### reg-shellbags

Loads the "information on the folder accessed by the user from local, network and removable storage devices" stored in the registry. Using the loaded data, you can check the time information of when a user accessed a specific folder, track evidence of deletion/overwriting of existing folders and track the MAC time for folder access through Explorer.

#### Syntax

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

Required Parameter

**FILE\_PATH**

Path to the registry file. Using a wildcard (\*) in the file name, you can retrieve all files containing a specific string pattern in the file name (e.g. D:\data\registry\*). If you provided the zippath option, input the registry file path in the ZIP file.

Optional Parameter

**zipcharset=CHARSET**

Character set to be used to decode the ZIP entry name and comment that are not encoded by UTF-8 encoding. Use the preferred MIME name or aliases registered in the following document: <http://www.iana.org/assignments/character-sets/character-sets.xhtml>

**zippath=ZIPFILE\_PATH**

Path to the ZIP file

#### Description

The output fields are as follows:

|  |  |  |
| --- | --- | --- |
| Field | Type | Description |
| file\_name | String | File name |
| file\_ext | String | File extension |
| last\_written | Date | Last written time |
| order | Integer | File order by extension |

#### Usage

Retrieve information by providing the file path.

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

Retrieve information when the zippath option is provided.

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

Sort the order field by file extension.

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