(In progress)
MACB Time
https://ptylu.github.io/

Windows NTFS contains 4 times:
- **M**odification : Modification Time
- **A**ccess : Access Time
- MFT record **C**hange : Metadata change
- **B**irth : File Creation Time

Windows Explorer can only show **M**odification, **A**ccess and **B**irth

Operation	**M**odification	**A**ccess	**C**hange (Metadata)	**B**irth
File Creation	Date Updated	Date Updated		Date Updated
File Modification	Date Updated	Date Updated (NO if registry key modification)		NO
File Copy	NO (Inherite)	YES		Date Updated
File Access	NO	NO*		NO

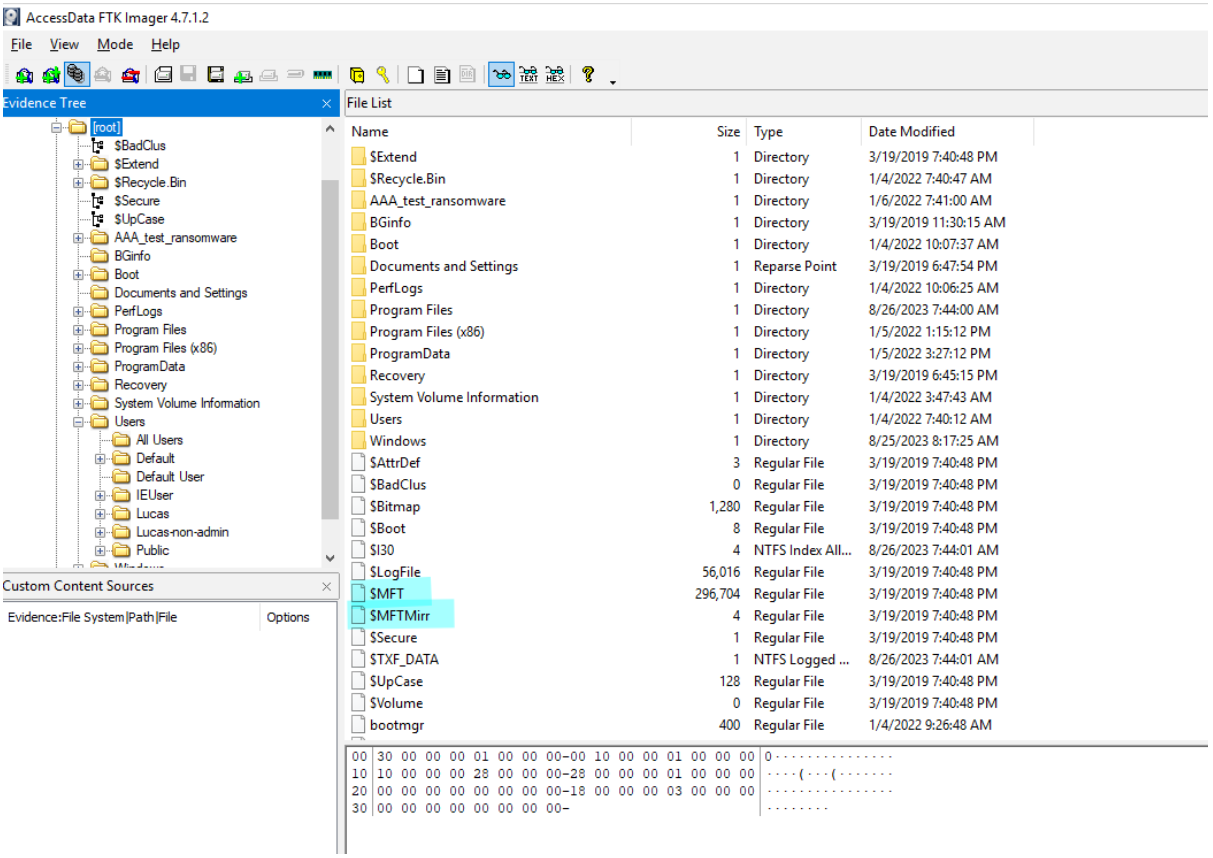
Hint 1 : If modification is before the Birth, means the file was copied.

