Timestamp changes in case of copy command (Win7, Win10)

Investigating timestamp differences between Windows 7 and Windows 10.
I intended to figure out how MACB timestamps of the original and the newly created files are changing during a file copy in Windows. I also checked the differences between the results of the GUI based copy and paste method and the command line based copy command. I compared the changes in case of an in-volume copy and in case of copying to a different volume as well.

Tools:

These are the tools that were used during my investigation.

- Microsoft Windows 10 64-bit v10.0.17134.345
- Microsoft Windows 7 Enterprise SP1
- 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)

MACB

An NTFS volume stores 8 different timestamps for a single file. These timestamps are the followings:

- Modified
- Accessed
- Changed (Info Entry date change)
- Birth (file creation time)

All of these 4 information snippets are stored in the **$STANDARD_INFO** and in the **$FILE_NAME** as well.

The difference between the two attributes:

- **$STANDARD_INFO**: can be modified by user level processes. Therefore it can be altered by anti-forensics utilities.
- **$FILE_NAME:** can only be modified by the system kernel. No known anti-forensics tools can modify it.

Method of investigation

1) I generated two files in an NTFS volume.
2) Copied one of the files with copy paste and the other one with copy command from command line into a different directory.
3) Generated two files in an NTFS volume to test out-of-volume copy.
4) Copied one of the files with copy paste and the other one with copy command from command line into a different volume.

After every step I generated an image of the affected volumes which resulted in 5 different images for both OSs.
I collected the $MFT files from the images and parsed their content with analyzeMFT.py. Finally I compared the collected timestamps.

Here are the timestamps of my tests (blues are the changed values and greens are the unchanged ones.):

1: Windows 7 test, In-Volume copy, STD timestamps:

State	Description	Std Info Creation date	Std Info Modification date	Std Info Access date	Std Info Entry date
Before copy	File generated for co	2018-11-03 00:22:08.914103	2018-11-03 00:22:58.132191	2018-11-03 00:22:58.132191	2018-11-03 00:23:07.601408
Before copy	File generated for copy	2018-11-03 00:22:08.914103	2018-11-03 00:22:08.914103	2018-11-03 00:22:08.914103	2018-11-03 00:22:52.765781
After copy	File generated for co	2018-11-03 00:22:08.914103	2018-11-03 00:22:58.132191	2018-11-03 00:22:58.132191	2018-11-03 00:23:07.601408
After copy	File generated for copy	2018-11-03 00:22:08.914103	2018-11-03 00:22:08.914103	2018-11-03 00:22:08.914103	2018-11-03 00:22:52.765781
Copied file	File generated for co	2018-11-03 00:28:42.936798	2018-11-03 00:22:58.132191	2018-11-03 00:28:42.936798	2018-11-03 00:23:07.601408
Copied file	File generated for copy	2018-11-03 00:27:24.938261	2018-11-03 00:22:08.914103	2018-11-03 00:27:24.938261	2018-11-03 00:27:24.938261

2: Windows 7 test, In-Volume copy, FN timestamps:

State	Description	FN Info Creation date	FN Info Modification date	FN Info Access date	FN Info Entry date
Before copy	Copy command	2018-11-03 00:22:08.914103	2018-11-03 00:22:58.132191	2018-11-03 00:22:58.132191	2018-11-03 00:22:58.132191
Before copy	GUI Copy and paste	2018-11-03 00:22:08.914103	2018-11-03 00:22:08.914103	2018-11-03 00:22:08.914103	2018-11-03 00:22:08.914103
After copy	Copy command	2018-11-03 00:22:08.914103	2018-11-03 00:22:58.132191	2018-11-03 00:22:58.132191	2018-11-03 00:22:58.132191
After copy	GUI Copy and paste	2018-11-03 00:22:08.914103	2018-11-03 00:22:08.914103	2018-11-03 00:22:08.914103	2018-11-03 00:22:08.914103
Copied file	Copy command	2018-11-03 00:28:42.936798	2018-11-03 00:28:42.936798	2018-11-03 00:28:42.936798	2018-11-03 00:28:42.936798
Copied file	GUI Copy and paste	2018-11-03 00:27:24.938261	2018-11-03 00:27:24.938261	2018-11-03 00:27:24.938261	2018-11-03 00:27:24.938261

3: Windows 7 test, Out-of-Volume copy, STD timestamps:

