### reg-user-assists

Loads information such as "the list of programs recently executed, the last run time, and the execution count" stored in the registry file. Using the loaded data, you can check the name and list of recently executed applications and use the time and number of recently executed applications for analysis.

#### Syntax

reg-user-assists [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 |
| key | String | Executable file path |
| session\_num | Integer | Session number |
| exec\_count | Integer | Number of times of execution |
| focus\_time | Integer | Time activated |
| last\_execution | Date | Last run time |
| last\_written | Date | Last written time |

#### Usage

Retrieve information by providing the file path.

reg-user-assists D:\data\registry\NTUSER.DAT

Retrieve information when the zippath option is provided.

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