J Inf Process Syst, Vol.18, No.3, pp.402~410, June 2022
https://doi.org/10.3745/JIPS.04.0245

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

A Study on the Processing of Timestamps in the Creation of Multimedia Files on Mobile Devices

Jaehyeok Han and Sangjin Lee*

Abstract

Digital data can be manipulated easily, so information related to the timestamp is important in establishing the reliability of the data. The time values for a certain file can be extracted following the analysis of the filesystem metadata or file internals, and the information can be utilized to organize a timeline for a digital investigation. Suppose the reversal of a timestamp is found on a mobile device during this process. In this case, a more detailed analysis is required due to the possibility of anti-forensic activity, but little previous research has investigated the handling and possible manipulation of timestamps on mobile devices. Therefore, in this study, we determine how time values for multimedia files are handled according to the operating system or filesystem on mobile devices. We also discuss five types of timestamps—file created (*C*), last modified (*M*), last accessed (*A*), digitalized (*Di*), and filename (*FN*) of multimedia files, and experimented with their operational features across multiple devices such as smartphones and cameras.

Keywords

Digital forensics, Filesystem, Multimedia, OS, Reversal, Smartphone, Timestamp

1. Introduction

Time information included in the metadata of a file or folder is a vital element of digital forensic investigations because it can be employed to observe chronological system activity or user behavior. Digital devices such as computers and smartphones record timestamps in various locations, such as in the filesystem for created or modified files, the filename, the file metadata, the web browser history, and internet service logs for storage or social media.

When looking at the MAC times, which are pieces of filesystem metadata that record the modification (*M*), access (*A*), and creation (*C*) of a file, this data typically exhibits the relation $C \leq M \leq A$. Thus, if the time value for modification is smaller than for creation, the timestamps are likely to have reversed. The reversal of timestamps can occasionally happen in Windows, and it may occur naturally for files that are uncompressed or copied from other volumes. Thus, if reversed timestamps are discovered, it is essential to determine whether this represents intentional falsification or a natural occurrence. In any investigation, it is important that temporal information is reliable so that the case can be clearly reconstructed [1].

In this paper, we studied how time values are processed and handled according to the operating system or filesystem for multimedia files on mobile devices, which can be transferred to other storage media.

Manuscript received January 14, 2021; first revision June 8, 2021; accepted June 27, 2021.

* **Corresponding Author:** Sangjin Lee (sangjin@korea.ac.kr)
School of Cybersecurity, Institute of Cyber Security & Privacy (ICSP), Korea University, Seoul, Korea (one01h@korea.ac.kr, sangjin@korea.ac.kr)

Because little empirical information is available about the reversal of timestamps on multimedia files and few studies of anti-forensics for mobile devices have been conducted [2], we investigate the processing of timestamps for multimedia files according to the operating system or filesystem and seek to understand the features related to timestamp reversal in the creation of these files on mobile devices.

2. Background and Related Works

2.1 Extraction of Timestamps from Multimedia Files

Mobile devices with built-in cameras save captured images as multimedia files (photo or video format) on storage media using a specific filesystem. The time values for the multimedia file can be extracted from the metadata of a filesystem or an internal file. *MAC* times can be extracted through filesystem analysis, and digitalized time (*Di*) can be found in exchangeable image file format (EXIF), which is internal metadata from the multimedia file. In addition, timestamps can be found in the filename (*FN*) because some digital devices, such as smartphones, cameras, or dashcams, use the timestamp as a filename when creating a new multimedia file. Some filesystems can also store the deletion time (e.g., EXT4) [3] or the last archive time (e.g., APFS) [4], but we will mainly discuss *MAC* times because SD cards and USB flash drives on mobile devices are typically formatted as FAT32 or exFAT. Thus, they have no fields for the last time the metadata was changed, deleted, or archived.

FAT32, exFAT, NTFS, and EXT4 are the most commonly used filesystems for storage media on Windows and Android systems. Each filesystem contains MAC times and filenames in the directory entry, $MFT entry ($STANDARD_INFORMATION, $FILE_NAME attributes), or inode [5]. The point when extracted timestamps from multimedia files is at which the operation related to taking photos and creating files is finished when the handler that makes the change is closed because timestamps are updated by various mechanisms of each system. Moreover, even if the timestamp has been manipulated, it can be detected for reliability in NTFS on Windows [6].