Timestomp
(Get-Item "C:\Users\Lucas\Documents\test_timestomp.txt").CreationTime=("27 August 2023 17:00:00")

$MFT

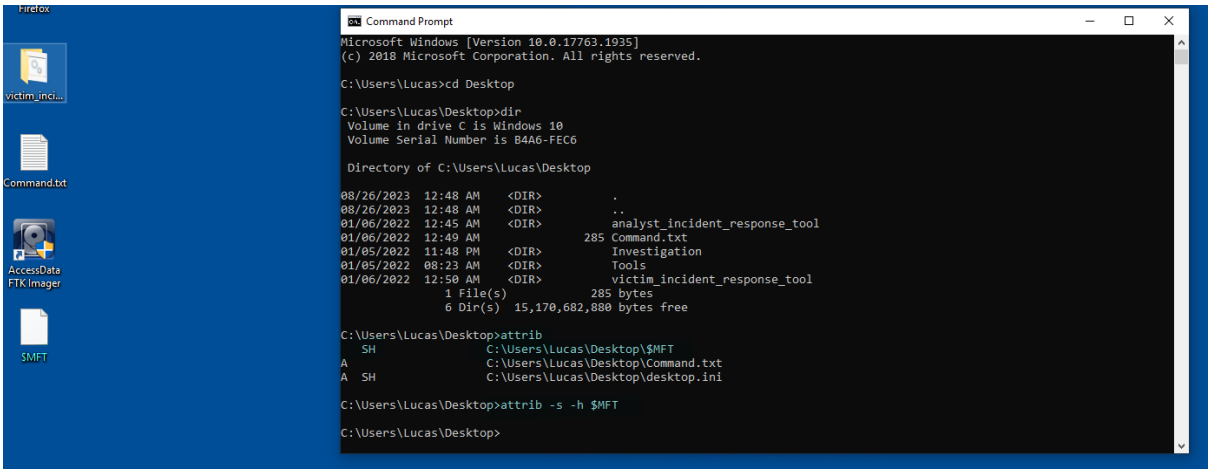
$MFT located in C:\$MFT
$MFTMirr is a backup of $MFT

1) Use of FTK Imager for the $MFT Dump



2) After $MFT Dump, need to launch the command (because hidden by default):

- attrib -s -h $MFT



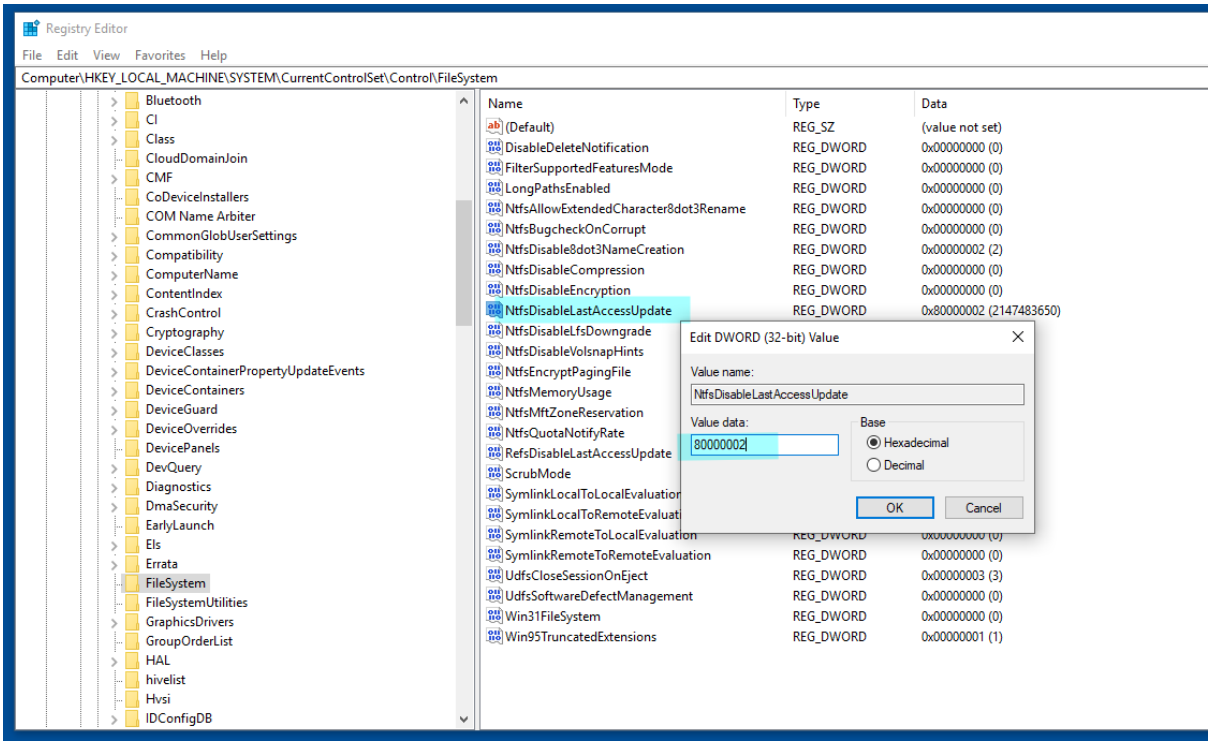
3) Use of Eric Zimmerman's tool MFTECmd.exe

