### timeline-activities

Windows 10のActivitiesCache.dbファイルからプログラム実行履歴を抽出します。

#### 構文

timeline-activities FILE\_PATH

必須パラメータ

**FILE\_PATH**

ActivitiesCache.dbファイルのパス。このファイルは C:\Users<username>\AppData\Local\ConnectedDevicesPlatform ディレクトリ内に生成されます。

#### 説明

コマンド実行後に出力されるフィールドの内容は、以下の表を参照してください。

**出力フィールド**

|  |  |  |  |
| --- | --- | --- | --- |
| フィールド | 型 | 名称 | 説明 |
| id | バイナリ | アクティビティID |  |
| executable | 文字列 | 実行ファイルパス | 例: {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe |
| activity\_type | 文字列 | 作業タイプ | 例: ExecuteOpen, InFocus, CopyPaste |
| payload\_app\_display\_name | 文字列 | アプリ表示名 | 例: コマンドプロンプト |
| payload\_display\_text | 文字列 | 表示テキスト | 例: コマンドプロンプト |
| payload\_description | 文字列 | 説明 |  |
| payload\_active\_duration | 32ビット整数 | アクティブ期間 | 秒単位 |
| start\_time | 日付 | アクティブ開始時刻 |  |
| end\_time | 日付 | アクティブ終了時刻 |  |
| last\_modified\_time | 日付 | 最終変更時刻 |  |
| last\_modified\_on\_client | 日付 | クライアント最終変更時刻 |  |
| expiration\_time | 日付 | 有効期限 |  |
| priority | 32ビット整数 | 重要度 | 例: 1, 3 |
| activity\_status | 32ビット整数 | アクティビティステータス | 例: 1 |
| user\_action\_state | 32ビット整数 | ユーザーアクション状態 | 例: 0 |
| created\_in\_cloud | 32ビット整数 | クラウド作成有無 | 例: 1, 0 |
| is\_read | 32ビット整数 | 既読フラグ | 例: 1, 0 |
| is\_local\_only | 32ビット整数 | ローカル専用フラグ | 例: 1, 0 |
| etag | 32ビット整数 | ETag |  |
| group\_app\_activity\_id | 文字列 | グループアプリアクティビティID |  |
| app\_activity\_id | 文字列 | アプリアクティビティID | GUID\パス形式 |
| parent\_activity\_id | バイナリ | 親アクティビティID |  |
| package\_id\_hash | 文字列 | パッケージIDハッシュ |  |
| platform\_device\_id | 文字列 | プラットフォームデバイスID |  |
| payload\_activation\_uri | 文字列 | ペイロードアクティベーションURI |  |
| payload\_background\_color | 文字列 | ペイロード背景色 | 例: light, black |
| payload\_content\_uri | 文字列 | ペイロードコンテンツパス |  |
| payload\_type | 文字列 | ペイロードタイプ | 例: UserEngaged |
| payload\_user\_timezone | 文字列 | ペイロードタイムゾーン | 例: Asia/Seoul |
| payload\_reporting\_app | 文字列 | ペイロードレポートアプリ | 例: ShellActivityMonitor |
| clipboard\_payload | 文字列 | クリップボードペイロード |  |
| tag | 文字列 | タグ |  |

#### 使用例

Windows 10タイムラインアーティファクトの参照

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