

Temporal Analysis in Digital Evidence

Frank LAW
Department of Computer Science
University of Hong Kong

Consider the situation

- An investigator raid a premises and locate a male who is suspected to have downloaded child pornography from the Internet
- Onsite examination revealed a number of child pornographic images inside the suspect's computer

Cont...

- The suspect was arrested and explained that he has no knowledge on the existence of the images. However, he admitted that he is the user of that computer.
- Is the evidences enough to prove the case in court?

Questions

- Can the digital evidences tell us more on:
 - What have done by the computer user?
 - When the images were downloaded?
 - Have the images be viewed by the computer user?
 - Do the computer user has knowledge on the existence of the images?

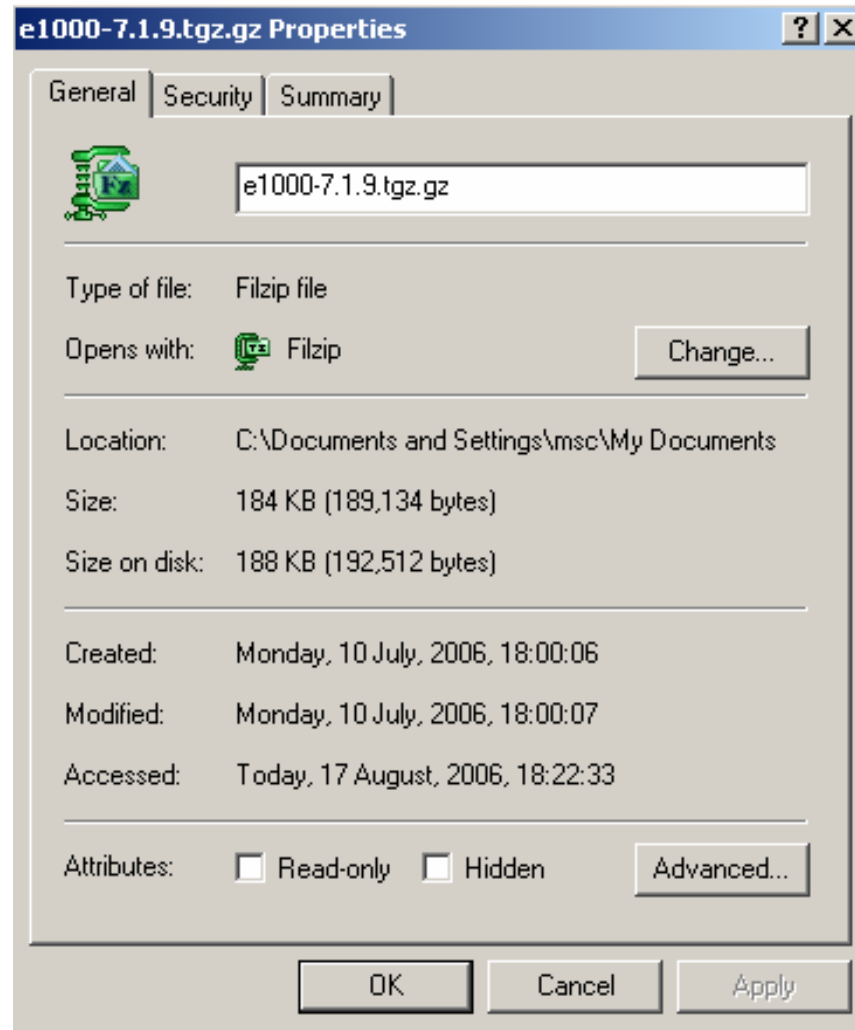
Solution – Temporal Analysis



Content

- What are digital timestamp?
- Approach in studying digital timestamp
- Rules for temporal analysis
- Applying rules to simulated cases
- Conclusion

File timestamp



What are File timestamp?

