8 윈도우 TimeLine 분석

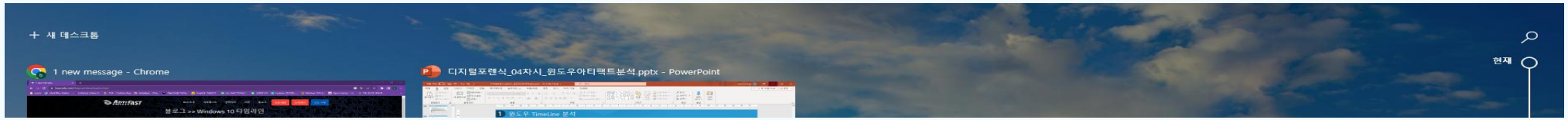
① Timeline개요

- Windows 10 타임라인은 Microsoft에서 Windows 10 2018년 4월 업데이트(Windows 10 버전 1803) 의 일부로 도입

- 이 기능을 통해 사용자는 현재 실행 중인 앱을 보고 열린 문서, 프로그램, 이미지, 비디오 또는 방문한 웹 사이트와 같은 이전 활동 확인 가능

- 사용자가 여러 장치에서 활동을 동기화 가능.

- Windows 10 타임라인은 기본적으로 활성화

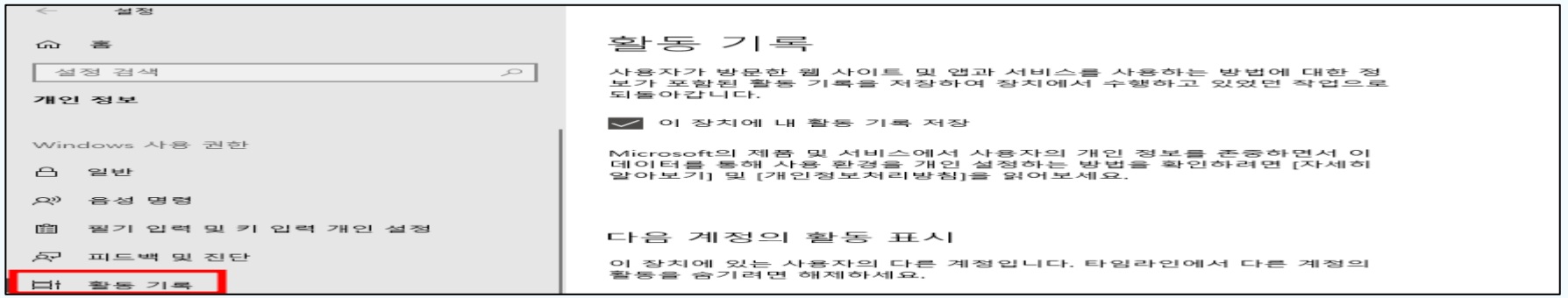


8 윈도우 TimeLine 분석

① Timeline개요

- 타임라인은 3~4일 간의 활동 기록만 볼 수 있으며 사용자는 30일 간의 활동을 추적하려면 Microsoft 365와 같은 서비스에 로그인해야 함.
- 기본적으로 타임라인은 이전 날짜 또는 특정 과거 날짜부터 작업 중이던 항목의 스냅샷을 표시
- 주석이 달린 스크롤 막대를 통해 현재 타임라인의 위치를 알 수 있으며, 스크롤하지 않으려는 경우 백업하고 싶은 항목이나 활동 검색 가능.

■ 시작 버튼 > 설정 > 개인 정보 > 활동 기록 > 내 Microsoft 계정 활동 데이터 관리 .



8 윈도우 TimeLine 분석

② Timeline 포렌식 관점

- Windows 10 타임라인은 응용 프로그램 이름, 응용 프로그램이 시작된 시간, 응용 프로그램 사용 기간 등 지난 30일 동안 컴퓨터에서 실행된 응용 프로그램에 대한 정보를 제공
- 이러한 유형의 정보는 조사관이 특정 장치에서 이전 이벤트를 재구성하는 데 도움이 될 수 있으므로 포렌식 가치 존재
- 파일, 문서 또는 응용 프로그램이 삭제된 경우에도 마찬가지로 포렌식 가치 존재.
- 구체적으로는 Edge 브라우저, Photo, News, Sports, Weather, Maps, Xbox, 기본 Office sutie, 파일 열기, 복사/붙여넣기, 윈도우 클립보드 기능과 관련된 특정 활동 유형을 기록할 뿐 아니라 시스템에서 현재 실행 중인 프로세스도 기록.
- 마이크로소프트에서 제공하는 클립보드와 복사/붙여넣기 활동에 관한 정보를 추가적으로 기록

