

Event Observation of Date-time Stamps for ADS Reconstruction

Da-Yu Kao^a, Yuan-Pei Chen^a, En-Cih Chang^b

^aDepartment of Information Management, Central Police University, Taiwan

^bTaipei City Police Department, Taiwan

^aCorresponding Author: dayukao@gmail.com

Abstract—Alternate Data Streams (ADS) is a method of information hiding that is only possible on NTFS file systems. Criminals are using it to hide data because the ADS can hide any size and type of data in NTFS file system. ADS is invisible to users. However, ADS operation updates the temporal attribute of cover medium, which could be a trace for ADS evaluating. Cover medium indicates to the file/folder which is used for ADS operation (creating, modifying and overwriting). In general file/folder operation, if we create (archive/copy) a file into folder, it updates certain timestamps attributes of folder and file itself. Same result takes place when modifying/overwriting the file within folder. Based on this concept, we took a file within folder as a cover medium and applied some operations (create, modify and overwrite) on it to observe the timestamps variation on both folder and cover medium.

Keywords—alternate data streams, timestamps, event reconstruction, digital investigation, cybercrime investigation

I. INTRODUCTION

In NTFS, there is one unnamed \$DATA attribute which is the data stream default for an NTFS file. The unnamed \$DATA attribute contains the standard file content of the file/folder. There are one or more named \$DATA attributes in every file/folder. Additional \$DATA attributes can be allocated to an MFT entry, but they must have names. A normal file can be attached with multiple ADS. In NTFS, the main data stream (\$DATA) is visible to the user. However, ADS is invisible to the user [6]. ADS can hide data as any format in additional \$DATA attributes of digital files. ADSs do not have any size limits and it does not affect the capacity of the file itself, which means that users wouldn't see any difference since results are too subtle for users to notice. No one will be known by just observing the file if it contains an extra executable or text file within ADS. Windows operating system does not provide any means for any Windows utility to detect the presence of ADS. Therefore, they are not detected by the vast majority of file management applications like Windows Explorer [4].

A use of ADS is tracking the source of downloaded file. Windows uses a simple technique to keep track of where binary files were downloaded from through the Internet (or by a network share). Each downloaded file is tagged with a hidden NTFS ADS file named "Zone.Identifier". However, ADS can be treated as an artifact by DOS command operation, which means that NTFS ADS files can be faked and be used to hide viruses. Moreover, those virus files can be hidden in a number of alternate streams within one file or multiple files.

In 2009, ADS was used by a click fraud Trojan named FFSearcherWeb Link. It used the stream name "Zone.Identifier", which is a stream name that Microsoft used to mark the files downloaded by Internet Explorer. Instead of a simple zone identifier, the Trojan implanted a DLL file containing the Trojan's code. The netcfgx.dll is attacked by DLL file, which is used for network configuration. The results were generally not noticed by users as they are subtle [5].

ADS can be used to hide not only viruses but Trojan code as well. With ADS manipulation, one file is effectively hidden behind another. The target file (cover medium) is the only one which is visible in Windows Explorer or via the dir command. Cover medium indicates to the file/folder which is used for ADS operation (creating, modifying and overwriting). In fact, the only telltale sign is that the date-time stamps of the visible file (cover medium) changes to the time that ADS operation has been executed. The modified time is the time that the content of the \$DATA and/or \$INDEX attributes were last modified [8]. However, every file format has unique timestamps variation rule of itself, no timestamps variation is the same, even applying same operations on them. In general file/folder operation, if we create (archive/copy) a file into folder, it updates certain timestamps attributes of folder and file itself. Same results take place when users modify/overwrite the file within folder. We took the files including the folders as a cover medium and applied some operations (create, modify and overwrite) on them to observe the timestamps variation on both folder and cover medium.

The main idea of this paper is how ADS affect the timestamps of cover medium and how ADS affect the timestamps of folders if ADS operations are applied in the file within folder. We also compare the timestamps of folder/file with ADS, when they are in the same operations (creating, modifying and overwriting).