- “Modified time (M)” - time when the file was last opened, edited and then saved. Sometimes called “Write time”.
- “Accessed time (A)” - the last time any activity was taken on the file
- “Created time (C)” - time when the file was created at that location on the disk

File timestamp properties

- File timestamp generally has two parts, the date part (year (YY), month (MM), and day (DD)) and the time part (hour (hh), minute (mm), second (ss))

<i>file system</i>	<i>Resolution</i>	<i>earliest time stamp</i>	<i>latest time stamp</i>
FAT/FAT 32	2s/1d/10ms	1980-01-01 00:00:00 <i>local</i>	2107-12-31 23:59:58 <i>local</i>
NTFS	100 ns	1601-01-01 00:00:01 <i>UTC</i>	
Unix/Linux	1 s	1970-01-01 00:00:00 <i>UTC</i>	

File timestamp properties

- In FAT/FAT32 (e.g. Windows 98, USB drive), the A time is updated most frequently on every access to the file.

File timestamp properties

- However, NTFS (e.g. Win2000, WinXP) updates A time of the file if the current A time in memory differs by more than an hour from the A time stored on disk.
- However, if other file attribute, e.g. M time, is updated, the one-hour rule is neglected and A time will be updated as well.

Temporal Analysis

- From the investigative point of view, MAC times were influenced and created by human through machine process.
- There should be specific patterns or trails available for investigator to explain certain phenomena or actions that had been carried out by the user (Casey 2002).

Temporal Analysis

- The traditional approach on temporal analysis is tedious and the result is often inconclusive (Boyd and Froster 2004).

