### reg-bam-entries

윈도우 10 (빌드 1709 이상)의 BAM (Background Activity Moderator)이 SYSTEM 레지스트리 하이브 파일에 기록한 데이터에서 계정별 프로그램 실행 흔적을 추출합니다.

#### 문법

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

필수 매개변수

**FILE\_PATH**

레지스트리 파일 경로. 파일 경로에 와일드카드(\*)를 사용하면 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

명령을 실행한 다음 출력되는 필드 내용은 다음 표를 참조하십시오.

**출력 필드**

|  |  |  |  |
| --- | --- | --- | --- |
| 필드 | 타입 | 이름 | 설명 |
| \_file | 문자열 | 레지스트리 하이브 파일 이름 | 예: SYSTEM |
| sid | 문자열 | 프로그램을 실행한 계정의 SID | 예: S-1-5-18 |
| file\_name | 문자열 | 실행 파일 이름 | 예: cmd.exe |
| file\_path | 문자열 | 실행 파일 경로 | 예: \Device\HarddiskVolume4\Windows\System32\cmd.exe |
| last\_execution | 날짜 | 최근 실행 일시 |  |

#### 사용 예

윈도우 10의 SYSTEM 하이브 파일에서 BAM 아티팩트 조회

reg-bam-entries D:\data\registry\SYSTEM