- **MFTECmd.exe -f C:\Users\Lucas\Desktop\$MFT --csv "C:\Users\Lucas\Desktop\out_mft"**

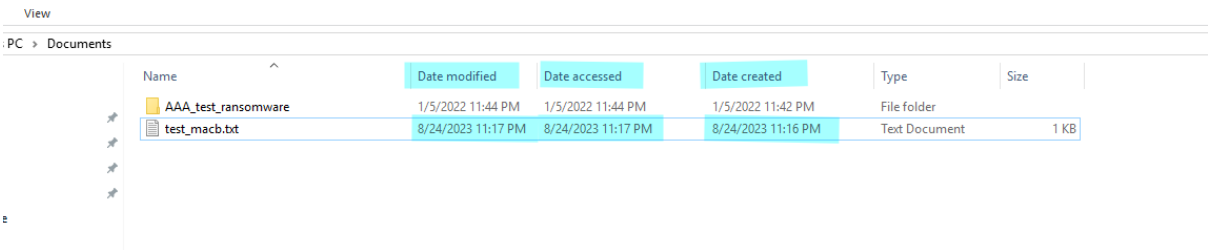
(1) Registry **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate** can be modified to ask the system to modify/not modify the Access time when file Modification. Below the parameters

- 0x80000000: User Managed, the “Last Access” updates are enabled,
- 0x80000001: User Managed, the “Last Access” updates are disabled,
- 0x80000002: System Managed, the “Last Access” updates are enabled,
- 0x80000003: System Managed, the “Last Access” updates are disabled.