② Timeline 포렌식 관점

■ 사용자 활동과 관련된 정보

- 애플리케이션 이름 - 타임라인 데이터를 보고하는 실행 파일의 이름.
- 표시 이름 – TimeLine 막대 표시 텍스트.
- 콘텐츠 - 앱에서 표시하는 콘텐츠.
- 활동 ID - 활동의 고유 식별자.
- 상위 활동 ID - 상위 활동의 고유 식별자
- 앱 활동 ID - 애플리케이션 활동의 고유 식별자
- 활동 유형 - 활동 유형(알림, 모바일 장치 백업, 앱/파일/페이지 열기, 사용 중인 앱/포커스, 클립보드 및 복사/붙여넣기).
- 플랫폼 - 실행 파일에 연결된 플랫폼.
- 로컬 전용 - 활동이 로컬에서 발생했는지 아니면 다른 장치에서 발생했는지 표시
- 플랫폼 장치 ID - 플랫폼 장치 ID
- 초점(focus) - 애플리케이션 사용 기간(초)
- Is Read - 활동을 읽었는지 여부를 표시
- 업로드 대기열에 있음 – 항목이 업로드 대기열에 있는지 여부를 표시
- 시작 날짜/시간 – 활동이 시작된 날짜/시간
- 종료 날짜/시간 - 활동이 종료된 날짜/시간.
- 클라우드에서 생성 날짜/시간 - 활동이 클라우드에 나열된 날짜/시간
- 마지막 수정 날짜/시간 - 활동이 마지막으로 수정된 날짜/시간.
- 클라이언트에서 마지막으로 수정한 날짜/시간 - 클라이언트 장치에서 활동이 마지막으로 수정된 날짜/시간.
- 만료 날짜/시간 - 활동 시작 시간으로부터 30일 후인 활동이 만료되는 날짜/시간
- 만든 날짜/시간 - 활동 항목이 만들어진 날짜/시간

3 Timeline 구조

■ Windows 10 타임라인 아티팩트의 위치

- 타임라인에 표시된 사용자 활성화

-%UserProfile%₩AppData₩Local₩ConnectedDevicesPlatform₩L.[profile]₩ActivitiesCache.db

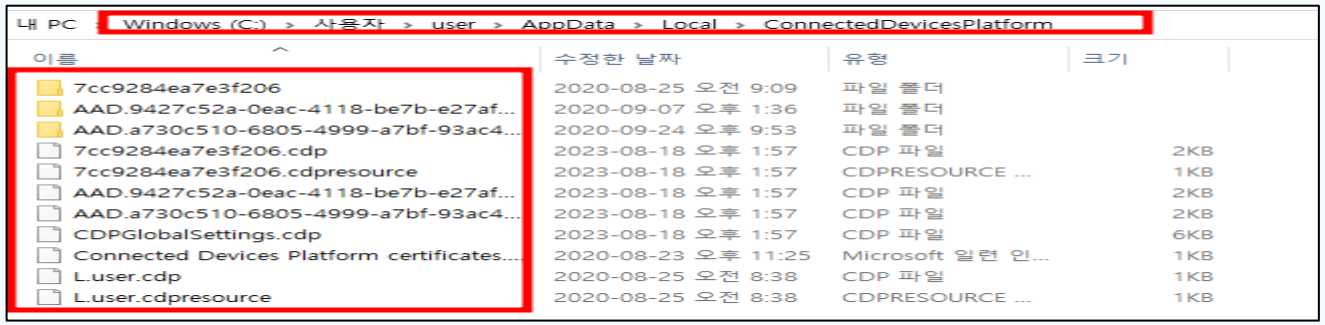
사용자 계정 유형	폴더명	레지스트리 경로
로컬 계정	L.{로컬 계정 명}	-
마이크로소프트 계정	{마이크로소프트 식별자(CID)}	NTUSER.DAT₩Software₩Microsoft₩IdentityCRL₩UserExtendedProperties
Office 365 혹은 Azure Activity Directory 계정	AAD.{보안 식별자(SID)}	NTUSER.DAT₩Software]Microsoft₩OneDrive₩Accounts

- 사용자는 로컬 계정 로그인 상태에서 마이크로소프트 계정으로 전환하는 것과 같이 시스템에서 기본으로 사용할 계정을 변경 가능. 로컬 계정에서 마이크로소프트 계정으로 전환하게 되면 기존에 존재하던 'L.{로컬계정명}' 폴더가 삭제되고 마이크로소프트 계정 폴더가 생성됨. 이 때, 'L.{로컬계정명}' 내 ActivityCache.db 파일에 기록된 데이터는 새로운 ActivityCache.db 파일에 유지되고 클라우드와 동기화 됨. 반대로 마이크로소프트 계정에서 로컬 계정으로 전환된 경우에도 이전 마이크로소프트 계정 사용 기록이 새로운 ActivityCache.db 항목에 포함됨.

