The Rules of Time on NTFS File System

K.P. Chow, Frank Y.W. Law, Michael Y.K. Kwan, K.Y. Lai

***Abstract*—With the rapid development and popularity of IT technology, criminals and mischievous computer users are given avenues to commit crimes and malicious activities. As forensic science has long been used to resolve legal disputes regarding different branches of science, computer forensics is developed naturally in the aspects of computer crimes or misbehaviors. In computer forensics, temporal analysis plays a significant role in the reconstruction of events or crimes. Indeed, temporal analysis is one of the attractive areas in computer forensics that caused a large number of researches and studies. It is the purpose of this paper to focus on temporal analysis on NTFS file system and to project intuitional rules on the behavioral characteristics of related digital files.**

***Index Terms*— time analysis, event reconstruction, MAC times**

I. Introduction

PREVIOUSLY, computer forensics has been regarded by investigators as locating and retrieval of digital data or recovering deleted or hidden data from computers. However, such forensics approaches are recognized insufficient as they do not shed light on the causes and correlations of the revealed digital data [2]. Today, there are numerous researches suggesting that event reconstruction is an important phase in the arena of computer forensics.

According to Brian and Eugene [2], Event reconstruction not only identifies the causes of the revealed data, it also establishes event sequence in the examined system. By such, investigators can set out hypotheses to formulate conclusions of the examination. Indeed, the recognition of event reconstruction in computer forensics has ignited a variety of researches focusing on scopes and perspectives. Of these researches on event reconstruction, they all identified that temporal or *MAC* (Modify, Access, Create) time analysis of the retrieved digital data is a crucial process that carries significant value in the event reconstruction phase. Temporal analysis is important because the timestamps of digital files could be very useful for reconstructing the sequence of events [4].

Temporal analysis on individual digital file has been adopted since the evolvement of computer forensics. However, it is not evidentially secure to rely on the timestamps of a particular file to prove a particular event occurred at the corresponding *MAC* times [7], which are pieces of file system metadata identifying when certain events pertaining to a computer file occurred most recently [9]. Sometimes *MAC* times analysis is also expected to extend its value to reveal an ordering of file operations into a timeline [2].

Different kinds of temporal analysis models are henceforth proposed in many researches. These proposed models, however, were abstract in nature and did not offer explicit or practical solutions to perform *MAC* times analysis. This lack of practical models in temporal analysis is aroused from the fact that different file systems employ different types of timestamp mechanisms. Furthermore, since file timestamps can be altered inherently by batch operations such as automated tools scanning, previewing activities, etc, it is difficult to determine whether a particular file was accessed or opened explicitly by the user.

The purpose of this paper is to provide behavioral characteristics of *MAC* times on NTFS file system so that validation basis for temporal analysis in event reconstruction models can be formulated. Through a number of hypothetical rules that have been verified experimentally, investigators can identify the reliability of timestamps that support or refute the chronological order of events. Moreover, since different file systems offer different *MAC* times behaviors, the methodologies adopted for NTFS in this paper can also be applied in other file systems.

Outline

The rest of this paper is organized as follows. Section 2 gives a literature review on the rules of time. Section 3 discusses the approach employed in this work. In Section 4, we present the hypothetical rules and the ideas behind each of them. These rules are subsequently justified with the experiments and findings depicted in Section 5. Section 6 describes some factors affecting the *MAC* times analysis. The application of the rules on some simulated cases will be discussed in Section 7. Finally, Section 8 gives a conclusion and proposes some future research directions.

II. Literature Review

Time analysis is not new in forensic discipline. Lee et al indicates in his literature that timeline analysis is paramount and vital in traditional forensic investigations as it can exploit causal connections between events to establish their chronological orders that are crucial in the evidential sense [6]. Usage of timeline analysis can be evident in a variety of incidents such as crime scene investigations, pathology, etc. On the digital front, as computer operations are based on discrete command set, digital data are indeed results of events

K.P. Chow, Frank Y.W. Law, Michael Y.K. Kwan and K.Y. Lai are with the Department of Computer Science, the University of Hong Kong .
(e-mail: chow@cs.hku.hk, franklaw@graduate.hku.hk, ykkwan@cs.hku.hk, kylai@cs.hku.hk).

with discrete timestamps. Casey has indicated that *MAC* times analysis is necessary to the reconstruction of digital events [5].

In digital forensics, file timestamps are vital attributes as they can establish the correct sequence of events and time spans that can lead to accurate activity reconstruction for investigations and for court proceedings. Reliable activity reconstruction not only reflects what has happened, but also shed light in the evaluation of digital evidence [8]. Time and again, timeline analysis on digital files is correlated to real evidence detected in traditional investigations. Furthermore, digital event reconstruction is also employed to establish accountability of a specific user for the incident.

Traditionally, timestamps have been used to show the creation, modified and access time of a particular digital file. However, file *MAC* times, in particular the *Last Access Time*, can easily be altered in many situations including system operations. As Boyd and Froster mentioned, experienced examiners are reluctant to draw their conclusions solely relying on the date and time information of a particular file because such information contain many potential pitfalls [3]. As a matter of fact, the more knowledge and experience that an examiner possesses the less they are willing to commit to a particular time or date. They would rather look at the whole picture of the timestamps of a group of files or folders in order to establish corroboration or verification of the authenticity of the revealed *MAC* times through event reconstruction.

Although there are papers presenting specific solutions to the problem of 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 most cases [3].

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 in file systems are handled at different operations on different operating systems. Moreover, there is no systematic documentation on the behavioral characteristics of file timestamps under different operations of the operating systems or applications.

III. Approach

With the advance of file system technology, the detailed information on MAC times of digital files are now available in various computing environments for computer users to perform analysis on the states and events happened on a machine. This might be of great value as these meta information, if still exists, allows us to reconstruct the events that were initiated by the computer user. However, there is still absent of any well-established methodology for the analysis of this valuable information though the treasuries exist in nearly every file system.

From the investigative point of view, *MAC* times were influenced and created by human through machine process and there should be specific patterns or trails available for investigator to explain certain phenomena or actions that had been carried out by the user. The traditional approach on event analysis spends heavy resources on dissecting the files' *MAC* times in order to make a conclusive assessment on the sequence of events and digital states. The process is tedious and the result is often inconclusive.

To streamline the digital forensic investigation process and to create a new statistical analyzing method on event reconstruction, a new heuristic approach is required to improve the efficiency, accuracy and admissibility of computer forensics findings complying with the court of law.

By consolidating the experiences acquired from digital forensic investigations, some commonly happened events are reasoned with the essences of *MAC* times. Being assessed to have high prospect in event reconstruction, some phenomena are observed and studied for projecting heuristic rules in *MAC* times analysis. These rules are expected to assist computer forensic examiner in investigating the digital events occurred.

IV. Hypothetical Rules And Ideas Behind

To assist the reconstruction of event through the analysis of *MAC* times, the following phenomena are observed and elaborated.

Observation: From the inherent states of a file, when it is freshly established in a file system without any modification, it is considered to be intact and is not updated after its creation.

Rule No. 1*: When M time is equal to C time, the file has neither been modified nor copied from another disk location. It is suggested that the file is still intact and has not been updated.*

Observation: From the intrinsic property of *MAC* times, the action of moving a file from one location to another location within the same partition, its modification time and creation time will not be modified. On the other hand, when moving a file from one location to another location in a different partition, it would cause the modification time before the creation time. Similar observation appears when copying a file from one location to another location in the same partition or in a different partition. This may be considered to be a faulty design in the file system, yet it is also an indicator for copying or moving of files.