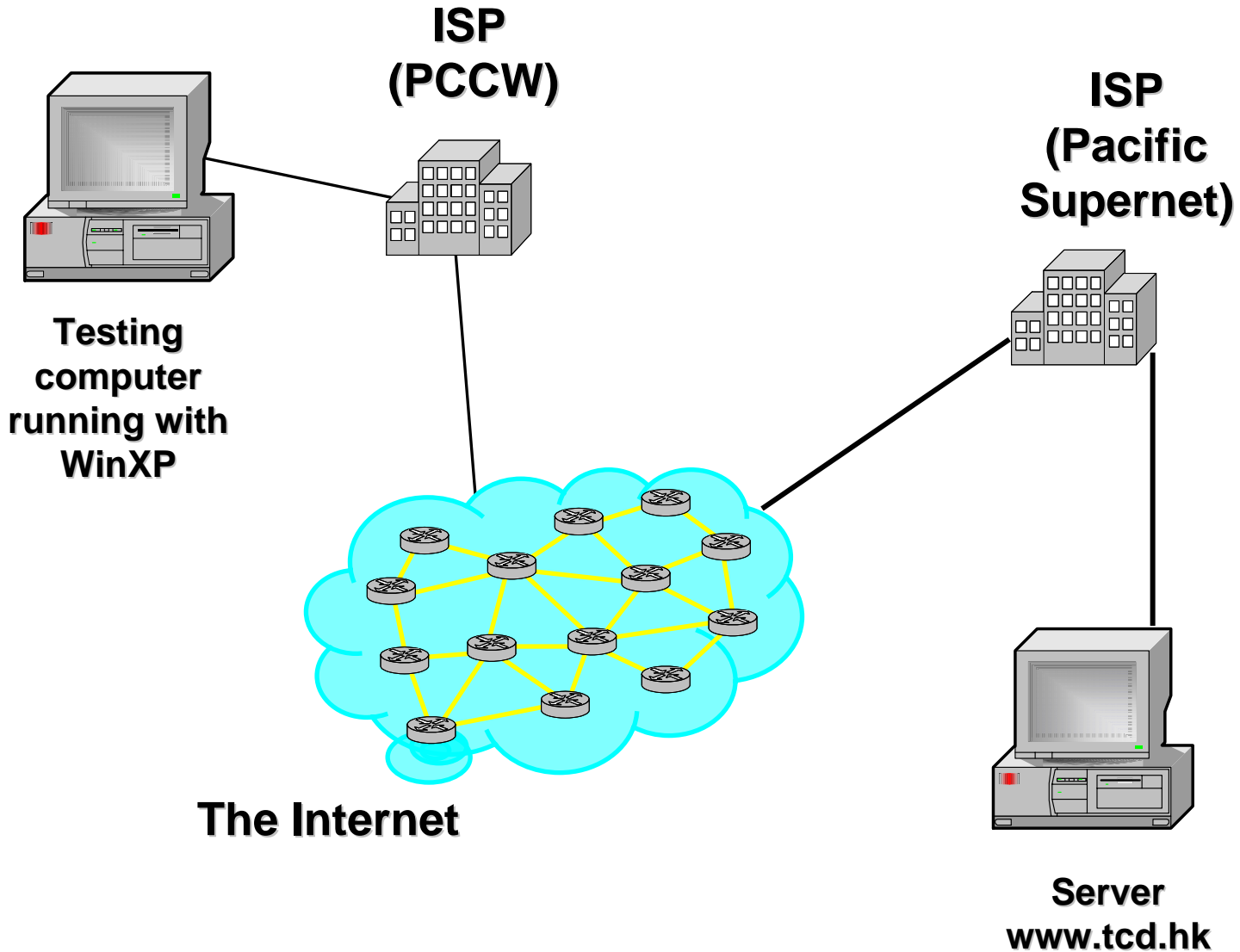
Our Approach

- New heuristic approach:-
 - Streamline digital forensic investigation process
 - Rules to assist computer forensic examiner to analyze digital events

Our Approach

- Analyze digital timestamp on NTFS (Windows XP) operating system
- Events and phenomena are studied for projecting heuristic rules in temporal analysis

Experiments



Rules for temporal analysis

Rule One

- *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.*

Observations

- Copying file within the same partition (volume). What happened to the time?
- How about copy the file to the other partition?

Observations

- Similar results are obtained when moving a file from one location to another location through the command “move” at command prompt.

Rule Two

- *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.*

Observations

- 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 observed during file(s) decompression.

Observations

- The ‘very close’ creation times are supposed to be generated by machine actions.
- The digital states of the created files may reveal some relevant human actions, e.g. backup.

Rule Three

- *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*

Observations

- Very often, large number of files inside a computer have very close access time. Why?

Rule Four

- *When a large number of files with “close” A times are found inside the hard drive, the files are likely to be scanned by some tool, e.g. anti-virus software or file searching tool.*

Observations

- 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 Five

- *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.*

Observations

- As a complement of Rule No. 4 & 5, inference is drawn when no specific patterns of MAC times could be observed.

Rule Six

- *When files within a folder have “scattered” A times, it is highly likely that the files are accessed individually.*

Observations

- How about downloading a file from the Internet? What is the MAC time?

Observations

- In a folder, if a batch of files have $M=C$ and C times very close, these files are probably downloaded from another system through network, e.g. Internet.
- Unlikely for a regular computer user to successively create a batch of files, e.g. multi-media files, within a very small time frame.

