

윈도우 아티팩트

분석 및 실습

금융보안원 침해대응부 침해대응기획팀 이승주 수석



INDEX

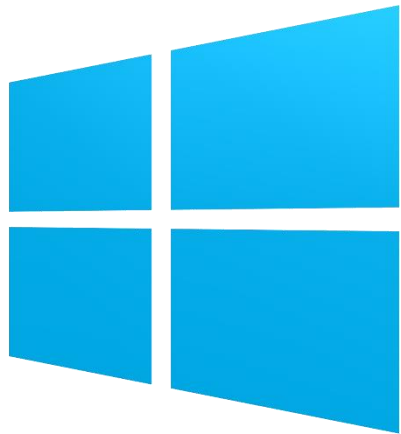
1. 윈도우 포렌식
2. 윈도우 아티팩트 종류별 설명



윈도우 포렌식

- 윈도우 포렌식 개요
- 윈도우 포렌식 수행 시 고려사항





윈도우 환경에서 수행하는 포렌식

- ◆ 윈도우 운영체제에서 수집할 수 있는 다양한 데이터(아티팩트)들을 기반으로 수행하는 디지털 포렌식



여러 아티팩트들을 종합적으로 활용

- ◆ 아티팩트란 OS, 프로그램 등을 사용하면서 생성되는 흔적을 의미
- ◆ 다양한 아티팩트에서 유의미한 정보를 추출하는 것이 중요

사용자 행위는
어디에 저장?

시스템, 프로그램
동작 원리는?

어떤 아티팩트를
참고?

윈도우 아티팩트 종류별 설명

- 레지스트리(Registry)
- 이벤트로그(EventLog)
- 바로가기(.lnk)
- 점프리스트(Jumplist)
- 알림(Notification)
- 프리패치(Prefetch)
- 휴지통
- 썸네일(Thumbnail)
- 아이콘캐시(IconCache)
- Web Artifact
- 이메일(Outlook)
- VSS
- NTFS 로그파일
- 타임라인
- Windows Index



윈도우 아티팩트 종류별 확인 내용 및 사용 도구 요약

아티팩트	확인 내용	도구
레지스트리	<ul style="list-style-type: none">프로그램 실행 이력, USB 사용 이력, 윈도우 설치 정보, 계정 정보 등	RegistryExplorer, UserAssistView 등
이벤트로그	<ul style="list-style-type: none">외부 로그인 이력, 전원 온/오프 기록, 보안 설정 변경 이력 등	Windows Message Analyzer, 기본 이벤트로그 뷰어
바로그가기	<ul style="list-style-type: none">프로그램 설치 여부 확인	LinkParser, WFA
점프리스트	<ul style="list-style-type: none">사용자가 최근 사용한 프로그램, 파일 이력 확인	JumpListExplorer
알림	<ul style="list-style-type: none">프로그램 팝업 메시지, 보안/업데이트 정보 등 확인	DB Browser for SQLite, SQLite Expert
프리패치	<ul style="list-style-type: none">프로그램 실행 여부 확인	WinPrefetchView
휴지통	<ul style="list-style-type: none">삭제된 파일 확인, 파일 복구	WFA
썸네일	<ul style="list-style-type: none">파일아이콘/사진/동영상/문서 존재 여부 확인	thumbcache_viewer
아이콘캐시	<ul style="list-style-type: none">파일아이콘/사진/동영상/문서 존재 여부 확인	thumbcache_viewer
웹 아티팩트	<ul style="list-style-type: none">웹 접속기록, 캐시, 다운로드 기록 확인	BrowsingHistoryView, ChromeCacheView
이메일	<ul style="list-style-type: none">이메일 송/수신 이력, 첨부파일 등 확인	ost-viewer.exe
VSS	<ul style="list-style-type: none">특정 시점의 볼륨 정보 확인, 공격 시점 또는 이전 시점 복구 가능	ShadowCopyView
NTFS 로그파일	<ul style="list-style-type: none">파일 생성, 수정, 삭제 여부 확인	NTFS Log Tracker
타임라인	<ul style="list-style-type: none">사용자가 최근 작업하던 문서, 웹페이지 등 추적 가능	DB Browser for SQLite
Windows Index	<ul style="list-style-type: none">윈도우에서 파일 검색 시 활용하는 Index 기록 확인	WinSearchDBAnalyzer(Win10), SIDR(Win11)

레지스트리(Registry)



레지스트리(Registry)

- 윈도우 운영체제와 응용 프로그램 운영에 필요한 정보를 가진 계층형 데이터베이스
 - 사용자 계정 정보
 - 자동시작 프로그램
 - 윈도우 설치 정보
 - 외부매체 사용 흔적
 - 프로그램 사용 흔적 등



레지스트리(Registry) - 주요 용어

- 레지스트리 키(Key) : 계층적 파일 시스템의 폴더와 비슷한 개념, 하위 키를 포함
- 레지스트리 값(Value) : 폴더에 속한 파일과 비슷한 개념, 레지스트리 내 데이터 저장
- 레지스트리 타입(Type) : 레지스트리 내 데이터가 가지는 종류를 표현
- 레지스트리 데이터(Data) : Value가 가지는 값

regedit 실행 화면

Root Key

레지스트리 편집기			
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)			
컴퓨터\HKEY_CURRENT_USER\Console			
컴퓨터	이름	종류	데이터
Root Key			
> HKEY_CLASSES_ROOT	(기본값)	REG_SZ	(값 설정 안 됨)
> HKEY_CURRENT_USER	ColorTable00	REG_DWORD	0x000c0c0c (789516)
> AppEvents	ColorTable01	REG_DWORD	0x00da3700 (14300928)
> Console	ColorTable02	REG_DWORD	0x000ea113 (958739)
> Control Panel	ColorTable03	REG_DWORD	0x00dd963a (14521914)
> Environment	ColorTable04	REG_DWORD	0x001f0fc5 (2035653)
> EUDC	ColorTable05	REG_DWORD	0x00981788 (9967496)
> Keyboard Layout			
Key	Value	Type	Data

레지스트리(Registry) – Root Key

루트 키	약어	설명
HKEY_CLASSES_ROOT	HKCR	<ul style="list-style-type: none">파일 확장자 연결 정보와 COM 객체 등록 정보별도의 하이브를 가지지 않고 다른 루트 키의 하위 키로 구성<ul style="list-style-type: none">HKEY_LOCAL_MACHINE\Software\ClassesHKEY_CURRENT_USER\Software\Classes
<u>HKEY_CURRENT_USER</u>	HKCU	<ul style="list-style-type: none">현재 시스템에 로그인 된 사용자의 프로파일 정보HKU\<USER SID> 참조
<u>HKEY_LOCAL_MACHINE</u>	HKLM	<ul style="list-style-type: none">시스템의 하드웨어, 소프트웨어 설정 및 기타 환경 정보시스템에 존재하는 하이브 파일과 메모리 하이브 모음
HKEY_USERS	HKU	<ul style="list-style-type: none">시스템의 모든 사용자와 그룹에 관한 프로파일 정보사용자 루트 폴더에 존재하는 NTUSER.DAT 파일의 내용
HKEY_CURRENT_CONFIG	HKCC	<ul style="list-style-type: none">시스템이 시작할 때 사용되는 하드웨어 프로파일 정보HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current 내용
HKEY_PERFORMANCE_DATA	HKPD	<ul style="list-style-type: none">성능 카운트/정보 저장, 하이브에 저장되지 않아 레지스트리 에디터에 표시되지 않음작업관리자의 성능 탭 또는 Windows API의 레지스트리 기능을 통해 볼 수 있음
HKEY_DYN_DATA	HKDD	<ul style="list-style-type: none">Windows 95, 98, Me에서 사용하였으며 현재는 사용하지 않음

레지스트리(Registry) – Type

번호	이름	설명
0x0	REG_NONE	종류 없음
0x1	REG_SZ	문자열 값
0x2	REG_EXPAND_SZ	확장할 수 있는 문자열 값. 환경 변수를 포함할 수 있다. 예) "%PATH%"
0x3	REG_BINARY	이진수 값 (임의의 데이터)
0x4	REG_DWORD/REG_DWORD_LITTLE_ENDIAN	DWORD 값 (32 비트) 정수 (0 ~ 4,294,967,295 [$2^{32} - 1$]) (Little Endian)
0x5	REG_DWORD_BIG_ENDIAN	DWORD 값 (32 비트) 정수 (0 ~ 4,294,967,295 [$2^{32} - 1$]) (Big Endian)
0x6	REG_LINK	심볼 링크 (유니코드)
0x7	REG_MULTI_SZ	다중 문자열 값 (고유한 문자열의 배열)
0x8	REG_RESOURCE_LIST	리소스 목록 (플러그 앤 플레이 하드웨어 열거 및 구성에 쓰임)
0x9	REG_FULL_RESOURCE_DESCRIPTOR	리소스 서술자 (플러그 앤 플레이 하드웨어 열거 및 구성에 쓰임)
0xA	REG_RESOURCE_REQUIREMENTS_LIST	리소스 요구 목록 (플러그 앤 플레이 하드웨어 열거 및 구성에 쓰임)
0xB	REG_QWORD/REG_QWORD_LITTLE_ENDIAN	QWORD 값 (64 비트 정수), 빅/리틀 엔디언 또는 정의되지 않음 (윈도우 2000에 도입)

