MAC Times, Mac Times, and More

Lee Whitfield, Subject Matter Expert, The SANS Institute
Lee Whitfield

Subject Matter Expert at the SANS Institute

Mac Disciple

Lost over 60 lbs in the last year (I’m proud of that so I’m going to boast about it)

Most photoshopped forensicator in history (Brian and J are dead to me)
Windows Time Stamps
Windows Forensic Analysis
Poster
You Can't Protect What You Don't Know About
digital-forensics.sans.org

Finding Unknown Malware - Step-By-Step

1. Run Microsoft ScanDisk
2. Check Event Viewer
3. Use a Malware Scanner
4. Use a Virus Total
5. Use a Malware Analysis Tool

Windows Time Rules
Setting

1. Configure System Time
2. Check Network Time Protocol
3. Use a Time同步 Tool
4. Use a Time synchronization Service

Digital Forensic Incident Response

SANS DFIR
Windows Time Rules

$STDFINFO

$FILENAME

Analysis

About

Making Sense - Step 1 - Step 2...
WTF?
Uh oh!
WTAF?
<table>
<thead>
<tr>
<th>Filename</th>
<th>Created</th>
<th>Last Written</th>
<th>Accessed</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>TakenFile2.docx</td>
<td>6/12/2012</td>
<td>6/17/2012</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
</tr>
<tr>
<td>TakenFile3.docx</td>
<td>1/7/2011</td>
<td>1/7/2011</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
</tr>
</tbody>
</table>
Man’s External Hard Drive (FILENAME Dates Only)

<table>
<thead>
<tr>
<th>Filename</th>
<th>Created</th>
<th>Last Written</th>
<th>Accessed</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>TakenFile1.docx</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
</tr>
<tr>
<td>TakenFile2.docx</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
</tr>
<tr>
<td>TakenFile3.docx</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
</tr>
<tr>
<td>TakenFile4.docx</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
</tr>
<tr>
<td>TakenFile5.docx</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
<td>12/12/2016</td>
</tr>
</tbody>
</table>
# Windows Time Rules

## $STDINFO

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Modified - No Change</td>
<td>Modified - No Change</td>
<td>Modified - No Change</td>
<td>Modified - No Change</td>
<td>Modified - No Change</td>
<td>Modified - Change</td>
<td>Modified - Change</td>
<td>Modified - No Change</td>
</tr>
<tr>
<td>Creation - No Change</td>
<td>Creation - No Change</td>
<td>Creation - No Change</td>
<td>Creation - No Change</td>
<td>Creation - No Change</td>
<td>Creation - No Change</td>
<td>Creation - No Change</td>
<td>Creation - No Change</td>
</tr>
</tbody>
</table>

## $FILENAME

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Modified - No Change</td>
<td>Modified - Change</td>
<td>Modified - Change</td>
<td>Modified - Change</td>
<td>Modified - Change</td>
<td>Modified - Change</td>
<td>Modified - Change</td>
<td>Modified - Change</td>
</tr>
<tr>
<td>Creation - No Change</td>
<td>Creation - Change</td>
<td>Creation - No Change</td>
<td>Creation - Change</td>
<td>Creation - No Change</td>
<td>Creation - No Change</td>
<td>Creation - No Change</td>
<td>Creation - No Change</td>
</tr>
<tr>
<td>File Deletion</td>
<td>Modified – No Change</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access – No Change</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creation – No Change</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metadata – No Change</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Windows Time Rules**

**SSDINFO**

<table>
<thead>
<tr>
<th>File Deletion</th>
<th>Modified – No Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access – No Change</td>
<td></td>
</tr>
<tr>
<td>Creation – No Change</td>
<td></td>
</tr>
<tr>
<td>Metadata – No Change</td>
<td></td>
</tr>
</tbody>
</table>
### External Hard Drive

<table>
<thead>
<tr>
<th>Filename</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>TakenFile1.docx</td>
<td>12/12/2016 19:31:47</td>
</tr>
<tr>
<td>TakenFile2.docx</td>
<td>12/12/2016 19:31:47</td>
</tr>
<tr>
<td>TakenFile3.docx</td>
<td>12/12/2016 19:31:48</td>
</tr>
<tr>
<td>TakenFile4.docx</td>
<td>12/12/2016 19:31:48</td>
</tr>
<tr>
<td>TakenFile5.docx</td>
<td>12/12/2016 19:31:49</td>
</tr>
</tbody>
</table>