❸ Timeline 구조

■ Windows 10 타임라인 아티팩트의 위치

- Windows 10 사용 시 기본 계정 유형에 따른 경로의 변경 사항을 제외하고는 생성되는 아티팩트 파일 유형은 동일



CDPGlobalSettings.cdp	%UserProfile%₩AppData₩Local₩ConnectedDevicesPlatform	활성/비활성 사용자 정보 및 Windows 10 Timeline 기능 설정 정보 등을 기록하는 json 파일
Connected Devices Platform certifications.sst		-
{계정ID}.cdp		클라우드에 마지막으로 동기화된 시간 정보 등을 기록하는 json 파일
ActivitiesCache.db	%UserProfile%₩AppData₩Local₩ConnectedDevicesPlatform₩{Account}	전체적인 사용자 PC 사용 활동 정보를 기록하는 데이터베이스 파일
ActivitiesCache.db-shm		
ActivitiesCache.db-wal		

③ Timeline 구조

■ CDPGlobalSettings.cdp 파일 구조

- CDPGlobalSettings.cdp 파일은 활성 및 비활성 사용자 Id 정보와, Windows 10 Timeline 설정 정보 등을 기록하는 json 유형의 파일.

- ActivityStoreInfo 키에는 활성화 및 비활성화 사용자 ID 정보가 기록되어 있으며

AfcPrivacySettings 키에는 Windows 10 Timeline 설정(활성화, 비활성화) 정보가 기록.


```
"ActivityStoreInfo" : [
  {
    "active" : false,
    "activityStoreId" : "6416202C-2560-60BB-35B7-501D8494851D",
    "stableUserId" : "L.user"
  },
  {
    "active" : true,
    "activityStoreId" : "692575BE-848D-E4E7-F1FA-07131897836F",
    "stableUserId" : "7cc9284ea7e3f206"
  },
  {
    "active" : true,
    "activityStoreId" : "59F3864E-A7CF-0D77-7A4A-AAFD71D8CBAA",
    "stableUserId" : "AAD.9427c52a-0eac-4118-be7b-e27afdcfcd07"
  },
  {
    "active" : true,
    "activityStoreId" : "50B6D846-9743-6D95-9EF2-A637162190B7",
    "stableUserId" : "AAD.a730c510-6805-4999-a7bf-93ac4cd1e811"
  }
],
"AfcPrivacySettings" : {
  "ActivityFeed" : 0,
  "CloudSync" : 0,
  "PublishUserActivity" : 0,
  "UploadUserActivity" : 1
},
```

③ Timeline 구조

■ {계정 ID}.cdp 파일 구조

- {계정ID}.cdp 파일은 클라우드에 마지막으로 동기화된 시간 정보 등을 기록하는 json 파일

- CNCNotificationURiLastSynced 키는 클라우드에 마지막으로 동기화된 시간 값을 기록


```
{
  "AfcDatabaseSettings" : {
    "DatabaseInstanceId" : 0,
    "LastUpdated" : "2020-08-23T23:27:31.656"
  },
  "AfsActivityTypes" : [],
  "AfsChannelUri" : "",
  "AfsEnvironment" : "",
  "AfsSubscriptionId" : "",
  "AfsSubscriptionUpdateTime" : "0000-00-00T00:00:00.000",
  "BaseRegisteredInfoHash" : "",
  "CNCNotificationUri" : "",
  "CNCNotificationUriExpirationTime" : "0000-00-00T00:00:00.000",
  "CNCNotificationUriLastSynced" : "0000-00-00T00:00:00.000",
  "DdsRegistrationExpiryTickCount" : 1916432846944,
```

