### timeline-activities

윈도우 10의 ActivitiesCache.db 파일에서 프로그램 실행 이력을 추출합니다.

#### 문법

timeline-activities FILE\_PATH

필수 매개변수

**FILE\_PATH**

ActivitiesCache.db 파일 경로. 이 파일은 C:\Users<username>\AppData\Local\ConnectedDevicesPlatform 디렉터리 내부에 생성됩니다.

#### 설명

명령을 실행한 다음 출력되는 필드 내용은 다음 표를 참조하십시오.

**출력 필드**

|  |  |  |  |
| --- | --- | --- | --- |
| 필드 | 타입 | 이름 | 설명 |
| id | 바이너리 | 액티비티 ID |  |
| executable | 문자열 | 실행 파일 경로 | 예: {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe |
| activity\_type | 문자열 | 작업 유형 | 예: ExecuteOpen, InFocus, CopyPaste |
| payload\_app\_display\_name | 문자열 | 앱 표시 이름 | 예: 명령 프롬프트 |
| payload\_display\_text | 문자열 | 표시 텍스트 | 예: 명령 프롬프트 |
| payload\_description | 문자열 | 설명 |  |
| payload\_active\_duration | 32비트 정수 | 활성화 기간 | 초 단위 |
| start\_time | 날짜 | 활성 시작 시각 |  |
| end\_time | 날짜 | 활성 종료 시각 |  |
| last\_modified\_time | 날짜 | 최종 변경 시각 |  |
| last\_modified\_on\_client | 날짜 | 클라이언트의 최종 변경 시각 |  |
| expiration\_time | 날짜 | 만료 시각 |  |
| priority | 32비트 정수 | 중요도 | 예: 1, 3 |
| activity\_status | 32비트 정수 | 액티비티 상태 | 예: 1 |
| user\_action\_state | 32비트 정수 | 사용자 액션 상태 | 예: 0 |
| created\_in\_cloud | 32비트 정수 | 클라우드에서 생성 여부 | 예: 1, 0 |
| is\_read | 32비트 정수 | 읽기 여부 | 예: 1, 0 |
| is\_local\_only | 32비트 정수 | 로컬 전용 여부 | 예: 1, 0 |
| etag | 32비트 정수 | ETag |  |
| group\_app\_activity\_id | 문자열 | 그룹 앱 액티비티 ID |  |
| app\_activity\_id | 문자열 | 앱 액티비티 ID | GUID\경로 형식 |
| parent\_activity\_id | 바이너리 | 부모 액티비티 ID |  |
| package\_id\_hash | 문자열 | 패키지 ID 해시 |  |
| platform\_device\_id | 문자열 | 플랫폼 장치 ID |  |
| payload\_activation\_uri | 문자열 | 페이로드 활성화 URI |  |
| payload\_background\_color | 문자열 | 페이로드 배경색 | 예: light, black |
| payload\_content\_uri | 문자열 | 페이로드 컨텐츠 경로 |  |
| payload\_type | 문자열 | 페이로드 유형 | 예: UserEngaged |
| payload\_user\_timezone | 문자열 | 페이로드 시간대 | 예: Asia/Seoul |
| payload\_reporting\_app | 문자열 | 페이로드 리포팅 앱 | 예: ShellActivityMonitor |
| clipboard\_payload | 문자열 | 클립보드 페이로드 |  |
| tag | 문자열 | 태그 |  |

#### 사용 예

윈도우 10 타임라인 아티팩트 조회

timeline-activities C:\Users\Logpresso\AppData\Local\ConnectedDevicesPlatform\L.Logpresso\ActivitiesCache.db