State	Description	Std Info Creation date	Std Info Modification date	Std Info Access date	Std Info Entry date
Before copy	Copy command	2018-11-03 00:33:45.764530	2018-11-03 00:33:45.764530	2018-11-03 00:33:45.764530	2018-11-03 00:33:52.238543
Before copy	GUI Copy and paste	2018-11-03 00:33:45.764530	2018-11-03 00:33:56.856152	2018-11-03 00:33:56.856152	2018-11-03 00:34:02.487761
After copy	Copy command	2018-11-03 00:33:45.764530	2018-11-03 00:33:45.764530	2018-11-03 00:33:45.764530	2018-11-03 00:33:52.238543
After copy	GUI Copy and paste	2018-11-03 00:33:45.764530	2018-11-03 00:33:56.856152	2018-11-03 00:33:56.856152	2018-11-03 00:34:02.487761
Copied file	Copy command	2018-11-03 00:39:41.559956	2018-11-03 00:33:45.764530	2018-11-03 00:39:41.559956	2018-11-03 00:33:52.238543
Copied file	GUI Copy and paste	2018-11-03 00:39:09.299101	2018-11-03 00:33:56.856152	2018-11-03 00:39:09.299101	2018-11-03 00:39:09.299101

4: Windows 7 test, Out-of-Volume copy, FN timestamps

State	Description	FN Info Creation date	FN Info Modification date	FN Info Access date	FN Info Entry date
Before copy	Copy command	2018-11-03 00:33:45.764530	2018-11-03 00:33:45.764530	2018-11-03 00:33:45.764530	2018-11-03 00:33:45.764530
Before copy	GUI Copy and paste	2018-11-03 00:33:45.764530	2018-11-03 00:33:56.856152	2018-11-03 00:33:56.856152	2018-11-03 00:33:56.856152
After copy	Copy command	2018-11-03 00:33:45.764530	2018-11-03 00:33:45.764530	2018-11-03 00:33:45.764530	2018-11-03 00:33:45.764530
After copy	GUI Copy and paste	2018-11-03 00:33:45.764530	2018-11-03 00:33:56.856152	2018-11-03 00:33:56.856152	2018-11-03 00:33:56.856152
Copied file	Copy command	2018-11-03 00:39:41.559956	2018-11-03 00:39:41.559956	2018-11-03 00:39:41.559956	2018-11-03 00:39:41.559956
Copied file	GUI Copy and paste	2018-11-03 00:39:09.299101	2018-11-03 00:39:09.299101	2018-11-03 00:39:09.299101	2018-11-03 00:39:09.299101

5: Windows 10 test, In-Volume copy, STD timestamps

State	Description	Std Info Creation date	Std Info Modification date	Std Info Access date	Std Info Entry date
Before copy	Copy command	2018-11-01 23:01:28.656260	2018-11-01 23:01:28.656260	2018-11-01 23:01:28.656260	2018-11-01 23:01:45.710007
Before copy	GUI Copy and paste	2018-11-01 23:01:50.649584	2018-11-01 23:01:50.649584	2018-11-01 23:01:50.649584	2018-11-01 23:02:00.784618
After copy	Copy command	2018-11-01 23:01:28.656260	2018-11-01 23:01:28.656260	2018-11-01 23:01:28.656260	2018-11-01 23:01:45.710007
After copy	GUI Copy and paste	2018-11-01 23:01:50.649584	2018-11-01 23:01:50.649584	2018-11-01 23:01:50.649584	2018-11-01 23:02:00.784618
Copied file	Copy command	2018-11-01 23:07:46.833050	2018-11-01 23:01:28.656260	2018-11-01 23:07:46.833050	2018-11-01 23:01:45.710007
Copied file	GUI Copy and paste	2018-11-01 23:05:45.170511	2018-11-01 23:01:50.649584	2018-11-01 23:05:45.170511	2018-11-01 23:02:00.784618

6: Windows 10 test, In-Volume copy, FN timestamps

State	Description	FN Info Creation date	FN Info Modification date	FN Info Access date	FN Info Entry date
Before copy	Copy command	2018-11-01 23:01:28.656260	2018-11-01 23:01:28.656260	2018-11-01 23:01:28.656260	2018-11-01 23:01:28.656260
Before copy	GUI Copy and paste	2018-11-01 23:01:50.649584	2018-11-01 23:01:50.649584	2018-11-01 23:01:50.649584	2018-11-01 23:01:50.649584
After copy	Copy command	2018-11-01 23:01:28.656260	2018-11-01 23:01:28.656260	2018-11-01 23:01:28.656260	2018-11-01 23:01:28.656260
After copy	GUI Copy and paste	2018-11-01 23:01:50.649584	2018-11-01 23:01:50.649584	2018-11-01 23:01:50.649584	2018-11-01 23:01:50.649584
Copied file	Copy command	2018-11-01 23:07:46.833050	2018-11-01 23:07:46.833050	2018-11-01 23:07:46.833050	2018-11-01 23:07:46.833050
Copied file	GUI Copy and paste	2018-11-01 23:05:45.170511	2018-11-01 23:05:45.170511	2018-11-01 23:05:45.170511	2018-11-01 23:05:45.170511