II. REVIEWS

Timestamps have been used to show the change, modification and access time of a particular digital file for a long time. However, file MAC times can easily be altered in many situations including ADS operations. Experienced examiners are reluctant to draw their own conclusions solely relying on the date and time information of a particular file because such information contains many potential pitfalls. Although there are papers discussing about timestamp evaluation, they did not provide sufficient grounds for

examiners to apprehend the problems comprehensively or that the presented solutions could not be applied in certain cases

As a matter of fact, forensic examiners or investigators who wish to use time-stamps as evidence are facing the challenge of shortage of documentation on how timestamps of file format are updated with different file operating. Moreover, there is no systematic documentation on the behavioral characteristics of file timestamps under different operations with ADS.

A. Alternate Data Streams (ADS)

ADS is a method of information hiding that is only possible on NTFS file systems. ADS can hide any size and type of data in NTFS file system. In NTFS file system as we have seen that file is stored as MFT Entry with set of attributes. Each attribute consists of a sequence of bytes called as stream [9]. The file's actual data is stored in default (unnamed) \$DATA attribute and file's metadata can be stored in additionally created \$DATA attribute. All the additional \$DATA attributes that are created for file are known as ADS. ADS is purely a feature of NTFS file system. It is ADSs that can be accessible with the following command line: "echo command", "notepad command" and "type command" (Table 1).

1) ADS Creating

The simplest way to create ADS in file is using "echo command". The method to create ADS in folder is same as the method we have seen earlier for creating ADS in files.

2) ADS Modifying

The method to modify ADS within file/folder is using "notepad command".

3) ADS Overwriting

The way to overwrite/store/hide ADS in an existing file/folder is using "type command".

Table 1. Three kinds of command line for ADS operation

Operation	General File/Folder
Creation	The ADS is created into the cover medium with "echo" command
Modification	The content of ADS within cover medium is modified with "notepad" command.
Overwriting	The ADS within cover medium is overwritten with "type" command.

B. Three Main Data Attributes and Four Main Timestamps Attributes

1) Three Main Data Attributes

There are three attributes that are important in forensics and are used in the NTFS file system and contain much of the metadata that a MFT entry records. They are the \$STANDARD_INFORMATION (\$SI for short) attribute, the \$FILE_NAME (\$FN for short) attribute, and the \$DATA attribute. The three main attributes discussed above are very important when considering timestamps. Window operation system stores any sort of data content in \$DATA attribute, and stores timestamps attributes in \$SI/\$FN attribute [6].

The \$SI attribute contains the timestamp information for that file. It is from this attribute that Windows determines the MAC times for a file that are displayed to the user when they view the properties of a file. The four date/time stamps are also recorded in the \$FN attribute, but they usually correspond to when the file was created, renamed, or moved. The \$DATA attribute has no defined value [8]. Every file has a \$DATA attribute, which contains the file content. When a file has more than one \$DATA attribute, the additional attributes are sometimes referred to as ADS [2].

2) Four Main Timestamps Attributes

There are four main timestamps attributes in NTFS, which are creation time, modification time, MFT entry modification time, and access time, or MACE-time. NTFS deals with every attribute as a file and maintains at least one MFT entry containing various attributes to store corresponding metadata and multiple date-time stamps [7]. Details for each attribute come from the \$AttrDef of NTFS' hidden system files. \$AttrDef is made up of multiple 160 byte records, and it contains attribute definitions. The attributes of \$SI and \$FN in the NTFS \$AttrDef file hold the following four forensically interesting values (EMAC for short) [1, 3]: MFT Entry modified (or metadata change) time (E-time), Last Modification Time (M-time), Last Access Time (A-time), and Creation time (C-time). \$MFT is Windows Master File Table it stores metadata about the files on a system. The \$MFT is located in the Windows registry. EMAC times record pieces of file system metadata when certain events pertaining to a digital file occurred most recently. They are updated in different circumstance. Windows does not often update \$FN temporal values when \$SI attributes are much sensitive to the file's diverse processes.

