International Journal of Engineering & Technology, 7 (2.33) (2018) 133-138

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A study on the APFS timestamps in MACOS

Jong-Hwa Song [1] *, Se Ho Kim [1], Song Yi Hwang [1], Seung Gyu Kim [1], Sung-Jin Lee [1]

[1] Div. of information and communication Baekseok University, Munam-Ro 76 Dongnam-Gu Cheonan-Si Chungcheongnam-Do, 30165, South Korea
**Corresponding author E-mail: atp7979@gmail.com*

Abstract

Background/Objectives: There are not many time analysis studies on High Sierra, the latest macOS (10.13) that has changed the file system from HFS+ toAPFS (Apple File System).
Methods/Statistical analysis: In this experiment, we tried various actions of the file and the directory with using the Sierra version of the internal drive and the High Sierra version of the external drive. The 'mdls' command and the time attributes of the Finder are used for comparing the metadata.The 'log show' command is also used for checking the system time modification. For analyzing the .DS_Store and the db.sqlite files, we used .DS_Store Parser and DB Browser for SQLite.
Findings: First of all, we briefly review time synchronization and APFS. And then, we compare the time records of HFS+ with those of APFS with differences. The unified logging file (tracev3) file with using the 'log show' command is analyzed and it is confirmed that the relevant log is left when the system time is changed. Next, we performed various actions on the files and directories of Sierra and High Sierra, and compiled the results as the tables. As a result, we found that the accessed time values were not updated well at high Sierra for the performance purpose. Finally, we also found the file attribute values in the DS_Store file in the RecycleBin and the database files in Document Revisions by default, and found that they can be used in forensic analysis.
Improvements/Applications: Furthermore, it is necessary to examine and analyze the change of the time attribute of the file when the file and folder are moved or copied with APFS formatted external storage device.

Keywords: *APFS; Forensics; Timestamp; Log Archive; .DS Store; Document Revisions*

1. Introduction

Timestamp is forensically important information on the digital evidence analysis. Like MS Windows, the time of the macOS computer is managed by the RTC (Real Time Clock) on the CMOS chip in the Logic Board.
In this study, the time record of the APFS (the changed file system of macOS High Sierra) is examined. And the record was compared with the corresponding timestamp metadata and investigated the difference from the previous version through the changing action of the file and the folder. The logs of the unified logging system are also examined. Finally, the timestamps in the hidden filein the Recycle Bin and the database file of Document Revisions were analyzed by the forensic tools.

2. Materials and methods

The papers on the time changing of MS Windows systemhave been extensively researched[1] and well-organized[2], but the time attribute especially in the case of macOS High Sierra distributed in September 2017, there is no forensic tool that can be analyzed yet, and there are not many papers related to it.
In this experiment, we tried various actions on the computer about files and folders using the Sierra version of the internal drive and the High Sierra version formatted as the APFS volume on the external drive. The result is displayed in the terminal window with the 'mdls' command and the time attribute values of the Finder window are used to compare the metadata information.
For analyzing the .DS_Store file in the Recycle Bin and db.sqlite database file in Document Revisions, we used .DS_Store Parser and DB Browser for SQLite.
The computer information used in the experiment is as follows.
MacBook Pro (13-inch, 2017, Four Thunderbolt 3 Ports),
Processor: 3.1GHz Intel Core i5
Memory: 16GB 2133 MHz LPDDR3
Graphic Card: Intel Iris Plus Graphics 650 1536 MB
Internal Drive: 512GB SSD, macOS (Sierra 10.12.6)
External Drice: 64GB SSD, macOS (High Sierra 10.13.1)

2.1. Macos time synchronization

Like MS Windows, macOS also uses a time server to receive the time when the Internet is connected and to synchronize the system's time. Three time servers (Apple Americas/U.S., Apple Asia, Apple Europe) are managed directly by Apple.
When installing the operating system, the macOS connect to the Internet, select the time zone to synchronize the time, and then use that time until the system is shut down. When the system is shut down, the RTC of the logic board calculates the system time, and the time information of the computer is maintained unless the battery completely discharged. If the battery has reached the end of its life, system time is reset to 2001.01.01(15:44).