레지스트리(Registry) - Hive

- 하이브(Hive)
 - 레지스트리 키, 하위 키 및 값에 대한 **논리적인 그룹**
 - 루트키(HKEY로 시작)부터 그 아래의 모든 키를 포함하는 트리 구조
- 하이브(Hive) 파일
 - 레지스트리 정보를 저장하고 있는 파일
 - 레지스트리를 구성하는 키(key), 값 등이 논리적인 구조로 저장
 - SAM, SECURITY, SYSTEM, SOFTWARE 등

레지스트리(Registry) – Hive 경로(1)

파일 경로에서 %로 둘러싸인 문자는 환경변수를 의미
-> set 명령어를 통해 확인 가능

이름	파일 경로	설명
NTUSER.DAT	%UserProfile%	<ul style="list-style-type: none">· 사용자 특정 데이터· HKEY_USERS\<SID>
UsrClass.dat	%UserProfile%\AppData\Local\Microsoft\Windows	<ul style="list-style-type: none">· 파일 연결 및 COM 레지스트리 항목· HKEY_USERS\<SID> \Classes
<u>SAM</u>	%SystemRoot%\System32\config	<ul style="list-style-type: none">· Security Account Manager, 로컬 계정/그룹 정보· HKEY_LOCAL_MACHINE\SYSTEM\SAM
<u>SECURITY</u>	%SystemRoot%\System32\config	<ul style="list-style-type: none">· 보안 데이터· HKEY_LOCAL_MACHINE\SYSTEM\SECURITY
<u>SOFTWARE</u>	%SystemRoot%\System32\config	<ul style="list-style-type: none">· 소프트웨어 데이터· HKEY_LOCAL_MACHINE\SYSTEM\SOFTWARE
<u>SYSTEM</u>	%SystemRoot%\System32\config	<ul style="list-style-type: none">· 시스템 데이터· HKEY_LOCAL_MACHINE\SYSTEM
DEFAULT	%SystemRoot%\System32\config	<ul style="list-style-type: none">· NTUSER.DAT 레지스트리의 템플릿 파일· HKEY_USERS\<SID>\DEFAULT

레지스트리(Registry) – Hive 경로(2)

이름	파일 경로	설명
BBI	%SystemRoot%\System32\config	· 백그라운드 작업 정보
BCD-Template	%SystemRoot%\System32\config	· BCD 레지스트리 템플릿 파일 · Windows 8 and later
COMPONENTS	%SystemRoot%\System32\config	· 윈도우 옵션과 관련한 데이터 · HKEY_LOCAL_MACHINE\COMPONENTS
DRIVERS	%SystemRoot%\System32\config	· 드라이버 데이터베이스 · Windows 8 and later
ELAM	%SystemRoot%\System32\config	· ELAM(Early Launch Anti-Malware) · Windows 8 and later
SCHEMA.DAT	%SystemRoot%\System32\SMI\Store\Machine	· SMI(Settings Management Infrastructure) · HKEY_LOCAL_MACHINE\SCHEMA
Amcache.hve	%SystemRoot%\AppCompat\Programs	· 응용 프로그램 호환 데이터베이스 · Windows 7 and later
Syscache.hve	%SystemDrive%\SystemVolumeInformation	· Volume Shadow Copy 관련 · Windows 7 and later

레지스트리(Registry) – Hive 실습

- **사용 도구**

- [FTK Imager](#) : Hive 파일 추출
- [regedit.exe](#) : 현재 시스템에 존재하는 레지스트리 하이브 분석 (윈도우 기본 프로그램)
- [RegistryExplorer](#) : 추출한 Hive 파일 분석 (Eric Zimmerman 개발)

- **실습 목적**

- 윈도우 설치 시간 확인
- 설치된 프로그램, 자동 시작 프로그램 목록 확인
- 사용자 계정 정보 확인
- 저장장치 연결 흔적 확인 등

레지스트리(Registry) – Hive 실습

- 윈도우 설치 시간

- 시스템 표준 시간 확인



- HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

- 윈도우 설치 시간 확인

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion

- InstallTime의 시간 정보가 실제 운영체제 설치 시간보다 이전일 경우, 수정 의심

- **InstallDate : Unix 32bit timestamp**

 InstallDate	REG_DWORD	0x5df09064 (1576046692)
 InstallTime	REG_QWORD	0x1d5afee7df22a77 (132205202927397495)

- **InstallTime : Windows 64bit timestamp**

- ◆ CurrentControlSet : 001 또는 다른 키에 대한 링크

- ◆ ControlSet001 : 가장 최근에 사용된 부팅 설정

- * SYSTEM 하위 Select 키 확인

레지스트리(Registry) – Hive 실습

- **자동시작 프로그램 (Autoruns 프로그램 통해 확인 가능)**
 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
 - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
 - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
 - **Run : 시스템이 부팅할 때 마다 실행**
 - **RunOnce : 1회 실행 후 삭제**
 - **RunOnceEx : 1회 실행 및 종료 후 삭제**

레지스트리(Registry) – Hive 실습

- 외부 저장매체 연결 흔적
 - HKLM\SYSTEM\CurrentControlSet\Enum\USB
 - VID #####&PID #####
 - 제조사ID(VID) 및 제품ID(PID) 확인 가능
 - HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR
 - 해당 시스템에서 사용했던 USB 장치 확인 가능
 - HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{GUID}
 - HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices
 - HKLM\SOFTWARE\Microsoft\Windows Search\VolumeInfoCache\Volume:
 - HKLM\SYSTEM\MountedDevices

레지스트리(Registry) – Hive 실습

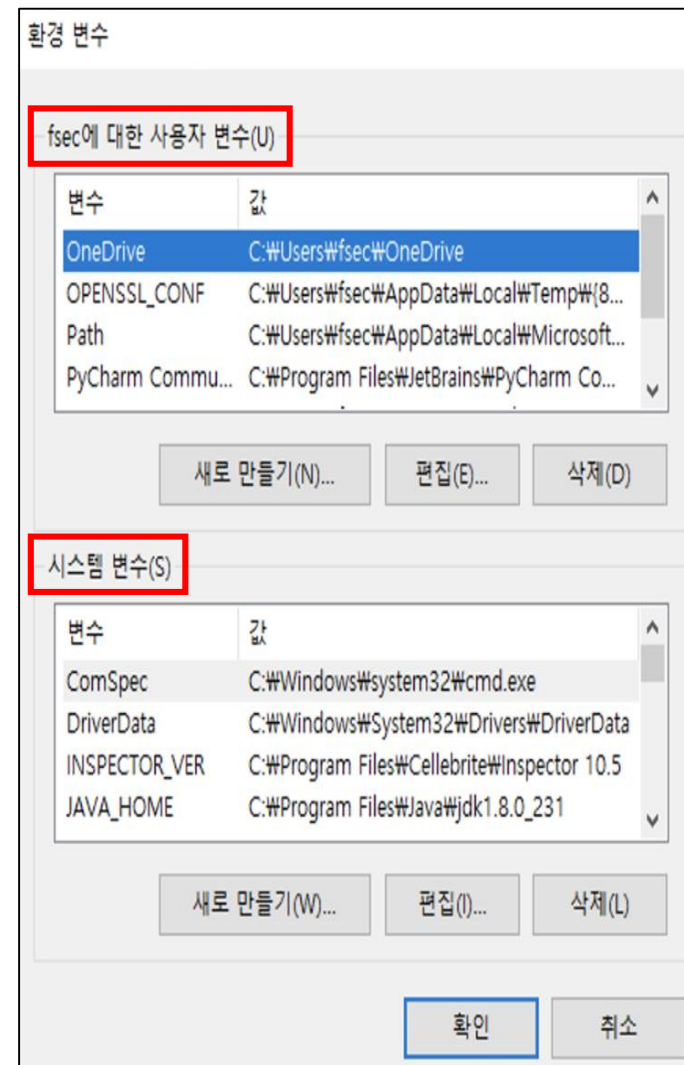
- 사용자 계정 정보

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\
 - S-1-5-18 : systemprofile
 - S-1-5-19 : LocalService
 - S-1-5-20 : NetworkService
 - S-1-5-21 : 사용자가 만든 계정
- 1000 이상은 user 권한
- 500은 administrator
- 최종 로그인 시간 : LocalProfileLoadTimeHigh/Low 순서대로 조합 후 계산
- Guest 계정 정보까지 확인할 수 있는 경로
 - HKLM\SAM\SAM\Domains\Account\Users\Names

레지스트리(Registry) – Hive 실습

• 환경변수 정보

- [내컴퓨터 - 오른쪽 클릭 - 속성 - 고급 시스템 설정 - 고급 - 환경 변수]
- **HKCU\Environment**
 - 사용자 환경변수 정보
 - 로컬 사용자별로 생성
- **HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment**
 - 시스템 환경변수 정보
 - 전체 사용자 공통으로 사용



레지스트리(Registry) – Hive 실습

- 최근 사용한 파일 및 프로그램
 - [OpenSavePidMRU](#)
 - 프로그램에 있는 메뉴를 통해 열기 또는 저장한 파일 정보
 - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidMRU
 - [LastVisitedPidMRU](#)
 - 프로그램에 있는 메뉴를 통해 접근한 파일 정보
 - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidMRU
- MRUListEx Value에 실행 순서 명시
- (도구) [OpenSaveFile Viewer](#)
 - 활성 상태인 윈도우에서만 사용 가능