Rule No. 2: *When M time is before C time, the file has been copied from one system into the same/another system or moved from one partition to another partition.*

Observation: When a bunch of files is copied or moved to the same folder in a single operation, they have very close creation times. The same phenomenon can be observed when extracting files from a compressed file into a certain folder. The 'very close' creation times are supposed to be generated by machine actions and the digital states of the files under the same folder may reveal some relevant human actions.

Rule No. 3: *In a folder, if files' M times are before C times and the files have "very close" C times, the files have been*

1) *copied from one system to the same or another system in a batch or*
2) *moved from one partition to another partition in a batch or*
3) *extracted from a compressed file.*

Observation: The feasibility of causing large number of files having "close" access time is explored and statistical data indicated that the only possibility to originate this situation is by machine act. Unlike individual machine process which is intentionally initiated by human, the findings suggest that the files are atomically touched by the machine for some goals, say virus or spyware scanning tools.

Rule No. 4*: When a large number of files with "close" A times are found inside the hard drive, those files are likely to be scanned by some tool, e.g. anti-virus software.*

Observation: The thumbnail preview of multimedia files is very convenient for ordinary users to readily identify the files they want. This process is explored to reveal if there is any trail leaving behind the preview, especially on the *MAC* times of the previewed files. One of the ways to make a folder having multi-media files with "close" access times is to conduct preview by the built-in thumbnail preview of Windows system. This rule works well in the situation where no other multi-media previewing tool exists on the material digital media.

Rule No. 5: *If image/video files within a folder have "close" A times, and no other image files have similar A times, the concerned image/video files are likely to be accessed or opened by file previewing tool, e.g. windows explorer, as thumbnails for previewing.*

Observation: As a complement of Rule No. 4 and Rule No. 5, inference is drawn when no specific patterns of *MAC* times could be observed. It is fundamental and is broad enough to cover many individual events happened on digital media.

Rule No. 6: *When files within a folder have "scattered" A times, it is highly likely that the files are accessed individually.*

Observation: When a file is downloaded from another system into the local system over the network, it is considered to be newly created on the local system such that its modification time equals to the creation time. This action is comparable to creating a file by the computer user manually. In a folder, if a batch of files have their creation time equal to their modification time and the C (M) times of these files are very close, these files are probably downloaded from another system through network, e.g. Internet, as it is unlikely for a regular computer user to successively create a batch of files (in particular, multi-media files) within a very small time frame.

Rule No. 7: *In a folder, if files' M times are equal to C times and the files have "very close" C (M) times, the files may have been downloaded in a batch from another system over the network.*

V. Experiments and Findings

Experiments are designed to justify and corroborate the essence of the hypothetical rules under simulated scenarios where various file-related operations are involved. Two machines with identical configurations are employed as the testing machine (TM) and the web server (WS). The outline of the experiments and summary of the findings will be presented in the following.

Experiment Setup

Operating system – Windows XP SP2
System configuration – P4 CPU 2.40 GHz, 1 GB RAM
Hard drive – 60GB (C:\: 40GB, D:\: 20GB)
File system – NTFS
Time – synchronized with the time server at time.windows.com

Ten simulated scenarios are studied. *MAC* times of the files are examined after each action is carried out. Unless specified explicitly, the operations are done on the testing machine (TM).

Scenario 1: File creation / file access

A text file and an image file are separately created on C drive. The files are then opened and viewed several times without editing its content. The files are subsequently edited and saved under the same file names.

Findings

- When a file is created, the file system assigns values of *MAC* times to it. At the time of creation, the values of *M*, *A* and *C* times are equal, i.e. *M* = *A* = *C*.
- Both *M* and *C* times remain unchanged when the file is accessed or opened whilst *A* time is updated in the course of the access.
- *M* time is updated only if there is a modification to the file content.

The findings corroborate with hypothetical Rule No. 1. Experimental results are given in *Table A1-1*, *Table A1-2* and *Table A1-3* in Appendix.

Scenario 2: Copying files

A text file and an image file are separately created on C drive. The files are then copied to D drive.

Findings

- During the course of copying, a new file having an unmodified content is created on the disk. When a file having the same content of the original file is created on the designated location, its *C* time is updated.
- When the file is being copied, the content of the file is not modified, *M* time remains the same. *A* time is updated as the file is accessed in the course of file creation. Therefore, *A* time is equal to *C* time, which is beyond M time.

The findings corroborate with hypothetical Rule No. 2. Experimental results are given in *Table A2-1* and *Table A2-2* in Appendix.

Scenario 3: Moving files

A text file and an image file are separately created on C drive. The files are then moved to D drive through a drag and drop action in the windows file explorers.

Findings

- Moving a file involves deleting the file from the original location and creating a new file at the designated location. *MAC* times are not relevant to file deletion.
- When the new files are created, both *A* and *C* times are updated, i.e. *A* = *C*, whilst *M* time, which is before A/C time, remains unchanged since no modification is done to the file content.

The findings corroborate with hypothetical Rule No. 2. Experimental results are given in *Table A2-1* and *Table A3-1* in Appendix.

Scenario 4: Batch process – Copying files

To simulate copying files in a batch operation, ten text files and ten image files are created on C drive. These files are then copied to D drive within the same disk.

Findings

- During batch copying, both *A* and *C* times of the files are updated.
- The *C* times of these copied files are very close (nearly the same in this example)
- There would be a delay on *A* and *C* times when the files are large in size.
- M times remain unchanged.

The findings corroborate with hypothetical Rule No. 3. Experimental results are given in *Table A4-1* and *Table A4-2* in Appendix.

Scenario 5: Batch process – Moving files

To simulate moving files in a batch operation, ten text files and ten image files are created on C drive. The files are then moved to D drive through a drag and drop action in the windows file explorers.

Findings

- The results resemble that of batch copying discussed above.

The findings corroborate with hypothetical Rule No. 3. Experimental results are given in *Table A4-1* and *Table A5-1* in Appendix.

Scenario 6: Batch process – Downloading files

A download management software is used to simulate downloading files in a batch operation. Ten text files and ten image files are created on WS (the machine hosting the web server). The hyperlinks o these files are inputted to the download management software manually. The download operation is launched subsequently and these files are downloaded to TM one after another.

Findings

- *M*, *A* and *C* times of the downloaded files are updated to the download time and the values of M, A and C times are equal, i.e. *M* = *A* = *C*
- The M and C times of these downloaded file are very close.
- There are delays on *M*, *A* and *C* times when the files are large in size, depending on the download bandwidth. The smaller the bandwidth, the greater the delay.

The findings corroborate with hypothetical Rule No. 7. Experimental results are given in *Table A6-1* and *Table A6-2* in Appendix.

Scenario 7: Extracting files from a compressed file

Ten text files and ten image files are compressed into two zip files, ‘text.zip’ and ‘image.zip’ respectively. These zip files are extracted to two directories after being copied from C drive to D drive.

Findings

- The results resemble that of batch copying discussed above.

The findings corroborate with hypothetical Rule No. 3. Experimental results are given in *Table A7-1* and *Table A7-2* in Appendix.

