

Windows time rules aren't same for some file extensions

2023-08-31

Jihun Son, Jisoo Kim



고려대학교 정보보호대학원
Korea University
School of Cybersecurity



DFRC Korea University
Digital Forensic Research Center

Windows time rules aren't same for some file extensions

Summary

- **Windows time rules look inconsistent depending on file extensions**
 - '.docx', '.pptx' files look like they **DOES NOT** follow the existing time rules
 - M, A, C time in \$FILE_NAME are changed when file content is modified
 - But '.txt' files look like they **DOES** follow the rules
- **The root cause is how the executables(MS Office Programs) work**
 - MS Office programs do not edit the file content, they create new MFT entry
 - Similar example can be found when we use 'vim' editor in Unix/Linux
 - Therefore, Executable programs should be considered when we investigate file timestamps

Windows time rules aren't same for some file extensions

Windows time rules

- There are some common rules for timestamps in \$STANDARD_INFORMATION(\$SI) and \$FILE_NAME(\$FN)
- SANS poster and some blogs document these rules

Windows® Time Rules¹								
\$Standard_Information Win10 v1903								
File Creation	File Access	File Modification	File Rename	File Copy (new file)	Local File Move	Volume File Move (move via CLI)	Volume File Move (cut/paste via Explorer)	File Deletion (shift+delete)
Modified – Time of File Creation	Modified – No Change	Modified – Time of Data Modification	Modified – No Change	Modified – Inherited from Original	Modified – No Change	Modified – Inherited from Original	Modified – Inherited from Original	Modified – No Change
Access – Time of File Creation	Access – Time of Access (No Change if System Volume > 2GB GDI)	Access – Time of Data Modification	Access – No Change	Access – Time of File Copy	Access – No Change	Access – Time of File Move via CLI	Access – Time of Cut/Paste	Access – No Change
Metadata – Time of File Creation	Metadata – No Change	Metadata – Time of Data Modification	Metadata – Time of File Rename	Metadata – Time of File Copy	Metadata – Time of Local File Move	Metadata – Inherited from Original	Metadata – Inherited from Original	Metadata – No Change
Creation – Time of File Creation	Creation – No Change	Creation – No Change	Creation – No Change	Creation – Time of File Copy	Creation – Time of File Move via CLI	Creation – Time of File Move via CLI	Creation – Inherited from Original	Creation – No Change
\$Standard_Information Win11 v22H2								
File Creation	File Access	File Modification	File Rename	File Copy (new file)	Local File Move	Volume File Move (move via CLI)	Volume File Move (cut/paste via Explorer)	File Deletion (shift+delete)
Modified – Time of File Creation	Modified – No Change	Modified – Time of Data Modification	Modified – No Change	Modified – Inherited from Original	Modified – No Change	Modified – Inherited from Original	Modified – Inherited from Original	Modified – No Change
Access – Time of File Creation	Access – Time of Access	Access – Time of Data Modification²	Access – Time of Rename³	Access – Time of File Copy	Access – Time of Local File Move	Access – Time of File Move via CLI	Access – Time of Cut/Paste	Access – No Change
Metadata – Time of File Creation	Metadata – No Change	Metadata – Time of Data Modification	Metadata – Time of File Rename	Metadata – Inherited from Original	Metadata – Time of Local File Move	Metadata – Time of File Move via CLI	Metadata – Time of Cut/Paste	Metadata – No Change
Creation – Time of File Creation	Creation – No Change	Creation – No Change	Creation – No Change	Creation – Time of File Copy	Creation – Time of File Move via CLI	Creation – Time of File Move via CLI	Creation – Inherited from Original	Creation – No Change

	\$FILENAME															
	File Creation	File Access	File Modification	File Rename	File Copy (copy-paste)		File Copy (copy-paste) to new folder		Local File Move (cut-paste)	Volume File Move (CLI)	Volume File Move (cut-paste)		File Recycled	File Deletion (shift delete)	Create ADS	Modify ADS
					Original file	New copy	Original file	New copy	New file	New file	Original file record	New file				
Last modified time	Time of File Creation	No Change	No Change	Win 10: No change Win 11: Previous \$STD_INF O Last modified time	No Change	Time of File Copy	No Change	Time of File Copy	Win 10: No change Win 11: Previous \$STD_INF O Last modified time	Time of file move	No Change	Time of file move	Win 10: No change Win 11: Previous \$STD_INF O Last modified time	No Change	No Change	No Change
Last access time	Time of File Creation	No Change	No Change	Win 10: No change Win 11: Previous \$STD_INF O Last access time	No Change	Time of File Copy	No Change	Time of File Copy	Win 10: No change Win 11: Previous \$STD_INF O Last access time	Time of file move	No Change	Time of file move	Win 10: No change Win 11: Previous \$STD_INF O Last access time	No Change	No Change	No Change
Metadata a time	Time of File Creation	No Change	No Change	Win 10: No change Win 11: Previous \$STD_INF O Metadata time	No Change	Time of File Copy	No Change	Time of File Copy	Win 10: No change Win 11: Previous \$STD_INF O Metadata time	Time of file move	No Change	Time of file move	Win 10: No change Win 11: Previous \$STD_INF O Metadata time	No Change	No Change	No Change
Creation time	Time of File Creation	No Change	No Change	No Change	No Change	Time of File Copy	No Change	Time of File Copy	No Change	Time of file move	No Change	Time of file move	No Change	No Change	No Change	No Change

