyuunnnn\A...
642	74ae8704a1518abd.png	1845608 B	31 KB	1845696 B	31 KB					C:\Users\Whyuunnnn\A...
643	deef37cedb9b7f6f.png	1877678 B	11 KB	1877766 B	11 KB					C:\Users\Whyuunnnn\A...

21cb489a69da2d3d.png - 256x138

제311조(전송서등) ① 제2조의 규정 이외에 피고인 또는 피고인이 아닌 자가 작성한 전송서나 그 전송을 기재한 서류로서 그 작성자 또는 전송자의 자필이거나 그 서형 또는 날인이 없는 것(피고인 또는 피고인이 아닌 자가 작성하거나 전송한 내용이 포함된 문자·사진·영상 등의 정보로서 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체에 저장된 것을 포함한다. 이하 이 조에서 같다)은 공판준비나 공판기일에서 그 작성자 또는 전송자의 진술에 의하여 그 진술의 진정함이 증명된 때에는 증거로 할 수 있다. 단, 피고인의 진술을 기재한 서류는 공판준비 또는 공판기일에서 그 작성자의 진술에 의하여 그 진술의 진정함이 증명되고 그 진술이 특히 신빙할 수 있는 상태하에서 행하여 진 때에 한하여 피고인의 공판준비 또는 공판기일에서의 진술에 불구하고 증거로 할 수 있다. <개정 2016.5.29.>

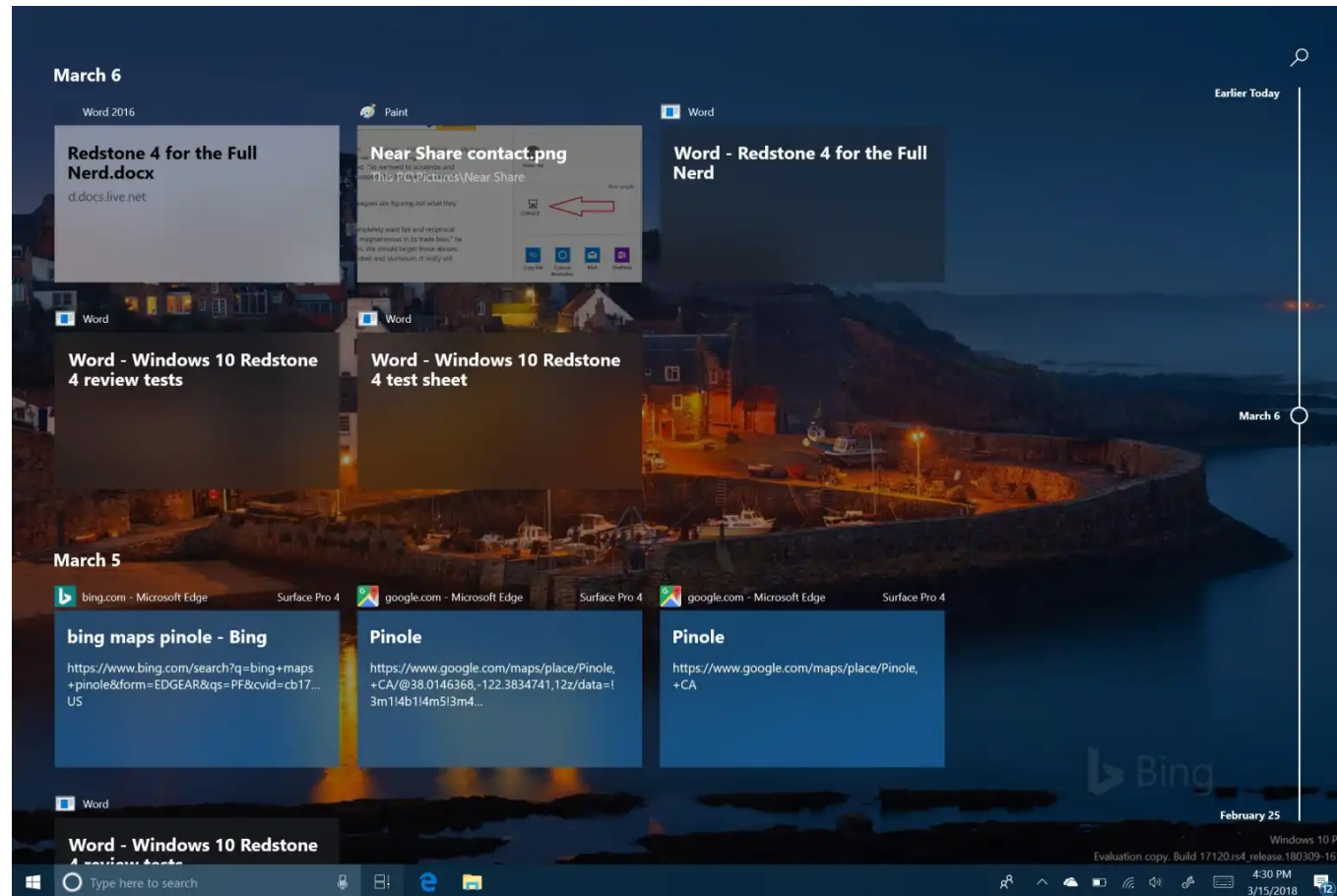
② 제1항 본문에도 불구하고 전송서의 작성자가 공판준비나 공판기일에서 그 진술의 진정을 부인하는 경우에는 과학적 분석결과에 기초한 디지털포렌식 자료, 감정 등 객관적 방법으로 진술의 진정함이 증명되는 때에는 증거로 할 수 있다. 다만, 피고인 아닌 자가 작성한 전송서는 피고인 또는 변호인이 공판준비 또는 공판기일에 그 기재 내용에 관하여 작성자를 신문할 수 있었을 것을 요한다. <개정 2016.5.29.>