Scenario 8: Execution of automated scanning tool

A number of anti-virus/anti-spyware software and the Windows built-in file searching utility will be used to examine the effect of the automated scanning on *A* time.

A folder containing hundreds of files in different file types is created. Each of the scanning tools, one after another, is configured to scan this specific folder. Table I records the effect of the execution of the software on the *A* time of the files.

TABLE I

Software	Modification of A time?
Norton Anti-virus 2006	Yes
e-Trust EZ anti-virus v7.1.8.0	Yes
F-prot anti-virus v3.16c	Yes
McAfee virus scan 2005	Yes
Microsoft Windows Defender Beta 2	Yes
Spybot SD v1.4	No
Pc-cillin 2005	No
WinXP file searching tool	Yes

Findings

- Some anti-virus/spyware tools require opening the file to reveal any embedded virus/spyware therein and therefore will access the file during its scanning process. The files are found to have very close *A* times after execution of these tools.

If automatic scanning tools are scheduled to conduct periodic scanning of files inside the computer, it may cause an implication on the analysis of *MAC* times since the *A* time is longer referred to the last accessed time by the user.

Should the computer forensic investigator detect a large number of files within the same computer having “close” *A* times, it is highly likely that the concerned files are scanned by automatic scanning software or have been accessed by searching tools. Before conducting the *MAC* times analysis, care must be taken to identify this kind of software in order to relate its impact on the file’s *MAC* times.

The findings corroborate with hypothetical Rule No. 4.

Scenario 9: Preview of image/video files by Windows file explorer

140 image files and 10 video files in various formats and sizes are downloaded from different sources on the Internet. All of them are saved to the same local folder.

The built-in Windows file explorer is used to preview the files in thumbnail mode and the content area is set to display 42 files (7 X 6) per one preview. The first 42 files (in alphabetical order) are previewed successfully and the file explorer is closed after that.

Findings

- The hidden file, *Thumbs.db*, is created under the same directory after the preview. Its *C* time is equal to the time of preview while its *M* time is updated after each preview in the thumbnail mode.
- Depending on the size of the browsing windows or the folder icon, the *A* times of the exhibited files will be simultaneously updated within a transient time.
- If a file cannot be displayed (say, for its size being out of the file browsing area) in thumbnail, its *A* time is not updated after a preview.

The findings corroborate with hypothetical Rule No.5.

Thumbs.db is a file used in the windows environment that stores a cache for Windows Explorer's thumbnail view. It speeds up the process of thumbnail preview and is actually a database of the miniature images that existed in the folder from which they are initiated. Being hidden system files, they may be unknown to computer users. Whenever files are added to the folder, new records and miniature graphics will be created. By examining the content and MAC times of *Thumbs.db*, it may provide insights to the forensic examiner on what and when the images inside the folders are previewed in the thumbnail mode.

Scenario 10: Individual access to files within the same folder

A total of ten text files are created separately under the same directory. The files are then individually opened with Notepad. A number of them have their content modified before being saved. The rest of them are left unmodified before closing.

Findings

- No specific pattern could be observed from *M* and *A* times when the files are being accessed individually at various moments.

Under this circumstance, MAC times analysis provides little investigation value. The findings corroborate with hypothetical Rule No. 6. Experimental results are given in *Table A10-1* in Appendix.

VI. Factors That May Affect MAC Times Analysis

In spite of the behavioral characteristics of MAC times observed on the NTFS file system, these values are sensitive and vulnerable to various factors in the common computing environment. Some of these factors are elaborated in detail in this section.

Due care in retrieving MAC times

MAC times are sensitive since a simple click on a file generally will update its *A* time. Besides, during the course of investigation, execution of any application may risk updating the *A* time of its related files about which we may not notice in the system. As a result, the best way to examine MAC times is from a cloned image of the media or mounting the media read-only so that *A* times can be protected from accidental updates.

BIOS and System Clock Setting

Furthermore, the value of MAC times is updated in accordance to the BIOS or Operating System clock. If the clock is not configured accurately, MAC times of the files would carry little value for investigation.

Multi-user System

If the system being examined is a busy multi-user system, files are possible to be shared among different users. Besides, should the access control of the system be relatively inadequate, users getting access to the system may have access to others’ files as well. The user-non-specific MAC times may not be properly correlated with the suspect and makes the analyzed result insignificant.

Disabling of “Last Access Update” in the system

In both windows and Linux systems, users could disable the update of last access time by using the “fsutil” utility or by mounting with “noatime” respectively. Under this circumstance, the *A* time of newly created files will resemble their *C* times. This environment setting definitely affects the result of MAC times analysis since *A* times could no longer be used as reference to the last access time to the files.

Automated scanning tool

In consideration with the findings in Scenario 9, there exists a number of automated scanning programs by which the *A* times of the files inside the computer would be affected. If the *A* time is critical for proving the last access time of a file by the user, the existence of these automatic scanning tools would cause a great implication if the scanning was done after the human access to the file.

File attribute manipulation program

Apart from scanning tools, a number of software programs are available for an average user to view and modify file dates and attributes, including the Modification, Access, and Creation times of one file or a batch of files in the directory tree. Computer forensic examiner should be vigilant on the existence of these programs which may be in use to manipulate the MAC times of files for misleading surface appearance.

VII. Applying the Rules to Simulated Cases

To examine the practicability of the fundamental *MAC* times analysis with the rules developed in this paper, we study the application of these rules on the following simulated cases.

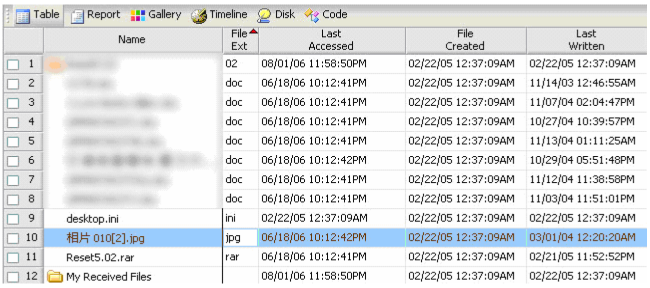
A. Case 1: Child porn images/videos download

A computer simulating the following behaviours of a paedophile having possessed materials of child pornography is used for the testing:

- A number of suspected child pornographic images and videos are downloaded to a computer from the Internet either in a batch or individually, including a compressed file.
- The paedophile has previewed the images/videos in thumbnails.
- In order to backup the child pornography, the paedophile has in several occasions copied the files from one disk location to another disk location.
- Anti-virus software is installed in the computer to protect it from infection of any computer virus.

The hard disk of the computer is examined with the use of the computer forensic tool *Encase*. The computer is run under the NTFS file system and the system clock is confirmed to be accurate. The following are the observations from the analysis of *MAC* times of the files inside the computer.