레지스트리(Registry) – Hive 실습

- 응용 프로그램 실행 흔적 ([UserAssist](#))
 - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
 - 최근 실행한 프로그램 목록, 마지막 실행 시간, 실행 횟수 등의 정보를 기록 (ROT-13 인코딩)
 - [실행파일 기록](#): {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
 - [바로가기 기록](#): {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count
 - (도구) [UserAssistView.exe](#)
 - 활성 상태인 윈도우에서만 사용 가능

레지스트리(Registry) – Hive 실습

- 응용 프로그램 실행 흔적 ([MUICache](#))
 - HKCU\Software\Classes\Local Settings\MuiCache
 - HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache
 - 다중 언어를 지원하기 위해 프로그램 이름을 캐시화 하는 기능 (추후 사용 위해 이름 저장)
 - 응용 프로그램 이름, 전체 경로 확인 가능, 실행파일 삭제 또는 경로를 변경해도 캐시 내 데이터 유지
 - (도구) [MUICacheView.exe](#)
 - 활성 상태인 윈도우에서만 사용 가능

레지스트리(Registry) – Hive 실습

- 응용 프로그램 실행 흔적 ([AmCache](#))

- %SystemDrive%\Windows\AppCompat\Programs\Amcache.hve
- 프로세스 생성 시 프로그램 경로를 임시로 저장하기 위한 용도로 사용
- 응용 프로그램과 Prefetch가 삭제되도 AmCache에 데이터 유지
- 프로그램 이름, 버전, 실행경로, 설치 시간, 파일 해시(SHA1) 등 확인 가능
- 외부 저장장치로부터 실행된 프로그램에 대한 정보 저장 (안티 포렌식 프로그램 등)
- (도구) [AmcacheParser.exe](#)
 - 명령어 : AmcacheParser.exe -f "[Amcache.hve경로]" --csv [파일 생성 경로]

레지스트리(Registry) – Hive 실습

- 응용 프로그램 실행 흔적 ([AppCompatCache 또는 ShimCache](#))
 - HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache
 - HKLM\SYSTEM\ControlSet001\Control\Session Manager\AppCompatCache
 - 응용 프로그램간 호환성 해결을 위해 생성(악성코드 실행 시 주로 생성)
- (도구) [AppCompatCacheParser](#)
 - 명령어 : AppCompatCacheParser.exe -f [SYSTEM 하이브] --csv [파일 생성 경로]

레지스트리(Registry) – Hive 실습

- 응용 프로그램 실행 흔적 ([Shellbags](#))
 - HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
 - 폴더 열람 시 생성, 외부 저장장치, 원격 드라이브에 존재하는 폴더도 기록
 - Shellbags 용량이 충분할 경우, 삭제된 폴더도 남음
 - (도구) [ShellBagsExplorer.exe](#)
 - 관리자 권한으로 실행
 - 오프라인 하이브 분석 시 UsrClass.dat 추출 후 실행 (.LOG1, .LOG2 존재 시 같이 추출 필요)
 - %UserProfile%\Appdata\Local\Microsoft\Windows\UsrClass.dat

이벤트로그(EventLog)



이벤트로그(EventLog)

- 윈도우 운영체제 사용 시 발생하는 이벤트들을 기록한 로그
- 각 **로그별로 Event ID가 할당**됨
- 시스템 시작/종료 이력, 로그인/로그아웃 기록, 원격 연결 흔적 등 존재
- 시스템 이상 징후 파악, 사용자 행위 분석, 내/외부 침해 흔적 분석 등 확인 가능
- 윈도우 Vista 이전에는 .evt, 이후에는 **.evtx 파일 형태**로 저장
- (위치) %SystemRoot%\System32\winevt\Logs
- **(프로그램) Microsoft Message Analyzer, 이벤트 뷰어**



이벤트로그(EventLog) – 주요 이벤트로그

- **System**
 - 윈도우 시스템에서 발생한 이벤트 기록 (드라이버, 구성요소 오류 등)
 - 미리 정의되어 있음
- **Application**
 - 시스템 구성요소를 제외한 모든 응용프로그램에서 발생한 이벤트 기록
 - 응용프로그램 개발자가 기록할 이벤트 내용 정의
- **Security**
 - 파일 생성/열기 등 데이터 사용 이벤트, 로그인 성공/실패와 같은 보안 정책 등 기록
 - 윈도우 관리자가 기록할 데이터 유형 변경 가능
- **Setup**
 - 응용프로그램 설치 및 설정과 관련된 이벤트 기록

이벤트로그(EventLog) – EVTX 내부 정보

속성	설명
Source	이벤트를 기록한 소프트웨어
<u>Event ID</u>	<u>특별한 이벤트 유형을 식별하는 값</u>
Level	이벤트의 심각도를 6가지로 분류
User	이벤트 발생에 대한 사용자 이름
Operational Code	이벤트가 발생했을 때 활동이나 시점을 식별하는 숫자 값을 포함
Log	이벤트가 기록된 로그의 이름
Task Category	이벤트 게시자의 하위 구성요소 또는 활동을 표현하는데 사용
Keywords	이벤트를 검색하거나 필터링 하는데 사용할 수 있는 범주
Computer	이벤트가 발생한 컴퓨터 이름
Date and Time	이벤트가 기록된 날짜 및 시간 (64bit, Little-Endian 방식)
Process ID	이벤트를 생성하는 과정에 대한 식별번호
Thread ID	이벤트 생성 tread의 식별번호

이벤트로그(EventLog) - 속성

속성	설명
정보 (Information)	어플리케이션, 드라이버 등 성공적인 이벤트에 대하여 기록 Ex) 네트워크 드라이버가 성공적으로 로드될 때 기록
오류 (Error)	데이터나 기능 손실 서비스 시작 실패와 같은 중요 문제 기록
경고 (Warning)	애플리케이션에서 데이터나 기능 손실 없이 회복할 수 있는 심각하지 않지만 추후 문제가 발생할 수 있는 문제 기록 Ex) 디스크 사용량이 많은 경우
심각 (Critical)	데이터의 문제가 심각성을 일으킬 수 있을 때 기록
실패 감사 (Failure Audit)	감사 대상에 대한 접근 시도 실패 Ex) 시스템 로그인 실패
성공 감사 (Success Audit)	감사대상에 대한 접근시도 성공 기록

이벤트로그(EventLog) – 설정

- 미리 설정한 최대 크기 도달 시, 기존 이벤트 파일에 데이터를 덮어씀
- **(레지스트리 내 경로 확인)** HKLM\SYSTEM\ControlSet001\Services\EventLog\
- **(프로그램)** 이벤트 뷰어, Microsoft Message Analyzer
- **(gpedit.msc)** [컴퓨터 구성] – [관리 템플릿] – [Windows 구성 요소] – [이벤트 로그 서비스]
- **(로컬 보안 정책)** 이벤트 로그에 기록될 감사 범위 설정 가능
 - 보안 설정 – 로컬 정책 – 감사 정책

이벤트로그(EventLog) – Windows Message Analyzer 주요 표현식

- eventlog.**EventID**==4624 and eventlog.Message **contains** "로그온 유형: [tab]3" and (not eventlog.Message contains "Kerberos")
- eventlog.**Message** contains "192.168.200."
- ***eventid==4624** and ***message** contains "192.168.200"
 - eventid 입력 후 "tab" 키를 누르면 자동으로 입력
- 이벤트 ID Grouping, 이벤트로그 내 정보(DestinationIP 등) Grouping 가능

이벤트로그(EventLog) – 주요 Event ID

[참고] 이벤트 ID 검색

1. kb.eventtracker.com
2. ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

범주	종류	ID	내용
컴퓨터 시작	Security	4608	Windows 시작
	System	12	시작
	System	6005	이벤트 로깅 서비스 시작
	System	6009	부팅 시 OS 버전, 빌드번호, 서비스팩 수준, 기타 시스템 관련 정보 기록
컴퓨터 종료	System	1074	Windows 종료
	System	13	종료
	System	42	시스템 절전 모드 (Sleep)
	Security	1100	이벤트 로깅 서비스 종료
	System	6006	이벤트 로깅 서비스 멈춤
	System	6008	시스템 비정상 종료
화면 보호기	Security	4802	화면보호기 호출
	Security	4803	화면보호기 해제

이벤트로그(EventLog) – 주요 Event ID

범주	종류	ID	내용
로그온	Security	4624	계정 로그인 성공
	Security	4625	계정 로그인 실패
특수 로그인	Security	4672	특수 권한을 새 로그인에 할당
원격 로그인	Security	4648	명시적 자격 증명을 사용하여 로그인 시도
로그오프	Security	4634	계정 로그오프 (로그온 세션 소멸)
	Security	4647	사용자가 로그오프 시작함
로그 삭제	Security	1102	감사 로그 삭제
	System	104	시스템, 응용프로그램에서 로그 삭제