2.2. Macos high sierra

The biggest change in the Mac OS High Sierra version is that the file system has changed from HFS + to APFS. In addition, there are changes to the introduction of Metal 2 (hardware accelerated

computing API), HEVC video support, VR support enhancement, and basic applications.High Sierra's market share of macOS is around 5.44%, which is expected to rise in the future.[3]

2.3. APFS time record

The Table 1 shows HFS + and APFS file records. In the HFS + file system, it measured the time in seconds starting from 1940-01-01, and only 'DateAdded' entry used the unsigned 32bits UNIX epoch time starting from 1970-01-01. Time records are found in the catalog file (folder).
In the APFS file system, all timestamps are changed from 32 bits to 64 bits and stored as unsigned values. The APFS timestamp value record is measured in nanoseconds starting from 1970-01-01. All timestamps are given a value of UTC +00:00, and time records are found in the BTLN (B-Tree Leaf Node) file.4
In the HFS + catalog file (folder), the important items in the record are Create Date, Content Modification Date, Attribute Modification Date, and Access Date. The function of each item is as follows. [5] The Create Date is the date and time the file (folder) was created. The Content Modification Date is the date and time the file (folder)'s contents were last changed. The Attribute Modification Date is the last date and time that any field in the file (folder)'s catalog record was changed. The Access Date is the date and time the file (folder)'s contents were last read.
These items are matched with the APFS BTLN file record's Date Created, Date last Written, Date iNode mod, and Date accessed values, respectively.

2.4. APFS time metadata

For the result of the Figure 1 below, 'abc.txt' file and 'a' folder were created at first.(touch abc.txt, mkdir a) Afterwards modifying and saving the contents of abc.txtand moving abc.txt to a folder. (Move abc .txt a) Output is the metadata of the 'abc.txt' through the 'mdls' command in terminal.

Table 1: HFS+ Catalog File (Folder) Record Vs APFS BTLN File Record

SInt16	Record Type	UInt16	Unknown
UInt16	Flags	UInt64	Parent ID
UInt32	Valence	UInt64	Node-ID
UInt32	File(Folder)ID (CNID)	UInt64	Date Created
UInt32	Create Date	UInt64	Date last Written
UInt32	ContentModification Date	UInt64	Date iNode mod.
UInt32	AttributeModification Date	UInt64	Date accessed
UInt32	Access Date	UInt64	Hardlinks to file
UInt32	Backup Date	UInt64	Unknown
HFSPlusBSDInfo[16 Bytes] Permissions		UInt32	Unknown
File(Folder)Info[16 Bytes] UserInfo		UInt32	Unknown
ExtendedFile(Folder)Info[16Bytes] FinderInfo		UInt64	Unknown
UInt32	TextEncoding	UInt32	Owner ID
UInt32	Reserved	UInt32	Group ID
		UInt64	Flags

