### evtx-file

EVTX形式のWindowsイベントログファイルから、イベントチャネル、イベントプロバイダー、イベントID、イベントタスクなどの情報を照会します。

#### 構文

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

必須パラメーター

**FILE\_PATH**

EVTX形式のWindowsイベントログファイルのパス。ファイルパスにワイルドカード（\*）を使用すると（例：D:\data\evtx\*.evtx）、パターンに一致するすべてのファイルを一括で照会できます。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EVTXファイルのパスを指定してください。

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）。下記ドキュメントに記載された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 |
| \_time | 日付 | イベント発生時刻 |
| computer | 文字列 | コンピュータ名 |
| channel | 文字列 | イベントチャネル |
| provider | 文字列 | イベントプロバイダー |
| event\_id | 整数 | イベントID |
| task | 整数 | イベントタスク |
| level | 整数 | イベントレベル |
| record\_id | 整数 | レコードID |
| msg | 文字列 | イベントメッセージ |
| event\_data | マップ | イベントデータ |

#### 使用例

ファイルパスを指定して照会

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

zippathで指定したZIPファイル内のEVTXイベントファイルを照会

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

イベントプロバイダーがMySQLであるイベントを照会

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

EVTX\_WHITEメッセージパターンに一致しないイベントのみを照会

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