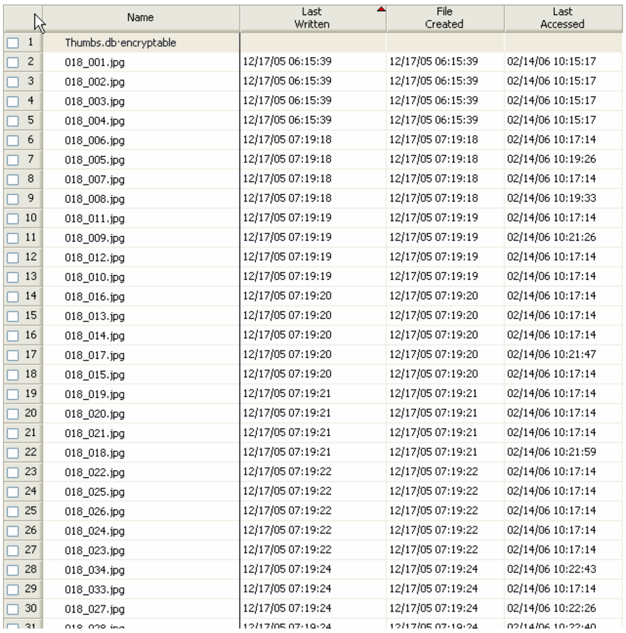
1st *Finding:* A suspected child pornographic image was found under the path *D:\backup\Documents and Settings\User\My Documents* (Figure 1). The *MAC* times of the file are examined and *M* time is found to be ahead of C time. By applying *Rule No.2*, it is believed that this file was either copied or moved from other location to the current location. As well, the folder – *backup*, is named in accordance with the conjecture that the user has copied or moved the file to the revealed disk location as a backup.



	Name	File Ext	Last Accessed	File Created	Last Written
1	[redacted]	02	08/01/06 11:58:50PM	02/22/05 12:37:09AM	02/22/05 12:37:09AM
2	[redacted]	doc	06/18/06 10:12:41PM	02/22/05 12:37:09AM	11/14/03 12:46:55AM
3	[redacted]	doc	06/18/06 10:12:41PM	02/22/05 12:37:09AM	11/07/04 02:04:47PM
4	[redacted]	doc	06/18/06 10:12:41PM	02/22/05 12:37:09AM	10/27/04 10:39:57PM
5	[redacted]	doc	06/18/06 10:12:41PM	02/22/05 12:37:09AM	11/13/04 01:11:25AM
6	[redacted]	doc	06/18/06 10:12:42PM	02/22/05 12:37:09AM	10/29/04 05:51:48PM
7	[redacted]	doc	06/18/06 10:12:41PM	02/22/05 12:37:09AM	11/12/04 11:38:58PM
8	[redacted]	doc	06/18/06 10:12:41PM	02/22/05 12:37:09AM	11/03/04 11:51:01PM
9	desktop.ini	ini	02/22/05 12:37:09AM	02/22/05 12:37:09AM	02/22/05 12:37:09AM
10	相片 010[2].jpg	jpg	06/18/06 10:12:42PM	02/22/05 12:37:09AM	03/01/04 12:20:20AM
11	Reset5.02.rar	rar	06/18/06 10:12:41PM	02/22/05 12:37:09AM	02/21/05 11:52:52PM
12	My Received Files		08/01/06 11:58:50PM	02/22/05 12:37:09AM	02/22/05 12:37:09AM

Fig. 1. Image files located at *D:\backup\Documuments and Settings\User\My Documents*

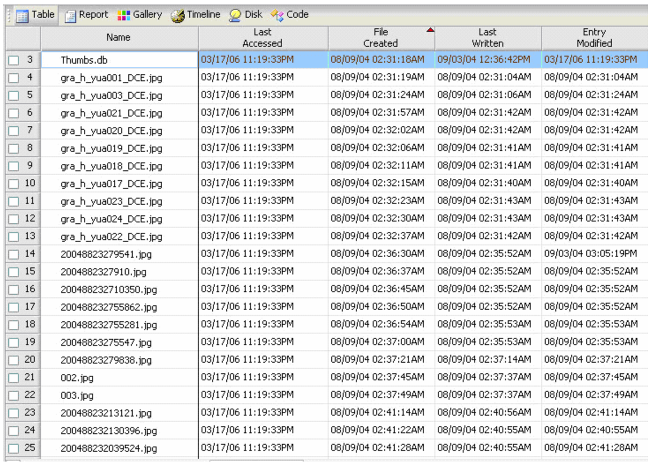
2nd *Finding:* Upon further searching, a folder under the path *C:\downloads\* is located with 41 suspected child pornographic images in jpg format identified therein (Figure 2). C times of the image files are equal to its M times and they are closely established on 2005-12-17. By applying *Rule No. 7*, it is very likely that the files have been downloaded in a batch from another system to their current location. Furthermore, *Rule No. 1* suggests that the image files are still intact and have not been updated after downloading.



	Name	Last Written	File Created	Last Accessed
1	Thumbs.db·encryptable			
2	018_001.jpg	12/17/05 06:15:39	12/17/05 06:15:39	02/14/06 10:15:17
3	018_002.jpg	12/17/05 06:15:39	12/17/05 06:15:39	02/14/06 10:15:17
4	018_003.jpg	12/17/05 06:15:39	12/17/05 06:15:39	02/14/06 10:15:17
5	018_004.jpg	12/17/05 06:15:39	12/17/05 06:15:39	02/14/06 10:15:17
6	018_006.jpg	12/17/05 07:19:18	12/17/05 07:19:18	02/14/06 10:17:14
7	018_005.jpg	12/17/05 07:19:18	12/17/05 07:19:18	02/14/06 10:19:26
8	018_007.jpg	12/17/05 07:19:18	12/17/05 07:19:18	02/14/06 10:17:14
9	018_008.jpg	12/17/05 07:19:18	12/17/05 07:19:18	02/14/06 10:19:33
10	018_011.jpg	12/17/05 07:19:19	12/17/05 07:19:19	02/14/06 10:17:14
11	018_009.jpg	12/17/05 07:19:19	12/17/05 07:19:19	02/14/06 10:21:26
12	018_012.jpg	12/17/05 07:19:19	12/17/05 07:19:19	02/14/06 10:17:14
13	018_010.jpg	12/17/05 07:19:19	12/17/05 07:19:19	02/14/06 10:17:14
14	018_016.jpg	12/17/05 07:19:20	12/17/05 07:19:20	02/14/06 10:17:14
15	018_013.jpg	12/17/05 07:19:20	12/17/05 07:19:20	02/14/06 10:17:14
16	018_014.jpg	12/17/05 07:19:20	12/17/05 07:19:20	02/14/06 10:17:14
17	018_017.jpg	12/17/05 07:19:20	12/17/05 07:19:20	02/14/06 10:21:47
18	018_015.jpg	12/17/05 07:19:20	12/17/05 07:19:20	02/14/06 10:17:14
19	018_019.jpg	12/17/05 07:19:21	12/17/05 07:19:21	02/14/06 10:17:14
20	018_020.jpg	12/17/05 07:19:21	12/17/05 07:19:21	02/14/06 10:17:14
21	018_021.jpg	12/17/05 07:19:21	12/17/05 07:19:21	02/14/06 10:17:14
22	018_018.jpg	12/17/05 07:19:21	12/17/05 07:19:21	02/14/06 10:21:59
23	018_022.jpg	12/17/05 07:19:22	12/17/05 07:19:22	02/14/06 10:17:14
24	018_025.jpg	12/17/05 07:19:22	12/17/05 07:19:22	02/14/06 10:17:14
25	018_026.jpg	12/17/05 07:19:22	12/17/05 07:19:22	02/14/06 10:17:14
26	018_024.jpg	12/17/05 07:19:22	12/17/05 07:19:22	02/14/06 10:17:14
27	018_023.jpg	12/17/05 07:19:22	12/17/05 07:19:22	02/14/06 10:17:14
28	018_034.jpg	12/17/05 07:19:24	12/17/05 07:19:24	02/14/06 10:22:43
29	018_033.jpg	12/17/05 07:19:24	12/17/05 07:19:24	02/14/06 10:17:14
30	018_027.jpg	12/17/05 07:19:24	12/17/05 07:19:24	02/14/06 10:22:26
31	018_028.jpg	12/17/05 07:19:24	12/17/05 07:19:24	02/14/06 10:22:40

Fig. 2. Image files located at *C:\download\*

3rd *Finding:* Another folder, with 27 suspected child pornographic images in jpg format located, is found in the path *D:\bt\photo\jap\* (Figure 3). The files' *M* times are checked to be before their *C* times and therefore *Rule No. 3* can be applied. Furthermore, *A* times of the image files are very close, within the range of 1 second, and there exists the hidden file *thumbs.db* in the same directory. These phenomena suggest that the images inside the folder had been previewed in thumbnails – *Rule No. 5* applied.