Windows time rules aren't same for some file extensions

Existing time rules for Windows 11

- **MACB Timestamps in Windows**
 - M(Modify, Last Modified Time), A(Access, Last Access Time)
C(Change, \$MFT Modified), B(Birth, Created Time)

Scenario	\$STANDARD_INFORMATION				\$FILE_NAME			
	M	A	C	B	M	A	C	B
File Creation	Time of File Creation	Time of File Creation	Time of File Creation	Time of File Creation	Time of File Creation	Time of File Creation	Time of File Creation	Time of File Creation
File Modification	Time of File Modification	Time of File Modification	Time of File Modification	Unchanged	Unchanged	Unchanged	Unchanged	Unchanged
File Rename	Unchanged	Time of File Rename	Time of File Rename	Unchanged	Previous \$SI Mtime	Previous \$SI Atime	Previous \$SI Ctime	Unchanged

*M(Modify) / A(Access) / C(Change) / B(Birth)

\$FN isn't changed by file modication! ←

Windows time rules aren't same for some file extensions

Experiment summary

■ Setup

- Windows 11 Pro (Version: 23H2, OS build: 22631.2129)
- NTFS formatted .vhd 1GB

■ Action

- Execute 1) file creation, 2) file modification, 3) file rename to '.txt', '.docx', '.pptx' files
- Track timestamp changes in \$STANDARD_INFO and \$FILE_NAME

■ Result

- '.txt' file **DOES** follow the existing time rules
- '.docx' and '.pptx' files **DOES NOT** follow the rules (\$FILE_NAME, File modification)

Windows time rules aren't same for some file extensions

Experiment

- File creation of '.docx'

	Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text	
	1545FC00	46	49	4C	45	30	00	03	00	B4	5F	50	00	00	00	00	00	FILE0...'_P.....	Birth
	1545FC10	01	00	01	00	38	00	01	00	50	01	00	00	00	04	00	008...P.....	Modify
	1545FC20	00	00	00	00	00	00	00	00	05	00	00	00	2B	00	00	00+...	Change
\$SI ←	1545FC30	02	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00`...	Access
	1545FC40	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00H.....	
	1545FC50	DC	01	7C	DC	EF	D6	D9	01	DC	01	7C	DC	EF	D6	D9	01	Ü. ÜïÖÙ.Ü. ÜïÖÙ.	
	1545FC60	BF	7C	09	DE	EF	D6	D9	01	DC	01	7C	DC	EF	D6	D9	01	¿ .PïÖÙ.Ü. ÜïÖÙ.	
	1545FC70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	1545FC80	00	00	00	00	08	01	00	00	00	00	00	00	00	00	00	00	
\$FN ←	1545FC90	00	00	00	00	00	00	00	00	30	00	00	00	70	00	00	000...p...	
	1545FCA0	00	00	00	00	00	00	03	00	54	00	00	00	18	00	01	00T.....	
	1545FCB0	05	00	00	00	00	00	05	00	DC	01	7C	DC	EF	D6	D9	01Ü. ÜïÖÙ.	
	1545FCC0	DC	01	7C	DC	EF	D6	D9	01	DC	01	7C	DC	EF	D6	D9	01	Ü. ÜïÖÙ.Ü. ÜïÖÙ.	
	1545FCD0	DC	01	7C	DC	EF	D6	D9	01	00	00	00	00	00	00	00	00	Ü. ÜïÖÙ.....	
	1545FCE0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	
	1545FCF0	09	00	44	00	46	00	52	00	43	00	2E	00	64	00	6F	00	..D.F.R.C...d.o.	
	1545FD00	63	00	78	00	00	00	00	00	40	00	00	00	28	00	00	00	c.x.....@...(...	

