mftecmd Forensic Cheat Sheet

Field	Analyst Use / Why It Matters
EntryNumber	File’s unique ID in the MFT. Use when mapping activity or correlating with other records.
SequenceNumber	Detects stale vs. active entries. If mismatch, file was deleted/reused.
InUse	Quick check: is this file/folder currently active or deleted?
ParentEntryNumber / ParentPath	Places the file in its directory context. Useful for reconstructing paths.
ParentSequenceNumber	Helps validate parent directory integrity (spotting MFT reuse).
FileName / Extension	Obvious: what’s it called, and what kind of file is it. Watch for mismatched extensions.
FileSize	Actual file length. Compare with ADS or memory-mapped files.
ReferenceCount	Number of hard links. Higher count → file may exist in multiple directories.
ReparseTarget	Shows redirection (symlinks, junctions, mount points). Red flag for persistence tricks.
IsDirectory	Directory vs. file — helps scope which artifacts to dig into.
HasAds	Alerts you to Alternate Data Streams (common malware hiding spot).
IsAds	Lets you know this row is itself an ADS, not the main file.
SI<FN	Compare SI and FN timestamps. Mismatches often = time stomping.
uSecZeros	All microseconds = zero → timestamps likely fabricated/copied.
Copied	Flag that file may have been copied, not created from scratch. Great for exfil/movement tracing
SiFlags	File flags (Hidden, System, Read-only, Archive). Hidden/System → check closer.
NameType	Which name type is stored. Win32 common; DOS/POSIX may indicate compatibility quirks.
Created0x10 / 0x30	Two creation timestamps from different attributes. Differences = copy/tampering.
LastModified0x10 / 0x30	Same idea for modified. Differences matter in anti-forensics detection.
LastRecordChange0x10 / 0x30	When metadata was changed. Compare across attributes for manipulation detection.
LastAccess0x10 / 0x30	Last access times. Often unreliable but useful for activity reconstruction.
UpdateSequenceNumber (USN)	Journal ID. Track exact change events via USN Journal analysis.
LogfileSequenceNumber (LSN)	Journal checkpoint. Correlate with NTFS $LogFile for operations.
SecurityId	Maps to security descriptor. Confirms access rights at time of creation.
ObjectIdFileDroid	Object ID used by Windows features. Rare, but links across moves/renames.
LoggedUtilStream	Indicates presence of logged utility stream. Check for EFS/TxF handling.
ZoneIdContents	From Zone.Identifier ADS (Mark of the Web). Shows if file was downloaded.
SourceFile	Where the MFT record came from (baseline $MFT vs. exported). Good for chain of custody.