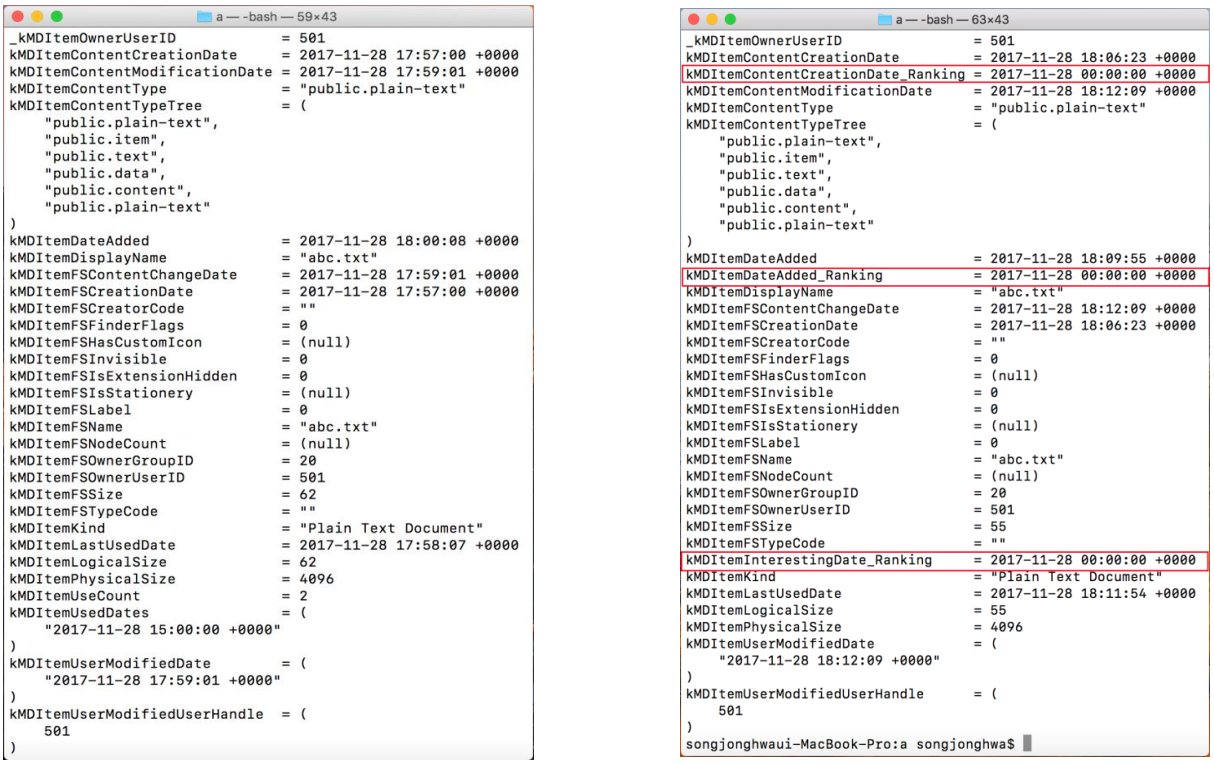


Fig. 1: File Metadata in Terminal (Sierra [10.12.6] vs High Sierra [10.13.1]).

The time attribute's contents in the metadata can be summarized as shown in the following Table 2.[6]
For the 'kMDItemDateAdded'attribute, the contentsare made by the reference[7]. Three attributes with the array structure are the Apple's unique feature that stores their time values each time you access, modify, or create them.[8]Unlike Apple's own program, these array timestamps are not stored well for the files such as Word, PDF and so on.
The four attribute values with the name of the ranking are not yet known.

Table 2: Metadata Attribute Keys

KMD Item Content Creation Date	The date that the contents of the file were created. A CF Date
Kmd Item Content Modification Date	The date and time that the contents of the file were last modified. A CF Date
kMD Item Date Added	An HFS+ metadata attribute that happens to be indexed by Spotlight (undocumented)
kMD Item FS Content Change Date	The date the file contents last changed. A CF Date
kMD Item FS Creation Date	The date and time that the file was created. A CFDate
kMD Item Last Used Date	The date and time that the file was last used. Launch Services update this value automatically every time a file is opened by double clicking, or by asking Launch Services to open a file. A CF Date.
kMD Item Used Dates	Undocumented (array)
kMD Item User Modified Date	Undocumented (array)
kMD Item User Created Date	Undocumented (array)
kMD Item Content Creation Date_ Ranking	Undocumented
kMD Item Date Added_ Ranking	Undocumented
kMD Item Interesting Date_ Ranking	Undocumented
kMD Item Last Used Date_ Ranking	Undocumented