이벤트로그(EventLog) – 주요 Event ID

로그온 유형	분류	설명
2	대화식	콘솔에서 키보드로 로그인 (KVM 포함)
3	네트워크	네트워크를 통한 원격 로그인 (파일 공유, IIS 접속 등)
4	스케줄	스케줄에 등록된 배치 작업 실행 시 미리 설정된 계정 정보 로그인
5	서비스	서비스가 실행될 때 미리 설정된 계정 정보로 로그인
7	잠금해제	화면 보호기 잠금 해제 로그인
8	네트워크	유형 3과 비슷하나 계정 정보를 평문으로 전송할 때 발생
9	새자격	실행(RunAS)에서 프로그램 실행시 /netonly 옵션을 줄때 발생
10	원격 대화식	터미널 서비스, 원격 접속, 원격 지원으로 로그인
11	캐시된 대화식	PC에 캐시로 저장된 암호로 자동 입력 로그인

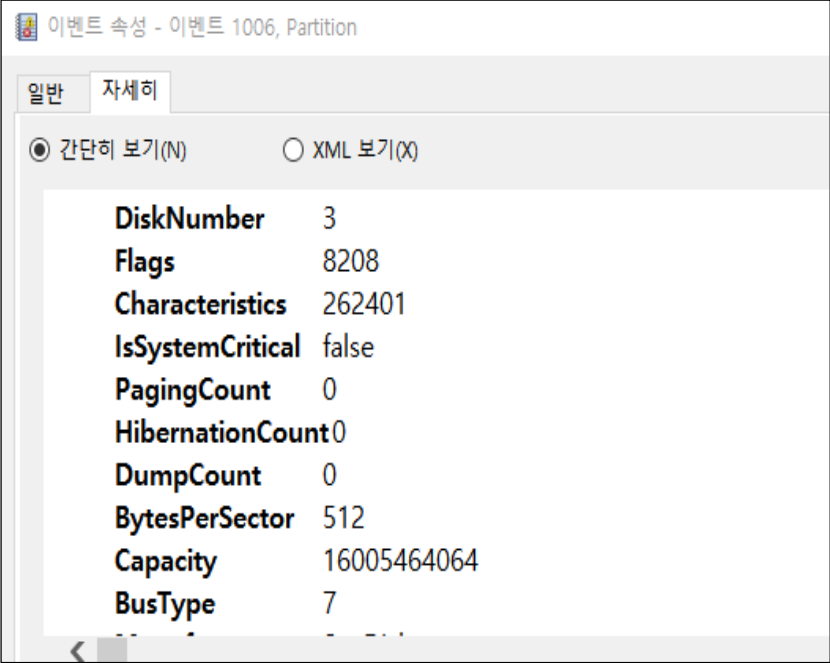
이벤트로그(EventLog) – 주요 Event ID

범주	종류	ID	내용
사용자 계정 추가/변경/삭제	Security	4720	사용자 계정 생성
		4722	사용자 계정 활성화
		4725	사용자 계정 비활성화
		4726	사용자 계정 삭제
		4738	사용자 계정 변경
		4740	사용자 계정 잠김
		4781	사용자 계정 이름 변경
암호 재설정	Security	4723	암호 변경 시도
		4724	암호 설정 또는 재설정

이벤트로그(EventLog) – 주요 Event ID

범주	종류	ID	내용
저장 장치 연결/해제	System	10000	장치 드라이버 설치/업데이트 (시작)
		10100	장치 드라이버 설치/업데이트 (완료)
		225	장치 연결 해제 (경고 – 강제 제거)
	Microsoft-Windows-Partition%4Diagnostic	1006	파티션 연결/해제
	Microsoft-Windows-Kernel-PnP/Device Configuration	400	장치 구성
저장 장치 사용 정보	Microsoft-Windows-Ntfs%4Operational	142	볼륨 내 미사용 영역 크기
		145	저장 장치 정보 및 입출력 지연 시간 정보
		151	최근 삭제된 파일 수
		158	최근 파일시스템 입출력 정보 (읽기, 쓰기, 트림 등)

이벤트로그(EventLog) – 주요 Event ID



데이터	설명
Capacity	장치 전체 용량
Bus type	장치 버스 타입
Manufacture	장치 제조사
Model	장치 제품명
Revision	장치 버전
Serial Number	장치 시리얼 번호
Partition Count	장치의 파티션 수 (값이 0보다 크면 연결, 0이면 해제)
Mbr	MBR(Master Boot Record) 데이터
Vbr#	VBR(Volume Boot Record) 데이터

값	의미
0	Unknown
1	SCSI
2	ATAPI
3	ATA
4	1394
5	SSA
6	Fibre Channel
7	USB
8	RAID
9	Iscsi
10	SAS
11	SATA
12	SD
13	MMC
14	Virtual (Reserved)
15	File-Backed Virtual
16	Storage spaces
17	NVMe

이벤트로그(EventLog) – 주요 Event ID

범주	종류	ID	내용
원격접속 로그온/오프	Security	4799	원격으로 로그인한 정보
		4624	원격 데스크톱: 사용자 로그인 성공
		4625	원격 데스크톱: 사용자 로그인 실패
		4634	원격 데스크톱: 사용자 로그오프
	Microsoft-Windows-TerminalServices-RemoteConnectionManager.evtx	1149	원격 데스크톱: 사용자 인증 성공
세션 정보	Microsoft-Windows-TerminalServices-LocalSessionManager	21	원격 데스크톱 서비스: 세션 로그인 성공
		22	원격 데스크톱 서비스: 셸 시작 알림 받음
		23	원격 데스크톱 서비스: 세션 로그오프 성공
		24	원격 데스크톱 서비스: 세션 연결 끊김
		25	원격 데스크톱 서비스: 세션 다시 연결 성공

이벤트로그(EventLog) – 주요 Event ID

범주	종류	Event ID	Description
윈도우 디펜더 (백신)	Microsoft-Windows-Windows Defender%4Operational.evtx	1000	백신 검사 시작
		1001	백신 검사 종료
		1005	백신 검사 실패
		1006	악성 소프트웨어 발견
		1007	악성 SW로부터 시스템 보호를 위한 작업 수행
		1015	의심스러운 동작 감지
		1116	악성 소프트웨어 검색
		1117	악성 SW로부터 시스템 보호를 위한 작업 수행
		1150	백신이 정상 실행됨
		1151	Endpoint Protection 상태 보고(UTC)
		2000	백신이 정상적으로 업데이트
		5000	실시간 보호 기능이 사용됨
		5001	실시간 보호 검사 기능이 사용되지 않음
		5004	실시간 보호 기능 구성이 변경
		5007	백신 구성이 변경

이벤트로그(EventLog) – 침해사고 시 참고

분류	이벤트	행위
로그 삭제	Security	감사 로그 삭제
	System	로그 삭제 – 시스템, 응용프로그램

분류	이벤트	행위
네트워크	Microsoft-Windows-NetworkProfile%4Operational.evtx	네트워크상태
	Microsoft-Windows-WLAN-AutoConfig%4Operational.evtx	무선네트워크 사용
	Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx	원격 데스크톱 사용
	Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx	
	Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx	

이벤트로그(EventLog) – 침해사고 시 참고

분류	이벤트	행위
시스템	Security.evtx System.evtx Microsoft-Windows-DateTimeControlPanel%4Operational.evtx	시스템 시간 변경
	Security.evtx	사용자 로그인/로그 오프/사용자 계정
	System.evtx	시스템 시작/종료
	Microsoft-Windows-Windows Defender%4Operational.evtx	윈도우 디펜더
분류	이벤트	행위
프로그램	Microsoft-Windows-Application-Experience%4Program-Inventory.evtx	프로그램 설치
	Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx	프로그램 호환성
	Security.evtx	프로세스 생성/종료
	Microsoft-Windows-TaskScheduler/Operational.evtx	작업 스케줄러 실행

바로가기(.lnk)



바로가기(.lnk)

- 파일 등 객체를 빠르게 참조하기 위한 파일 (확장자 .lnk)
 - %UserProfile%\Desktop
 - %UserProfile%\Appdata\Roaming\Microsoft\Windows\Start Menu
 - %ProgramData%\Microsoft\Windows\Start Menu
 - %UserProfile%\Appdata\Roaming\Microsoft\Windows\Recent
 - %UserProfile%\Appdata\Roaming\Microsoft\Internet Explorer\Quick Launch
 - %UserProfile%\Appdata\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar
- 원본파일이 삭제 시 링크파일 정보를 통해 사용자 행위 추적 가능
- 특정 응용프로그램 사용 여부 확인 가능
- (도구) **LinkParser, WFA(Windows File Analyzer)**

점프리스트(Jumplist)