2.2 States of the Timestamp

Extracted timestamps are occasionally represented as a form of natural language (e.g., September 20th, 2020 [7]) or a human-readable string using ASCII codes (e.g., 2020-09-20, 14:31:55 Z [8]); however, they can only be retrieved in practice when converted because they are stored in hexadecimal format (e.g., 0x4B E9 66 5F, Unix time - 32 bits LE). MS-DOS time [9], Windows file time, and Unix time are examples of timestamp representations that do not always contain the same information, especially in terms of the resolution (Table 1). The resolution of the creation time in FAT32 is ten milliseconds (10-2 seconds, centisecond). In contrast, the time of the last modification has a resolution of 2 seconds and the last accessed time has a resolution of a day [10].

Because each file system within a volume supports different time resolutions, the damage of their precisions can remain when a file is moved to another volume. This is regarded as a kind of information loss in digital investigation. Also, when analyzing a file's metadata, it can lead to misunderstandings if the file operation is executed and the update of the time value is delayed. Therefore, understanding the processing of timestamps of files between volumes is required.

Table 1. Resolutions of timestamps on filesystem metadata

Filesystem		FAT32	exFAT	NTFS	EXT4
Timestamp		MS-DOS time (32 bits)	MS-DOS time (32 bits)	Windows file time (64 bits)	Unix time (32/64 bits)
Resolution of time (Precision)	Created	10^{-2} s	10^{-2} s	10^{-7} s	10^{-9} s
	Last modified	2 s	10^{-2} s	10^{-7} s	10^{-9} s
	Last accessed	1 day	2 s	10^{-7} s	10^{-9} s
	Metadata changed	N/A	N/A	10^{-7} s	10^{-9} s
	File deleted	N/A	N/A	N/A	1 s

3. Experiments on the Processing of Timestamps

3.1 Approach and Experimentation

To understand the mechanism of timestamps in creating a multimedia file on mobile devices, we considered common usages and activities when taking pictures and selected subjects, as shown in Table 2. Since information about the timestamps of media files can be extracted from the filesystem or internal file metadata, in the present study, the relation between the five timestamps, including *MACDiFN* time values, is studied. In particular, we examine the reversal of the timestamps for multimedia files when moving them from a mobile device to a PC.

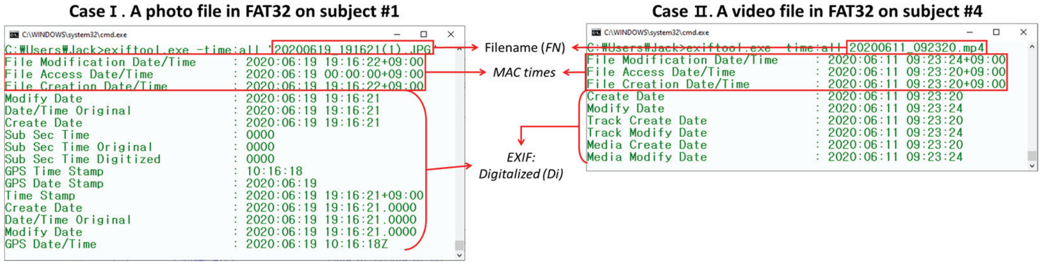
Table 2. Subjects of the experiment and settings of digital devices

	Subject 1	Subject 2	Subject 3	Subject 4	Subject 5
Device type	Smartphone	Smartphone	Smartphone	Smartphone	Action camera
Model	SHV-E330L	SMN-910S	SM-G935S	LG-F320	GoPro HERO5 Black
OS	Android 4.4.2	Android 6.0.1	Android 8.0.0	Android 5.0.1	ver 01.50
App (package)	com.sec.android.app.camera (ver 2.0)	com.sec.android.app.camera (ver 3.0)	com.sec.android.app.camera (ver 7.6.59)	com.lge.camera (ver 4.8.8)	N/A
Filesystem	FAT32(default), exFAT	FAT32(default), exFAT	FAT32, exFAT(default)	FAT32(default), exFAT	FAT32(default), exFAT

In experiments as a dataset, we employed the preloaded camera app and various modes to take photo or video files, including burst and panorama modes. The reason for selecting multiple products was to determine whether there is a difference according to the manufacturer, OS version, or camera app version. As a result, we could confirm that the handling of timestamps for creating multimedia files differs due to these factors.