3. Results and discussion

3.1. Logging system (tracev3) analysis

Tracev3 is a new system log file from macOS sierra. It hasthe binary format, and isreferred to as log orlog archive. The Apple developer documentation states that it will replace the existing ASL (Apple System Log).9 to collect the logs, you need to save them as an unified archive type using the ‘collect’ option of log, which is macOS's internal program. The collected archive files can be analyzed using the ‘log show’ command. If you look at the Figure 2 above, you can see that the date attribute value is changed from 2017.11.29(15:42:33) to 2017.11.19 (13:42:11) (about 10 days and 2 hours) ahead. The Date & Time item in the System Preferences changes the system time. If the date attribute is suddenly changed in a log file that is written in order, it can be seen that the system time is modified.[10] Of course, this also can bechecked by the ‘Timesync’ or 'systemwallclock time adjusted' statement in the log.

3.2. File and directory metadata analysis

The following Tables [Table 3] [Table 4] examine possible actions on files and directories in macOS Sierra.You can see that the results from the left hand side and the right side are different depending on the behavior. If the time attribute value is changed, 'C' is displayed. Otherwise, '-' value is displayed. In the symbolic link file, 'X' is displayed because no additional date exists. (C: Changed, -: Not Changed X: Not Existed)

The tables below [Table 5] [Table 6] compare the results after doing the same in macOS High Sierra. Comparing the behavior with that in Sierra, someattribute values are changed, and most accessed values are not recorded except for click actions. This seems to be intended to improve performance by limiting the number of times SSD drives are write, and seems to be similar to the previouscase of subtracting the additional day attribute value-when it changed from MS Windows XP to MS Windows 7.
(C: Changed, -: Not Changed X: Not Existed)

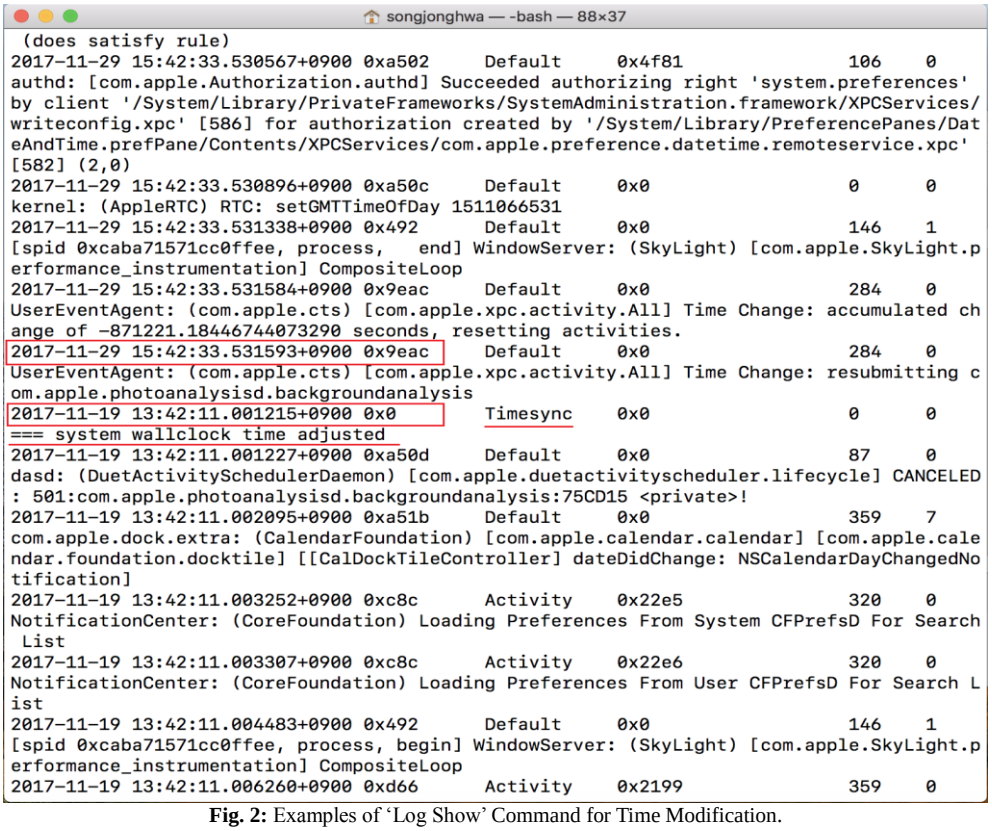


Fig. 2: Examples of ‘Log Show’ Command for Time Modification.