7: Windows 10 test, Out-of-Volume copy, STD timestamps:

State	Description	Std Info Creation date	Std Info Modification date	Std Info Access date	Std Info Entry date
Before copy	Copy command	2018-11-01 23:11:05.227076	2018-11-01 23:11:05.227076	2018-11-01 23:11:05.227076	2018-11-01 23:11:14.314711
Before copy	GUI Copy and paste	2018-11-01 23:11:17.669939	2018-11-01 23:11:17.669939	2018-11-01 23:11:17.669939	2018-11-01 23:11:26.199282
After copy	Copy command	2018-11-01 23:11:05.227076	2018-11-01 23:11:05.227076	2018-11-01 23:11:05.227076	2018-11-01 23:11:14.314711
After copy	GUI Copy and paste	2018-11-01 23:11:17.669939	2018-11-01 23:11:17.669939	2018-11-01 23:11:17.669939	2018-11-01 23:11:26.199282
Copied file	Copy command	2018-11-01 23:14:12.647560	2018-11-01 23:11:05.227076	2018-11-01 23:14:12.647560	2018-11-01 23:11:14.314711
Copied file	GUI Copy and paste	2018-11-01 23:13:41.369963	2018-11-01 23:11:17.669939	2018-11-01 23:13:41.369963	2018-11-01 23:11:26.199282

8: Windows 10 test, Out-of-Volume copy, FN timestamps

State	Description	FN Info Creation date	FN Info Modification date	FN Info Access date	FN Info Entry date
Before copy	Copy command	2018-11-01 23:11:05.227076	2018-11-01 23:11:05.227076	2018-11-01 23:11:05.227076	2018-11-01 23:11:05.227076
Before copy	GUI Copy and paste	2018-11-01 23:11:17.669939	2018-11-01 23:11:17.669939	2018-11-01 23:11:17.669939	2018-11-01 23:11:17.669939
After copy	Copy command	2018-11-01 23:11:05.227076	2018-11-01 23:11:05.227076	2018-11-01 23:11:05.227076	2018-11-01 23:11:05.227076
After copy	GUI Copy and paste	2018-11-01 23:11:17.669939	2018-11-01 23:11:17.669939	2018-11-01 23:11:17.669939	2018-11-01 23:11:17.669939
Copied file	Copy command	2018-11-01 23:13:41.369963	2018-11-01 23:13:41.369963	2018-11-01 23:13:41.369963	2018-11-01 23:13:41.369963
Copied file	GUI Copy and paste	2018-11-01 23:14:12.647560	2018-11-01 23:14:12.647560	2018-11-01 23:14:12.647560	2018-11-01 23:14:12.647560

Results

The following conclusion can be drawn based on the investigation:
There is no difference in timestamp changes based on the target of the copy function. Copying a file onto the same volume or onto a different volume did not show any differences.

The only difference we are able to see is that the usage of copy command modifies one additional timestamp in case of Windows 7. This one additional timestamp is the Entry date timestamp of $STANDARD_INFO.

Table for timestamp changes during the copy. It only contains differences between the original file and the newely generated copy of that file.

	In-volume copy				**Out-of-volume Copy**			
	Copy command		**GUI copy and paste**		**Copy command**		**GUI copy and paste**	
	Win7	Win10	Win7	Win10	Win7	Win10	Win7	Win10
Std Info Creation date	Changed	Changed	Changed	Changed	Changed	Changed	Changed	Changed
Std Info Modification date	No change	No change	No change	No change	No change	No change	No change	No change
Std Info Access date	Changed	Changed	Changed	Changed	Changed	Changed	Changed	Changed
Std Info Entry date	No change	No change	Changed	No change	No change	No change	Changed	No change
FN Info Creation date	Changed	Changed	Changed	Changed	Changed	Changed	Changed	Changed
FN Info Modification date	Changed	Changed	Changed	Changed	Changed	Changed	Changed	Changed
FN Info Access date	Changed	Changed	Changed	Changed	Changed	Changed	Changed	Changed
FN Info Entry date	Changed	Changed	Changed	Changed	Changed	Changed	Changed	Changed