### ntfs-usnjrnl

USNジャーナルファイルからイベント発生時刻、ファイルパスおよびファイル名、ファイルの作成/削除などの操作情報を照会します。取得したデータはMFTファイルと結合してタイムライン分析が可能です。

#### 構文

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

必須パラメータ

**FILE\_PATH**

USNジャーナルファイルのパス。ファイルパスにワイルドカード（\*）を使用すると（例: D:\data\NTFS\*）、パターンに一致するすべてのファイルを一度に照会できます。zippathオプションと併用する場合は、ZIPファイル内に含まれるUSNジャーナルファイルのパスを指定してください。

オプションパラメータ

**zipcharset=CHARSET**

ZIPエントリのエンコーディング形式（デフォルト: utf-8）。下記ドキュメントに登録されているPreferred MIME NameまたはAliasesを使用してください: <https://www.iana.org/assignments/character-sets/character-sets.xhtml>

**zippath=ZIPFILE\_PATH**

ZIPファイルのパス

#### 説明

出力されるフィールドの内容は以下の表を参照してください。

出力フィールド

|  |  |  |
| --- | --- | --- |
| フィールド | 型 | 説明 |
| \_time | 日付 | イベント発生時刻 |
| file\_name | 文字列 | ファイル名 |
| file\_no | 整数 | ファイル番号 |
| file\_ref | 整数 | ファイルリファレンス |
| parent\_file\_no | 整数 | 親ファイル番号 |
| parent\_file\_ref | 整数 | 親ファイルリファレンス |
| reason | リスト | イベント操作。フラグ情報は下記表を参照 |
| usn | 整数 | アップデートシーケンス番号 |

フラグ情報

reasonフィールドに出力されるフラグ情報の内容は、以下の表を参照してください（USN\_RECORD\_V3 structure (winioctl.h)、<https://docs.microsoft.com/ja-jp/windows/win32/api/winioctl/ns-winioctl-usn_record_v2> 参照）。

|  |  |  |
| --- | --- | --- |
| フラグ | 16進数値 | 説明 |
| DATA\_OVERWRITE | 0x00000001 | 既定の$DATA属性にデータを上書き |
| DATA\_EXTEND | 0x00000002 | 既定の$DATA属性にデータが追加 |
| DATA\_TRUNCATION | 0x00000004 | 既定の$DATA属性のデータが短縮 |
| NAMED\_DATA\_OVERWRITE | 0x00000010 | 名前付き$DATA属性にデータを上書き |
| NAMED\_DATA\_EXTEND | 0x00000020 | 名前付き$DATA属性にデータが追加 |
| NAMED\_DATA\_TRUNCATION | 0x00000040 | 名前付き$DATA属性のデータが短縮 |
| FILE\_CREATE | 0x00000100 | ファイルまたはディレクトリが作成 |
| FILE\_DELETE | 0x00000200 | ファイルまたはディレクトリが削除 |
| EA\_CHANGE | 0x00000400 | ファイルの拡張属性が変更 |
| SECURITY\_CHANGE | 0x00000800 | アクセス権限が変更 |
| RENAME\_OLD\_NAME | 0x00001000 | オブジェクト名変更時の変更前の名前 |
| RENAME\_NEW\_NAME | 0x00002000 | オブジェクト名変更時の変更後の名前 |
| INDEXABLE\_CHANGE | 0x00004000 | インデックス状態が変更 |
| BASIC\_INFO\_CHANGE | 0x00008000 | 1つ以上のファイル/ディレクトリ属性またはタイムスタンプが変更 |
| HARD\_LINK\_CHANGE | 0x00010000 | ハードリンクが作成または削除 |
| COMPRESSION\_CHANGE | 0x00020000 | 圧縮状態が変更（圧縮または圧縮解除） |
| ENCRYPTION\_CHANGE | 0x00040000 | 暗号化状態が変更（暗号化または復号化） |
| OBJECT\_ID\_CHANGE | 0x00080000 | オブジェクトIDが変更 |
| REPARSE\_POINT\_CHANGE | 0x00100000 | Reparse pointが変更 |
| STREAM\_CHANGE | 0x00200000 | 名前付き$DATA属性の作成、削除、または変更 |
| TRANSACTED\_CHANGE | 0x00400000 | 指定ストリームがTxFトランザクションコミットで修正 |
| INTEGRITY\_CHANGE | 0x00800000 | 整合性設定が変更 |
| CLOSE | 0x80000000 | ファイル/ディレクトリをクローズ |

#### 使用例

ファイルパスを指定して照会

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

zippathオプションで指定したZIPファイル内のUSNジャーナルファイルを照会

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

実行ファイルの削除履歴を照会

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

NTFSマスターファイルと結合してタイムライン分析

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