### reg-shim-cache

レジストリファイル内のAppCompatCacheキー（HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache\AppCompatCache）に保存されているすべての実行ファイルのパス、サイズ、最終実行時刻などの情報を照会します。取得したデータから実行ファイルの名前、パス、サイズ情報および最終実行時刻を確認でき、インシデント分析に活用することが可能です。

#### 構文

reg-shim-cache [zipcharset=CHARSET] [zippath=ZIPFILE\_PATH] FILE\_PATH

必須パラメータ

**FILE\_PATH**

レジストリファイルのパスを入力します。ファイルパスにワイルドカード（\*）を使用すると（例：D:\data\registry\*）、パターンに一致するすべてのファイルを一括で照会できます。zippathオプションと併用する場合は、ZIPファイル内に含まれるファイルのパスを指定してください。

オプションパラメータ

**zipcharset=CHARSET**

ZIPエントリのエンコーディング形式（デフォルト：utf-8）。次のドキュメントに登録されているPreferred MIME NameまたはAliasesを使用してください: <https://www.iana.org/assignments/character-sets/character-sets.xhtml>

**zippath=ZIPFILE\_PATH**

ZIPファイルのパス

#### 説明

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 | 説明 |
| file\_path | 文字列 | 実行ファイルのパス |
| modified\_at | 日付 | 修正日時 |

#### 使用例

ファイルパスを指定して照会

reg-shim-cache D:\data\registry\SYSTEM

zippathオプションを指定して照会

reg-shim-cache zippath=D:\data\registry.zip registry\SYSTEM