4 Timeline 분석

- ActivitiesCache.db 파일 분석

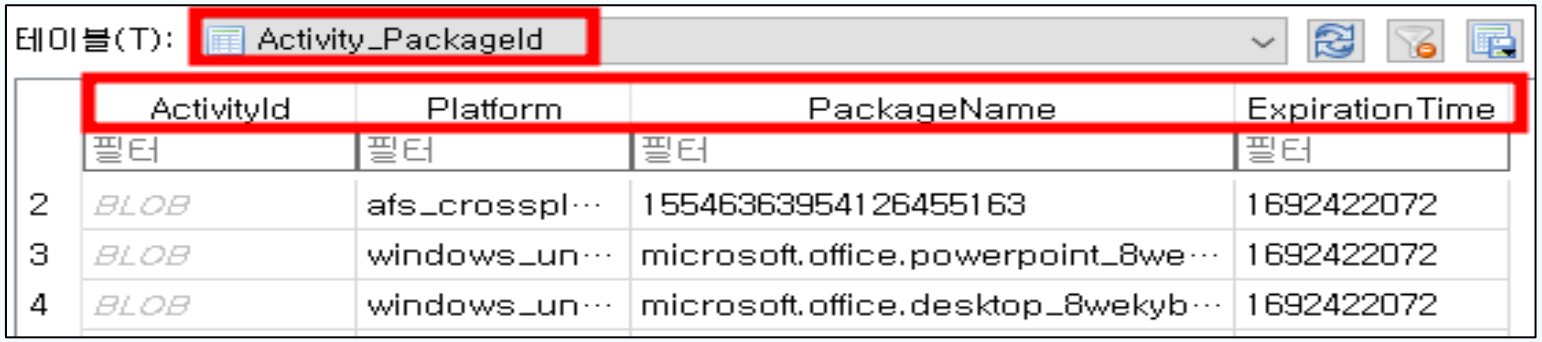
- ActivitiesCache.db은 전체적인 사용자 PC 사용 활동 정보를 기록하는 데이터베이스 유형의 파일로 가장 핵심이 되는 주요 파일
- ActivitiesCache.db 는 SQLite 데이터베이스이며 여러 테이블을 포함
- Activity_PackageId, Activity, ActivityOperation 테이블은 가장 핵심

테이블 명	설명
Metadata	Activity 유형 및 데이터베이스가 생성된 마지막 시간 정보
ManualSequence	마지막 활동 Etag 정보
Activity_PackageId	Activity와 ActivityOperations 테이블 간의 트랜잭션 정보
ActivityAssetCache	Empty
AppSettings	Empty
Activity	사용자 활동에 관한 정보
ActivityOperation	타임라인으로부터 제거된 타일 정보
DataEncryptionKeys	데이터 암호화를 위한 키 정보

4 Timeline 분석

- Activity_PackageId 테이블 분석
  - Acitivity_PackageID는 Activity 테이블과 ActivityOperations 테이블 간의 트랜잭션 정보를 기록
- 테이블 필드 정보로ActivityId, Platform, PackageName, ExpirationTime 구성

ActivityId	Activity 테이블과 ActivityOperation 테이블의 Id 필드에 매칭
Platform	이벤트와 관련된 활동 및 응용 프로그램 유형 정보를 기록
PackageName	사용자가 실행한 파일 경로와 파일 이름을 기록
ExpirationTime	이벤트가 처음 트리거된 시간으로부터 30일 (UTC) 이후의 시간 정보를 기록


테이블(T): Activity_PackageId

	ActivityId	Platform	PackageName	ExpirationTime
	필터	필터	필터	필터
2	BLOB	afs_crosspl···	155463639541264551 63	1692422072
3	BLOB	windows_un···	microsoft.office.powerpoint_8we···	1692422072
4	BLOB	windows_un···	microsoft.office.desktop_8wekyb···	1692422072

