### reg-shellbags

레지스트리 파일에서 사용자가 로컬, 네트워크 및 이동식 저장 장치에서 접근한 폴더 정보를 조회합니다. 조회한 데이터는 사용자가 특정 폴더에 접근한 시간 정보 확인, 존재하는 폴더의 삭제/덮어쓰기에 대한 증거 조사, 탐색기를 통한 폴더 접근에 대한 MAC 타임(Modification, Access, Metadata Change) 추적에 사용할 수 있습니다.

#### 문법

reg-shellbags [zipcharset=CHARSET] [zippath=ZIPFILE\_PATH] FILE\_PATH

필수 매개변수

**FILE\_PATH**

레지스트리 파일 경로를 입력합니다. 파일 경로에 와일드카드(\*)를 사용하면(예: D:\data\registry\*) 패턴과 일치하는 모든 파일을 한 번에 조회할 수 있습니다. zippath 옵션과 함께 사용하는 경우, ZIP 파일에 포함된 레지스트리 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 |
| file\_name | 문자열 | 파일 이름 |
| file\_ext | 문자열 | 파일 확장자 |
| last\_written | 날짜 | 마지막으로 쓰여진 시간 |
| order | 정수 | 확장자별 파일 순서 |

#### 사용 예

파일 경로를 입력하여 조회

reg-shellbags D:\data\registry\NTUSER.DAT

zippath 옵션으로 지정한 ZIP 압축 파일 안에 있는 레지스트리 파일을 조회

reg-shellbags zippath=D:\data\registry.zip registry\NTUSER.DAT

파일 확장자별 순서 정렬

reg-shellbags D:\data\registry\NTUSER.DAT | sort file\_ext, order