	Name	Last Accessed	File Created	Last Written	Entry Modified
3	Thumbs.db	03/17/06 11:19:33PM	08/09/04 02:31:18AM	09/03/04 12:36:42PM	03/17/06 11:19:33PM
4	gra_h_yua001_DCE.jpg	03/17/06 11:19:33PM	08/09/04 02:31:19AM	08/09/04 02:31:04AM	08/09/04 02:31:04AM
5	gra_h_yua003_DCE.jpg	03/17/06 11:19:33PM	08/09/04 02:31:24AM	08/09/04 02:31:06AM	08/09/04 02:31:24AM
6	gra_h_yua021_DCE.jpg	03/17/06 11:19:33PM	08/09/04 02:31:57AM	08/09/04 02:31:42AM	08/09/04 02:31:42AM
7	gra_h_yua020_DCE.jpg	03/17/06 11:19:33PM	08/09/04 02:32:02AM	08/09/04 02:31:42AM	08/09/04 02:31:42AM
8	gra_h_yua019_DCE.jpg	03/17/06 11:19:33PM	08/09/04 02:32:06AM	08/09/04 02:31:41AM	08/09/04 02:31:41AM
9	gra_h_yua018_DCE.jpg	03/17/06 11:19:33PM	08/09/04 02:32:11AM	08/09/04 02:31:41AM	08/09/04 02:31:41AM
10	gra_h_yua017_DCE.jpg	03/17/06 11:19:33PM	08/09/04 02:32:15AM	08/09/04 02:31:40AM	08/09/04 02:31:40AM
11	gra_h_yua023_DCE.jpg	03/17/06 11:19:33PM	08/09/04 02:32:23AM	08/09/04 02:31:43AM	08/09/04 02:31:43AM
12	gra_h_yua024_DCE.jpg	03/17/06 11:19:33PM	08/09/04 02:32:30AM	08/09/04 02:31:43AM	08/09/04 02:31:43AM
13	gra_h_yua022_DCE.jpg	03/17/06 11:19:33PM	08/09/04 02:32:37AM	08/09/04 02:31:42AM	08/09/04 02:31:42AM
14	20048823279541.jpg	03/17/06 11:19:33PM	08/09/04 02:36:30AM	08/09/04 02:35:52AM	09/03/04 03:05:19PM
15	2004882327910.jpg	03/17/06 11:19:33PM	08/09/04 02:36:37AM	08/09/04 02:35:52AM	08/09/04 02:35:52AM
16	200488232710350.jpg	03/17/06 11:19:33PM	08/09/04 02:36:45AM	08/09/04 02:35:52AM	08/09/04 02:35:52AM
17	200488232755862.jpg	03/17/06 11:19:33PM	08/09/04 02:36:50AM	08/09/04 02:35:52AM	08/09/04 02:35:52AM
18	200488232755281.jpg	03/17/06 11:19:33PM	08/09/04 02:36:54AM	08/09/04 02:35:53AM	08/09/04 02:35:53AM
19	20048823275547.jpg	03/17/06 11:19:33PM	08/09/04 02:37:00AM	08/09/04 02:35:53AM	08/09/04 02:35:53AM
20	20048823279838.jpg	03/17/06 11:19:33PM	08/09/04 02:37:21AM	08/09/04 02:37:14AM	08/09/04 02:37:21AM
21	002.jpg	03/17/06 11:19:33PM	08/09/04 02:37:45AM	08/09/04 02:37:37AM	08/09/04 02:37:45AM
22	003.jpg	03/17/06 11:19:33PM	08/09/04 02:37:49AM	08/09/04 02:37:37AM	08/09/04 02:37:49AM
23	20048823213121.jpg	03/17/06 11:19:33PM	08/09/04 02:41:14AM	08/09/04 02:40:56AM	08/09/04 02:41:14AM
24	200488232130396.jpg	03/17/06 11:19:33PM	08/09/04 02:41:22AM	08/09/04 02:40:55AM	08/09/04 02:40:55AM
25	200488232039524.jpg	03/17/06 11:19:33PM	08/09/04 02:41:28AM	08/09/04 02:40:55AM	08/09/04 02:41:28AM

Fig. 3. Image files located at *D:\bt\photo\jap\*

In addition, if the *thumbs.db* database file was analyzed, the caches of thumbnail images being displayed in the windows explorer could be obtained as well (Figure 4).

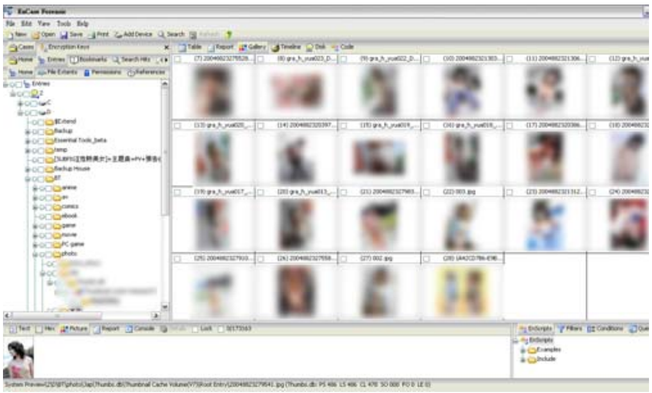
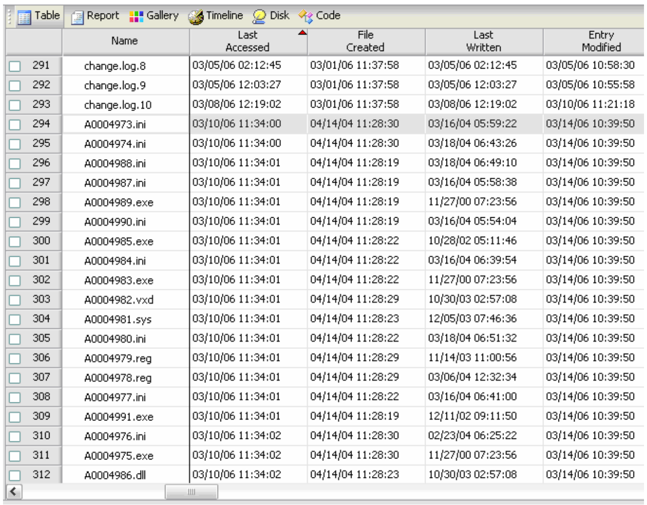


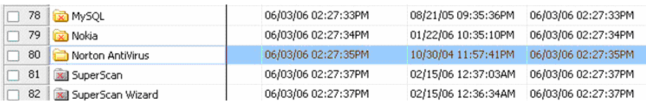
Fig. 4. Thumbnails extracted from *thumbs.db* at *D:\bt\photo\jap\*

4th Finding: With the general view of all files inside drive C, a large number of files are found to be accessed at small hours on a specific date (Figure 5). Together with the detection of a Norton anti-virus software installed in the computer (Figure 6), by applying *Rule No. 4*, the files are likely to be scanned by the anti-virus software.