Windows time rules aren't same for some file extensions

Experiment

- File modification of '.docx'

	Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text	
	15460400	46	49	4C	45	30	00	03	00	CF	6B	50	00	00	00	00	00	FILE0...İkP....	Birth
	15460410	01	00	01	00	38	00	01	00	80	01	00	00	00	04	00	008...€.....	Modify
	15460420	00	00	00	00	00	00	00	00	06	00	00	00	2D	00	00	00-....	Change
\$SI ←	15460430	02	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00`....	Access
	15460440	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00H.....	
	15460450	DC	01	7C	DC	EF	D6	D9	01	C2	56	98	9D	F0	D6	D9	01	Ü. ÜİÖÜ. ÂV~.đÖÜ.	
	15460460	50	FE	9C	9D	F0	D6	D9	01	D9	EE	9A	9D	F0	D6	D9	01	Ppæ.đÖÜ. Ùİš.đÖÜ.	
	15460470	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	15460480	00	00	00	00	08	01	00	00	00	00	00	00	00	00	00	00	
\$FN ←	15460490	00	00	00	00	00	00	00	00	30	00	00	00	70	00	00	000...p...	
	154604A0	00	00	00	00	00	00	04	00	54	00	00	00	18	00	01	00T.....	
	154604B0	05	00	00	00	00	00	05	00	DC	01	7C	DC	EF	D6	D9	01Ü. ÜİÖÜ.	
	154604C0	C2	56	98	9D	F0	D6	D9	01	ED	A0	9A	9D	F0	D6	D9	01	ÂV~.đÖÜ. í š.đÖÜ.	
	154604D0	C2	56	98	9D	F0	D6	D9	01	00	30	00	00	00	00	00	00	ÂV~.đÖÜ..0.....	
	154604E0	F5	2F	00	00	00	00	00	00	20	00	00	00	00	00	00	00	õ/.....	
	154604F0	09	00	44	00	46	00	52	00	43	00	2E	00	64	00	6F	00	..D.F.R.C...d.o.	
	15460500	63	00	78	00	00	00	00	00	40	00	00	00	28	00	00	00	c.x.....@...(...	

Windows time rules aren't same for some file extensions

Experiment

- File rename of '.docx'

	Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text	
	15460400	46	49	4C	45	30	00	03	00	4D	73	50	00	00	00	00	00	FILE0...MsP....	Birth
	15460410	01	00	01	00	38	00	01	00	90	01	00	00	00	04	00	008.....	Modify
	15460420	00	00	00	00	00	00	00	00	07	00	00	00	2D	00	00	00-...	Change
\$SI ←	15460430	04	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00`...	Access
	15460440	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00H.....	
	15460450	DC	01	7C	DC	EF	D6	D9	01	C2	56	98	9D	F0	D6	D9	01	Ü. ÜïÖÙ. ÂV~. ðÖÙ.	
	15460460	DE	F1	F5	A1	F1	D6	D9	01	9F	05	6F	A2	F1	D6	D9	01	pñõ; ñÖÙ. Ÿ. ɔƒñÖÙ.	
	15460470	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	15460480	00	00	00	00	08	01	00	00	00	00	00	00	00	00	00	00	
\$FN ←	15460490	00	00	00	00	00	00	00	00	30	00	00	00	80	00	00	000...€...	
	154604A0	00	00	00	00	00	00	06	00	64	00	00	00	18	00	01	00d.....	
	154604B0	05	00	00	00	00	00	05	00	DC	01	7C	DC	EF	D6	D9	01Ü. ÜïÖÙ.	
	154604C0	C2	56	98	9D	F0	D6	D9	01	50	FE	9C	9D	F0	D6	D9	01	ÂV~. ðÖÙ. Ppæ. ðÖÙ.	
	154604D0	D9	EE	9A	9D	F0	D6	D9	01	00	30	00	00	00	00	00	00	Üïš. ðÖÙ. .0.....	
	154604E0	F5	2F	00	00	00	00	00	00	20	00	00	00	00	00	00	00	õ/.....	
	154604F0	11	00	44	00	46	00	52	00	43	00	5F	00	63	00	68	00	..D.F.R.C._.c.h.	
	15460500	61	00	6E	00	67	00	65	00	64	00	2E	00	64	00	6F	00	a.n.g.e.d...d.o.	

