### ntfs-logfile

Retrieves information such as file name, creation/modification/access time, and redo/undo operation type in a NTFS transaction log file. With this command, you can see the history of file creation, deletion and renaming.

#### Syntax

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

Required Parameter

**FILE\_PATH**

Path to the NTFS log file. Using a wildcard (\*) in the file name, you can retrieve all files containing a specific string pattern in the file name (e.g. D:\data\NTFS\*). If you provided the zippath option, input the NTFS file path in the ZIP file.

Optional Parameter

**zipcharset=CHARSET**

Character set to be used to decode the ZIP entry name and comment that are not encoded by UTF-8 encoding. Use the preferred MIME name or aliases registered in the following document: <http://www.iana.org/assignments/character-sets/character-sets.xhtml>

**zippath=ZIPFILE\_PATH**

The path to the ZIP file.

#### Description

Output Fields

After running the ntfs-logfile command, the output fields are as follows:

|  |  |  |
| --- | --- | --- |
| Field | Type | Description |
| access\_at | Date | Last access time |
| client\_data\_length | Integer | Record volume |
| created\_at | Date | Time of creation |
| file\_name | String | File name |
| flags | Integer | Flag |
| lsn | Integer | Log file sequence number |
| mft\_head | String | MFT header |
| mft\_link\_count | Integer | Number of entries referencing the corresponding file |
| mft\_lsn | Integer | MFT log file sequence number |
| modified\_at | Date | Last modification time |
| page | Integer | Page number |
| prev\_lsn | Integer | Previous log file sequence number |
| record\_type | Integer | Record type (2: checkpoint record, 1: other records) |
| redo\_len | Integer | Size of redo data |
| redo\_offset | Integer | Offset of redo data |
| redo\_op | String | Redo operation code |
| undo\_len | Integer | Size of undo data |
| undo\_offset | Integer | Offset of undo data |
| undo\_op | String | Undo operation code |

Redo\_op and Undo\_op Operation Codes

Operation Codes output to the redo\_op and undo\_op fields are as follows:

|  |  |
| --- | --- |
| `redo\_op`/`undo\_op` | Hex value |
| 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 |

#### Usage

Retrieve by providing a file path.

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

Retrieve when the zippath option is provided.

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

Retrieve logs where the redo\_op is related to any initialize\_file\_record\_segment or delete operation.

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