Cases of the reversal of timestamps were not easy to find for mobile devices. Still, we had identified such cases occurring due to structural restrictions of the filesystem and date/time representation. Furthermore, we determined the mechanisms for multimedia file creation on mobile devices and for copying files from a mobile device to a PC, which involves moving them from FAT32 or exFAT to NTFS or EXT4. To produce these experimental results, we compared the timestamps for photo and video files concerning standard file operations for five mobile devices (Table 2). We generated multimedia files based on expected scenarios, including taking photos, recording video, taking screenshots from a video, restarting the recording of a video after pausing, and copying and pasting a file. A SanDisk Micro SDHC Ultra 32GB was used as the external storage media for storing the files. We used EnCase (ver. 8.09) to extract and analyze timestamps from the filesystem and ExifTool [11] by Phil Harver to read EXIF data in JPEG and MP4 format. In this process, DCode [12] had used to decode the timestamp data, and the time zone is standardized as Korea Standard Time (KST, UTC+09).

In summarizing the experimental results, the relation between the five timestamps for the photo is basically $Di \leq FN \leq C \leq M \leq A$. The digitalized time or filename value is smaller than *MAC* times because the operation on mobile devices for the file creation usually takes precedence over the process for the filesystem. In other words, the operation on the processing of timestamps in creating multimedia files is due to the difference between the camera application and the library for managing the filesystem on the operating system. This relationship can be easily observed if you look at the Case I in Fig. 1; it can be seen that $Di = FN \leq C = M = A$. However, in mobile devices, different manufacturers handle multimedia in different ways. In particular, we have confirmed through experiments that it is more easily occurred in case of a lack of performance to process multimedia on the mobile device.



Case Ⅰ. A photo file in FAT32 on subject #1

```
C:₩Users₩Jack>exiftool.exe -time:all '20200619_191621(1).JPG'
File Modification Date/Time     : 2020:06:19 19:16:22+09:00
File Access Date/Time           : 2020:06:19 00:00:00+09:00
File Creation Date/Time         : 2020:06:19 19:16:22+09:00
Modify Date                     : 2020:06:19 19:16:21
Date/Time Original              : 2020:06:19 19:16:21
Create Date                     : 2020:06:19 19:16:21
Sub Sec Time                    : 0000
Sub Sec Time Original           : 0000
Sub Sec Time Digitized          : 0000
GPS Time Stamp                  : 10:16:18
GPS Date Stamp                  : 2020:06:19
Time Stamp                      : 2020:06:19 19:16:21+09:00
Create Date                     : 2020:06:19 19:16:21.0000
Date/Time Original              : 2020:06:19 19:16:21.0000
Modify Date                     : 2020:06:19 19:16:21.0000
GPS Date/Time                   : 2020:06:19 10:16:18Z
```

Case Ⅱ. A video file in FAT32 on subject #4

```
C:₩Users₩Jack>exiftool.exe -time:all 20200611_092320.mp4
File Modification Date/Time     : 2020:06:11 09:23:24+09:00
File Access Date/Time           : 2020:06:11 09:23:20+09:00
File Creation Date/Time         : 2020:06:11 09:23:20+09:00
Create Date                     : 2020:06:11 09:23:20
Modify Date                     : 2020:06:11 09:23:24
Track Create Date               : 2020:06:11 09:23:20
Track Modify Date               : 2020:06:11 09:23:24
Media Create Date               : 2020:06:11 09:23:20
Media Modify Date               : 2020:06:11 09:23:24
```

Fig. 1. Examples of extracting time values from a photo and a video using ExifTool.