Rule Seven

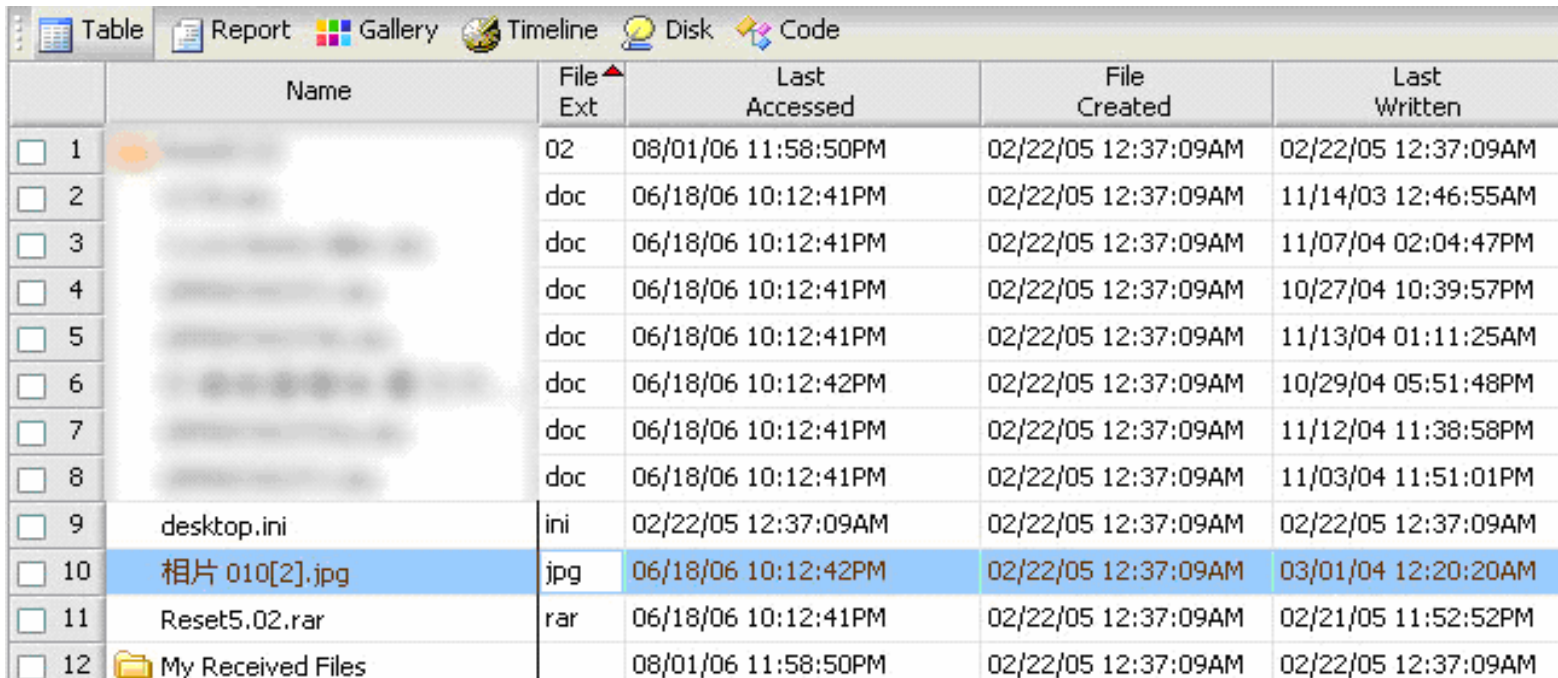
- *In a folder, if files' M times are equal to C times and the files have “very close” C (M) times, the files may have been downloaded in a batch from another system over the network.*

Applying on simulated cases

- Possession of Child Pornography
- BT Case

Possession of Child Pornography

- *D:\backup\Documents and Settings\User\My Documents*
- Rule two – A “backup” of child porn file



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

Batch download of files

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

- Files recovered from C:\downloads
- Rule Seven - likely to be downloaded in batch
- Rule One - intact

Preview of files

	Name	Last Accessed	File Created	Last Written	Entry Modified	
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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

- Existence of thumbs.db at *D:\bt\photo\jap*
- Rule Three – Backup files
- Rule Five – Thumbnails preview