4 Timeline 분석

■ Activity_PackageId 테이블 분석

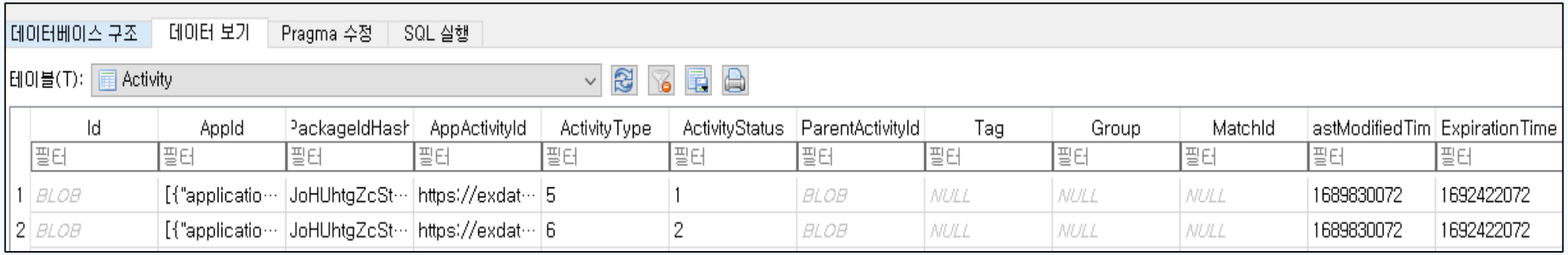
-Platform 값

Platform 값	설명
x_exe_path	독립형 실행 파일 경로
afs_crossplatformhost	클라우드 동기화 사용 가능 활동 (로컬 계정 사용시 존재 안함)
host	알 수 없음. 테스트 결과 보통 공백 혹은 Edge 및 Office 365에 관한 정보를 기록함
packageid	알 수 없음. 기본 프로그램과 사용자 설치 프로그램 정보를 기록함
windows_win32	설치된 소프트웨어 (UWP 제외)
windows_universal	윈도우 UWP 어플리케이션
android	안드로이드 어플리케이션
ios	iOS 어플리케이션
msa	Microsoft 어플리케이션
web	웹 어플리케이션

4 Timeline 분석

- Activity 테이블 분석

- Activity 테이블은 Windows 10 Timeline 타일에 관한 활동 정보를 기록



	Id	AppId	PackageIdHash	AppActivityId	ActivityType	ActivityStatus	ParentActivityId	Tag	Group	MatchId	LastModifiedTim	ExpirationTime
	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터
1	BLOB	[{"applicatio…	JoHUhtgZcSt…	https://exdat…	5	1	BLOB	NULL	NULL	NULL	1689830072	1692422072
2	BLOB	[{"applicatio…	JoHUhtgZcSt…	https://exdat…	6	2	BLOB	NULL	NULL	NULL	1689830072	1692422072

컬럼명	설명
Appid	JSON 형식 레코드로 실행한 파일 정보를 기록 [{"application":"powerpoint.activity.windows.com","platform":"host"},{"application":"15546363954126455163","platform":"afs_crossplatform"},{"application":"Microsoft.Office.PowerPoint_8wekyb3d8bbwe!microsoft.pptim","platform":"windows_universal"},{"application":"Microsoft.Office.Desktop_8wekyb3d8bbwe!PowerPoint","platform":"windows_universal"},{"application":"com.microsoft.office.powerpoint","platform":"android"},{"application":"com.microsoft.Office.PowerPoint","platform":"ios"},{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}₩₩Microsoft Office₩₩Office15₩₩POWERPNT.EXE","platform":"windows_win32"},{"application":"{6D809377-6AF0-444b-8957-A3773F02200E}₩₩Microsoft Office₩₩Office15₩₩POWERPNT.EXE","platform":"windows_win32"},{"application":"{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}₩₩Microsoft Office₩₩Office14₩₩POWERPNT.EXE","platform":"windows_win32"},{"application":"{6D809377-6AF0-444b-8957-A3773F02200E}₩₩MicrosoftOffice₩₩Office14₩₩POWERPNT.EXE","platform":"windows_win32"},{"application":"000000000003EDF6","platform":"msa"},{"application":"Microsoft.Office.PowerPoint_8wekyb3d8bbwe!microsoft.pptim","platform":"packageId"},{"application":"","platform":"alternateId"}]