Table 3. Experimental results for the resolution of timestamps on FAT32 and exFAT volume and features about time data for the multimedia files (exceptional cases)

Dataset	Filesystem	Digitalized (*Di*)	Created (*C*)	Last modified(*M*)	Last accessed (*A*)
P#1	FAT32	2020-09-02 13:45:21	2020-09-02 **13:45:21**	2020-09-02 **13:45:20**	2020-09-02
P#2	FAT32	2020-09-02 **13:45:20**	2020-09-02 **13:45:21**	2020-09-02 13:45:21	2020-09-02
P#3	exFAT	2020-09-02 13:45:20	2020-09-02 13:45:21	2020-09-02 **13:45:21**	2020-09-02 **13:45:20**
V#1	FAT32	2020-09-02 13:45:41	2020-09-02 **13:45:41**	2020-09-02 **13:45:40**	2020-09-02
V#2	exFAT	2020-09-02 **13:45:41**	2020-09-02 **13:45:41**	2020-09-02 **13:45:41**	2020-09-02 **13:45:31**

In exceptional cases, the relation is no longer established, and the reversal of time values was identified. We discovered these cases when a number of photos were taken within 1 second or when a video was recorded for 1 second or more. Regarding the timestamps from a video file stored in the smartphone on the right side of Fig. 1, the last modified time value is greater than the last accessed time value. The following examples in Table 3 show some exceptions that timestamps were reversed. For P#1, P#3, and V#1 cases, the created and last modified times were reversed because of resolutions of timestamps on filesystem metadata. In the case of P#2, the timing at which the multimedia file, which is handled by the camera application or filesystem library, has a slightly different point between the camera application and the filesystem library is slightly different in seconds. For video files, a particular time indicates the start and end of the recording, so *A* and *Di*, *C*, *M* times represent shooting start and end in subjects #1 to #4, respectively. The following is a list of the filenames and scenarios of each dataset in Table 3, and the *FN* indicates the start time of the shooting. Since the filename is assigned as a time value in seconds, a delimiter is additionally included after the filename, such as P#2 and P#3, in order to distinguish files with the same filename within 1 second.

- P#1: 20200902_134521.jpg – A first photo taken at Sep. 02, 13:45:21.
  [*C* > *M*, reversed due to the resolution of time values supported by FAT32]
- P#2: 20200902_134521(0).jpg – A second photo taken at Sep. 02, 13:45:21.
  [*FN* = *Di* < *C*, *C* may not coincide with *FN* or *Di* due to the sequence of internal operations]
- P#3: 20200902_134521(1).jpg – A third photo taken at Sep. 02, 13:45:21.
  [*M* > *A*, reversed due to the resolution of time values supported by exFAT]
- V#1: 20200902_134531.mp4 – Video files recorded at Sep. 02, 13:45:31 for 10 seconds.
  [*C* > *M*, reversed due to the resolution of time values supported by FAT32]
- V#2: 20200902_134531.mp4 – Video files recorded at Sep. 02, 13:45:31 for 10 seconds.
  [*FN* < *Di*, *M* > *A*, reversed due to determination of time values by action to start (*FN, A*) or end (*Di, C, M*) video recording]

Since exFAT has higher precision than FAT32, we will look at examples related to this. As described in Section 2.2, when a file is created in a storage medium formatted with exFAT, the interval of MAC times could occur from 0.01 to 2 seconds logically. In practice, however, it was confirmed that the time difference could vary for each device due to the method of using the time increment value, as shown in Table 4. Among ours, subjects #1 to #3 and #5 use only 0 and 100, and subject #4 uses all of 0 to 199 for *MAC* times. With regard to processing for the video file, unlike the previous results, *Di*, *C* and *M*, *A* times represent shooting start and end respectively in subject #5 as seen in the V#3.

- P#4: 20200902_134521.jpg – A photo taken at Sep. 02, 13:45:21 on subject #1, #2, #3 and #5.
  [*M* < *A*, *A* may not coincide with *C* or *M* due to usage of the time increment value for centisecond]
- P#5: 20200902_134521.jpg – A photo taken at Sep. 02, 13:45:21 on subject #4.
  [*M* < *A*, *A* may not coincide with *C* or *M* due to usage of the time increment value for centisecond]
- V#3: G0017331.mp4 – Video recorded at Sep. 02, 13:45:31 for 10 seconds on subject #5.
  [*C* < *M*, Subject #5 sets *FN*, *Di*, *C* of a file as a start timestamp of video recording and *M*, *A* of a file as an end timestamp (Also includes the same issue as P#5)]

In addition, because GoPro assigns filenames so that the number increases according to the order in which the files are created, extracting a specific time value from the filename was limited, but only the order of creation between multimedia files could be checked. Another mobile device that uses this method for assigning a filename is an iPhone [13]. However, we have not included it in the experimental subject since it can mostly be acquired through logical imaging.

