### hive-file

Retrieves information such as the account and group, security policy, OS information, USB device, and program usage history from a registry hive file.

#### Syntax

hive-file [zipcharset=CHARSET] [zippath=ZIPFILE\_PATH] FILE\_PATH

Required Parameter

**FILE\_PATH**

Path to the registry hive 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 hive file path in the ZIP file. There are five registry hive files.

|  |  |  |  |
| --- | --- | --- | --- |
| File | Purpose | Registry Path | Extraction Information |
| SAM | Account and access records | HKEY\_LOCAL\_MACHINE\SAM | Account and group |
| SECURITY | Security policy and privilege | HKEY\_LOCAL\_MACHINE\Security | Security policy |
| SOFTWARE | Installation program | HKEY\_LOCAL\_MACHINE\Software | OS version, OS installation date, OS installation directory and owner account |
| SYSTEM | System settings | HKEY\_LOCAL\_MACHINE\System | Host name, time zone, system shutdown time, USB device and the like |
| NTUSER.DAT | User settings | HKEY\_USERS\.DEFAULT | List of files you opened |

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 | Subkey |
| type | String | Type |
| name | String | Registry name |
| value | Object | Registry data |
| last\_written | Date | Last written time |

#### Usage

Retrieve information by providing the file path.

hive-file D:\data\registry\SYSTEM

Retrieve information when the zippath option is provided.

hive-file zippath=D:\data\registry.zip registry\SYSTEM

Check the Windows OS information.

hive-file D:\data\registry\SOFTWARE | search key=="ROOT\\Microsoft\\Windows NT\\CurrentVersion"