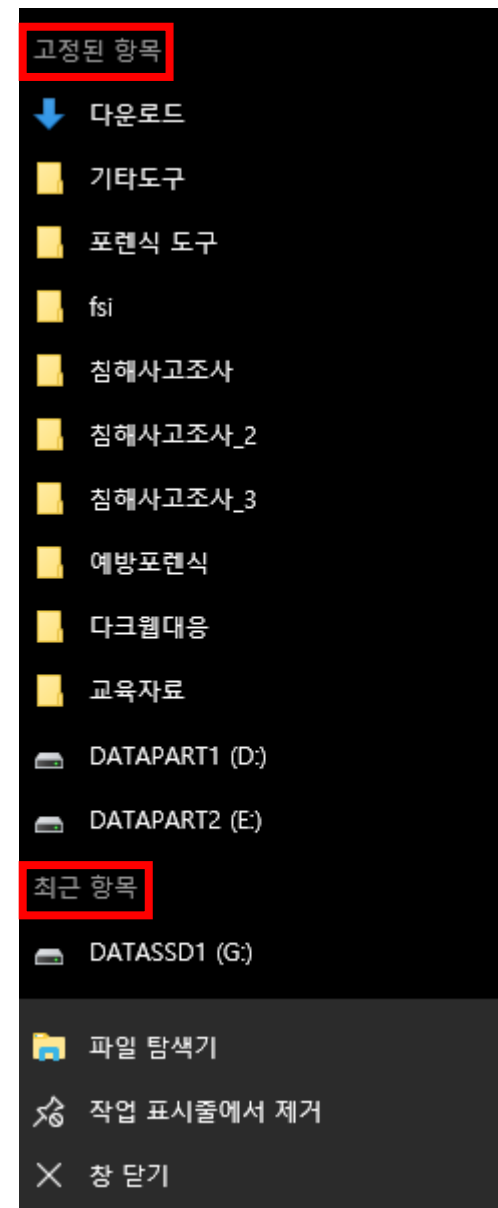
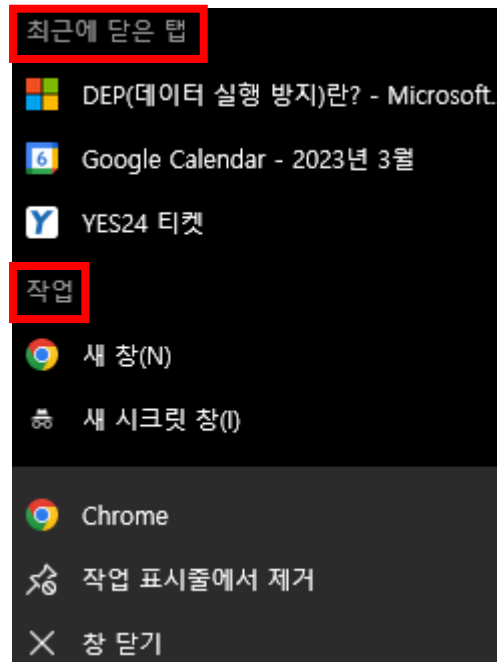
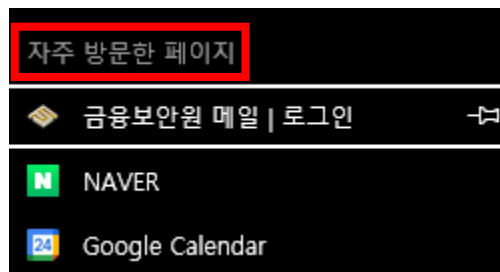
점프리스트(Jumplist)

- 최근 사용한 파일 및 폴더에 빠르게 접근하기 위한 기능
- 사용자가 접근한 파일 또는 실행한 프로그램 정보를 지속적으로 저장 **AutomaticDestinations**
 - 운영체제가 자동으로 남기는 항목 (Frequent, Pinned로 구성)
- **CustomDestinations**
 - 응용 프로그램이 자체적으로 관리하는 항목 (Recent, Tasks로 구성)
- 위 2개 폴더는 동일한 경로에 위치
 - %UserProfile%\AppData\Roaming\Microsoft\Windows\Recent
- (도구) **JumpListsView**

윈도우 아티팩트 설명

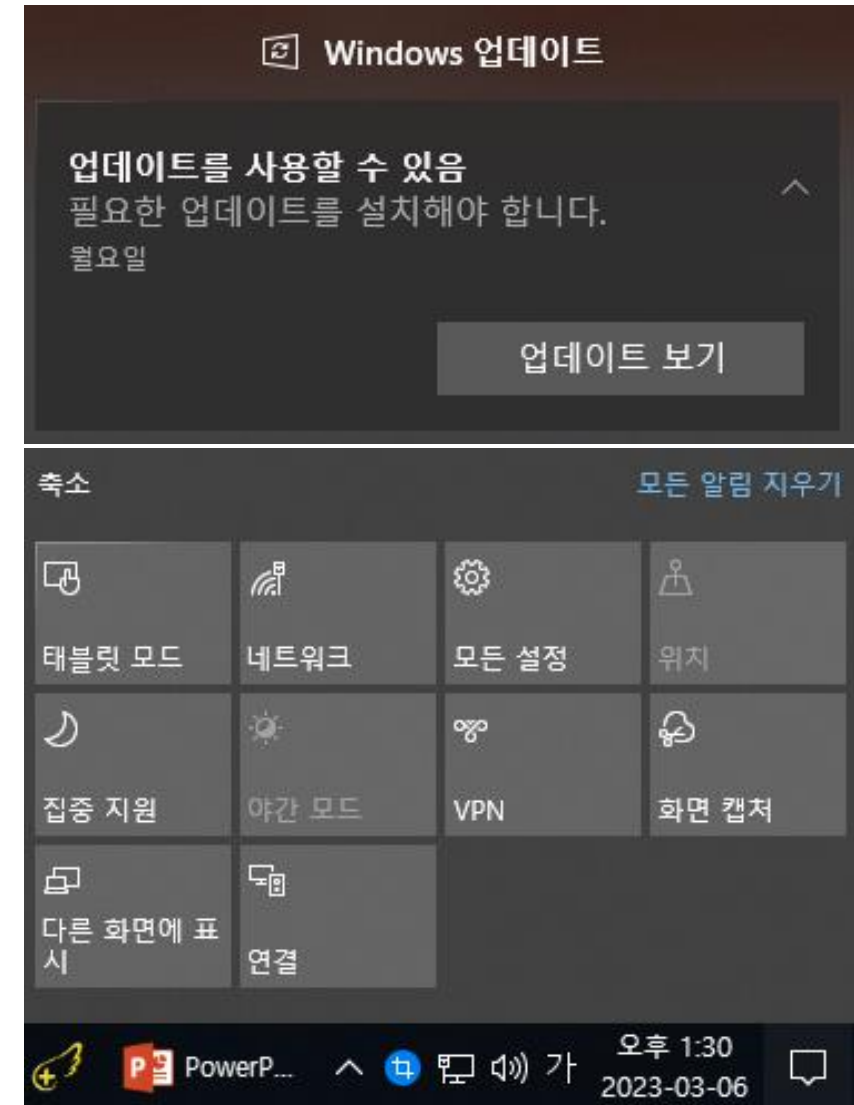
점프리스트(Jumplist) 구성

- **Recent**(최근 항목) : 사용자가 최근 사용한 파일 또는 폴더
- **Frequent**(자주 사용하는 항목) : 사용자가 자주 방문한 경로
- **Tasks**(작업) : 응용 프로그램에서 지원하는 작업 목록
- **Pinned**(사용자 고정) : 사용자가 고정시킨 작업 목록



알림(Notification)

- Windows 8 이후에 추가된 기능
- 시작 메뉴 또는 화면 오른쪽에 표시
- 수신한 알림(Alert)을 데이터베이스 파일로 저장
- 알림 예시
 - 응용 프로그램의 Push/Popup 메시지
 - 보안/업데이트 정보
 - 알림 개수 표시 등
- 일정, 프로그램 동작 여부 등 확인 가능



알림(Notification) – 파일

- SQLite 데이터베이스 파일 형태로 저장
 - `%UserProfile%\AppData\Local\Microsoft\Windows\Notifications\wpndatabase.db`
- 주요 테이블
 - **Notification** : 실제 알림 내용, **최근 3일간 받은 알림 데이터**만 기록
 - **NotificationHandler** : 알림을 생성한 각 프로그램에 해당하는 ID 확인

프리패치(Prefetch)



프리패치(Prefetch)

- 프로그램 시작 시 성능 향상을 위해 개발
 - 프로그램 실행 정보를 파일 형태로 미리 저장(.pf 확장자)
 - 미리 메모리에 로드 후, 프로그램 실행 시 디스크가 아닌 메모리에서 읽음
- 파일 위치 : %SystemRoot%\Prefetch
- 레지스트리 설정을 통해 프리패치 사용 여부 설정 가능
 - HKLM\SYSTEM\ControlSet001\Control\Session Manager\Memory Management\Prefetch Parameter
- 프로그램 사용 시간이 10초 미만일 경우에는 생성되지 않음
- 최대 300~500개의 프리패치 파일 저장
- (도구) WinPrefetchView.exe

휴지통(\$Recycle.Bin)