Table 3: File Metadata Analysis in Macos Sierra (10.12)

SHELL(terminal)					GUI(finder)				
Contents	Accessed	Modified	Changed	Created	Contents	Accessed	Modified	Changed	Created
Creation(touch)	C	C	C	C	Modification(app.)	C	C	C	-
Modification(vi)	C	C	C	C	Read(double click)	C	-	-	-
Read(cat)	-	-	-	-	Copy(cp)-original	-	-	-	-
Copy(cp)-original	-	-	-	-	Copy(cp)-duplicate	C	-	C	-
Copy(cp)-duplicate	C	C	C	C	Copy(Cmd+C,V)-original	-	-	-	-
Move(mv)	-	-	C	-	Copy(Cmd+C,V)-duplicate	C	-	C	-
Symbolic link(ln-s)-original	-	-	-	-	Get Info	-	-	-	-
Symbolic link(ln-s)-link file	C	C	X	C	Make Alias-original	-	-	-	-
Symbolic link(click)-original	C	-	-	-	Make Alias-duplicate	C	C	C	C
Symbolic link(click)-link file	-	-	X	-	Quick Look	-	-	-	-
Hard link(ln)-original	-	-	-	-	Move	-	-	C	-
Hard link(ln)-link file	-	-	-	-	Rename	-	-	-	-
Hard link(click)-original-	C	-	-	-					
Hard link(click)-link file	C	-	-	-					

Table 4: Directory Metadata Analysis in Macos Sierra (10.12)

SHELL(terminal)					GUI(finder)				
Contents	Accessed	Modified	Changed	Created	Contents	Accessed	Modified	Changed	Created
Creation(mkdir)	C	C	C	C	Creation(right click)	C	C	C	C
Change directory(cd)	-	-	-	-	Open(double click)	C	-	-	-
Linux shell(ls)	-	-	-	-	Move file to directory (Drag&Drop)	-	C	-	-
Move file to directory(mv)	-	C	-	-	File duplicate in directory (Duplicate)	-	C	-	-
File Creation in directory(touch)	-	C	-	-	Duplication-original	-	-	-	-
Copy(cp -r)-original	-	-	-	-	Duplication-duplicate	C	-	C	-
Copy(cp -r)-duplicate	C	C	C	C	Copy(copy&paste)-original	-	-	-	-
Move(mv a/ b/)-a directory	-	-	C	-	Copy(copy&paste)-duplicate	C	-	C	-
Move(mv a/ b/)-b directory	-	C	-	-	Copy(cmd+C,V)-original	-	-	-	-
Symbolic link-original	-	-	-	-	Copy(cmd+C,V)-duplicate	C	-	C	-
Symbolic link-link directory	C	C	X	C	Move(Drag&Drop a/->b/)-a/	-	-	C	-
Symbolic link(click)-original	C	-	-	-	Move(Drag&Drop a/->b/)-b/	-	C	-	-
Symbolic link(click) -ink Directory at Finder	-	-	X	-					
Symbolic link(click) link Directory at Terminal	C	-	-	-					

Table 5: File Metadata Analysis in Macos High Sierra (10.13)

