### evtx-file

Retrieves information such as the event channel, event provider, event ID, event operation and the like from an EVTX Windows event log file.

#### Syntax

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

Required Parameter

**FILE\_PATH**

Path to the Windows event log 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\evtx\*.evtx). If you provided the zippath option, input the EVTX 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**

Path to the ZIP file.

#### Description

The output fields are as follows:

|  |  |  |
| --- | --- | --- |
| Field | Type | Description |
| \_time | Date | Time at which the event occurred |
| computer | String | Computer name |
| channel | String | Event channel |
| provider | String | Event provider |
| event\_id | Integer | Event ID |
| task | Integer | Event task |
| level | Integer | Event level |
| record\_id | Integer | Recored ID |
| msg | String | Event message |
| event\_data | Map | Event data |

#### Usage

Retrieve information by providing the file path.

evtx-file D:\data\evtx\System.evtx

Retrieve information when the zippath option is provided.

evtx-file zippath=D:\data\evtx.zip evtx\System.evtx

Retrieve an event whose event provider is MySQL.

evtx-file D:\data\evtx\application.evtx | search provider=="MySQL"

Retrieve events that do not match the EVTX\_WHITE message pattern.

evtx-file D:\data\evtx\application.evtx | mpsearch msg [ lookuptable EVTX\_WHITE ] | search len(\_mp\_result) == 0