4 Timeline 분석

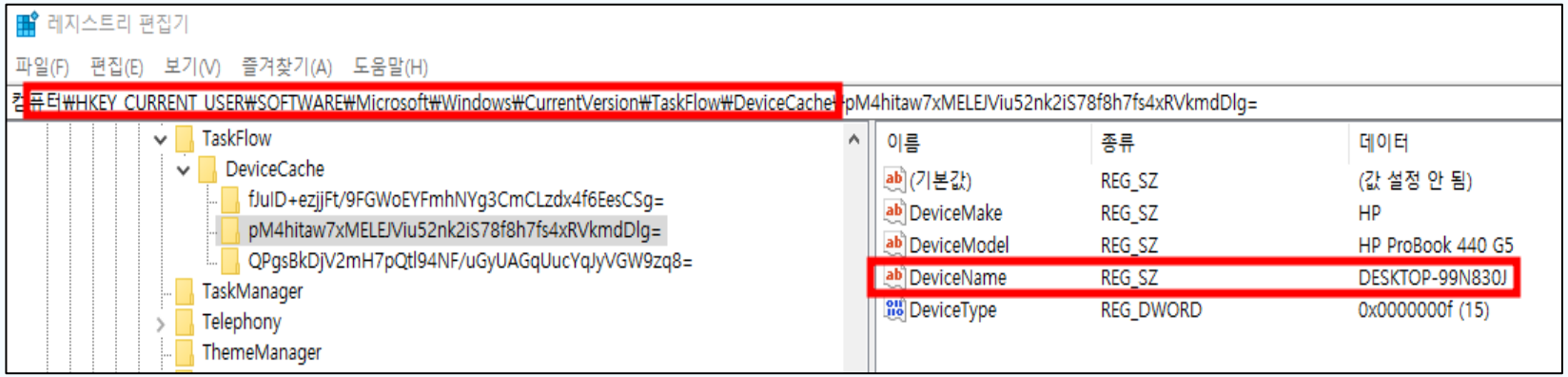
■ Activity 테이블 분석

컬럼명	설명
PackageIdHash	파일 해시 값 정보를 기록.
ActivityType	파일 및 응용 프로그램 focus 정보를 기록. 5: 파일/응용 프로그램이 열려 있음, 6: 파일/응용 프로그램이 화면에 초점 되어 있음
AppActivityId	실행한 문서 파일 이름 혹은 Edge 브라우저를 통해 방문하거나 검색한 URL 정보를 기록. https://****.sharepoint.com/personal/********/Documents/Microsoft Teams 채팅 파일/****_20230720.pptx
ActivityStatus	타일의 상태 정보를 기록. 1: Active (어플리케이션이 열려 있음), 2: Updated (이전의 Active entry가 업데이트됨), 3: Deleted (타임라인으로부터 타일이 제거됨)
LastModifiedTime	이벤트가 마지막으로 발생한 시간을 기록
ExpirationTime	LastModifiedTime에서 30일 후 시간을 기록
LastModifiedOnClient	클라이언트에서 마지막으로 수정된 날짜를 기록
CreatedInCloud	클라우드에서 생성된 날짜를 기록.
StratTime	실행 파일이 클릭된 시간을 기록
EndTime	보통 LastModifiedTime과 동일하나 Activity Type이 6인 경우 in-focues 종료 시간 표시

4 Timeline 분석

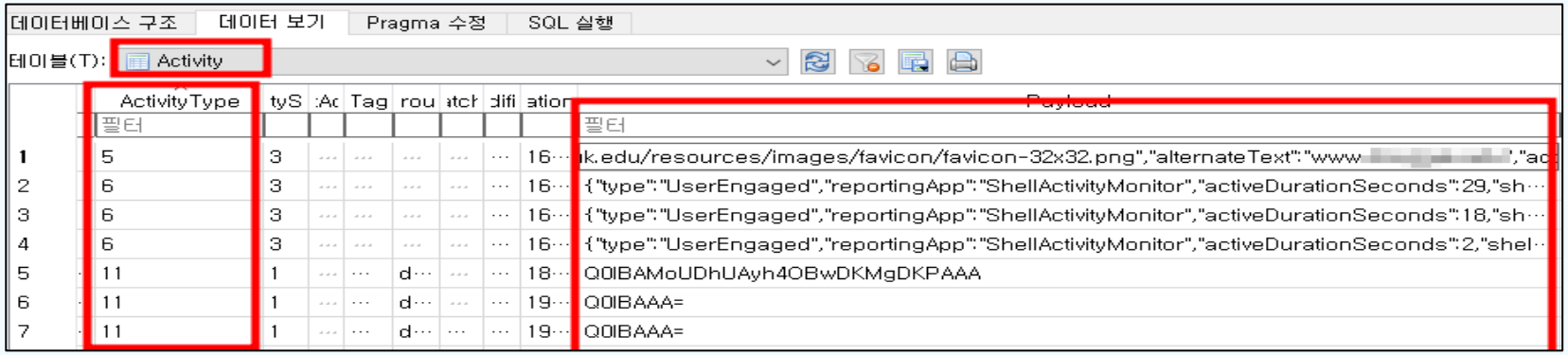
■ Activity 테이블 분석

컬럼명	설명
PlatformDeviceID	NTUSER.dat₩Software₩Microsoft₩Windows₩CurrentVersion₩TaskFlow₩DeviceCache₩ 레지스트리 경로에 존재하는 사용자 기기 ID 정보를 기록



4 Timeline 분석

■ Activity 테이블 분석

컬럼명	설명
Payload	JSON 형식의 레코드로 파일 및 응용 프로그램에 대한 세부사항을 기록. 이는 ActivityType 유형에 따라 아래와 같은 정보가 기록됨. - ActivityType 5: 프로세스/파일 이름 정보 (displayText) - ActivityType 6: 이벤트에 참여한 시간 (초 단위) (activeDurationSeconds)  ActivityType이 5일 때 기록된 정보는 display Text 키를 통해 파일 정보를 확인 가능 Windows 10 클립보드는 ActivityType 번호가 11로 Payload에 Base64로 인코딩 되어 저장 복사/붙여넣기는 ActivityType 16으로 데이터를 복사/붙여넣기 한 응용 프로그램의 데이터가 기록

4 Timeline 분석

■ ActivityOperation 테이블 분석

- ActivityOperation 테이블은 Windows 10 Timeline에서 마우스 우클릭을 통해 제거된 타일 정보를 기록.