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, 사용자가 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 아키텍처 자이.pdf	C:\Users\...	file:///C:/Users/User/Downloads/x86 x86_64 아키텍처 자이.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.
- 파일, 폴더 경로 , 생성, 접근, 인덱싱된 시간 정보 , Summary 정보 등 확인 가능



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.

- **SIDR**는 `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_9ZT77f8&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=rEoBox5lzkoh 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

- Summary 정보를 통해 해당 파일의 내용 확인 가능

System_ItemName	System_ItemPathDisplay	System_ItemDate	System_Search_GatherTime
https://www.microsoft.com/ko-kr/edge/welcome?form=MA13FJ	winrt:///S-1-5-21-44020401-28T16:58:01.7464130Z	2024-01-28T16:58:01.7464130Z	2024-01-28T16:58:01.7508640Z
https://www.office.com/	winrt:///S-1-5-21-44020401-28T16:58:01.7486360Z	2024-01-28T16:58:01.7486360Z	2024-01-28T16:58:01.7643372Z
https://www.bing.com/search?q=hxd&form=WSBEDG&q=CT&	winrt:///S-1-5-21-44020401-28T16:58:01.7464510Z	2024-01-28T16:58:01.7464510Z	2024-01-28T16:58:01.8119503Z
https://www.bing.com/search?q=aint&form=WSBEDG&q=SW&	winrt:///S-1-5-21-44020401-28T16:58:01.7464620Z	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 많이 있다.
 - Mac 포렌식, Linux 포렌식, 모바일 포렌식 등등
 - [forensic-artifacts](#), [13Cubed](#), [DFIRScience](#), [SANSForensics](#), [Ali Hadi](#), [ArtifactParsers](#), [awesome-forensics](#), [FrequentlyAskedDFIRQuestions](#), [The Hitchhikers Guide to DFIR: Experiences From Beginners and Experts](#) 등 찾아볼 수 있는 경로는 많이 있다.
 - 새로운 정보를 주기적으로 찾고자 하는 마인드 필요 - 컴퓨터 모든 분야 해당
- 아직 발견되지 않은 새로운 아티팩트들이 존재할 수도 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](#)