### reg-shim-cache

레지스트리 파일에서 AppCompatCache 키(HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache\AppCompatCache)에 저장된 모든 실행 파일의 경로, 크기, 마지막 실행 시간 등의 정보를 조회합니다. 조회한 데이터는 실행 파일의 이름, 경로, 크기 정보 및 마지막 실행 시간을 확인할 수 있고, 침해사고 분석에 활용할 수 있습니다.

#### 문법

reg-shim-cache [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 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\_path | 문자열 | 실행 파일 경로 |
| modified\_at | 날짜 | 수정일시 |

#### 사용 예

파일 경로를 입력하여 조회

reg-shim-cache D:\data\registry\SYSTEM

zippath 옵션을 입력한 경우, 조회

reg-shim-cache zippath=D:\data\registry.zip registry\SYSTEM