### evtx-file

EVTX 윈도우 이벤트 로그 파일에서 이벤트 채널, 이벤트 공급자, 이벤트 ID, 이벤트 작업 등의 정보를 조회합니다.

#### 문법

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

필수 매개변수

**FILE\_PATH**

EVTX 윈도우 이벤트 로그 파일의 경로. 파일 경로에 와일드카드(\*)를 사용하면(예: D:\data\evtx\*.evtx) 패턴과 일치하는 모든 파일을 한 번에 조회할 수 있습니다. zippath 옵션과 함께 사용하는 경우, ZIP 파일에 포함된 EVTX 파일의 경로를 입력하십시오.

선택 매개변수

**zipcharset=CHARSET**

ZIP 엔트리 인코딩 형식 (기본값: utf-8). 다음 문서에 등록된 Preferred MIME Name이나 Aliases를 사용합니다: <https://www.iana.org/assignments/character-sets/character-sets.xhtml>

**zippath=ZIPFILE\_PATH**

ZIP 파일의 경로.

#### 설명

출력되는 필드 내용은 다음 표를 참조하십시오.

출력 필드

|  |  |  |
| --- | --- | --- |
| 필드 | 타입 | 설명 |
| \_time | 날짜 | 이벤트 발생 시각 |
| computer | 문자열 | 컴퓨터명 |
| channel | 문자열 | 이벤트 채널 |
| provider | 문자열 | 이벤트 공급자 |
| event\_id | 정수 | 이벤트 ID |
| task | 정수 | 이벤트 작업 |
| level | 정수 | 이벤트 레벨 |
| record\_id | 정수 | 레코드 ID |
| msg | 문자열 | 이벤트 메세지 |
| event\_data | 맵 | 이벤트 데이터 |

#### 사용 예

파일 경로를 입력하여 조회

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

zippath으로 지정한 ZIP 파일 안에 있는 EVTX 이벤트 파일을 조회

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

이벤트 공급자가 MySQL인 이벤트 조회

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

EVTX\_WHITE 메시지 패턴과 일치하지 않는 이벤트 목록만 조회

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