### hive-file

레지스트리 하이브 파일에서 계정 및 그룹, 보안 정책, OS 정보, USB 장치, 프로그램 사용 내역 등의 정보를 조회합니다.

#### 문법

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

필수 매개변수

**FILE\_PATH**

레지스트리 파일의 경로. 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 하이브 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

하이브 파일과 출력되는 필드 내용은 다음 표를 참조하십시오.

하이브 파일

|  |  |  |  |
| --- | --- | --- | --- |
| 파일 | 용도 | 레지스트리 경로 | 추출 정보 |
| SAM | 계정 및 접속 기록 | HKEY\_LOCAL\_MACHINE\SAM | 계정, 그룹 |
| SECURITY | 보안 정책 및 권한 | HKEY\_LOCAL\_MACHINE\Security | 보안 정책 |
| SOFTWARE | 설치 프로그램 | HKEY\_LOCAL\_MACHINE\Software | OS 버전, OS 설치일, OS 설치 디렉터리, 소유자 계정 |
| SYSTEM | 시스템 설정 | HKEY\_LOCAL\_MACHINE\System | 호스트명, 시간대, 시스템 종료시각, USB 장치 등 |
| NTUSER.DAT | 사용자 설정 | HKEY\_USERS\.DEFAULT | 열어본 파일 목록 |

출력 필드

|  |  |  |
| --- | --- | --- |
| 필드 | 타입 | 설명 |
| key | 문자열 | 서브 키 |
| type | 문자열 | 타입 |
| name | 문자열 | 레지스트리 이름 |
| value | 객체 | 레지스트리 데이터 |
| last\_written | 날짜 | 마지막으로 쓰여진 시간 |

#### 사용 예

파일 경로를 입력하여 조회

hive-file D:\data\registry\SYSTEM

zippath 옵션을 입력한 경우, 조회

hive-file zippath=D:\data\registry.zip registry\SYSTEM

윈도우 OS 정보 확인

hive-file D:\data\registry\SOFTWARE | search key=="ROOT\\Microsoft\\Windows NT\\CurrentVersion"