SHELL(terminal)					GUI(finder)				
Contents	Accessed	Modified	Changed	Created	Contents	Accessed	Modified	Changed	Created
Creation(touch)	X	C	C	C	Modification(app.)	C	C	-	-
Modification(vi)	X	C	C	C	Read(double click)	C	-	-	-
Read(cat)	-	-	-	-	Copy(cp)-original	-	-	-	-
Copy(cp)-original	-	-	-	-	Copy(cp)-duplicate	X	-	C	-
Copy(cp)-duplicate	X	C	C	C	Copy(Cmd+C,V)-original	-	-	-	-
Move(mv)	-	-	C	-	Copy(Cmd+C,V)-duplicate	X	-	C	-
Symbolic link(ln-s)-original	-	-	-	-	Get Info	-	-	-	-
Symbolic link(ln-s)-link file	X	C	C	C	Make Alias-original	-	-	-	-
Symbolic link(click)-original	C	-	-	-	Make Alias-duplicate	X	C	C	C
Symbolic link(click)-link file	-	-	-	-	Quick Look	-	-	-	-
Hard link(ln)-original	-	-	-	-	Move	-	-	C	-
Hard link(ln)-link file	-	-	C	-	Rename	-	-	-	-
Hard link(click)-original-	C	-	-	-					
Hard link(click)-link file	C	-	-	-					

Table 6: Directory Metadata Analysis in Macos High Sierra (10.13)

SHELL(terminal)					GUI(finder)				
Contents	Accessed	Modified	Changed	Created	Contents	Accessed	Modified	Changed	Created
Creation(mkdir)	X	C	C	C	Creation(right click)	X	C	C	C
Change directory(cd)	-	-	-	-	Open(double click)	C	-	-	-
Linux shell(ls)	-	-	-	-	Move file to directory (Drag & Drop)	-	C	-	-
Move file to directory(mv)	-	C	-	-	File duplicate in directory (Duplicate)	-	C	-	-
File Creation in directory(touch)	-	C	-	-	Duplication-original	-	-	-	-
Copy(cp -r)-original	-	-	-	-	Duplication-duplicate	X	-	C	-
Copy(cp -r)-duplicate	X	C	C	C	Copy(copy & paste)-original	-	-	-	-
Move(mv a/ b/)-a directory	-	-	C	-	Copy(copy & paste)-duplicate	X	-	C	-
Move(mv a/ b/)-b directory	-	C	-	-	Copy(cmd+C,V)-original	-	-	-	-
Symbolic link-original	-	-	-	-	Copy(cmd+C,V)-duplicate	X	-	C	-
Symbolic link-link directory	X	C	C	C	Move(Drag&Drop a/->b/)-a/	-	-	C	-
Symbolic link(click)-original	C	-	-	-	Move(Drag&Drop a/->b/)-b/	-	C	-	-
Symbolic link(click) -link Directory at Finder	-	-	-	-					
Symbolic link(click) -link Directory at Terminal	C	-	-	-					

(C: Changed, -: Not Changed X: Not Existed)

3.3. DS_store and document revisions

The .DS_Store is a special macOS file that is created in every directory that the finder accesses. The .DS_Store file in the Recycle Bin is very useful forensically, because the modified date is recorded in it.[11]The Figure 3 below shows the corresponding property using the .DS_Store Parser which we have developed. The modD and moDD values are the modification time(235590342450641), which should be divided by 65536, the interval for one second, and then examined through the HFS + Timestamp Converter.

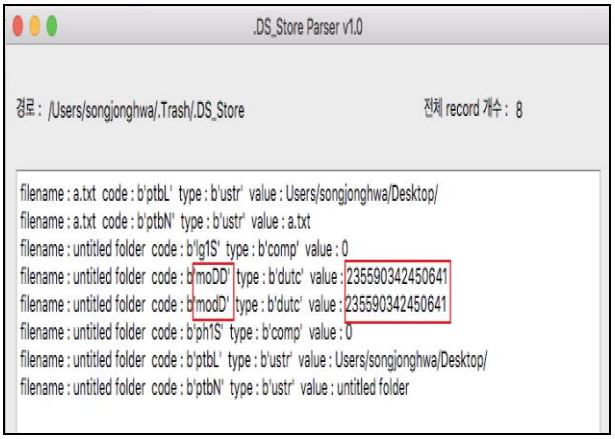


Fig. 3: DS_Store Timestamp.