3) Temporal Patten of Text File, Word File and Folder

Before talking about ADS evaluation, it is important to understand the timestamps variations of files/folders. In this section, three kinds of operations (creating, modifying and overwriting) are applied on file/folder. Three kinds of operations are listed in Table 2.

a) Creation Operation

The blank file is added with double click, write the content and archive after named it.

● Creation of File

When a file is created, the creation, modification, access, and MFT entry modification times in the \$SI and \$FN attributes are determined as a single file creation time. In other words, it is possible to determine that a folder has been created at a particular location because the time information fields of all attributes contain the same value (Figure 1 and Figure 2) [9].

● Creation of Folder

Folders and files have time information in their \$FN and \$SI attributes, and the time information of all attributes is determined by the folder creation time [1, 9]. The time change pattern resulted from "Creation" operation is simple. All of the timestamps both in \$SI and \$FN are adjusted to the file copy operation time. When we examine the "Creation" time, we can find some different cases in \$SI (Figure 3) [10].

b) Modification Operation

The archived file is opened with double-click, change the content and archive it.

● Modification in General File

To verify changes in time information as a result of file modification, two applications programmed Notepad for Windows and Microsoft Office Word were used to modify the contents of document files [9]. Because time information in an MS Word file does not rely on the operating system or file system, but it is generated and maintained by MS Word itself. As shown by the experimental results, there were some differences in how time attributes were changed during storage of results which had been modified by application programs. This occurred because certain application programs created temporary files or recreated files for storage purposes during data modification [9]. In general file, two timestamps are changed by the “Update” operation. “MFT entry modification time” is changed to update operation time [10].

● Modification in MS Word/Office file

If the modification is executed on MS Office, the behavior of timestamps is different from general files. All of the timestamps in \$SI and \$FN are set to the file save time, except the “Creation” time (Figure 1 and Figure 2) [1, 10].

● Modification in folder

We update folder names as a modification way. In \$SI attribute, the MFT entry modification time is replaced. The time information in the \$FN attribute is replaced by the existing time value of the \$SI attribute (Figure 3) [1, 9].

c) Overwriting Operation

The file is covered with the same name by using cut-and-paste methods. The overwriting operations replace an existing file with another file with the same name. After the overwriting operation executed, two timestamps of the overwritten file are updated in \$SI. The “MFT entry modified time” is changed to the “Overwrite” operation time. The Write time” is timestamps come from the “Write time” of a source file. The remaining fields are unchanged. \$FN fields are all unchanged [10].

● File Overwriting

The “MFT entry modification time” is changed to the overwriting time [1, 10]. The MFT entry modification time serves as the overwritten time value in Vista and subsequent Windows versions (Figure 1 and Figure 2).

● Folder Overwriting

In folder overwriting, there are generally no changes in time attributes (Figure 3). The time information in the \$FN attribute is replaced by the existing time value of the \$SI attribute [1].

Table 2. Three kinds of operations on file/folder

Operation	General File/Folder
Creation	The blank file is added with double-click application, write the content and archive after named it.
Modification	The archived file is opened with double-click, change the content and archive it.
Overwriting	The file is covered with the same name by using cut-and-paste methods.