	Name	Last Accessed	File Created	Last Written	Entry Modified
□ 291	change.log.8	03/05/06 02:12:45	03/01/06 11:37:58	03/05/06 02:12:45	03/05/06 10:58:30
□ 292	change.log.9	03/05/06 12:03:27	03/01/06 11:37:58	03/05/06 12:03:27	03/05/06 10:55:58
□ 293	change.log.10	03/08/06 12:19:02	03/01/06 11:37:58	03/08/06 12:19:02	03/10/06 11:21:18
□ 294	A0004973.ini	03/10/06 11:34:00	04/14/04 11:28:30	03/16/04 05:59:22	03/14/06 10:39:50
□ 295	A0004974.ini	03/10/06 11:34:00	04/14/04 11:28:30	03/18/04 06:43:26	03/14/06 10:39:50
□ 296	A0004988.ini	03/10/06 11:34:01	04/14/04 11:28:19	03/18/04 06:49:10	03/14/06 10:39:50
□ 297	A0004987.ini	03/10/06 11:34:01	04/14/04 11:28:19	03/16/04 05:58:38	03/14/06 10:39:50
□ 298	A0004989.exe	03/10/06 11:34:01	04/14/04 11:28:19	11/27/00 07:23:56	03/14/06 10:39:50
□ 299	A0004990.ini	03/10/06 11:34:01	04/14/04 11:28:19	03/16/04 05:54:04	03/14/06 10:39:50
□ 300	A0004985.exe	03/10/06 11:34:01	04/14/04 11:28:22	10/28/02 05:11:46	03/14/06 10:39:50
□ 301	A0004984.ini	03/10/06 11:34:01	04/14/04 11:28:22	03/16/04 06:39:54	03/14/06 10:39:50
□ 302	A0004983.exe	03/10/06 11:34:01	04/14/04 11:28:22	11/27/00 07:23:56	03/14/06 10:39:50
□ 303	A0004982.vxd	03/10/06 11:34:01	04/14/04 11:28:29	10/30/03 02:57:08	03/14/06 10:39:50
□ 304	A0004981.sys	03/10/06 11:34:01	04/14/04 11:28:23	12/05/03 07:46:36	03/14/06 10:39:50
□ 305	A0004980.ini	03/10/06 11:34:01	04/14/04 11:28:22	03/18/04 06:51:32	03/14/06 10:39:50
□ 306	A0004979.reg	03/10/06 11:34:01	04/14/04 11:28:29	11/14/03 11:00:56	03/14/06 10:39:50
□ 307	A0004978.reg	03/10/06 11:34:01	04/14/04 11:28:29	03/06/04 12:32:34	03/14/06 10:39:50
□ 308	A0004977.ini	03/10/06 11:34:01	04/14/04 11:28:22	03/16/04 06:41:00	03/14/06 10:39:50
□ 309	A0004991.exe	03/10/06 11:34:01	04/14/04 11:28:19	12/11/02 09:11:50	03/14/06 10:39:50
□ 310	A0004976.ini	03/10/06 11:34:02	04/14/04 11:28:30	02/23/04 06:25:22	03/14/06 10:39:50
□ 311	A0004975.exe	03/10/06 11:34:02	04/14/04 11:28:30	11/27/00 07:23:56	03/14/06 10:39:50
□ 312	A0004986.dll	03/10/06 11:34:02	04/14/04 11:28:23	10/30/03 02:57:08	03/14/06 10:39:50

Fig. 5. Files suspected to be scanned by automated scanning tool



□ 78	MySQL		06/03/06 02:27:33PM	08/21/05 09:35:36PM	06/03/06 02:27:33PM
□ 79	Nokia		06/03/06 02:27:34PM	01/22/06 10:35:10PM	06/03/06 02:27:34PM
□ 80	Norton AntiVirus		06/03/06 02:27:35PM	10/30/04 11:57:41PM	06/03/06 02:27:35PM
□ 81	SuperScan		06/03/06 02:27:37PM	02/15/06 12:37:03AM	06/03/06 02:27:37PM
□ 82	SuperScan Wizard		06/03/06 02:27:37PM	02/15/06 12:36:34AM	06/03/06 02:27:37PM

Fig. 6. Detection of Norton Anti-virus software

Assessment

According to the above findings, the user is suspected of backing up a single child pornographic image under the path *D:\backup\Documents and Settings\User\My Documents* as well as downloading and copying a number of child pornographic images to the locations *C:\download* and *D:\bt\photo\jap\*. In particular, the 'very close' *A* times in *D:\bt\photo\jap\* and the existence of the *thumbs.db* indicated that the user had previewed the images inside the folder. Though there exists an automated scanning tool which may affect the *A* times in question, it is revealed that the thumbnail preview was done after the files had been scanned.

Judging from the above, if the suspect is the sole user of the computer, there are circumstantial evidences suggesting that he should have certain degree of knowledge about the child pornography found inside his computer.

B. *Case 2: BitTorrent (BT) seeding*

In this simulated case, a computer network of two computers is used to activate the BitTorrent protocol. These computers are configured as a seeder computer *S* and a tracker server *T*, with both of them running under NTFS file system and had their system clocks set to match the time reported from the time server at *stdtime.gov.hk*.

The following actions are conducted in order to ignite the BitTorrent operation:

Action (a): A digital movie stored on an DVD optical disc was copied onto *S*; Timestamps of the digital movie file on the DVD optical disc and its copy on S are shown in Table II and Table III, respectively.

TABLE II

File name	Size (in bytes)	Creation	Last Access	Last Written	Hash Value
AVSEQ01.dat	606,891,308	20/5/01 13:22:54	-	20/5/01 13:22:54	c3ba5bb0

TABLE III

File name	Size (in bytes)	Creation	Last Access	Last Written	Hash Value
AVSEQ01.dat	606,891,308	15/1/05 23:46:09	16/1/05 23:46:09	20/5/01 13:22:54	c3ba5bb0

Action (b): A torrent file was created by using BitComet program installed at *S*; Its timestamps are shown in Table IV.

TABLE IV

File name	Size (in bytes)	Creation	Last Access	Last Written	Hash Value
AVS.torrent	90,748	16/1/05 11:46:00	16/1/05 11:46:00	16/1/05 11:46:00	d7d878f2

Action (c): The created torrent file was activated and by such *S* was connected to the configured Tracker server *T*; Table V shows the timestamp of the activated torrent file on S.

TABLE V

File name	Size (in bytes)	Creation	Last Access	Last Written	Hash Value
AVS.torrent	90,748	16/1/05 11:46:00	16/1/05 12:48:02	16/1/05 11:46:00	d7d878f2

Analytical results of the recorded *MAC* times of files at *S* in regard to the above mentioned actions are illustrated in Table VI.