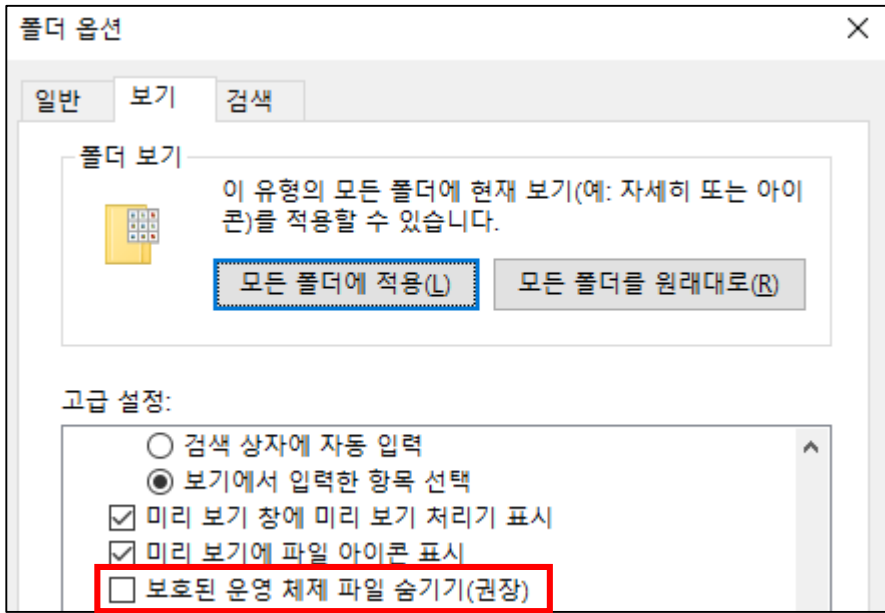


휴지통(\$Recycle.Bin)

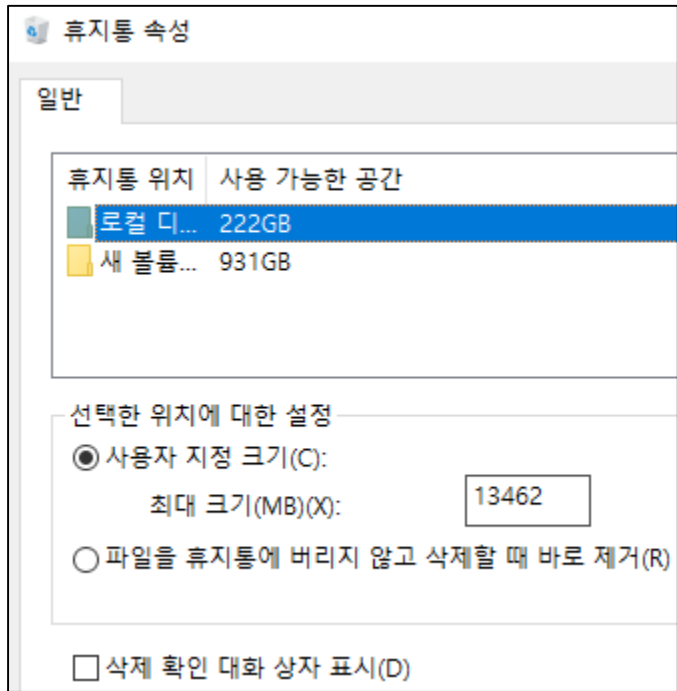
- 로컬 디스크로 인식되는 볼륨별로 생성
 - 플로피 디스크, 이동식 디스크일 경우 생성되지 않음
 - 휴지통 아이콘 자체는 1개만 존재
- 사용자 SID 별로 삭제된 파일 관리
 - 특정 사용자가 휴지통을 통해 파일을 삭제한 행위 파악 가능
- 휴지통으로 삭제 시, 휴지통 폴더에 삭제된 파일과 관련된 아티팩트 존재
- 휴지통 속성에서 디스크별 휴지통 할당 크기 확인 가능



휴지통(\$Recycle.Bin) 속성 확인



체크해제 시 확인 가능



윈도우 아티팩트 설명

휴지통(\$Recycle.Bin) 구조

- 경로 : Volume₩\$Recycle.Bin₩<SID>₩
- 삭제된 파일 : \$R<임의 문자열 6자리>.<원본 파일 확장자>
- 삭제 관련 메타데이터 파일 : \$I<임의 문자열 6자리>.<원본 파일 확장자>
 - 원본 파일의 경로, 휴지통으로 이동된 시각 등
- \$I 파일을 통해 삭제 행위 확인 가능
 - 파일 삭제 후 복원해도 남아있음
 - "휴지통비우기" 시 사라짐
- (도구) WFA(Windows File Analyzer)

```
C:\$RECYCLE.BIN\₩S-1-5-21-3886893730-2345976719-3495697317-1002>dir
C 드라이브의 볼륨에는 이름이 없습니다.
볼륨 일련 번호: 966E-EE60

C:\$RECYCLE.BIN\₩S-1-5-21-3886893730-2345976719-3495697317-1002 디렉터리

2023-03-06   오후 10:59                90 $ICM3GRG.txt
2023-03-06   오후 10:59                90 $IMKNYZN.rtf
2023-03-06   오후 10:59                 0 $RCM3GRG.txt
2023-03-06   오후 10:59                 7 $RMKNYZN.rtf
               4개 파일                187 바이트
               0개 디렉터리  95,058,079,744 바이트 남음

C:\$RECYCLE.BIN\₩S-1-5-21-3886893730-2345976719-3495697317-1002>
```

썸네일(Thumbnail)



썸네일(Thumbnail)








- 큰 그래픽 이미지를 축소한 것으로 많은 이미지를 빠르게 탐색하기 위한 목적
- 썸네일 생성 후 데이터베이스 형식으로 저장
 - 한 번이라도 생성된 썸네일은 원본 사진을 삭제하더라도 지워지지 않음
 - thumbcache.db 파일
 - %UserProfile%\AppData\Local\Microsoft\Windows\Explorer\thumbcache_#.db
- 썸네일의 크기(# : 16, 32, 48 ... 2560)별로 구분하여 저장
- (도구) Thumbs Viewer(Win XP), Thumbcache Viewer(Vista 이후)

아이콘캐시(IconCache)



아이콘캐시(IconCache)

- 아이콘 파일 내 리소스 영역(.rsrc)에 저장된 아이콘 정보를 캐시 파일 형태로 저장
 - 프로그램의 아이콘 시각화 시, PE 구조의 rsrc 영역 접근을 위한 부하 감소
- (도구) Thumbs Viewer(Win XP), Thumbcache Viewer(Vista 이후)**

 iconcache_16.db	2023-02-20 오후 10:09	Data Base File	3,072KB
 iconcache_32.db	2023-03-04 오후 11:10	Data Base File	9,216KB
 iconcache_48.db	2023-03-04 오후 8:34	Data Base File	3,072KB
 iconcache_96.db	2022-12-15 오후 9:00	Data Base File	1KB
 iconcache_256.db	2023-03-04 오후 4:19	Data Base File	8,192KB
 iconcache_768.db	2022-12-15 오후 9:00	Data Base File	1KB
 iconcache_1280.db	2022-12-15 오후 9:00	Data Base File	1KB

아이콘캐시(IconCache) – 윈도우 버전별 저장 방식

- **Windows XP**
 - %SystemDrive%\Documents and Settings\%UserName%\Local Settings\Application Data\IconCache.db
- **Windows Vista, 7, 8.1**
 - %UserProfile%\AppData\Local\IconCache.db
- **Windows 10, 11**
 - %UserProfile%\AppData\Local\Microsoft\Windows\Explorer\Iconcache_#.db
 - 썸네일 캐시 데이터베이스(thumbcache_#.db) 구조와 동일

썸네일(Thumbnail), 아이콘 캐시(IconCache) 활용

- 사진, 동영상, 문서 등 멀티미디어 파일의 존재 확인 가능
 - Windows 탐색기로 미리보기 하였을 때 자동으로 썸네일 생성
 - 이미 삭제한 사진, 동영상, 문서의 존재 여부 확인 가능
 - Windows XP는 폴더에 기록되므로 폴더가 존재하면 획득 가능
 - Windows Vista 이후의 경우 thumbcache_#.db 파일이 존재하면 획득 가능
- 파일 일부 내용 확인 가능
 - 문서 파일의 경우 첫 페이지가 썸네일이 되기 때문에 일부 내용 확인 가능
- 프로그램 사용 흔적 확인 가능
 - 안티포렌식 도구 사용 흔적, 아이콘이 존재하는 악성코드 흔적 등

Web Artifact



Web Artifact

- 웹 브라우저 사용 시 생성되는 흔적
- 웹 히스토리, 웹 캐시, 웹 쿠키, 웹 다운로드 목록 등 존재
- 각 브라우저마다 다른 형태로 존재
- 주요 브라우저 종류: Chrome, Edge, Whale, Safari, Firefox, Internet Explorer 등



Web Artifact – 주요 정보

- **웹 히스토리**
 - 사용자가 직접 방문한 웹사이트의 접속 기록
 - 이미지, 텍스트, 아이콘, HTML, XML, 스크립트 파일 등
- **웹 캐시**
 - 웹 사이트 접속 시 방문사이트로부터 자동으로 전달받는 데이터
 - 브라우저 캐시, 프록시 캐시, 게이트웨이 캐시 존재
- **웹 쿠키**
 - 사용자의 접속 상태를 유지할 수 있도록 하기 위해 만든 임시 저장소
 - 자동 로그인, 자주 열람한 파일 정보, 다운로드 받은 파일 목록
- **웹 다운로드 목록**
 - 웹에서 다운로드 받은 파일의 안정적인 전송과 이력을 관리하는 리스트

Web Artifact – 웹 히스토리

- 사용자가 직접 방문한 웹 사이트의 접속 기록
- 월, 일별로 방문 기록을 분류하여 저장
- 세부 정보
 - 방문한 사이트의 URL
 - 방문 시간
 - 방문 횟수
 - 웹 사이트의 Title