The Figure 4 below shows that the corresponding time (235590342450641/65536=3594823340) using the converter is2017.11.29 (18:02:20) (UTC).

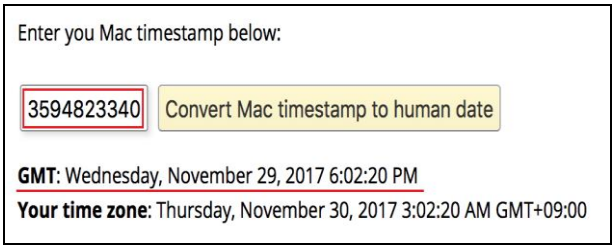
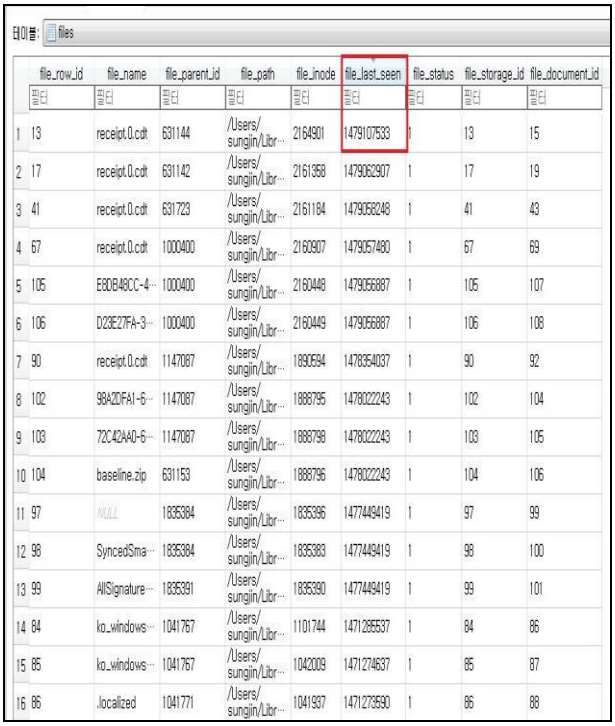


Fig. 4: Modd&Modd Time to Mac HFS+ Timestamp Converter.

Document Revisions is a special feature of macOS that stores a list of all document files are used within the operating system. Apple does not reveal its function or purpose in detail, so it is not exactly known, but from the digital forensics point of view, the database file itself generated by Document Revisions is important. The database file is in SQLite3 format. After changing the user's privileges, the data can be read using DB Browser for SQLite program. The 'file_last_seen' property is shown as belowThe Figure 5.


테이블: files

	file_row_id	file_name	file_parent_id	file_path	file_inode	file_last_seen	file_status	file_storage_id	file_document_id
	필터	필터	필터	필터	필터	필터	필터	필터	필터
1	13	receipt.0.cdt	631144	/Users/sungjin/Libr…	2164901	1479107533	1	13	15
2	17	receipt.0.cdt	631142	/Users/sungjin/Libr…	2161358	1479062907	1	17	19
3	41	receipt.0.cdt	631723	/Users/sungjin/Libr…	2161184	1479056248	1	41	43
4	67	receipt.0.cdt	1000400	/Users/sungjin/Libr…	2160907	1479057480	1	67	69
5	105	E6DB48CC-4…	1000400	/Users/sungjin/Libr…	2160448	1479056887	1	105	107
6	106	D23E27FA-3…	1000400	/Users/sungjin/Libr…	2160449	1479056887	1	106	108
7	90	receipt.0.cdt	1147087	/Users/sungjin/Libr…	1890594	1478354037	1	90	92
8	102	9BA2DFA1-6…	1147087	/Users/sungjin/Libr…	1888795	1478022243	1	102	104
9	103	72C42AA0-6…	1147087	/Users/sungjin/Libr…	1888798	1478022243	1	103	105
10	104	baseline.zip	631153	/Users/sungjin/Libr…	1888796	1478022243	1	104	106
11	97	NULL	1835384	/Users/sungjin/Libr…	1835396	1477449419	1	97	99
12	98	SyncedSma…	1835384	/Users/sungjin/Libr…	1835383	1477449419	1	98	100
13	99	AllSignature…	1835391	/Users/sungjin/Libr…	1835390	1477449419	1	99	101
14	84	ko_windows…	1041767	/Users/sungjin/Libr…	1101744	1471285537	1	84	86
15	85	ko_windows…	1041767	/Users/sungjin/Libr…	1042009	1471274637	1	85	87
16	86	.localized	1041771	/Users/sungjin/Libr…	1041937	1471273590	1	86	88