TABLE VI

Action	Description	Creation	Last Access	Last Written	Matched Rule
a	Movie on DVD	20/5/01 13:22:54	-	20/5/01 13:22:54	1
a	Copied Movie onto *S*	15/1/05 23:46:09	16/1/05 23:46:09	20/5/01 13:22:54	2
b	Created torrent file at *S*	16/1/05 11:46:00	16/1/05 11:46:00	16/1/05 11:46:00	1
c	Torrent file was activated at *S*	16/1/05 11:46:00	16/1/05 12:48:02	16/1/05 11:46:00	1, 6

Assessment

According to the findings, it is evident to say that the computer *S* has performed a series of actions which rendered it to be a seeder computer in a BitTorrent network. The files *MAC* times revealed from both computers *S* and *T* also authenticated their behaviors or sequence of events happened on them. The heuristic rules are therefore concluded applicable for the simulated case.

VIII. Conclusion

We discussed here a set of rules to determine the behavioral characteristics of MAC time for files on an NTFS file system with respect to a set of commonly used operations by end users, such as copy, modify, delete, access and download. We have also validated the set of rules subjectively and extensively using a set of well designed experiments. The rules can be used by computer forensic examiners to reconstruct the crime scenes that has committed inside a computer system. We have successfully applied the rules to two simulated cases: possession of child pornographic images/videos and BitTorrent(BT) seeding. With the rules, we are able to draw the conclusion that the user of the machine should have certain knowledge of the relevant files. Since different file systems offer different MAC times behaviors, the proposed set of rules will have to be modified in order to be used in another type of file system.

Appendix

Figures for Scenario 1:

Table A1-1
Initial MAC Times

File	M	A	C
C:\abc.txt	12:02:37 02/07/06	12:02:37 02/07/06	12:02:37 02/07/06
C:\abc.jpg	12:03:01 02/07/06	12:03:01 02/07/06	12:03:01 02/07/06

Table A1-2
MAC Times after Open and View

File	M	A	C
C:\abc.txt	12:02:37 02/07/06	12:27:01 02/07/06	12:02:37 02/07/06
C:\abc.jpg	12:03:01 02/07/06	12:28:10 02/07/06	12:03:01 02/07/06

Table A1-3
MAC Times after Edit and Save

File	M	A	C
C:\abc.txt	12:55:12 02/07/06	12:55:12 02/07/06	12:02:37 02/07/06
C:\abc.jpg	12:58:03 02/07/06	12:58:03 02/07/06	12:03:01 02/07/06

Figures for Scenario 2:

Table A2-1
Initial MAC Times

File	M	A	C
C:\abc1.txt	13:00:02 02/07/06	13:00:02 02/07/06	13:00:02 02/07/06
C:\abc1.jpg	13:01:03 02/07/06	13:01:03 02/07/06	13:01:03 02/07/06

Table A2-2
MAC Times after Copy

File	M	A	C
D:\abc1.txt	13:00:02 02/07/06	13:03:10 02/07/06	13:03:10 02/07/06
D:\abc1.jpg	13:01:03 02/07/06	13:03:10 02/07/06	13:03:10 02/07/06

Figures for Scenario 3:

Table A3-1
MAC Times after Move

File	M	A	C
C:\abc1.txt	13:00:02 02/07/06	13:11:23 02/07/06	13:11:23 02/07/06
C:\abc1.jpg	13:01:03 02/07/06	13:11:28 02/07/06	13:11:28 02/07/06

Figures for Scenario 4:

TABLE A4-1
Initial MAC Times

Text File [1]	M, A, C	Image File [2]	M, A, C
1.txt [1]	13:10:03 02/07/06	a.jpg	13:15:55 02/07/06
2.txt	13:10:50 02/07/06	b.jpg	13:16:30 02/07/06
3.txt	13:11:12 02/07/06	c.jpg	13:17:12 02/07/06
4.txt	13:11:42 02/07/06	d.jpg	13:17:31 02/07/06
5.txt	13:12:04 02/07/06	e.bmp [3]	13:18:42 02/07/06
6.txt	13:13:02 02/07/06	f.bmp [4]	13:20:15 02/07/06
7.txt	13:13:45 02/07/06	g.jpg	13:20:37 02/07/06
8.txt	13:14:20 02/07/06	h.jpg	13:21:11 02/07/06
9.txt	13:14:58 02/07/06	i.jpg	13:22:05 02/07/06
10.txt	13:15:30 02/07/06	j.jpg	13:22:45 02/07/06

1. Text files are of size approximately equal to *2 KB*
2. Image files are of sizes ranging from *25KB* to *50KB*
3. *e.bmp* has the file size of *5.41MB*
4. *f.bmp* has the file size of *10.45MB*

TABLE A4-2
MAC Times after Copy

File	M	A, C	File	M	A, C
1.txt	13:10:03 02/07/06	14:10:04 02/07/06	a.jpg	13:15:55 02/07/06	14:10:22 02/07/06
2.txt	13:10:50 02/07/06	14:10:04 02/07/06	b.jpg	13:16:30 02/07/06	14:10:22 02/07/06
3.txt	13:11:12 02/07/06	14:10:04 02/07/06	c.jpg	13:17:12 02/07/06	14:10:22 02/07/06
4.txt	13:11:42 02/07/06	14:10:04 02/07/06	d.jpg	13:17:31 02/07/06	14:10:22 02/07/06
5.txt	13:12:04 02/07/06	14:10:04 02/07/06	e.bmp	13:18:42 02/07/06	14:10:23 02/07/06
6.txt	13:13:02 02/07/06	14:10:04 02/07/06	f.bmp	13:20:15 02/07/06	14:10:25 02/07/06
7.txt	13:13:45 02/07/06	14:10:04 02/07/06	g.jpg	13:20:37 02/07/06	14:10:25 02/07/06
8.txt	13:14:20 02/07/06	14:10:04 02/07/06	h.jpg	13:21:11 02/07/06	14:10:25 02/07/06
9.txt	13:14:58 02/07/06	14:10:04 02/07/06	i.jpg	13:22:05 02/07/06	14:10:25 02/07/06
10.txt	13:15:30 02/07/06	14:10:04 02/07/06	j.jpg	13:22:45 02/07/06	14:10:25 02/07/06

Figures for Scenario 5:

TABLE A5-1
MAC Times after Move

File	M	A, C	File	M	A, C
1.txt	13:10:03 02/07/06	21:50:12 02/07/06	a.jpg	13:15:55 02/07/06	21:56:27 02/07/06
2.txt	13:10:50 02/07/06	21:50:12 02/07/06	b.jpg	13:16:30 02/07/06	21:56:27 02/07/06
3.txt	13:11:12 02/07/06	21:50:12 02/07/06	c.jpg	13:17:12 02/07/06	21:56:27 02/07/06
4.txt	13:11:42 02/07/06	21:50:12 02/07/06	d.jpg	13:17:31 02/07/06	21:56:27 02/07/06
5.txt	13:12:04 02/07/06	21:50:12 02/07/06	e.bmp	13:18:42 02/07/06	21:56:28 02/07/06
6.txt	13:13:02 02/07/06	21:50:12 02/07/06	f.bmp	13:20:15 02/07/06	21:56:29 02/07/06
7.txt	13:13:45 02/07/06	21:50:12 02/07/06	g.jpg	13:20:37 02/07/06	21:56:29 02/07/06
8.txt	13:14:20 02/07/06	21:50:13 02/07/06	h.jpg	13:21:11 02/07/06	21:56:29 02/07/06
9.txt	13:14:58 02/07/06	21:50:13 02/07/06	i.jpg	13:22:05 02/07/06	21:56:29 02/07/06
10.txt	13:15:30 02/07/06	21:50:13 02/07/06	j.jpg	13:22:45 02/07/06	21:56:29 02/07/06