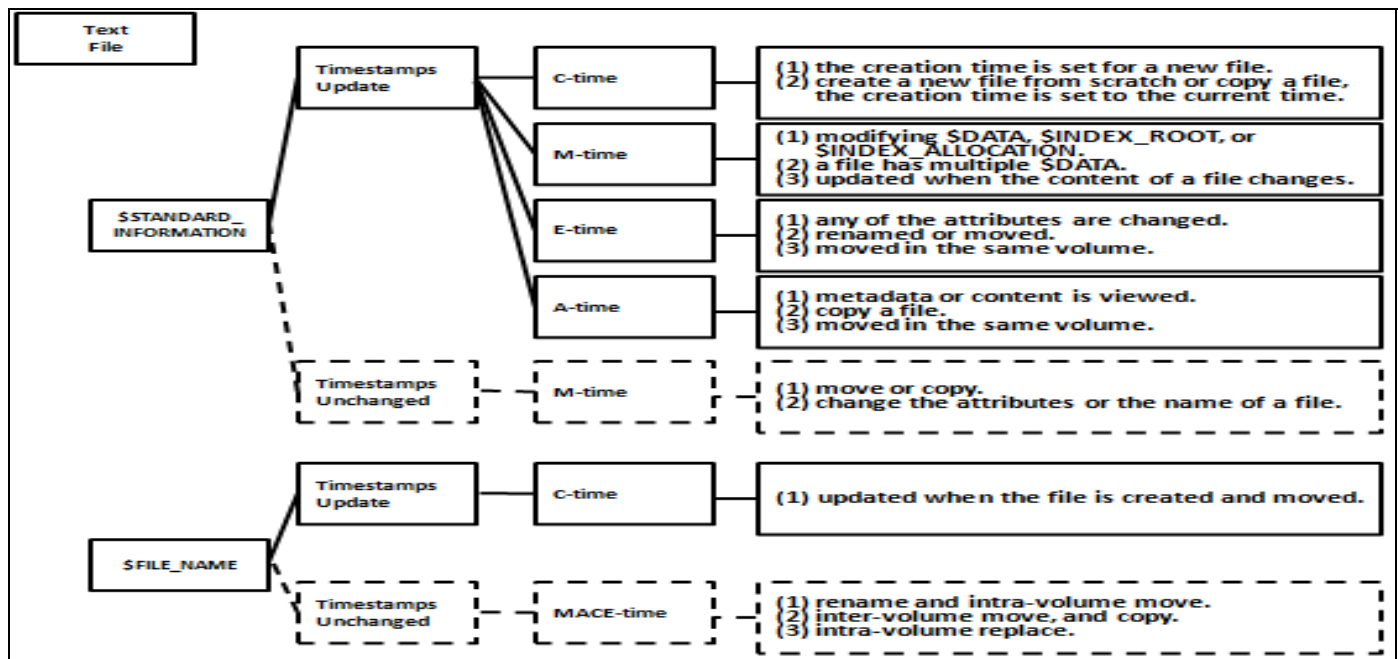


Figure 1. Temporal Pattern of Text File

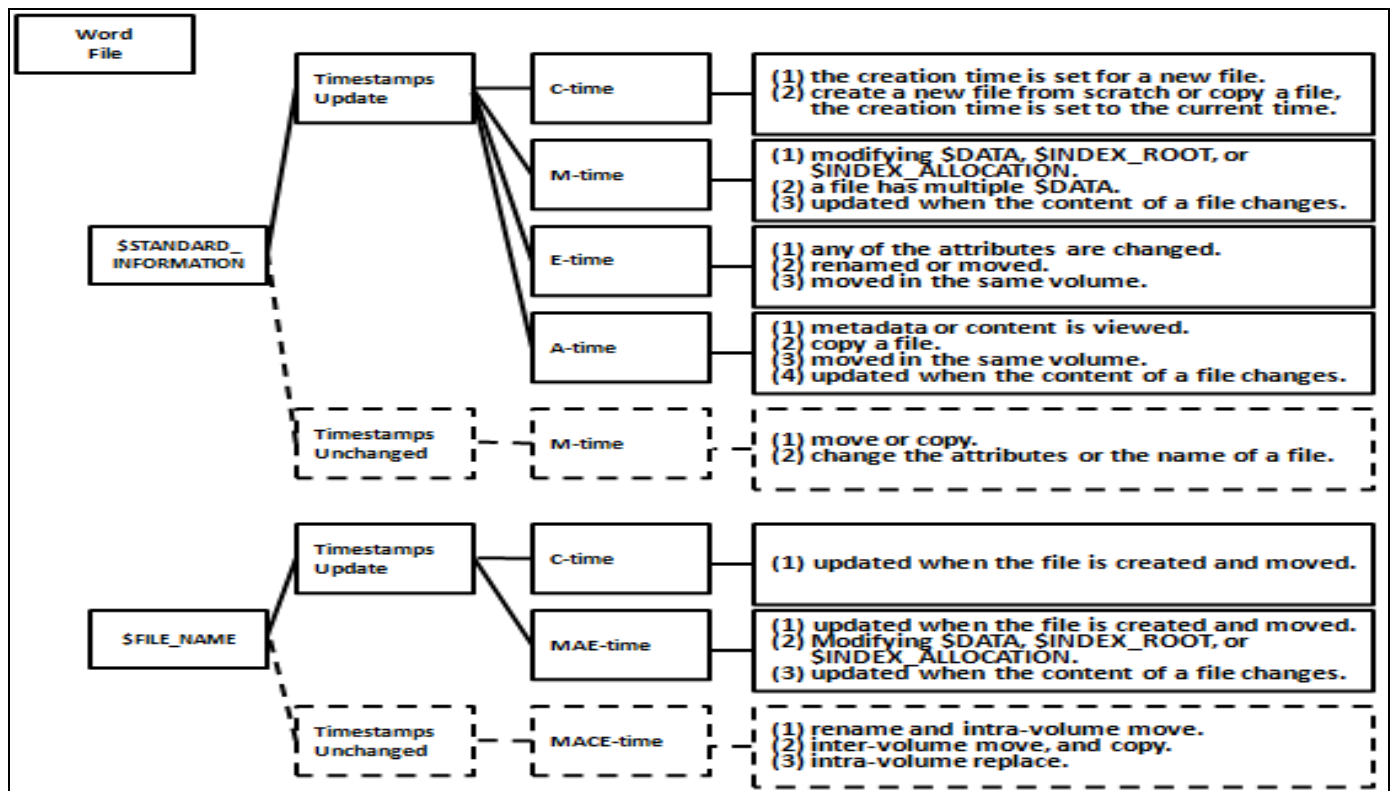


Figure 2. Temporal Pattern of Word

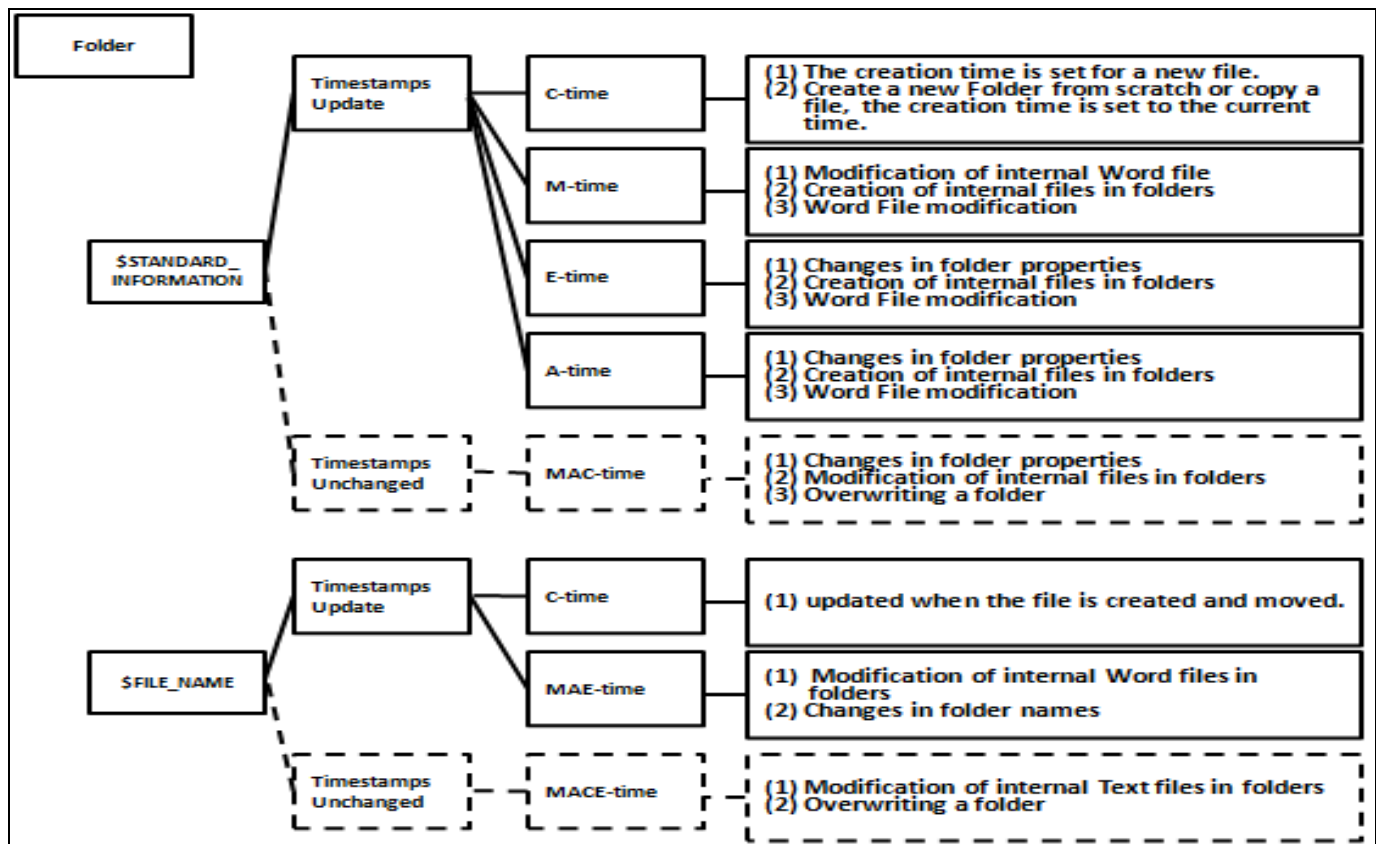


Figure 3. Temporal Pattern of Folder

III. EXPERIMENTAL DESIGN

A. Experimental Procedure

This experiment takes Five Digital Forensic Model Stages as Experimental Procedure to illustrate what we have done in this research. (Figure 4)

1) Identification stage

Both mechanism of \$SI.MACE-time and of \$FN.MACE-time on Folder/File are confirmed in this experiment. In this experiment, the operations (creating, modifying and overwriting) are applied on folder/file for temporal observation.

2) Collection Stage

This experiment carried out ADS operation in cover medium (Word file/Text file) by using DOS Command, such as creating ADS with "echo" command, modifying ADS with "notepad" command, and overwriting ADS with "type" command.

3) Examination Stage

This experiment executed ADS operations to the cover medium (Word file/Text file) within the folder, like ADS creating, ADS modifying, and ADS overwriting. For inspecting the indirect effects of folder that is caused by the ADS operations of cover medium.

4) Analysis Stage

This experiment identified the temporal features of each ADS operation which were listed and established as an index for incident Scenario evaluation.

5) Presentation Stage

We made a comparison table for distinguishing the difference of timestamp between general files/folders with ADS operations.

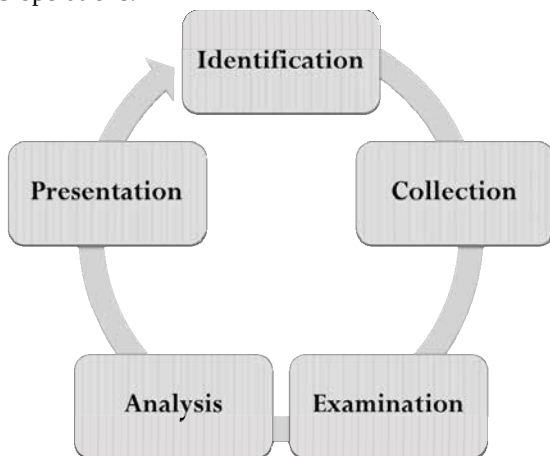


Figure 4. Application of Digital Forensic Model Stages

B. Experimental Environment

To simplify this experiment, the file sizes in this paper are less than 1 MB. The research environment for the experiments is illustrated below.