- ActivityOperation 테이블에는 타일이 제거되면 새로운 ETag 값과 새로운 ActivityStatus 및 OperationType 값이 할당된 레코드가 생성

- Windows 10 Timeline은 사용자가 "모두 지우기" 옵션을 통해서 모든 타일을 제거할 수 있지만, 데이터베이스에는 삭제된 정보가 유지됨.

테이블(T): ActivityOperation

	OperationOrder	Id	OperationType	AppId	PackageIdHash	AppActivityId	ActivityType	ParentActivityId	Tag	Group	MatchId
	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터
1	129816	BLOB	1	[{"applicatio…	YNLZe4hPe…	default$wind…	12	BLOB	windows.dat…	default$wind…	NULL
2	129817	BLOB	1	[{"applicatio…	YNLZe4hPe…	default$wind…	12	BLOB	windows.dat…	default$wind…	NULL
3	129820	BLOB	1	[{"applicatio…	YNLZe4hPe…	default$wind…	12	BLOB	windows.dat…	default$wind…	NULL

9 윈도우 휴지통(Recycle Bin) 분석

- 윈도우 휴지통(Recycle Bin) 분석 개요
- 윈도우 휴지통(Recycle Bin) 구조
- 윈도우 휴지통(Recycle Bin) 분석

9 윈도우 휴지통(Recycle Bin) 분석

1 윈도우 휴지통(Recycle Bin) 분석 개요

- 윈도우에서 파일을 삭제할 경우, 기본적으로 삭제된 파일은 휴지통(Recycle.Bin) 영역으로 이동
- 추후 복원이 필요하면 복원 가능
- $RECYCLE.BIN 폴더로 존재

- $RECYCLE.BIN 폴더는 휴지통의 정보를 담고 있는 폴더

- 해당 폴더가 각 파티션별로 생기는 이유는 각 파티션이 논리적으로 다른 공간이기 때문에 해당 파티션에서 파일 및 폴더 등을 제거 하였을 때 각각의 파티션의 휴지통 공간으로 파일 정보 등이 이동하기 때문

- 다만 Windows 내에서 표시되는 휴지통에서는 관리의 편의성을 위하여 모든 파티션의 휴지통 공간에 저장된 정보를 함께 표시

② 윈도우 휴지통(Recycle Bin) 구조

- SID

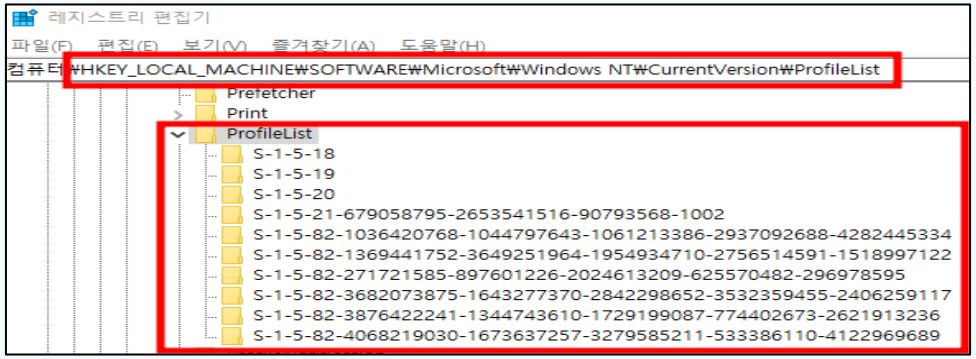
 - 휴지통 폴더 밑에 사용자 SID 이름으로 휴지통 폴더 생성.

 - 각 파티션마다 따로 휴지통 폴더 생성.