Figures for Scenario 6:

TABLE A6-1
Initial MAC Times

Text File [1]	M, A, C	Image File [2]	M, A, C
1a.txt [1]	14:33:11 02/07/06	a1.jpg	13:15:55 02/07/06
2a.txt	14:33:58 02/07/06	b2.jpg	13:16:30 02/07/06
3a.txt	14:34:31 02/07/06	c3.jpg	13:17:12 02/07/06
4a.txt	14:35:05 02/07/06	d4.jpg	13:17:31 02/07/06
5a.txt	14:36:13 02/07/06	e5.bmp [3]	13:18:42 02/07/06
6a.txt	14:36:47 02/07/06	f6.bmp [4]	13:20:15 02/07/06
7a.txt	14:37:45 02/07/06	g7.jpg	13:20:37 02/07/06
8a.txt	14:38:06 02/07/06	h8.jpg	13:21:11 02/07/06
9a.txt	14:38:54 02/07/06	i9.jpg	13:22:05 02/07/06
10a.txt	14:39:09 02/07/06	j10.jpg	13:22:45 02/07/06

1. Text files are of size approximately equal to *2 KB*
2. Image files are of sizes ranging from *25KB* to *50KB*
3. *e5.bmp* has the file size of *5.7MB*
4. *f6.bmp* has the file size of *10.9MB*

TABLE A6-2
MAC Times after downloading

Text File	M, A, C	Image File	M, A, C
1a.txt	23:00:53 02/07/06	a1.jpg	23:00:54 02/07/06
2a.txt	23:00:53 02/07/06	b2.jpg	23:00:54 02/07/06
3a.txt	23:00:53 02/07/06	c3.jpg	23:00:54 02/07/06
4a.txt	23:00:53 02/07/06	d4.jpg	23:00:54 02/07/06
5a.txt	23:00:53 02/07/06	e5.bmp	23:00:55 02/07/06
6a.txt	23:00:53 02/07/06	f6.bmp	23:00:57 02/07/06
7a.txt	23:00:53 02/07/06	g7.jpg	23:00:57 02/07/06
8a.txt	23:00:54 02/07/06	h8.jpg	23:00:58 02/07/06
9a.txt	23:00:54 02/07/06	i9.jpg	23:00:58 02/07/06
10a.txt	23:00:54 02/07/06	j10.jpg	23:00:58 02/07/06

Figures for Scenario 7:

TABLE A7-1
Initial MAC Times

File	M	A	C
text.zip	14:15:12 02/07/06	14:15:12 02/07/06	14:15:12 02/07/06
image.zip	14:15:58 02/07/06	14:15:58 02/07/06	14:15:58 02/07/06

TABLE A7-2
MAC Times after Copy

File	M	A	C
text.zip	14:15:12 02/07/06	14:19:53 02/07/06	14:19:53 02/07/06
image.zip	14:15:58 02/07/06	14:19:53 02/07/06	14:19:53 02/07/06

TABLE A7-3
MAC Times after Extraction

File	M	A, C	File	M	A, C
1.txt	13:10:03 02/07/06	14:21:33 02/07/06	a.jpg	13:15:55 02/07/06	14:21:41 02/07/06
2.txt	13:10:50 02/07/06	14:21:33 02/07/06	b.jpg	13:16:30 02/07/06	14:21:41 02/07/06
3.txt	13:11:12 02/07/06	14:21:33 02/07/06	c.jpg	13:17:12 02/07/06	14:21:41 02/07/06
4.txt	13:11:42 02/07/06	14:21:33 02/07/06	d.jpg	13:17:31 02/07/06	14:21:41 02/07/06
5.txt	13:12:04 02/07/06	14:21:33 02/07/06	e.bmp	13:18:42 02/07/06	14:21:42 02/07/06
6.txt	13:13:02 02/07/06	14:21:33 02/07/06	f.bmp	13:20:15 02/07/06	14:21:43 02/07/06
7.txt	13:13:45 02/07/06	14:21:33 02/07/06	g.jpg	13:20:37 02/07/06	14:21:43 02/07/06
8.txt	13:14:20 02/07/06	14:21:34 02/07/06	h.jpg	13:21:11 02/07/06	14:21:43 02/07/06
9.txt	13:14:58 02/07/06	14:21:34 02/07/06	i.jpg	13:22:05 02/07/06	14:21:43 02/07/06
10.txt	13:15:30 02/07/06	14:21:34 02/07/06	j.jpg	13:22:45 02/07/06	14:21:43 02/07/06

Figures for Scenario 10:

TABLE A10-1
MAC Times after Random Accesses

File	M	A	C
a.txt	22:01:37 04/07/06	11:22:37 05/07/06	19:31:42 04/07/06
b.txt	20:11:14 04/07/06	12:03:01 05/07/06	19:32:15 04/07/06
c.txt	19:32:59 04/07/06	22:19:11 04/07/06	19:32:59 04/07/06
d.txt	19:34:10 04/07/06	10:32:56 05/07/06	19:34:10 04/07/06
e.txt	10:30:11 05/07/06	13:05:39 05/07/06	19:34:21 04/07/06
f.txt	19:35:02 04/07/06	22:02:31 04/07/06	19:35:02 04/07/06
g.txt	23:15:20 04/07/06	23:35:21 04/07/06	19:36:03 04/07/06
h.txt	19:45:11 04/07/06	23:38:10 04/07/06	19:36:45 04/07/06
i.txt	19:37:30 04/07/06	12:11:45 05/07/06	19:37:30 04/07/06
j.txt	10:32:39 05/07/06	12:10:03 05/07/06	19:38:22 04/07/06

REFERENCES

[1] Frank Y.W. Law, ‘Methodology of Event Analysis in Computer Forensics Investigation’, Master course project paper, The University of Hong Kong, August 2006.

[2] D. Brian, H. Eugene, ‘Defining event reconstruction of a digital crime scene’, Journal of Forensic Sciences 2004.

[3] C. Boyd, P. Forster, ‘Time and date issues in forensic computing – a case study’, Digital Investigation 2004, 1:18-23.

[4] E. Casey, ‘Digital Evidence and Computer Crime’, London: Academic Press, 2001

[5] E. Casey, ‘Uncertainty and Loss in Digital Evidence’, International Journal on Digital Evidence, Summer 2002, vol 1:2.

[6] H. Lee, T. Palmbach, M. Miller. ‘Henry Lee’s crime scene handbook’, London: Academic Press, 2001

[7] W. Malcom, ‘Unification of relative time frames of digital forensics’, Digital Investigation (2004) 1, 225-239.

[8] M. Vatis, ‘Law Enforcement Tools and technologies for Investigating Cyber Attack’, Dartmouth College, 2002

[9] MAC times, Wikipedia, available at http://en.wikipedia.org/wiki/MAC_times