Temporal Analysis in Digital Evidence

Frank LAW
Department of Computer Science
University of Hong Kong
Consider the situation

- An investigator raided 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.
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))

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

ISP (PCCW)

ISP (Pacific Supernet)

Testing computer running with WinXP

The Internet

Server

www.tcd.hk
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

- \textit{D:\backup\Documents and Settings\User\My Documents}\n
- Rule two – A “backup” of child porn file
Batch download of files

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

- Existence of thumbs.db at D:\bt\photo\jap\n- Rule Three – Backup files
- Rule Five – Thumbnails preview
Rule Four – Scanned by Anti-virus software
Overall Picture?
BT Operation

1. Copy to Computer
2. Create Torrent file
3. Publish Torrent file
4. Activate Torrent file & connect Tracker server
5. Through communication, Tracker server knows Computer A has 100% of data. Computer A is regarded as the seeder
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

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

• 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