Web Artifact – 주요 웹 브라우저 히스토리 경로

Name	Path
Chrome	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\History
Edge	%UserProfile%\AppData\Local\Microsoft\Edge\User Data\Default\History
Whale	%UserProfile%\AppData\Local\Naver\Naver Whale\User Data\Default\History

- **DB Browser for SQLite 도구 활용**
 - urls, visits 테이블 참고
- **BrowsingHistoryView 도구 활용**
 - 여러 웹 브라우저 히스토리 조회 동시 지원

Web Artifact – 웹 캐시 설명

- 사용자가 웹 사이트를 방문할 때 자동으로 전달 받는 데이터
- 웹 페이지를 표현하기 위한 이미지, 텍스트, 아이콘, HTML, XML, 스크립트 파일 등등이 포함됨
- 캐시를 통해 사이트 응답 시간 및 트래픽을 감소시키는 역할
- 세부 정보
 - 다운로드 URL
 - 다운로드 시간
 - 파일 이름
 - 데이터 저장 위치

Web Artifact – 웹 캐시 설명

- **브라우저 캐시**
 - CSS, JS, 이미지, 비디오 등 정적 리소스로 구성된 DB
 - 이미 방문한 페이지를 재방문하는 경우, 브라우저 캐시를 통해 응답시간을 줄일 수 있음
- **프록시 캐시**
 - 네트워크 관련 데이터(대기시간, 트래픽, 접근 정책, 제한 우회, 사용률 등)를 저장함
 - IPS(Intrusion Prevention System) 방화벽 역할로도 활용
- **게이트웨이 캐시**
 - 서버의 앞 단에 존재하며 요청에 대한 캐시를 관리하고, 이를 효율적으로 분배하여 저장함
 - 무한 대의 클라이언트들에게 한정된 수의 웹 서버 콘텐츠를 제공하는 역할

Web Artifact – 주요 웹 브라우저 캐시 경로

Name	Path
Chrome	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\
Edge	%UserProfile%\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\
Whale	%UserProfile%\AppData\Local\Naver\Naver Whale\User Data\Default\Cache\Cache_Data\
IE	%UserProfile%\AppData\Local\Microsoft\Windows\WebCache\

- (도구) **ChromeCacheView**

Web Artifact – 웹 쿠키

- 사용자의 접속 상태를 유지하기 위해 활용되는 임시 저장소
 - 자동 로그인, 열람한 정보 내역, 다운로드 받았던 자료 목록 등
- 세부 정보
 - 사이트 명
 - 쿠키 수정/만료 시간
 - 이름 관련 정보
- 제한 사항
 - 클라이언트 당 300개의 쿠키만 저장이 가능함
 - 하나의 도메인 당 20개의 쿠키 값만 가질 수 있음
 - 하나의 쿠키는 최대 4KB까지만 저장할 수 있음

Web Artifact – 주요 웹 브라우저 쿠키 경로

Name	Path
Chrome	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies
Edge	%UserProfile%\AppData\Local\Microsoft\Edge\User Data\Default\Network\Cookies
Whale	%UserProfile%\AppData\Local\Naver\Naver Whale\User Data\Default\Network\Cookies

- DB Browser for SQLite 도구 활용
 - cookies 테이블 참조

Web Artifact – 웹 다운로드 설명

- 웹 브라우저를 통해 사용자가 직접 다운로드한 파일 목록(자동적으로 다운로드 되는 캐시와는 구분)
- 웹 히스토리 파일에 함께 존재
- 세부 정보
 - 다운로드 파일 경로 및 내용
 - 다운로드 URL
 - 다운로드한 파일 크기
 - 다운로드 시간

Web Artifact – 주요 웹 브라우저 다운로드 목록 경로

Name	Path
Chrome	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\History
Edge	%UserProfile%\AppData\Local\Microsoft\Edge\User Data\Default\History
Whale	%UserProfile%\AppData\Local\Naver\Naver Whale\User Data\Default\History

- DB Browser for SQLite 도구 활용
 - download 테이블 참고

이메일(Outlook)



이메일(Outlook)

- 사용자가 **Outlook**을 통해 관리한 이메일(내용, 첨부파일 등)을 확인할 수 있는 아티팩트
- **.ost** : 이메일 연동 시, 기본으로 생성되는 Outlook 메일 파일
 - (경로) %UserProfile%\AppData\Local\Microsoft\Outlook\
- **.pst** : 내보내기를 통해 생성(백업 용도)되는 Outlook 메일 파일
- **.msg** : 개별 메시지 저장을 위해 사용되는 Outlook 메일 파일
- (도구) **Systools OST Viewer**

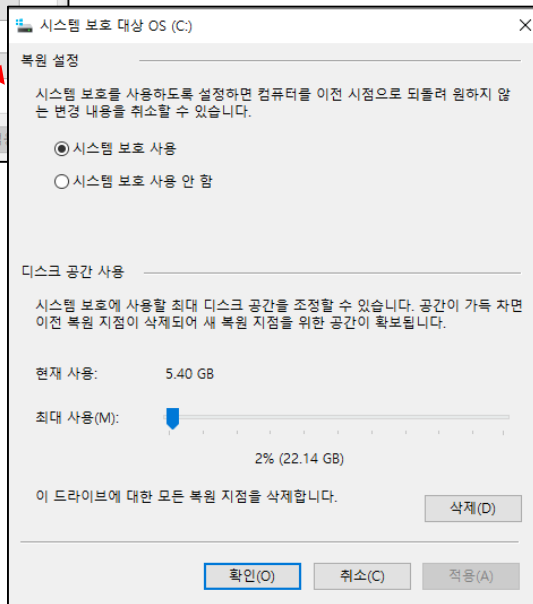
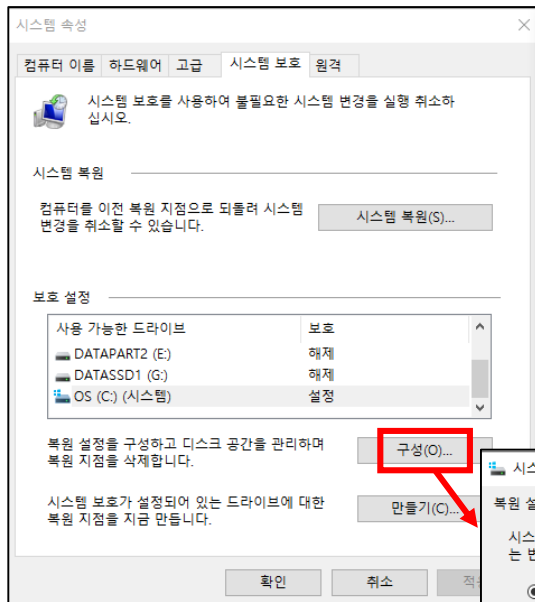
VSS



VSS(Volume Shadow copy Service)

- 특정 시점의 파일, 폴더본을 포함한 볼륨의 스냅샷을 보관하는 기능
- [제어판 – 시스템 – 고급 시스템 설정 – 시스템 보호] 탭에서 설정 가능
- **vssadmin list shadows**를 통해 저장 경로 확인 가능
 - mklink /d [볼륨경로]를 통해 심볼릭 링크 생성 가능
 - 특정 드라이브의 VSS 정보 확인 시 명령어 맨 끝에 **/for=[볼륨명]**: 입력
- 공격자가 삭제한 공격 도구 등 복구 가능
- 악의적 드라이버 설치 흔적(미인증 드라이버 설치 시 복원지점 생성)
- (도구) ShadowCopyView

VSS(Volume Shadow copy Service)



Snapshot Name	Explorer Path	Volume Path	Volume Name	Originating Machi...	Service Machine	Creation Time	Attributes
\\#?#GLOBALROOT#Device#HarddiskVolumeShadowCopy8	\\#?#GLOBALROOT#Device#HarddiskVolumeShadowCopy8	\\#?#GLOBALROOT#Device#HarddiskVolumeShadowCopy8	\\#?#GLOBALROOT#Device#HarddiskVolumeShadowCopy8	DESKTOP-3LQ7RDL	DESKTOP-3LQ7RDL	2024-02-26 오후 12:13:32	Persistent, Client-A
\\#?#GLOBALROOT#Device#HarddiskVolumeShadowCopy9	\\#?#GLOBALROOT#Device#HarddiskVolumeShadowCopy9	\\#?#GLOBALROOT#Device#HarddiskVolumeShadowCopy9	\\#?#GLOBALROOT#Device#HarddiskVolumeShadowCopy9	DESKTOP-3LQ7RDL	DESKTOP-3LQ7RDL	2024-03-07 오전 6:14:41	Persistent, Client-A

