### ntfs-mft

Retrieve information such as file path and name, file volume, disk allocation volume, file creation/modification/access time, and the existence of directories in an NTFS master file. Using the retrieved data, you can analyze the entire file and folder structure, extract deleted files or folders and browse alternate data stream (ADS) hidden information.

#### Syntax

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

Required Parameter

**FILE\_PATH**

Path to the NTFS MFT 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 MFT 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**

Path to the ZIP file

#### Description

The output fields are as follows:

|  |  |  |
| --- | --- | --- |
| Field | Type | Description |
| no | Integer | File number |
| file\_name | String | File name |
| file\_path | String | File path |
| file\_size | Integer | File size |
| alloc\_size | Integer | Allocated size |
| in\_use | Boolean | In-use flag |
| is\_dir | Boolean | Directory flag |
| link\_count | Integer | Number of hard links referencing the file |
| created\_at | Date | Creation time of the $FILE\_NAME attribute |
| modified\_at | Date | Last modification time of the $FILE\_NAME attribute |
| access\_at | Date | Last access time of the $FILE\_NAME attribute |
| mft\_modified\_at | Date | Last MFT modification time of the $FILE\_NAME attribute |
| std\_created\_at | Date | Creation time of the $STANDARD\_INFORMATION attribute |
| std\_modified\_at | Date | Last modification time of the $STANDARD\_INFORMATION attribute |
| std\_access\_at | Date | Last access time of the $STANDARD\_INFORMATION attribute |
| std\_mft\_modified\_at | Date | Last MFT modification time of the $STANDARD\_INFORMATION attribute |
| is\_readonly | Boolean | Read-only flag |
| is\_hidden | Boolean | Hidden flag |
| is\_system | Boolean | System flag |
| is\_archive | Boolean | Archive flag |
| is\_device | Boolean | Device flag |
| is\_normal | Boolean | Normal flag |
| is\_temp | Boolean | Temporary flag |
| is\_sparse | Boolean | Sparse file flag |
| is\_reparse | Boolean | Reparse point flag |
| is\_compressed | Boolean | Compression flag |
| is\_offline | Boolean | Offline flag |
| is\_indexed | Boolean | Index flag |
| is\_encrypted | Boolean | Encryption flag |
| lsn | Integer | Log sequence number |
| seq | Integer | Sequence |
| file\_ref | Integer | File reference |
| parent\_file\_ref | Integer | Parent file reference |
| parent\_no | Integer | Parent file number |

#### Usage

Retrieve information by providing the file path.

ntfs-mft D:\data\NTFS\test\_MFT

Retrieve information when the zippath option is provided.

ntfs-mft zippath=D:\data\NTFS.zip NTFS\test\_MFT

Load the list of deleted hidden files.

ntfs-mft D:\data\NTFS\test\_MFT | search not(in\_use) and not(is\_dir) and is\_hidden