### ntfs-usnjrnl

Retrieves operational information such as the time of the event occurrence, file path and name, and file creation/deletion. You can perform analyze the timeline by joining the retrieved data with the MFT file.

#### Syntax

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

Required Parameter

**FILE\_PATH**

Path to the USNJRNL journal 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 USNJRNL journal 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 (default: utf-8). 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

Output Fields

The output field is as follows:

|  |  |  |
| --- | --- | --- |
| Field | Type | Description |
| \_time | Date | Time at which the event occurred |
| file\_name | String | File name |
| file\_no | Integer | File number |
| file\_ref | Integer | File reference |
| parent\_file\_no | Integer | Parent file number |
| parent\_file\_ref | Integer | Parent file reference |
| reason | List | Event behavior. Refer to Reason Flags. |
| usn | Integer | Update sequence number |

Reason Flags

For more information, see the document **USN\_RECORD\_V3 structure (winioctl.h)**: <https://docs.microsoft.com/en-us/windows/win32/api/winioctl/ns-winioctl-usn_record_v2>

|  |  |  |
| --- | --- | --- |
| Reason flag | Hex | Description |
| DATA\_OVERWRITE | 0x00000001 | Data has been overwritten on the default $DATA attribute. |
| DATA\_EXTEND | 0x00000002 | Data has been added to the default $DATA. |
| DATA\_TRUNCATION | 0x00000004 | Data has been truncated on the default $DATA attribute. |
| NAMED\_DATA\_OVERWRITE | 0x00000010 | Data has been overwritten on the named default $DATA attribute. |
| NAMED\_DATA\_EXTEND | 0x00000020 | Data has been added to the named default $DATA attribute. |
| NAMED\_DATA\_TRUNCATION | 0x00000040 | Data has been truncated on the named default data attribute. |
| FILE\_CREATE | 0x00000100 | The file or directory has been created for the first time. |
| FILE\_DELETE | 0x00000200 | The file or directory is deleted. |
| EA\_CHANGE | 0x00000400 | The extended attributes of the file or directory have changed. |
| SECURITY\_CHANGE | 0x00000800 | The access permission has been changed. |
| RENAME\_OLD\_NAME | 0x00001000 | The old name when the file or directory is renamed. |
| RENAME\_NEW\_NAME | 0x00002000 | The new name when the file or directory is renamed. |
| INDEXABLE\_CHANGE | 0x00004000 | The index status has been changed. |
| BASIC\_INFO\_CHANGE | 0x00008000 | One or more file/directory attributes or time stamps have been changed. |
| HARD\_LINK\_CHANGE | 0x00010000 | A hard link has been created or removed. |
| COMPRESSION\_CHANGE | 0x00020000 | The compression status has been changed (compressed or decompressed). |
| ENCRYPTION\_CHANGE | 0x00040000 | The encryption status has been changed (encrypted or decrypted). |
| OBJECT\_ID\_CHANGE | 0x00080000 | The object ID has been changed. |
| REPARSE\_POINT\_CHANGE | 0x00100000 | The reparse point has been changed. |
| STREAM\_CHANGE | 0x00200000 | An attribute of the named $DATA has been added, removed, or renamed. |
| TRANSACTED\_CHANGE | 0x00400000 | The given stream is modified through a committed TxF transaction. |
| INTEGRITY\_CHANGE | 0x00800000 | The integrity setting has been changed. |
| CLOSE | 0x80000000 | The file or directory is closed. |

#### Usage

Retrieve information by providing the file path.

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

Retrieve information when the zippath option is provided.

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

Load the deletion history of executable files.

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

Analyze the timeline by joining with the NTFS MFT file.

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