### wmi-objects-data

WMI (Windows Management Instrumentation) OBJECTS.DATA 파일에 저장된 CIM 개체를 조회합니다.

#### 문법

wmi-objects-data [zipcharset=CHARSET] [zippath=ZIPFILE\_PATH] FILE\_PATH

필수 매개변수

**FILE\_PATH**

OBJECTS.DATA 파일 경로. 이 파일은 C:\WINDOWS\system32\wbem\Repository\OBJECTS.DATA 경로에 위치합니다. zippath 옵션과 함께 사용하는 경우, ZIP 파일에 포함된 OBJECTS.DATA 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

명령을 실행한 다음 출력되는 필드 내용은 다음 표를 참조하십시오.

**출력 필드**

|  |  |  |  |
| --- | --- | --- | --- |
| 필드 | 타입 | 이름 | 설명 |
| \_file | 문자열 | 저장소 파일 이름 | 예: OBJECTS.DATA |
| \_time | 날짜 | 시각 |  |
| record\_type | 문자열 | 레코드 유형 | 예: CLASS\_DEFINITION, INSTANCE\_OBJECT, REGISTRATION |
| class\_name | 문자열 | 클래스 이름 | 예: Win32\_PageFileSetting |
| date1 | 날짜 | 날짜 1 |  |
| date2 | 날짜 | 날짜 2 |  |
| hash | 문자열 | 해시 값 |  |
| index\_key | 문자열 | 인덱스 키 |  |
| instance\_name | 문자열 | 인스턴스 이름 | 예: Connection, provider |
| name | 문자열 | 이름 | 예: CIM\_Setting |
| properties | 맵 | 속성 목록 |  |
| qualifiers | 맵 | 한정자 목록 |  |
| strings | 배열 | 문자열 목록 |  |
| super\_class\_name | 문자열 | 상위 클래스 이름 | 예: \_\_SystemClass, \_\_Provider, \_\_Event |

#### 사용 예

WMI 서브스크립션을 통한 실행 탐지 (T1546.003)

wmi-objects-data C:\windows\system32\wbem\Repository\OBJECTS.DATA | eval strings = strjoin("\n", strings) | search in(strings, "\*\_\_EventFilter\*", "\*\_\_EventConsumer\*", "\*\_\_FilterToConsumerBinding\*")