- 1) OS: Windows 7 Ultimate, 64-bit
- 2) File System: NTFS file system
- 3) Microsoft Office Suites: Word, PowerPoint and Excel.

4) Forensic Tool: Forensic Toolkit (FTK) 6.2.1

(<http://accessdata.com/product-download/ftk-download-page>)

5) File Size: The file sizes in this experiment are less than 1 MB.

C. Experimental Conception

The experiment design intended to support the timestamps analysis of digital evidence in ADS operations. The objective is to identify temporal features of ADS. The challenge of these experiments lies in the hidden date-time stamps not easily visible and extracted using regular File Explore in Windows. These hidden date-time stamps contain more critical information about the file operations, which require rigorous procedures to extract.

The concepts of this experiment are listed below:

1) How ADS affects the timestamps of cover medium, if we took folder/file (Word file/Text file) as cover medium and applied three kinds of ADS operations (create/modify/overwrite) on folder/file(Word file/Text file) (Figure 5).

2) The interaction feature of timestamps between folder and the cover medium, after applying ADS operations on cover medium.

3) The co-variation feature of timestamps between ADS and cover medium, after creating multiple ADS into cover medium.

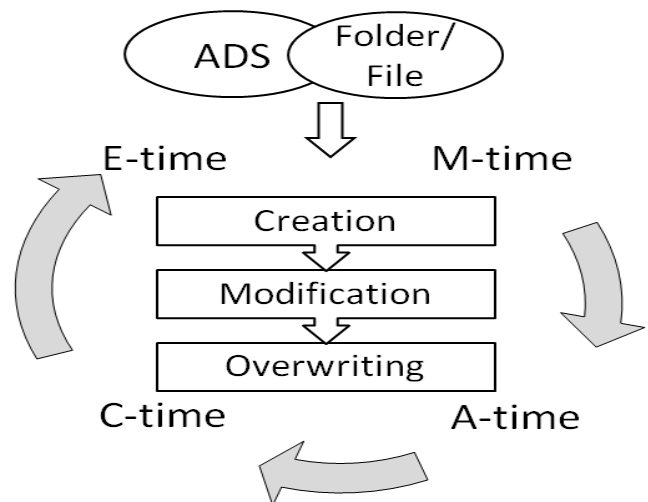


Figure 5. The Experiment Conception of ADS Operations

IV. DISCUSSIONS AND ANALYSES ON TEMPORAL ANALYSIS

In experiment procedure, three kinds of operations are applied on general file and ADS. They are "Creation", "Modification" and "Overwriting". For emphasizing the time attribute which is updated by operations, the updated data is denoted and showed with a word "Update". This experiment put general file part and ADS part together after applying same operation, for comparing time difference with each other.

The phases of experiment findings are divided into two parts for discussing the timestamps variation of folder after those three operations are applied to the file within folder. One

is general file operation, and another is ADS operation. For better understanding timestamp difference, the experiment made a comparison of General file and ADS. The significant timestamp differences are found between General File and ADS after each operation applied.

A. 1st Creation

In 1st general file creation, the \$SI.MAE-time of folder are updated after file creation, regardless of Word file or Text file. In ADS creation, only timestamps of cover medium is updated. No timestamps of folder is updated after ADS is created into cover medium.

B. 2nd Creation

In 2nd general file creation phase, the \$SI.MAE-time of folder are kept updated after 2nd file creation, regardless of Word file or Text file. Each file is taken as an individual one. It means that file creation did not update the timestamps of any other file within same folder. However, the timestamps of existing ADS are updated when new ADS operation is created.

C. Modification

In folder modification phase, the \$FN.EMA-time inherits from the time attributes of \$SI.EMA-time before the folder is modified. Only \$SI.E-time of folder is updated after folder modification. In general file modification, both \$FN.MAE-time and \$SI.MAE-time of Word file are updated after Word modification. The Word modification updates the \$SI.MACE-time of folder too. In ADS modification, ADS modification updates the \$SI.M-time of ADS itself. ADS modification updates the \$SI.EM-time of cover medium. ADS modification updates the \$SI.M-time of existing ADS too. It means that ADS modification makes all timestamps of data inside cover medium updated.