Table 4. Experimental results for the resolution of timestamps on exFAT volume and features about time data for the multimedia files

Dataset	Filesystem	Digitalized (*Di*)	Created (*C*)	Last modified(*M*)	Last accessed (*A*)
P#4	exFAT	2020-09-02 13:45:21	2020-09-02 **13:45:21.00**	2020-09-02 **13:45:21.00**	2020-09-02 **13:45:22**
P#5	exFAT	2020-09-02 13:45:21	2020-09-02 **13:45:22.13**	2020-09-02 **13:45:22.13**	2020-09-02 **13:45:24**
V#3	exFAT	2020-09-02 **13:45:31**	2020-09-02 **13:45:31.13**	2020-09-02 **13:45:41.35**	2020-09-02 **13:45:42**

3.2 Comparison with Experimental Data and Discussions

Most multimedia files are created with mobile devices, and fake photo or video files could be manipulated with techniques such as data forgery, composition, or deepfake. Timeline analysis, which is one of the useful methods for file manipulation detection as an anti-forensic activity, requires reliable information about timestamps. For this purpose, we analyzed a combination of multiple timestamps stored in a filesystem (*FN*, *C*, *M*, *A*) or a file (*Di*) without relying on a single timestamp [14].

Experimental results about the processing of timestamps in the creation of multimedia files on mobile devices are summarized in Table 5. Unlike the generally expected relation between timestamps, the timestamps were reversed or inconsistent soundly due to the difference in the representation and resolution of time values supported by a filesystem or the difference in the internal operation between devices. These results are things that could happen without being manipulated. Therefore, it is necessary to comprehensively and thoroughly determine whether malicious or anti-forensic activities had been applied from the analysis result of the target device supporting the camera function. Subsequent discussions relate to additional considerations for reliable factors and helpful information in digital investigations.

Table 5. Experimental results for the resolution of timestamps on FAT32 or exFAT volume and features about time data for the multimedia files on mobile devices

Type	Time resolution of a source file		Time series for the photo	User activity for the video
	FAT32	exFAT		
C (Created)	1 s	0.01–2 s	3	Finish (In case of S#5, Start)
M (Last modified)	2 s	0.01–2 s	4 (In case of S#5, 5)	Finish
A (Last accessed)	1 day	2 s	5 (In case of S#5, 4)	Start (In case of S#5, Finish)
Di (Digitalized)	1 s	1 s	1	Finish (In case of S#5, Start)
FN (Filename)	1 s (In case of S#5, N/A)	1 s (In case of S#5, N/A)	2	Start (In case of S#5, N/A)

Time series for the photos and videos. The relation between the five-time values extracted from the external storage is assessed. This relation is quite different from the photos and videos. For a photo file, the time series is $Di \leq FN \leq C \leq M \leq A$ but for a video file, it is $FN \leq A \leq Di \leq C \leq M$. As shown in Table

5, there are differences in the results depending on the device.

Because high-definition (HD) video recording has recently become supported by mobile devices, and it is common to take more than 1 second to create a multimedia file, there are cases where the last accessed time is reversed [15]. Moreover, time values that were seconds or less can be set to 0 when moving from FAT32 or exFAT to NTFS or EXT4, which is caused by the difference in the time precision supported by the filesystems. For example, the created time for a photo file on NTFS can be saved as “2020-09-20 15:41:09.0000000 (0x80 30 E7 05 19 8F D6 01).” In practice, the probability of this case occurring when using the system is very low, so it is likely to be the result of the file being moved from another volume formatted as FAT32, exFAT, or the adoption of an anti-forensic technique for the intentional falsification of time values [6,16].