Filename	Modified Time	Created Time	Entry Modified Time	File Size	Attributes	File Extension
\$Recycle.Bin	2024-02-08 오전 9:39:53	2018-09-15 오후 4:33:50	2024-02-08 오전 9:39:53		HSD	Bin
\$WINDOWS~BT	2023-01-19 오후 5:27:38	2023-01-19 오후 5:27:38	2023-01-19 오후 5:27:38		D	~BT
\$Windows~WS	2023-01-19 오후 5:27:32	2023-01-19 오후 5:27:32	2023-01-19 오후 5:27:32		HDI	~WS
Config.Msi	2024-02-19 오전 4:12:37	2024-02-19 오전 4:12:37	2024-02-19 오전 4:12:37		HSD	Msi
cygwin64	2023-12-19 오전 11:00:58	2023-12-19 오전 10:53:16	2023-12-19 오전 11:00:58		D	
dell	2022-06-27 오후 12:17:21	2011-02-16 오전 1:01:15	2022-06-27 오후 12:17:21		D	
Documents and Settings	2019-12-11 오후 3:44:10	2019-12-11 오후 3:44:10	2019-12-11 오후 4:05:03		HSDI	
Downloads	2020-05-11 오후 2:27:50	2020-01-28 오후 3:24:36	2020-05-11 오후 2:27:50		D	
Drivers	2016-08-23 오후 3:10:10	2016-08-23 오후 3:03:55	2016-08-23 오후 3:10:10		D	
drvtmp	2019-12-12 오후 4:00:47	2019-12-12 오후 4:00:47	2019-12-12 오후 4:00:47		D	
ESD	2023-01-19 오후 6:05:03	2023-01-19 오후 5:29:28	2023-01-19 오후 6:05:03		D	
Intel	2016-08-22 오후 11:01:07	2016-08-22 오후 11:01:07	2016-08-22 오후 11:01:07		D	
PerfLogs	2020-05-13 오후 5:27:17	2018-09-15 오후 4:33:50	2021-05-21 오후 10:47:19		D	
pgData93	2019-12-11 오후 2:52:32	2016-09-23 오전 11:35:53	2019-12-11 오후 2:52:32		D	
pgData96	2024-02-19 오후 4:13:09	2019-12-12 오후 5:04:15	2024-02-19 오후 4:13:09		D	
Program Files	2024-02-08 오후 12:17:52	2018-09-15 오후 4:33:50	2024-02-08 오후 12:17:52		RD	
Program Files (x86)	2023-09-26 오후 3:10:00	2018-09-15 오후 4:33:50	2023-09-26 오후 3:10:00		RD	
ProgramData	2024-02-19 오후 4:15:53	2018-09-15 오후 4:33:50	2024-02-19 오후 4:15:53		HDI	
Python27	2023-04-28 오전 8:55:49	2019-12-23 오전 10:59:38	2023-04-28 오전 8:55:49		D	
Recovery	2019-12-11 오후 3:24:39	2016-08-23 오후 4:34:20	2019-12-11 오후 3:24:39		D	
System Volume Information	2024-02-23 오전 10:32:02	2016-08-22 오후 10:28:54			HSD	
Temp	2023-06-15 오전 8:56:49	2019-12-23 오후 3:45:18	2023-06-15 오전 8:56:49		D	
USBLINK	2023-10-30 오후 2:09:32	2022-11-23 오후 3:00:30	2023-10-30 오후 2:09:32		D	
Users	2019-12-11 오후 4:05:03	2018-09-15 오후 3:09:26	2019-12-11 오후 4:05:03		RD	
vssadmin_link	2023-03-07 오전 11:03:39	2023-03-07 오전 11:03:39			D	
Windows	2024-02-26 오전 11:58:17	2018-09-15 오후 3:09:26	2024-02-26 오전 11:58:17		AD	
superid	2019-01-03 오후 4:56:14	2019-01-03 오후 4:56:14	2019-01-03 오후 4:56:14	36	A	superid

NTFS 로그파일



NTFS 로그파일

- 삭제된 파일의 경우 \$MFT에 데이터가 남아있지 않을 가능성이 높아 추적 어려움
- \$Logfile, \$UsnJrnl을 분석하여 삭제된 파일에 대한 히스토리 등 분석 가능
- **\$Logfile**
 - 전원 차단, 시스템 오류 등 발생 시 작업 중이던 파일 복구를 위해 사용
 - %SystemDrive%\\$LogFile
- **\$UsnJrnl**
 - 파일과 디렉터리에 변경이 수행된 후 내용만 기록
 - 파일 복원이 목적이 아니라, 파일이 존재했음을 확인하는 것이 목적
 - %SystemDrive%\\$Extend\%\$UsnJrnl:\$J
- **(도구) NTFS Log Tracker**

타임라인(Timeline)



타임라인(Timeline)

- 사용자가 최대 30일 동안 작업하던 문서, 웹페이지 등 추적이 가능한 기능
- [Windows + Tab] 키를 통해 확인 가능
- 사용자가 작업 중이던 내용에 대한 스냅샷 표시
- [Windows 설정 – 개인 정보 – 활동 기록] 에서 활성화/비활성화 가능
- **%UserProfile%\AppData\Local\ConnectedDevicesPlatform\[계정 ID]\ActivitiesCache.db**
 - 사용자 계정 유형에 따라 계정 ID 방식이 달라짐

사용자 계정 유형	폴더명
로컬 계정	L.{로컬 계정 명}
마이크로소프트 계정	{마이크로소프트 식별자(CID)}
Office 365 혹은 Azure Active Directory 계정	AAD.{보안 식별자(SID)}

타임라인(Timeline) – ActivitiesCache.db

테이블 명	설명
Activity	Activity 유형 및 데이터베이스가 생성된 마지막 시간 정보
ActivityOperation	타임라인으로부터 제거된 타일 정보
Activity_PackageID	Activity와 ActivityOperations 테이블 간의 트랜잭션 정보
Metadata	Activity 유형 및 데이터베이스가 생성된 마지막 정보

23696	[{"application":"{7C5A40EF-A0	ECB32AF3-1440-4086-94E3-5311F97F89C4
23697	[{"application":"Microsoft.Office	ECB32AF3-1440-4086-94E3-5311F97F89C4WG:₩교육자료₩침해사고 대응 담당자를 위한 디지털 포
23698	[{"application":"Microsoft.Office	ECB32AF3-1440-4086-94E3-5311F97F89C4WG:₩교육자료₩침해사고 대응 담당자를 위한 디지털 포
23699	[{"application":"Chrome","platf	ECB32AF3-1440-4086-94E3-5311F97F89C4
23700	[{"application":"Microsoft.Office	ECB32AF3-1440-4086-94E3-5311F97F89C4WG:₩교육자료₩침해사고 대응 담당자를 위한 디지털 포
23701	[{"application":"Microsoft.Office	ECB32AF3-1440-4086-94E3-5311F97F89C4WG:₩교육자료₩침해사고 대응 담당자를 위한 디지털 포
23702	[{"application":"Microsoft.O ...	디지털 포렌식 기본₩2024₩1차(24.05.08-10)₩(5) 침해사고 동향, 대응방안, 위협 인텔리전스.pptx ...
23703	[{"application":"Microsoft.Office	ECB32AF3-1440-4086-94E3-5311F97F89C4WG:₩교육자료₩침해사고 대응 담당자를 위한 디지털 포

Windows Index

Windows Index

- Windows Indexing

- PC에 존재하는 파일들의 메타데이터 정보를 분류하는 과정
- 파일 이름, 전체 파일 경로 등 모든 속성을 인덱싱
- 인덱싱을 결과를 기반으로 Windows Search 기능 동작

- (도구)

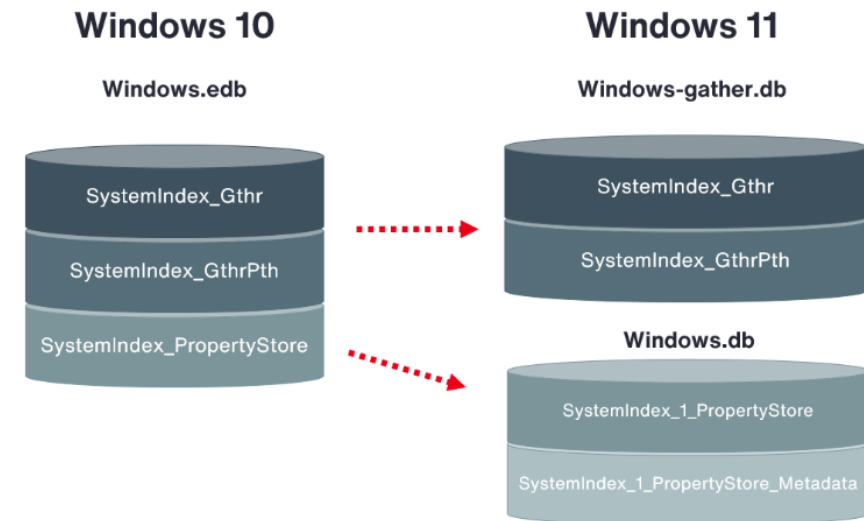
- [\(Win10\) WinSearchDBAnalyzer](#)
- [\(Win11\) SIDR\(Search Index DB Reporter\)](#)

- `sidr.exe -f json` [시스템에서 추출한 windows.edb 또는 windows.db 파일 경로]

- [\(Win10\)](#) %ProgramData%\Microsoft\Search\Data\Applications\Windows\Windows.edb
- [\(Win11\)](#) %ProgramData%\Microsoft\Search\Data\Applications\Windows\Windows.db

[참고]

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



윈도우 아티팩트 설명

(참고) Windows 11

포렌식 관점에서는 변화가 없다...

Windows 10



Windows 11

