[Topic]

Investigating the MACB timestamps change in case of file moving.
Checking how the timestamps are changing on Windows 7 and Windows 10 when moving the file to a different folder or to a different volume.

[Information]

Used Tools:

- Windows 7 Home Premium SP1 Version: 6.1 (build 7601) – I didn’t get the results I expected so I checked a different (older) version of Win7 as well.
- Windows 7 Enterprise SP1
- Windows 10 Enterprise Version: 1803
- FTK Imager 4.2 - for creating images about the drives and to save the MFT file
- analyzeMFT.py - for MFT parsing (https://github.com/dkovar/analyzeMFT)

The test was made between 11/4/2018 (Nov) and 11/5/2018 (Nov).

I tested this scenario with three different cut and paste methods:

- Command line: move command
- GUI-based CTRL-X and CTRL-V
- Drag and drop method (also gui based)

[Findings]

After summarizing my results I had some interesting findings:
1: There weren’t any differences between the results of my test on Windows 7 and Windows 10. Both of the OSs showed completely the same results.
This is especially interesting if we compare them to the SANS results on Windows 7/8 (https://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf) and the results by CyberForensicator on Windows 10. (http://cyberforensicator.com/2018/03/25/windows-10-time-rules/).

While SANS has an A for Win 7/8 and the other team has a B result for Win10 I got the same C result for both of the OSs.
(find a comparison below)

2: The Drag and Drop method has different functions behind it, depending on the target Volume. If the target is the same volume (and a different directory), the Drag and Drop method moves the file. If the target is a different volume, this method behaves as a file copy. Because of this, in case of out-of-volume copy the Drag and Drop method is not a test for cut and paste but a test for copy and paste.
Here are pictures which show this difference:
The file was copied from the D drive, and the target is the D in the first and E in the second one.

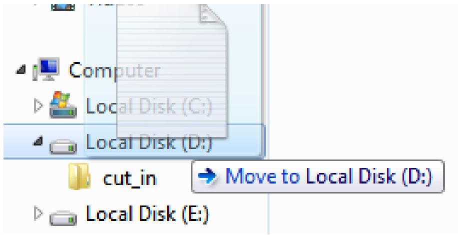


Illustration 1: In-volume Move

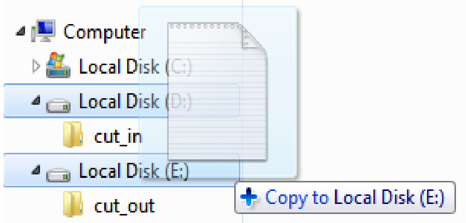


Illustration 2: Out-of-volume Copy

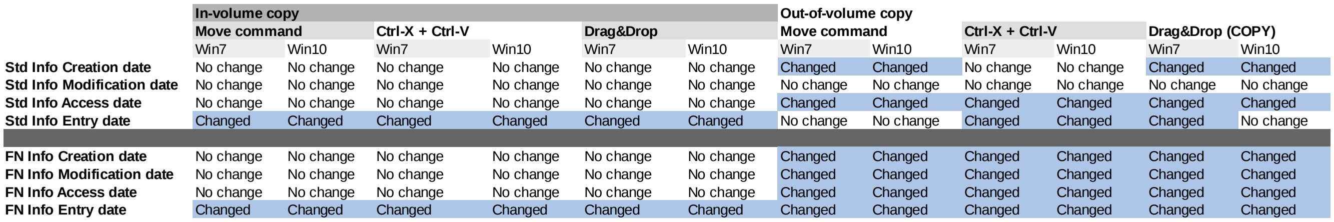
3: Only the Entry (STD and FN) date timestamp was changed in case of in-volume copy for every OSs and methods.

4: The timestamps of the original files in case of **out-of-volume** move weren't changed at all. The only thing that changed in case of the **command line moving** and **GUI-based CTRL-X CTRL-V** methods were the value of the 'Active' flag. This flag was switched from 'Active' to 'Inactive' on the original volume when the files were moved to a different volume. This means the file is no longer present on that volume. In case of Drag and Drop the result was different and non-relevant because as I stated earlier Drag and Drop is functioning as a copy function if we try to move something out-of-volume.

5: Additional findings with the help of Win 7 Home Premium. I compared the results of two different Win 7 versions but both of them changed the same timestamps.

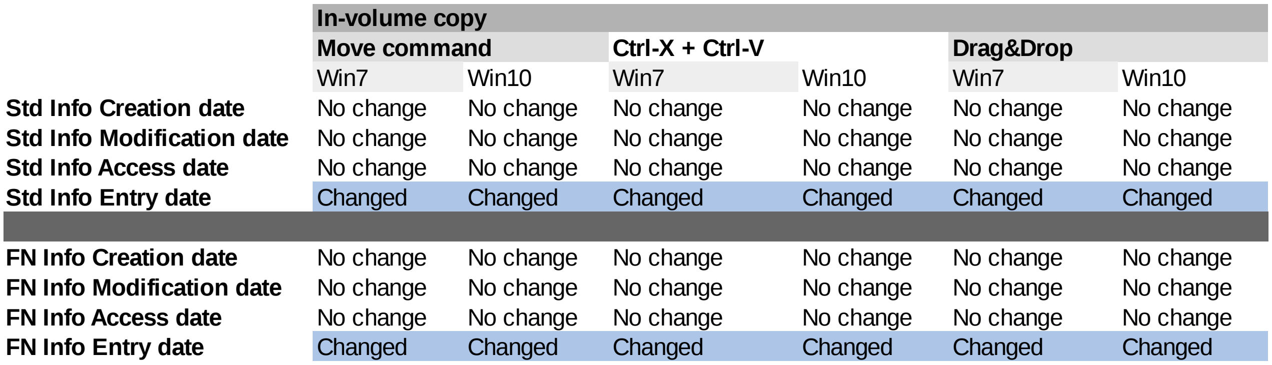
[Results]