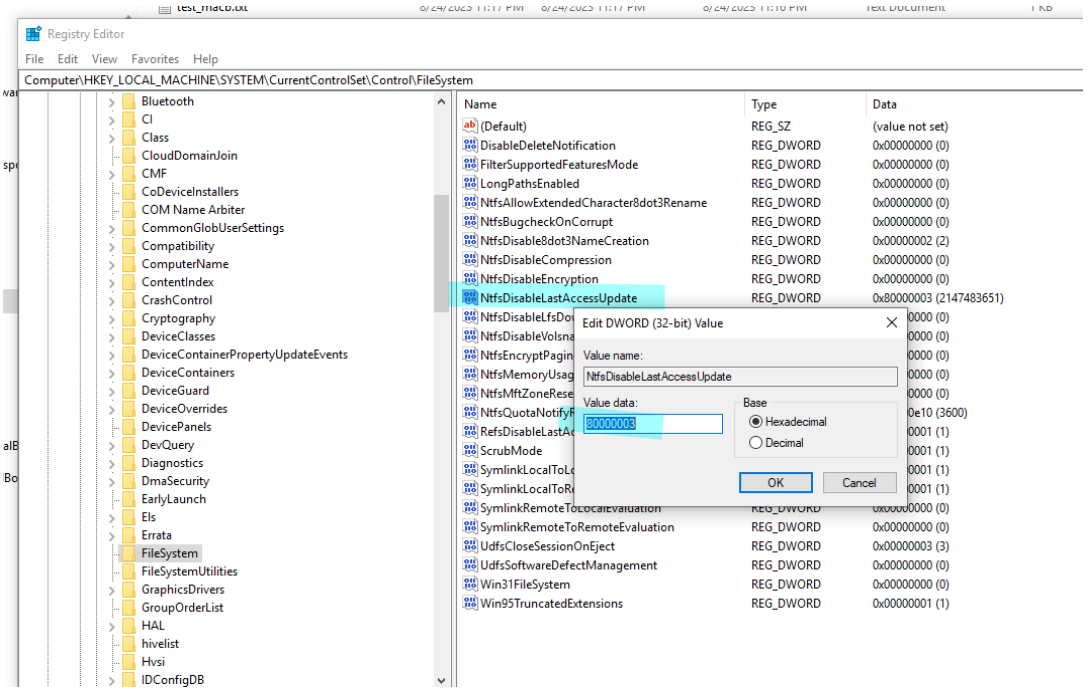
However, tested on Windows 10 and Windows 11, the modification of this Key doesn’t affect the property. The Access time is always updated !



Modification with 80000002 to enable the update



After file Modification, Date Modified and Date Accessed are the same

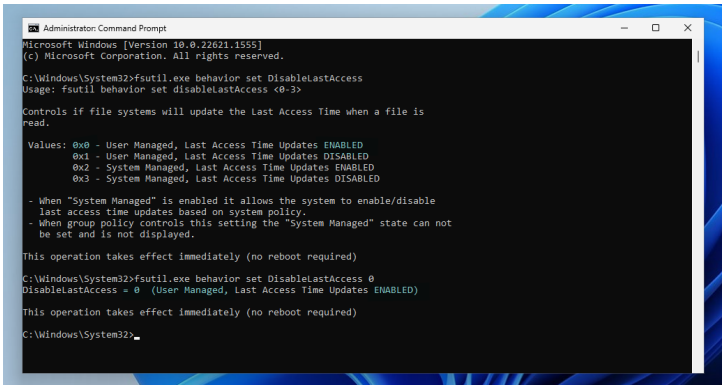


Modification with 80000002 to disable the update. Doesn't work

Tested on Windows 11, it's the same behavior. The registry key to disable the time update during file modification doesn't work

During my test, I discovered a tiny bug that was corrected on Windows 11. In windows 10, the value Enabled/Disabled were inverted

```
C:\Windows\system32>fsutil.exe behavior set DisableLastAccess
Usage: fsutil behavior set disableLastAccess <0-3>

 Values: 0x0 - User Managed, Last Access Updates Enabled
         0x1 - User Managed, Last Access Updates Disabled
         0x2 - System Managed, Last Access Updates Enabled
         0x3 - System Managed, Last Access Updates Disabled

 - When "System Managed" is enabled it allows the system to enable/disable
   last access time updates based on system policy.
 - If group policy is in effect or this registry key is uninitialized then
   the "System Managed" state can not be set and is not displayed.

C:\Windows\system32>fsutil.exe behavior set DisableLastAccess 0
DisableLastAccess = 0  (User Managed, Disabled)

C:\Windows\system32>fsutil.exe behavior set DisableLastAccess 1
DisableLastAccess = 1  (User Managed, Enabled)

C:\Windows\system32>fsutil.exe behavior set DisableLastAccess 2
DisableLastAccess = 2  (System Managed, Disabled)

C:\Windows\system32>fsutil.exe behavior set DisableLastAccess 3
DisableLastAccess = 3  (System Managed, Enabled)
```



REF
https://www.tenforums.com/tutorials/139015-enable-disable-ntfs-last-access-time-stamp-updates-windows-10-a.html