- 각 사용자 SID 확인

- HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩ProfileList

- cmd 명령어: wmic UserAccount Where LocalAccount=True Get SID




```
C:₩>wmic UserAccount Where LocalAccount=True Get SID
SID
S-1-5-21-679058795-2653541516-90793568-500
S-1-5-21-679058795-2653541516-90793568-503
S-1-5-21-679058795-2653541516-90793568-501
S-1-5-21-679058795-2653541516-90793568-1002
S-1-5-21-679058795-2653541516-90793568-504
```

② 윈도우 휴지통(Recycle Bin) 구조

- 구조

- 파티션 마다 생성

```
E:₩>dir /a
2023-08-31  오후 03:28    <DIR>          $RECYCLE.BIN
```

```
E:₩>cd $RECYCLE.BIN
E:₩$RECYCLE.BIN>dir /a
2023-08-31  오후 03:28    <DIR>          .
2023-08-31  오후 03:28    <DIR>          ..
2020-08-23  오후 11:37    <DIR>          S-1-5-18
2023-06-11  오전 11:13    <DIR>          S-1-5-21-679058795-2653541516-90793568-1002
               0개 파일                   0 바이트
               4개 디렉터리  108,938,260,480 바이트 남음
E:₩$RECYCLE.BIN>cd S-1-5-21-679058795-2653541516-90793568-1002
E:₩$RECYCLE.BIN₩S-1-5-21-679058795-2653541516-90793568-1002>dir
2023-09-01  오전 11:31                84  $IL6QDH1.pdf
2023-02-18  오후 12:19           751,537  $RL6QDH1.pdf
               2개 파일             751,621 바이트
               0개 디렉터리  108,652,199,936 바이트 남음
```

C:₩>dir /?
디렉터리에 있는 파일과 하위 디렉터리 목록을 보여 줍니다.

/A : 지정된 특성을 가진 파일을 표시

② 윈도우 휴지통(Recycle Bin) 구조

- 구조
  - $I와 $R 파일
    - 삭제된 데이터를 처리하고 관리하는 파일

종류	이름 규칙	내용
$R(Recycled 추정)	$R[임의문자열].[원본파일 확장자] 폴더는 확장자 없음	원본파일과 동일함
$I(Info2로 추정)	$I[임의 문자열].[원본파일 확장자] 폴더는 확장자 없음	삭제된 파일의 정보

- $I를 분석
  - 삭제 파일 이름, 확장자
  - 삭제되기 전 파일 경로, 이름
  - 파일 크기
  - 삭제시간

3 윈도우 휴지통(Recycle Bin) 분석

- $I 분석

Offset(h)	0x00	0x01	0x02	0x03	0x04	0x05	0x06	0x07	0x08	0x09	0x0A	0x0B	0x0C	0x0D	0x0E	0x0F
0x00	Header								File Size							
0x10	Deleted Timestamp								File Name Size				File Name			
0x20	File Name															

Offset	크기(Byte)	이름	설명
0x00~0x07	8 Byte	Header	파일 헤더
0x08~0x0F	8 Byte	File Size	원본 파일 크기
0x10~0x17	8 Byte	Deleted Timestamp	삭제된 파일의 시간 정보
0x18~0x1B	4 Byte	File Name Size	원본 파일 경로 크기
0x1C~	가변적	File Name	원본파일 경로(unicode)

③ 윈도우 휴지통(Recycle Bin) 분석

- 폴더 삭제

```
E:₩$RECYCLE.BIN>cd S-1-5-21-679058795-2653541516-90793568-1002
E:₩$RECYCLE.BIN₩S-1-5-21-679058795-2653541516-90793568-1002>dir
2023-09-01  오전 11:31                84 $IL6QDH1.pdf
2023-02-18  오후 12:19           751,537 $RL6QDH1.pdf
2023-09-01  오전 11:35                50 $INEV2NR
2023-09-01  오전 11:35    <DIR>          $RNEV2NR
               3개 파일             751,671 바이트
               1개 디렉터리  108,619,894,784 바이트 남음
```

- 폴더삭제

- $R과 $I 생성

- $I파일에서 삭제 이전 폴더에 대한 원래의 폴더명과 경로, 폴더를 삭제한 시간 기록.

- 폴더 하위의 폴더나 파일에 대해서는 $R, $I 생성하지 않음.

3 윈도우 휴지통(Recycle Bin) 분석

- 일반삭제와 완전삭제

- 일반삭제

- 휴지통으로 보내는 윈도우 시스템의 삭제 방식

- 완전삭제

- 휴지통을 경유하지 않고 바로 삭제(Shift키 + 삭제)
- 일반삭제라고 하더라도 용량이 크면 자동으로 완전삭제로 전환
- $MFT나 $Bitmap 같은 메타데이터 파일에서는 삭제된 것으로 플래그 상태를 처리
- 실제 데이터는 존재.

- 휴지통을 비우고 바로 윈도우 재부팅하게 되면 복구 가능성 낮아짐.