Rule for naming on a file. The filename (*FN*) of a multimedia file is created in consideration of the time or the sequence of its creation. “20200915_103518.jpg” for subjects #1 to 4 and “G0017330.JPG” for subject #5 are examples of these two filename strategies. Obviously, a time value can only be extracted from the former strategy, which was the case for subjects #1 to #4 in the present study. If two or more files are created within 1 second in burst mode, a separator is included at the end of the filename, such as “20200915_103518(1).jpg.” Occasionally, we observed several cases where the file with the larger number in parenthesis at the filename was created first. But it was found irregularly, and we could not explain why.

Folders containing files. To further confirm the analysis result, the time values for a folder containing multimedia files can also be extracted in the filesystem metadata analysis. When a file is added to a folder, the MAC times of the folder change, but the folder does not have EXIF data, and its name is fixed, such as “/sdcard/DCIM/camera/” or “/MTP Client Disk Volume/DCIM/100GOPRO/.”

The creation time and last modified time of the folder have the same value as the creation time of the file, and the last accessed time of the folder is the same as the creation time of the first file generated after connecting the storage medium to a mobile device. Thus, the time data for a camera folder has the sequence $A \leq C \leq M$, and when a new multimedia file is created, the folder creation and last modified times are updated with the corresponding times. So, it is possible to determine the connection history with more than one device.

Timestamps changes in the moving to the other volume. Multimedia files are used to be moved from a mobile device to a PC or transferred between different devices for viewing. During these operations, the volume in which the file is stored changes and its time information will be changed accordingly. In the case of Windows, which is the most used, the analysis of the time values in the NTFS [17] will be different from the information identified on the mobile device. The same result will be produced even if a different file system is formatted, such as EXT4 or APFS. Therefore, when moving a file between volumes, it is necessary to determine the resolution of timestamps supported by the filesystem. This is because the time values of the moved file are set to NULL if it does not support enough time information by the target volume. For example, if the last modified time in FAT is moved to NTFS, “2020-2020-09-02 13:45:21” is designated as “2020-09-02 13:45:21.0000000.”

Even when the time value is manipulated with an anti-forensic technique tool, this observation can be identified. Thus, it is necessary to examine other artifacts linked to the application's behavior in response to misinterpretation in this situation. For example, messengers work to delete or change the EXIF data to reduce the data size of the transmission. In other words, the results of analyzing timestamps in the digital investigation should be thoroughly examined, including multimedia files.

4. Concluding Remarks

In digital forensics, the extraction of time information from digital data is essential because it allows observing system activities and user behaviors in chronological order for the profiling [18-20] or can be applied as the sorting criteria to a digital evidence management system [21]. In the present study, we identified the relation between time values for multimedia files on five devices. This analysis is helpful for investigations in which the reversal of time values is discovered because it is important to know whether this represents an intentional falsification or a natural occurrence.

In this paper, we studied the processing of timestamps in the creation of multimedia files according to the operating system or filesystem on five mobile devices. As a result, we discovered the reversal of timestamps on mobile devices and discussed exceptional observations, but it usually works. Although relatively old mobile devices were used in the present study and only preloaded camera apps were investigated, we identified issues related to timestamps when files are moved to other volumes and highlighted the reliability of time values in this situation.

References

[1] S. Garfinkel, “Digital forensics XML and the DFXML toolset,” *Digital Investigation*, vol. 8, no. 3-4, pp. 161-174, 2012.

[2] C. Chen, X. Zhao, and M. C. Stamm, “Mislgan: an anti-forensic camera model falsification framework using a generative adversarial network,” in *Proceedings of 2018 25th IEEE International Conference on Image Processing (ICIP)*, Athens, Greece, 2018, pp. 535-539.

[3] H. Pomeranz, “Understanding EXT4 (Part 4): Demolition Derby,” 2011 [Online]. Available: https://www.sans.org/blog/understanding-ext4-part-4-demolition-derby/.

[4] Wikipedia, “Comparison of file systems,” 2015 [Online]. Available: https://en.wikipedia.org/wiki/Comparison_of_file_systems.

[5] B. Carrier, *File System Forensic Analysis*. Upper Saddle River, NJ: Addison-Wesley, 2005.

