UsnJrl:$J

Use Cases

- **Incident Response** — Gain insight into files that may have previously existed, been renamed, or modified by the Threat Actor
- **Law Enforcement** — Gain insight into files that may have previously existed, been renamed, or modified by the user
- **Students/Research** — Better understand the NTFS File System's arguably most useful artifact

Resources

- 13Cubed - NTFS Journal Forensics 🔗
- Advanced UsnJrnl Forensics PDF 🔗
- DFIR-02 - Journal Forensics 🔗
- Re-Introducing $UsnJrnl 🔗
- UsnJrnl Extraction for Efficient Investigation 🔗
- Wikipedia - USN Journal 🔗
- The Windows USN Journal 🔗

Location

- C:\$Extend\$UsnJrnl:$J

Versions

- USN_RECORD_V2 🔗
- USN_RECORD_V3 🔗
- USN_RECORD_V4 🔗

Background

- $J Is an Alternate Data Stream (ADS) for the $UsnJrnl
- Contains records of file system operations

Change Journal Records 🔗

Change Reasons

- **USN_REASON_BASIC_INFO_CHANGE 0x00008000** — A user has either changed one or more file or directory attributes (for example, the read-only, hidden, system, archive, or sparse attribute), or one or more time stamps.
- **USN_REASON_CLOSE 0x80000000** — The file or directory is closed.
- **USN_REASON_COMPRESSION_CHANGE 0x00020000** — The compression state of the file or directory is changed from or to compressed.
- **USN_REASON_DATA_EXTEND 0x00000002** — The file or directory is extended (added to).
- **USN_REASON_DATA_OVERWRITE 0x00000001** — The data in the file or directory is overwritten.
- **USN_REASON_DATA_TRUNCATION 0x00000004** — The file or directory is truncated.
- **USN_REASON_EA_CHANGE 0x00000400**
  - The user made a change to the extended attributes of a file or directory.
  - These NTFS file system attributes are not accessible to Windows-based applications.
- **USN_REASON_ENCRYPTION_CHANGE 0x00040000** — The file or directory is encrypted or decrypted.
- **USN_REASON_FILE_CREATE 0x00000100** — The file or directory is created for the first time.
- **USN_REASON_FILE_DELETE 0x00000200** — The file or directory is deleted.
- **USN_REASON_HARD_LINK_CHANGE 0x00010000**
  - An NTFS file system hard link is added to or removed from the file or directory.
  - An NTFS file system hard link, similar to a POSIX hard link, is one of several directory entries that see the same file or directory.
- **USN_REASON_INDEXABLE_CHANGE 0x00004000**
  - A user changes the FILE_ATTRIBUTE_NOT_CONTENT_INDEXED attribute.
  - That is, the user changes the file or directory from one where content can be indexed to one where content cannot be indexed, or vice versa. Content indexing permits rapid searching of data by building a database of selected content.
- **USN_REASON_INTEGRITY_CHANGE 0x00800000**
  - A user changed the state of the FILE_ATTRIBUTE_INTEGRITY_STREAM attribute for the given stream.
  - On the ReFS file system, integrity streams maintain a checksum of all data for that stream, so that the contents of the file can be validated during read or write operations.
- **USN_REASON_NAMED_DATA_EXTEND 0x00000020** — The one or more named data streams for a file are extended (added to).
- **USN_REASON_NAMED_DATA_OVERWRITE 0x00000010** — The data in one or more named data streams for a file is overwritten.
- **USN_REASON_NAMED_DATA_TRUNCATION 0x00000040** — The one or more named data streams for a file is truncated.
- **USN_REASON_OBJECT_ID_CHANGE 0x00080000** — The object identifier of a file or directory is changed.
- **USN_REASON_RENAME_NEW_NAME 0x00002000** — A file or directory is renamed, and the file name in the USN_RECORD_V2 structure is the new name.
- **USN_REASON_RENAME_OLD_NAME 0x00001000** — The file or directory is renamed, and the file name in the USN_RECORD_V2 structure is the previous name.
- **USN_REASON_REPARSE_POINT_CHANGE 0x00100000** — The reparse point that is contained in a file or directory is changed, or a reparse point is added to or deleted from a file or directory.
- **USN_REASON_SECURITY_CHANGE 0x00000800** — A change is made in the access rights to a file or directory.
- **USN_REASON_STREAM_CHANGE 0x00200000** — A named stream is added to or removed from a file, or a named stream is renamed.
- **USN_REASON_TRANSACTED_CHANGE 0x00400000** — The given stream is modified through a TxF transaction.