Windows time rules aren't same for some file extensions

Experiment result

- **Timestamp changes**
 - File Modification: M, A, C time of \$SI, \$FN changed
 - File Rename: A, C time of \$SI changed

Scenario	\$STANDARD_INFORMATION				\$FILE_NAME			
	M	A	C	B	M	A	C	B
File Creation (10:02:46)	10:02:46 .8782556	10:02:46 .8782556	10:02:49 .4831807	10:02:46 .8782556	10:02:46 .8782556	10:02:46 .8782556	10:02:46 .8782556	10:02:46 .8782556
File Modification (10:08:10)	10:08:10 .8641986	10:08:10 .8811993	10:08:10 .8947024	10:02:46 .8782556	10:08:10 .8641986	10:08:10 .8641986	10:08:10 .8792045	10:02:46 .8782556
File Rename (10:15:27)	10:08:10 .8641986	10:15:28 .4787615	10:15:27 .6852702	10:02:46 .8782556	10:08:10 .8641986	10:08:10 .8811993	10:08:10 .8947024	10:02:46 .8782556

*M(Modify) / A(Access) / C(Change) / B(Birth)

\$FN does not follow existing time rules! ←

Windows time rules aren't same for some file extensions

Experiment result

- We found that Windows time rules look inconsistent depending on file extensions
 - '.docx', '.pptx' files DOES NOT follow the existing time rules
 - M, A, C time are changed when file is modified
 - But '.txt' files follow the rules

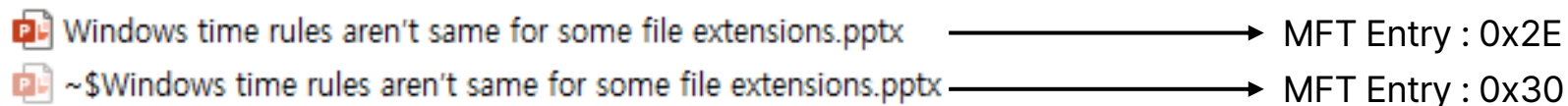
Scenario	\$STANDARD_INFORMATION				\$FILE_NAME			
	M	A	C	B	M	A	C	B
File Creation								
File Modification					Inconsitent point			
File Rename								

Windows time rules aren't same for some file extensions

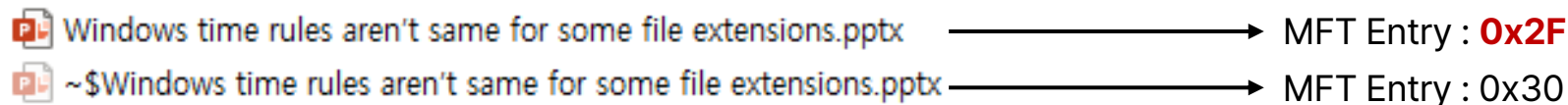
Finding the root cause

■ How the MS Office Programs work

- When we open the '.pptx' file

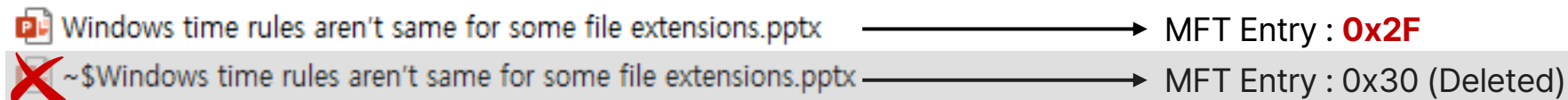


- When we save the '.pptx' file (even with no changes)



Create new file and
overwrite existing file

- When we close the '.pptx' file



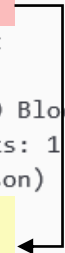
Windows time rules aren't same for some file extensions

Finding the root cause

- Windows time rules are look inconsistent depending on file extensions
 - But they are consistent, the real problem is how executable programs work
- Similar example can be found when we use 'vim' editor in Unix/Linux

```
hunjison@DESKTOP-5FB4L42:~$ stat hunjison.txt
File: hunjison.txt
Size: 15          Blocks: 0          IO Block: 4096   regular file
Device: 2h/2d    Inode: 4222124650738720 Links: 1
Access: (0644/-rw-r--r--)  Uid: ( 1000/hunjison)   Gid: ( 1000/hunjison)
Access: 2023-02-27 13:08:41.142442500 +0900
Modify: 2022-12-21 18:50:10.351397800 +0900
Change: 2023-01-02 13:26:26.787861700 +0900
Birth: -
```

```
hunjison@DESKTOP-5FB4L42:~$ vim hunjison.txt
hunjison@DESKTOP-5FB4L42:~$ stat hunjison.txt
File: hunjison.txt
Size: 16          Blocks: 0          IO Block: 4096   regular file
Device: 2h/2d    Inode: 5066549580837596 Links: 1
Access: (0644/-rw-r--r--)  Uid: ( 1000/hunjison)   Gid: ( 1000/hunjison)
Access: 2023-08-31 15:11:20.992668200 +0900
Modify: 2023-08-31 15:11:20.992668200 +0900
Change: 2023-08-31 15:11:20.993653400 +0900
Birth: -
```



- Therefore, Executable programs should be considered when we investigate file timestamps