### reg-shellbags

レジストリファイルから、ユーザーがローカル、ネットワーク、およびリムーバブルストレージでアクセスしたフォルダー情報を照会します。取得したデータは、ユーザーが特定フォルダーへアクセスした時刻の確認、存在するフォルダーの削除・上書きに関する証拠調査、エクスプローラーによるフォルダーアクセスのMACタイム（Modification, Access, Metadata Change）追跡に利用できます。

#### 構文

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

必須パラメーター

**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度に照会できます。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レジストリファイルのパスを入力してください。

オプションパラメーター

**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）。以下のドキュメントに登録された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\_name | 文字列 | ファイル名 |
| file\_ext | 文字列 | ファイル拡張子 |
| last\_written | 日付 | 最終書き込み時刻 |
| order | 整数 | 拡張子ごとのファイル順序 |

#### 使用例

ファイルパスを指定して照会

reg-shellbags D:\data\registry\NTUSER.DAT

zippathオプションで指定したZIPアーカイブ内のレジストリファイルを照会

reg-shellbags zippath=D:\data\registry.zip registry\NTUSER.DAT

ファイル拡張子ごとに順序でソート

reg-shellbags D:\data\registry\NTUSER.DAT | sort file\_ext, order