D. Overwriting

In general folder overwriting phase, no timestamps is updated. If the source and the target contain same file (same filename and format), the source folder has only caused \$SI.E-time of overwritten file updated. In ADS overwriting phase, ADS overwriting makes the \$SI.EM-time of cover medium updated. ADS overwriting has also updated the \$SI.M-time of other ADS.

V. CONCLUSION

Pattern finding may or may not play a role in crime reconstruction, but the progressive application of ADS experiment is evident. We took three kinds of operations and applied those operations to general file and ADS. We also took three kinds of data format to implement the experiment; they are folder, Word file and Text file. This paper described some patterns for evaluating if ADS are hidden in folder (Word/Text) or not. The application of file metadata and ADS analysis assists in accurately correlating activities from date-time stamp evidence. The utility of these patterns can be applied in forensic investigation. The contributions of this

paper are to establish date-time stamp patterns for folder (Text/Word files) and their follow-up ADS operations.

ACKNOWLEDGMENT

This research was partially supported by the Ministry of Science and Technology of the Republic of China under the Grants MOST 107-2221-E-015-002-.

REFERENCES

- [1] Bang, J., Yoo, B., Lee, S., "Analysis of Changes in File Time Attributes With File Manipulation," Digital Investigation, vol. 7, pp. 135-144, 2011.
- [2] Carrier, B. File System Forensic Analysis, Chapters 8-13. Pearson Education. 2005
- [3] Casey, E., Handbook of Digital Forensics and Investigation, Elsevier Inc., pp.209-300, 2010.
- [4] Conrad, C., "Alternate Data Streams in NTFS," 2BrightSparks, <https://www.2brightsparks.com/resources/articles/NTFS-Alternate-Data-Stream-ADS.pdf>
- [5] DaBoss, "NTFS ADS Viruses," Computer Knowledge, <https://www.cknow.com/cms/ututor/ntfs-ads-viruses.html>
- [6] Ding, X. and Zou, H., "Reliable Time Based Forensics in NTFS," 2010 Annual Computer Security Applications Conference, Austin, Texas, USA, Dec. 6-10, 2010.
- [7] Kao, D. Y., "Cybercrime Investigation Countermeasure Using Created-Accessed-Modified Model in Cloud Computing Environments," The Journal of Supercomputing, Vol. 72, No. 1, pp 141-160, Jan. 2016.
- [8] Kelsey, L. R., "A Forensic Comparison of NTFS and FAT32 File Systems," https://www.marshall.edu/forensics/files/RusbarskyKelsey_Research-Paper-Summer-2012.pdf
- [9] Mahant, S. H. and Meshram, B.B., "ADS Examiner: Tool for NTFS Alternate Data Streams Forensics Analysis," International Journal of Engineering Research & Technology (IJERT), Vol. 1, No. 4, Jun. 2012.
- [10] Pearson, S. and Watson, R., Digital Triage Forensics: Processing the Digital Crime Scene, Elsevier Inc., Burlington, 2010.



Dayu Kao is an Associate Professor at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan. He is responsible for various recruitment efforts and training programs for Taiwan civil servants, police officers or ICT technicians. He has an extensive background in law enforcement and a strong interest in information security, ICT governance, technology-based investigation, cyber forensics, human resource development, and public sector globalization. He was a detective and forensic police officer at Taiwan's Criminal Investigation Bureau (under the National Police Administration). With a Master degree in Information Management and a PhD degree in Crime Prevention and Correction, he had led several investigations in cooperation with police agencies from other countries for the past 20 years. He can be reached at camel@mail.cpu.edu.tw.



Yuan-Pei Chen is a master student at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan.



En-Cih Chang was a student at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan. Since 2018, she is an information lieutenant at Taipei City Police Department, Taiwan.