### ntfs-logfile

NTFS 트랜잭션 로그 파일에서 파일 이름, 생성/수정/접근일시, Redo/Undo 작업 유형을 조회합니다. 이 명령으로 파일 생성, 삭제, 이름 변경 등의 내역을 확인할 수 있습니다.

#### 문법

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

필수 매개변수

**FILE\_PATH**

NTFS 트랜잭션 로그 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 NTFS 트랜잭션 로그 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 |
| access\_at | 날짜 | 접근일시 |
| client\_data\_length | 정수 | 레코드 크기 |
| created\_at | 날짜 | 생성일시 |
| file\_name | 문자열 | 파일 이름 |
| flags | 정수 | 플래그 |
| lsn | 정수 | 로그파일 시퀀스 넘버 |
| mft\_head | 문자열 | mft 헤더 |
| mft\_link\_count | 정수 | 해당 파일을 참조하는 엔트리 갯수 |
| mft\_lsn | 정수 | mft 로그파일 시퀀스 넘버 |
| modified\_at | 날짜 | 수정일시 |
| page | 정수 | 페이지 번호 |
| prev\_lsn | 정수 | 이전 로그파일 시퀀스 넘버 |
| record\_type | 정수 | 레코드 타입 (2=체크포인트 레코드, 1=그외 레코드) |
| redo\_len | 정수 | redo 데이터 크기 |
| redo\_offset | 정수 | redo 데이터 시작 |
| redo\_op | 문자열 | redo 작업 |
| undo\_len | 정수 | undo 데이터 크기 |
| undo\_offset | 정수 | undo 데이터 시작 |
| undo\_op | 문자열 | undo 작업 |

Redo\_op, Undo\_op 작업 코드

redo\_op와 undo\_op 필드에 출력되는 작업 코드는 다음 표를 참조하십시오.

|  |  |
| --- | --- |
| `redo\_op`/`undo\_op` | 16진수 값 |
| noop | 0x00 |
| compensation\_log\_record | 0x1 |
| initialize\_file\_record\_segment | 0x2 |
| deallocate\_file\_record\_segment | 0x3 |
| write\_end\_of\_file\_record\_segment | 0x4 |
| create\_attribute | 0x5 |
| delete\_attribute | 0x6 |
| update\_resident\_value | 0x7 |
| update\_non\_resident\_value | 0x8 |
| update\_mapping\_pairs | 0x9 |
| delete\_dirty\_clusters | 0xa |
| set\_new\_attribute\_size | 0xb |
| add\_index\_entry\_root | 0xc |
| delete\_index\_entry\_root | 0xd |
| add\_index\_entry\_allocation | 0xe |
| delete\_index\_entry\_allocation | 0xf |
| set\_index\_entry\_ven\_allocation | 0x12 |
| update\_file\_name\_root | 0x13 |
| update\_file\_name\_allocation | 0x14 |
| set\_bits\_in\_non\_resident\_bitmap | 0x15 |
| clear\_bits\_in\_non\_resident\_bitmap | 0x16 |
| prepare\_transaction | 0x19 |
| commit\_transaction | 0x1a |
| forget\_transaction | 0x1b |
| open\_non\_resident\_attribute | 0x1c |
| open\_attribute\_table\_dump | 0x1d |
| dirty\_page\_table\_dump | 0x1f |
| transaction\_table\_dump | 0x20 |
| update\_record\_data\_root | 0x21 |

#### 사용 예

파일 경로를 입력하여 조회

ntfs-logfile D:\data\NTFS\test\_LogFile

zippath으로 지정한 ZIP 파일 안에 있는 NTFS 트랜잭션 로그 파일을 조회

ntfs-logfile zippath=D:\data\NTFS.zip NTFS\test\_LogFile

initialize\_file\_record\_segment이거나, delete를 포함하는 redo\_op 로그 조회

ntfs-logfile D:\data\NTFS\test\_LogFile | sort lsn | search redo\_op == "initialize\_file\_record\_segment" or redo\_op == "\*delete\*"