Result about the changes in a table:



	In-volume copy						**Out-of-volume copy**					
	Move command		**Ctrl-X + Ctrl-V**		**Drag&Drop**		**Move command**		**Ctrl-X + Ctrl-V**		**Drag&Drop (COPY)**	
	Win7	Win10	Win7	Win10	Win7	Win10	Win7	Win10	Win7	Win10	Win7	Win10
Std Info Creation date	No change	No change	No change	No change	No change	No change	Changed	Changed	No change	No change	Changed	Changed
Std Info Modification date	No change	No change	No change	No change	No change	No change	No change	No change	No change	No change	No change	No change
Std Info Access date	No change	No change	No change	No change	No change	No change	Changed	Changed	Changed	Changed	Changed	Changed
Std Info Entry date	Changed	Changed	Changed	Changed	Changed	Changed	No change	No change	Changed	Changed	Changed	No change
FN Info Creation date	No change	No change	No change	No change	No change	No change	Changed	Changed	Changed	Changed	Changed	Changed
FN Info Modification date	No change	No change	No change	No change	No change	No change	Changed	Changed	Changed	Changed	Changed	Changed
FN Info Access date	No change	No change	No change	No change	No change	No change	Changed	Changed	Changed	Changed	Changed	Changed
FN Info Entry date	Changed	Changed	Changed	Changed	Changed	Changed	Changed	Changed	Changed	Changed	Changed	Changed

The same results in 2 different tables for better visibility



	In-volume copy					
	Move command		**Ctrl-X + Ctrl-V**		**Drag&Drop**	
	Win7	Win10	Win7	Win10	Win7	Win10
Std Info Creation date	No change	No change	No change	No change	No change	No change
Std Info Modification date	No change	No change	No change	No change	No change	No change
Std Info Access date	No change	No change	No change	No change	No change	No change
Std Info Entry date	Changed	Changed	Changed	Changed	Changed	Changed
FN Info Creation date	No change	No change	No change	No change	No change	No change
FN Info Modification date	No change	No change	No change	No change	No change	No change
FN Info Access date	No change	No change	No change	No change	No change	No change
FN Info Entry date	Changed	Changed	Changed	Changed	Changed	Changed

	Out-of-volume copy					
	Move command		Ctrl-X + Ctrl-V		Drag&Drop (COPY)	
	Win7	Win10	Win7	Win10	Win7	Win10
Std Info Creation date	Changed	Changed	No change	No change	Changed	Changed
Std Info Modification date	No change	No change	No change	No change	No change	No change
Std Info Access date	Changed	Changed	Changed	Changed	Changed	Changed
Std Info Entry date	No change	No change	Changed	Changed	Changed	No change
FN Info Creation date	Changed	Changed	Changed	Changed	Changed	Changed
FN Info Modification date	Changed	Changed	Changed	Changed	Changed	Changed
FN Info Access date	Changed	Changed	Changed	Changed	Changed	Changed
FN Info Entry date	Changed	Changed	Changed	Changed	Changed	Changed

How are the timestamps changing as a result of cut and paste?

One can see that a lot of timestamps are changing during the execution of this function. The new values after the command are pretty straightforward. In every situation the value of the timestamps which are changed is going to be the date and time of the move/paste.

There is only one scenario which contains a different timestamp change. In case we are moving a file inside the volume (the method and the OS doesn't matter) the new value of the FN Info Entry date is going to be the previous (pre move) value of the Std Info Entry date instead of the usual move time.

[Comparison]

SANS timestamp changes:

I compared it to the closest one. They are not exactly the same. The closest one from my test was the Ctrl-X Ctrl-V GUI-based method. SANS possibly used this method during its investigation (according to their whitepaper this was the used method: *https://www.sans.org/reading-room/whitepapers/forensics/filesystem-timestamps-tick-36842*).

	SANS		My test	
	In volume	Out-of-volume	In volume	Out-of-volume
Std Info Creation date	No change	No change	No change	No change
Std Info Modification date	No change	No change	No change	No change
Std Info Access date	No change	Changed	No change	Changed
Std Info Entry date	Changed	Changed	Changed	Changed
FN Info Creation date	No change	Changed	No change	Changed
FN Info Modification date	Changed	Changed	No change	Changed
FN Info Access date	No change	Changed	No change	Changed
FN Info Entry date	Changed	Changed	Changed	Changed

CyberForensicator timestamp changes:

Again, I compared it to my closest one. In this case it was command line-based move command. One can notice that I could find a perfect fit for the out-of-volume copies but not for the in-volume ones.

	Cyber Forensicator		**My test**	
	In volume	Out-of-volume	In volume	Out-of-volume
Std Info Creation date	No change	Changed	No change	Changed
Std Info Modification date	No change	No change	No change	No change
Std Info Access date	No change	Changed	No change	Changed
Std Info Entry date	Changed	No change	Changed	No change
FN Info Creation date	No change	Changed	No change	Changed
FN Info Modification date	No change	Changed	No change	Changed
FN Info Access date	No change	Changed	No change	Changed
FN Info Entry date	No change	Changed	Changed	Changed

According to my results the main numbering are not the only ones that counts in Windows, in case of investigation. Different versions and updates are important as well. My investigation is newer than the linked ones and the different timestamp changes might be the results of a newer function, a fresher version of Windows (this is just an assumption since I got the same results for an older Win7 Home as well).

For better visibility, this time I left out the detailed dates and times and only put the results and facts into the report.