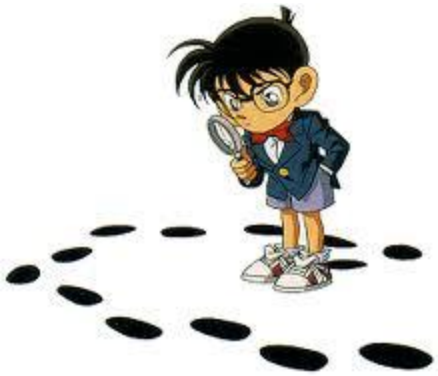
The Rules of Time on NTFS File System

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



Presented By:

Muhammad Naseer Ali Bajwa

February 17, 2013

Curtain Raiser

1. Introduction
2. Proposed Approach
3. Observations and Corollaries
4. Experiments and Findings
5. Factors Affecting MAC Analysis
6. Case Study
7. Conclusion

1. Introduction

- PREVIOUSLY, computer forensics was thought to be all about locating and retrieving digital data.

- CURRENTLY, it has advanced to finding cause and correlation of the revealed data

- A step towards Event Reconstruction

1. Introduction

(Cont.)

- Event Reconstruction
  - Identifies the cause of the relevant data
  - Establishes event sequence in the examined system

1. Introduction

(Cont.)

- Temporal Time Analysis
  - Timestamps of digital files could be very useful for event reconstruction
  - Involves Modify, Access, Create (MAC) times
  - Not evidentially authentic enough, on its own, to help draw any conclusion.
  - Difficult to know if a file was accessed by human or software

1. Introduction

(Cont.)

- NTFS File System
  - First introduced in 1993 in Windows NT
  - An upgrade of File Allocation Table(FAT)
  - Has extended support for metadata
  - Improved performance
  - Better reliability and security
  - Uses File System Journaling

2. Proposed Approach

- Exploits specific patterns hidden in metadata to explain certain phenomenon or action
- Shifts focus from dissecting the files' MAC times to interpreting the available information
- Consolidates heuristics with the essence of MAC times based on observation and studies of temporal analysis

3. Observations and Corollaries

- **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 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.*

3. Observations and Corollaries

(Cont.)

- **Observations:**
  - Moving/Copying a file within the same partition does not change M time and C time.
  - Moving/Copying a file to a different partition causes M time before C time.
- **Rule 2:**
  - *When M time is before C time, the file has been copied from one system to the same/another system or moved from one partition to another partition.*

3. Observations and Corollaries

(Cont.)

- **Observation:**
  - Copying or Moving bunch of files to the same folder in a single operation result in very close C times.
- **Rule 3:**
  - *In a folder, if files' M times are before C times and the files have "very close" C times, the files have been*
    - *copied from one system to the same or another system in a batch*
    - *moved from one partition to another partition in a batch*
    - *extracted from a compressed file.*

3. Observations and Corollaries

(Cont.)

- **Observation:**
  - The feasibility of causing large number of files having “close” access times dictates that the action is initiated by machine/software.
- **Rule 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.*

3. Observations and Corollaries

(Cont.)

- **Observation:**
  - The thumbnail preview of multimedia files is very convenient for ordinary users to readily identify the files they want.
  - A folder having multi-media files with “close” access times suggests that the files are previewed by some tool.
- **Rule 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.*

3. Observations and Corollaries

(Cont.)

- **Observation:**
  - When files are accessed randomly by a user, no particular pattern exists in Files' Access time in a folder

- **Rule 6:**
  - *When files within a folder have "scattered" A times, it is highly likely that the files are accessed individually.*

3. Observations and Corollaries

(Cont.)

- **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
- **Rule 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.*

4. Experiments and Findings

1. File Creation / File Access

– Corroborates with Rule 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

4. Experiments and Findings

(Cont.)

2. Copying/Moving Files

– Corroborates with Rule 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

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

4. Experiments and Findings

(Cont.)

3. Batch Process: Copying Files

– Corroborates with Rule 3

TABLE A4-1
Initial MAC Times

Text File [1]	M, A, C	Image File [2]	M, A, C
1.txt	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*

4. Experiments and Findings

(Cont.)

3. Batch Process: Copying Files

– Corroborates with Rule 3

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

4. Experiments and Findings

(Cont.)

4. Batch Process: Moving Files

– Corroborates with Rule 3

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

4. Experiments and Findings

(Cont.)

5. Batch Process: Downloading Files

– Corroborates with Rule 7

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*

4. Experiments and Findings

(Cont.)

5. Batch Process: Downloading Files

– Corroborates with Rule 7

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

4. Experiments and Findings

(Cont.)

6. Extracting Files from an archive

– Corroborates with Rule 3

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

4. Experiments and Findings

(Cont.)

6. Extracting Files from an archive

– Corroborates with Rule 3

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

4. Experiments and Findings

(Cont.)

7. Execution of Automated Scanning Tool

– Corroborates with Rule 4

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

4. Experiments and Findings

(Cont.)

8. Preview of Image/Video Files using 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.

4. Experiments and Findings

(Cont.)

8. Preview of Image/Video Files using Windows File Explorer

- **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.

4. Experiments and Findings

(Cont.)

9. Individual Access to Files in the same folder:

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

5. Factors Affecting MAC Analysis

- Due Care in Retrieving MAC Time
- BIOS and System Clock Settings
- Multi-User Systems
- Disabling of LAU in the System
- Automated Scanning Tools
- File Attribute Manipulation Program

6. Case Study

- A computer simulating the following behaviors 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.

6. Case Study

(Cont.)

- **Finding 1:**

Table | Report | Gallery | Timeline | Disk | Code

	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*

6. Case Study

(Cont.)

- **Finding 2:**

	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				

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

6. Case Study

(Cont.)

- **Finding 3:**

Table | Report | Gallery | Timeline | Disk | Code

	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*

6. Case Study

(Cont.)

- **Finding 4:**

Table | Report | Gallery | Timeline | Disk | Code

	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

6. Case Study

(Cont.)

- **Assessment**
  - The suspect backed up a single child pornographic image under the path

    D:\backup\Documents and Settings\User\My Documents
  - The user downloaded and copied a number of images to the locations

    C:\download and *D:\bt\photo\jap*.
  - 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.

7. Conclusion

- The paper discussed a set of rules to determine the behavioral characteristics of MAC times for files on an NTFS file system with respect to a set of commonly used operations by end users.
- The set of rules are validated subjectively and extensively using a set of well designed experiments. T
- The rules can be used by computer forensic examiners to reconstruct the crime scenes that has committed inside a computer system.
- With the rules, the investigator can draw the conclusion whether the user of the machine had any 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.

Any Question?