[6] D. Palmbach and F. Breitinger, “Artifacts for detecting timestamp manipulation in NTFS on windows and their reliability,” *Forensic Science International: Digital Investigation*, vol. 32, article no. 300920, 2020. https://doi.org/10.1016/j.fsidi.2020.300920

[7] C. G. Lim, Y. S. Jeong, and H. J. Choi, “Survey of temporal information extraction,” *Journal of Information Processing Systems*, vol. 15, no. 4, pp. 931-956, 2019.

[8] *Date and time—Representations for information interchange—Part 1: Basic rules*, ISO 8601-1:2019, 2019.

[9] Microsoft, “MS-DOS Date and Time,” 2021 [Online]. Available: https://docs.microsoft.com/en-us/windows/win32/sysinfo/ms-dos-date-and-time.

[10] Microsoft, “File times,” 2021 [Online]. Available: https://docs.microsoft.com/en-us/windows/win32/sysinfo/file-times.

[11] P. Harvey, "ExifTool version 12.14,” 2022 [Online]. Available: https://exiftool.org/.

[12] Digital Detective, "DCode version 5.2,” 2022 [Online]. Available: https://www.digital-detective.net/dcode/.

[13] J. O. Nelson, “Comparative analysis of iPhone image data across various transfer methods,” Ph.D. dissertation, University of Colorado, Denver, CO, 2020

[14] P. Yacovetta, “Benefits of using multiple timestamps during timeline analysis in digital forensics,” 2010 [Online]. Available: https://www.sans.org/blog/benefits-of-using-multiple-timestamps-during-timeline-analy sis-in-digital-forensics/.

[15] E. Antsilevich, “Capturing timestamp precision for digital forensics,” James Madison University, Harrisonburg, VA, Report No. JMU-INFOSEC-TR-2009-002, 2009.

[16] T. Gobel and H. Baier, “Anti-forensics in ext4: on secrecy and usability of timestamp-based data hiding,” *Digital Investigation*, vol. 24, pp. S111-S120, 2018.

[17] T. Knutson, “Filesystem timestamps: what makes them tick?,” 2016 [Online]. Available: https://www.sans.org/white-papers/36842/.

[18] A. Nieto and R. Rios, “Cybersecurity profiles based on human-centric IoT devices,” *Human-centric Computing and Information Sciences*, vol. 9, article no. 39, 2019. https://doi.org/10.1186/s13673-019-0200-y

[19] M. A. Alqarni, S. H. Chauhdary, M. N. Malik, M. Ehatisham-ul-Haq, and M. A. Azam, “Identifying smartphone users based on how they interact with their phones,” *Human-centric Computing and Information Sciences*, vol. 10, article no. 7, 2020. https://doi.org/10.1186/s13673-020-0212-7

[20] S. Hayat, A. Rextin, A. Idris, and M. Nasim, “Text and phone calls: user behaviour and dual-channel communication prediction,” *Human-centric Computing and Information Sciences*, vol. 10, article no. 11, 2020. https://doi.org/10.1186/s13673-020-00217-x

[21] J. Jeong, D. Kim, B. Lee, and Y. Son, “Design and implementation of a digital evidence management model based on Hyperledger Fabric,” *Journal of Information Processing Systems*, vol. 16, no. 4, pp. 760-773, 2020.

Jaehyeok Han **https://orcid.org/0000-0001-5724-0775**

He received B.S. in Natural Science College of Mathematics from the University of Seoul (UOS) and an M.E. degree in the School of Cybersecurity from Korea University in 2011 and 2016, respectively. Since March 2016, he has been with the School of Cybersecurity from Korea University as a Ph.D. student and has worked with the investigative agency as a researcher of Digital Forensic Research Center (DRFC) at Institute of Cyber Security & Privacy (ICSP). His current research interests include digital forensics, information security, and cryptography system.

Sangjin Lee **https://orcid.org/0000-0002-6809-5179**

He received a Ph.D. degree from the Department of Mathematics, Korea University, in 1994. From 1989 to 1999, he was a Senior Researcher with the Electronics and Telecommunications Research Institute, South Korea. He has been running the Digital Forensic Research Center, Korea University, since 2008. He is currently the President of the Division of Information Security, Korea University. He has authored or coauthored over 130 articles in various archival journals and conference proceedings and over 200 articles in domestic journals. His research interests include digital forensics, data processing, forensic framework, incident response, etc..