Fig. 5: Db_Sqlite File of Document Revisions.

If you also use this date to the Epoch & UNIX Time Converter, you can see that the time is 2016.11.14 (07:12:13) (UTC) as shown in Figure 6.

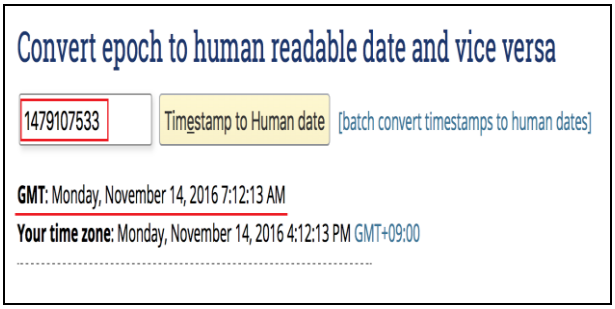


Fig. 6: File_Last_Seen Time to Epoch & UNIX Timestamp Converter.

4. Conclusion

APFS, Apple's new file system, added a few metadata about time. The unified logging system used from the sierra version allows you to knowthe changing time of the system. It also investigated the time changes of files and folders through various actions on the computer. As a result, some attribute information is different from the two versions.

Especially, it was possible to guess the specific time that the user is doing through investigating the hidden files such as DS_Store and Document Revisions's database.

Furthermore, it is necessary to examine and analyze the change of the time attribute of the file when the file and folder are moved or copied with APFS formatted external storage device.

References

[1] Tony Knutson, Filesystem Timestamps: What Makes Them Tick? , STI Graduate Student Research, 2016, (https://www.sans.org/reading-room/whitepapers/forensics/filesystem-timestamps-tick-36842)

[2] Rob Lee, Windows 7 MFT Entry Timestamp Properties,SANS Digital Forensics and Incident Response Blog, (https://digital-

forensics.sans.org/blog/2010/04/12/windows-7-mft-entry-timestamp-properties)
[3] Desktop macOS Version Market Share Worldwide (http://gs.statcounter.com/os-version-market-share/macos/desktop/worldwide)
[4] Kurt H. Hansen, Fergus Toolan, Decoding the APFS file system, Digital Investigation, 2017, 22, pp.107–132.
[5] Technical Note TN1150 HFS Plus Volume Format (https://developer.apple.com/legacy/library/technotes/tn/tn1150.html)
[6] Documentation of MDItem (https://developer.apple.com/documentation/coreservices/mditem-jb5)
[7] Patrick Olsen, Mac DFIR – HFS+ Date Added Timestamp (http://sysforensics.org/2016/08/mac-dfir-hfs-filesystem-date-added/)
[8] Lee Whitfield, MAC Times, Mac Times, and More (https://www.sans.org/summit-archives/file/summit-archive-1498168030.pdf)
[9] Documentation of Logging (https://developer.apple.com/documentation/os/logging)
[10] Xiaoxi Fan, Detection of Backdating the System Clock in Windows (https://www.sans.org/reading-room/whitepapers/forensics/detection-backdating-system-clock-windows-37682)
[11] Hojung, Mac OS X Artifact (DS_Store) (http://www.ylabs.co.kr/index.php?mid=board_mac_forensics&listStyle=viewer&document_srl=30115).