### ntfs-usnjrnl

USN 저널 파일에서 이벤트 발생 시각, 파일 경로 및 이름, 파일 생성/삭제 등의 작업 정보를 조회합니다. 조회한 데이터로 MFT 파일과 조인하여 타임라인 분석이 가능합니다.

#### 문법

ntfs-usnjrnl [zipcharset=CHARSET] [zippath=ZIPFILE\_PATH] FILE\_PATH

필수 매개변수

**FILE\_PATH**

USN 저널 파일의 경로. 파일 경로에 와일드카드(\*)를 사용하면(예: D:\data\NTFS\*) 패턴과 일치하는 모든 파일을 한 번에 조회할 수 있습니다. zippath 옵션과 함께 사용하는 경우, ZIP 파일에 포함된 USN 저널 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 |
| \_time | 날짜 | 이벤트 발생 시각 |
| file\_name | 문자열 | 파일 이름 |
| file\_no | 정수 | 파일 번호 |
| file\_ref | 정수 | 파일 레퍼런스 |
| parent\_file\_no | 정수 | 부모 파일 번호 |
| parent\_file\_ref | 정수 | 부모 파일 레퍼런스 |
| reason | 리스트 | 이벤트 동작. 플래그 정보는 아래 표 참고 |
| usn | 정수 | 업데이트 시퀀스 넘버 |

플래그 정보

reason 필드에 출력되는 플래그 정보는 내용은 다음 표를 참조하십시오(USN\_RECORD\_V3 structure (winioctl.h), <https://docs.microsoft.com/ko-kr/windows/win32/api/winioctl/ns-winioctl-usn_record_v2> 참조).

|  |  |  |
| --- | --- | --- |
| 플래그 | 16진수 값 | 설명 |
| DATA\_OVERWRITE | 0x00000001 | 기본 $DATA 속성에 데이터를 겹쳐씀 |
| DATA\_EXTEND | 0x00000002 | 기본 $DATA 속성에 데이터가 추가됨 |
| DATA\_TRUNCATION | 0x00000004 | 기본 $DATA 속성에 데이터가 줄어듬 |
| NAMED\_DATA\_OVERWRITE | 0x00000010 | 이름 있는 $DATA 속성에 데이터를 겹쳐씀 |
| NAMED\_DATA\_EXTEND | 0x00000020 | 이름 있는 $DATA 속성에 데이터가 추가됨 |
| NAMED\_DATA\_TRUNCATION | 0x00000040 | 이름 있는 $DATA 속성에 데이터가 줄어듬 |
| FILE\_CREATE | 0x00000100 | 파일이나 디렉터리가 생성됨 |
| FILE\_DELETE | 0x00000200 | 파일이나 디렉터리가 삭제됨 |
| EA\_CHANGE | 0x00000400 | 파일의 확장된 속성이 변경됨 |
| SECURITY\_CHANGE | 0x00000800 | 접근 권한이 변경됨 |
| RENAME\_OLD\_NAME | 0x00001000 | 객체명 변경 시, 변경 전 이름 |
| RENAME\_NEW\_NAME | 0x00002000 | 객체명 변경 시, 변경 후 이름 |
| INDEXABLE\_CHANGE | 0x00004000 | 인덱스 상태가 변경됨 |
| BASIC\_INFO\_CHANGE | 0x00008000 | 하나 이상의 파일/디렉터리 속성이나 타임스탬프가 변경됨 |
| HARD\_LINK\_CHANGE | 0x00010000 | 하드 링크가 생성되었거나 삭제됨 |
| COMPRESSION\_CHANGE | 0x00020000 | 압축 상태가 변경됨(압축 또는 압축 해제) |
| ENCRYPTION\_CHANGE | 0x00040000 | 암호화 상태가 변경됨(암호화 또는 복호화) |
| OBJECT\_ID\_CHANGE | 0x00080000 | 객체 ID가 변경됨 |
| REPARSE\_POINT\_CHANGE | 0x00100000 | Reparse point가 변경됨 |
| STREAM\_CHANGE | 0x00200000 | 이름 있는 $DATA 속성의 생성, 삭제, 또는 변경됨 |
| TRANSACTED\_CHANGE | 0x00400000 | 주어진 스트림이 TxF 트랜잭션 커밋을 통해 수정됨 |
| INTEGRITY\_CHANGE | 0x00800000 | 무결성 설정이 변경됨 |
| CLOSE | 0x80000000 | 파일/디렉터리를 닫음 |

#### 사용 예

파일 경로를 입력하여 조회

ntfs-usnjrnl D:\data\NTFS\test\_UsnJrnl

zippath 옵션으로 지정한 ZIP 파일 안에 있는 USN 저널 파일을 조회

ntfs-usnjrnl zippath=D:\data\NTFS.zip NTFS\test\_UsnJrnl

실행 파일을 삭제한 이력 조회

ntfs-usnjrnl D:\data\NTFS\test\_UsnJrnl | search file\_name == "\*.exe" and string(reason) == "\*DELETE\*"

NTFS 마스터 파일과 조인하여 타임라인 분석

ntfs-usnjrnl D:\data\NTFS\test\_UsnJrnl | streamjoin type=left file\_no [ ntfs-mft D:\data\NTFS\test\_MFT | rename no as file\_no | fields file\_no, file\_path, in\_use, is\_dir ] | eval reason = strjoin(" | ", reason) | fields \_time, file\_path, reason, in\_use, is\_dir