File scanned by Anti-virus software

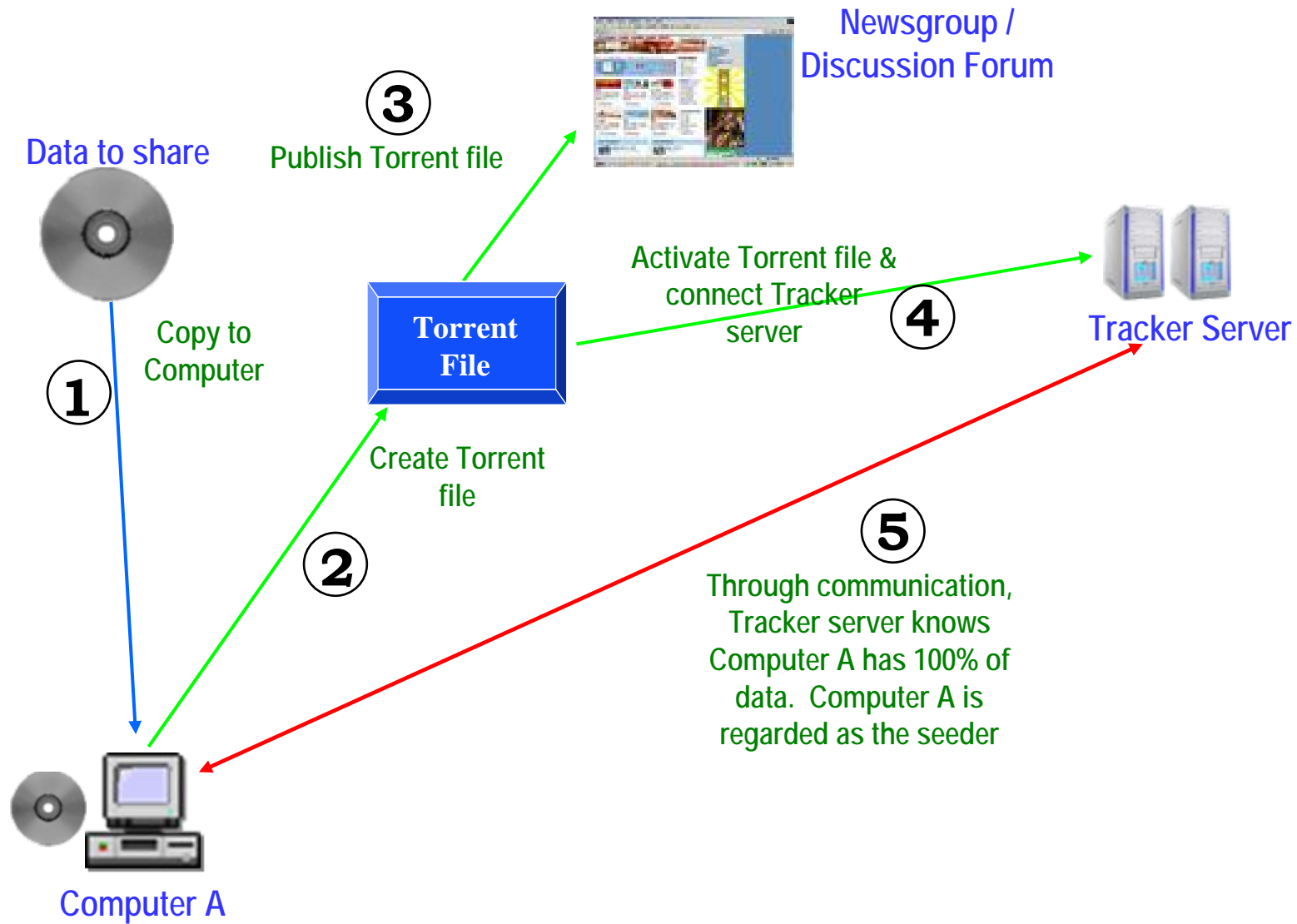
	Name	Last Accessed	File Created	Last Written	Entry Modified
<input type="checkbox"/>	291	change.log.8	03/01/06 11:37:58	03/05/06 02:12:45	03/05/06 10:58:30
<input type="checkbox"/>	292	change.log.9	03/01/06 11:37:58	03/05/06 12:03:27	03/05/06 10:55:58
<input type="checkbox"/>	293	change.log.10	03/01/06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

Rule Four –
Scanned
by Anti-
virus
software

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

Overall Picture?

BT Operation



BT Operation

1. Loading films onto his computer
2. Creating the torrent files
3. Publishing the torrent files on newsgroup so that others know where to download them
4. Activating the torrent files
5. Keeping his computer connected to enable downloading by others

Bitorrent Case

Action	Creation	Access	Modification	Rule
Movie on DVD	20/5/01 13:22:54	-	20/5/01 13:22:54	1
Copied Movie	15/1/05 23:46:09	16/1/05 23:46:09	20/5/01 13:22:54	2
Created torrent file	16/1/05 11:46:00	16/1/05 11:46:00	16/1/05 11:46:00	1
Activation of Torrent File	16/1/05 11:46:00	16/1/05 12:48:02	16/1/05 11:46:00	1, 6

Overall Picture?

Factors that may affect analysis

- Due care in retrieving MAC times
- BIOS and System Clock Setting
- Multi-user System
- Disabling of “Last Access Update” in the system
- File attribute manipulation program, e.g. AttributeMagic

Conclusion

- File digital timestamps were influenced and created by human through machine process
- There should be specific patterns or trails available for explaining certain phenomena or actions that had been carried out by the user

Conclusion

- Temporal Analysis study the behavior of the user via the analysis of digital timestamps
- The heuristic rules provide a swift approach to assist temporal analysis
- With the rules, we are able to draw the conclusion that the user of the machine should have certain knowledge of the relevant files, which may be useful if proving the “intent” of the user in some cases.

Question