### Former Company Laptop

**$USNJRNRL**

<table>
<thead>
<tr>
<th>Filename</th>
<th>Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>TakenFile1.docx</td>
<td>12/12/2016 19:31:47</td>
</tr>
<tr>
<td>TakenFile2.docx</td>
<td>12/12/2016 19:31:47</td>
</tr>
<tr>
<td>TakenFile3.docx</td>
<td>12/12/2016 19:31:48</td>
</tr>
<tr>
<td>TakenFile4.docx</td>
<td>12/12/2016 19:31:48</td>
</tr>
<tr>
<td>TakenFile5.docx</td>
<td>12/12/2016 19:31:49</td>
</tr>
</tbody>
</table>
A Recent Case – Concluded

- No evidence of “specialist” copying software installed or run on the computer
- Evidence clearly shows that the files were cut and paste
- Man’s new employer is no longer suspected of aiding in copying of other company’s confidential data
- Forensic expert came to the wrong conclusion
Mac Time Stamps
MacOS (HFS+) Time Stamps

MacOS (HFS+) contains time stamps in the Catalog (Apple version of FAT or $MFT):

- Created
- Modified (Last Written)
- Accessed
- Record Change
- Added Date

HFS+ 32-bit Values

Unix 32-bit Value (Seriously Apple?)
HFS+ File Creation
HFS+ File Modification
HFS+ File Duplication
HFS+ Volume Move
Copy / Volume File Move – HFS+ to FAT

- Created – Inherited From Original
- Last Written – Inherited From Original
- Accessed – Date (Time) of Copy
Copy / Volume File Move – FAT to HFS+

- Created – Inherited From Original
- Modified (Last Written) – Inherited From Original
- Accessed – Time of Copy
- Record Change – Time of Copy
- Added Date – Time of Copy
Copy / Volume File Move – Metadata Files

Each file copied from HFS+ to FAT has an accompanying “._” file.

E.g. File “picture.jpg”, copied from HFS+ to FAT will result in “picture.jpg” and “._picture.jpg”

Time stamps for the “._” metadata files are updated as follows

• Created – Time of Copy
• Last Written – Time of Copy
• Accessed – Time of Copy
Copy / Volume File Move – NTFS to HFS+

- Created – Inherited From Original
- Modified (Last Written) – Inherited From Original
- Accessed – Time of Copy
- Record Change – Time of Copy
- Added Date – Time of Copy
Copy / Volume File Move – HFS+ to NTFS

- Created (SIA) – Inherited From Original
- Last Written (SIA) – Inherited From Original
- Accessed (SIA) – Time of Copy
- Metadata Change (SIA) – Time of Copy
- Created (FILETIME) – Time of Copy
- Last Written (FILETIME) – Time of Copy
- Accessed (FILETIME) – Time of Copy
- Metadata Change (FILETIME) – Time of Copy
Defining File Access
Defining File Access – File Used
Spotlight Times – Modified Arrays

```java
kMDItemUserModifiedDate = (  
  "2016-10-17 13:29:40 +0000",  
  "2016-10-17 17:27:34 +0000",  
  "2016-10-17 18:40:35 +0000"
)
kMDItemUserModifiedUserHandle = (  
  501,  
  501,  
  501
)```
Spotlight Times – Created Arrays (?)

```python
kMDItemUserCreatedDate = (
"2016-10-06 20:23:16 +0000",
"2016-10-07 16:44:41 +0000"
)

kMDItemUserCreatedUserHandle = (501, 501)
```
Main Points

• Know your file times and how they are updated.
• MAC times are NOT UPDATED on deletion.
• Use the guides if a set of file times seem confusing.
• For MacOS devices Access doesn’t necessarily mean Accessed.
• Use Spotlight to its full investigative advantage.
• Don’t twist and bend the facts to make them fit your opinion. Let the facts speak for themselves.