A Forensically Robust Method For Acquisition Of iCloud Data

By

Kurt Oestreicher

Presented At

The Digital Forensic Research Conference

DFRWS 2014 USA Denver, CO (Aug 3rd - 6th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

A forensically robust method for acquisition of iCloud data

Kurt Oestreicher

Champlain College

Background

- Data stored on cloud services increasingly important to forensic investigations
- As of June 2013:
  - 320 million user accounts
  - 900 billion iMessages
  - 125 billion photo uploads (Kahn, 2013)
- With introduction of OS X 10.9 Mavericks, Apple continues to expand the capabilities of its cloud service

iCloud Offerings

- Synchronization of contacts, calendars, email, notes, and reminders across devices as well as access the data through the iCloud.com web interface.
- Backups of devices to iCloud, including music, apps, books, Camera Roll (photos and videos), device settings, and app data.
- iWork documents can be stored in iCloud and pushed to all devices. These documents can now be edited through the iCloud.com web interface.
- Third party developers that utilize the iCloud Storage API can allow files from their applications to be stored in iCloud
- If enabled, Photostream can automatically upload up to 1,000 photos from the user's device for storage and synchronization across platforms

Related Research

- Recent research examined retrieval of files and metadata stored on cloud services of Dropbox, Google Drive, and Microsoft SkyDrive.
- Results of this research indicated that, while MD5 values remained unchanged, the timestamp metadata was unreliable (Quick and Choo, 2013).

Research Problem:

Create a forensically robust method for acquisition of iCloud data

- Method needs to be developed to download iCloud data to examination computer
- Integrity of acquired data must be verified
- iCloud and Mavericks updates changed many of the data structures and locations in the file system.

Research Questions

- Where are the iCloud-synched files located on the operating system ?
- Are the files downloaded during the acquisition process identical to the original files ?
- Are the MD5 hash values identical ?
- If the values are different, compare the two files to attempt to establish what has changed.
- Has the timestamp metadata been changed ?
- If the metadata has been changed is it forensically significant ?

Legal Considerations

- Apple's data storage centers are located in multiple jurisdictions, creating complications for investigators seeking authorization to access this data.
- This research does not address these concerns and the assumption is made that all legal and jurisdictional authorities have been obtained prior to accessing cloud data.

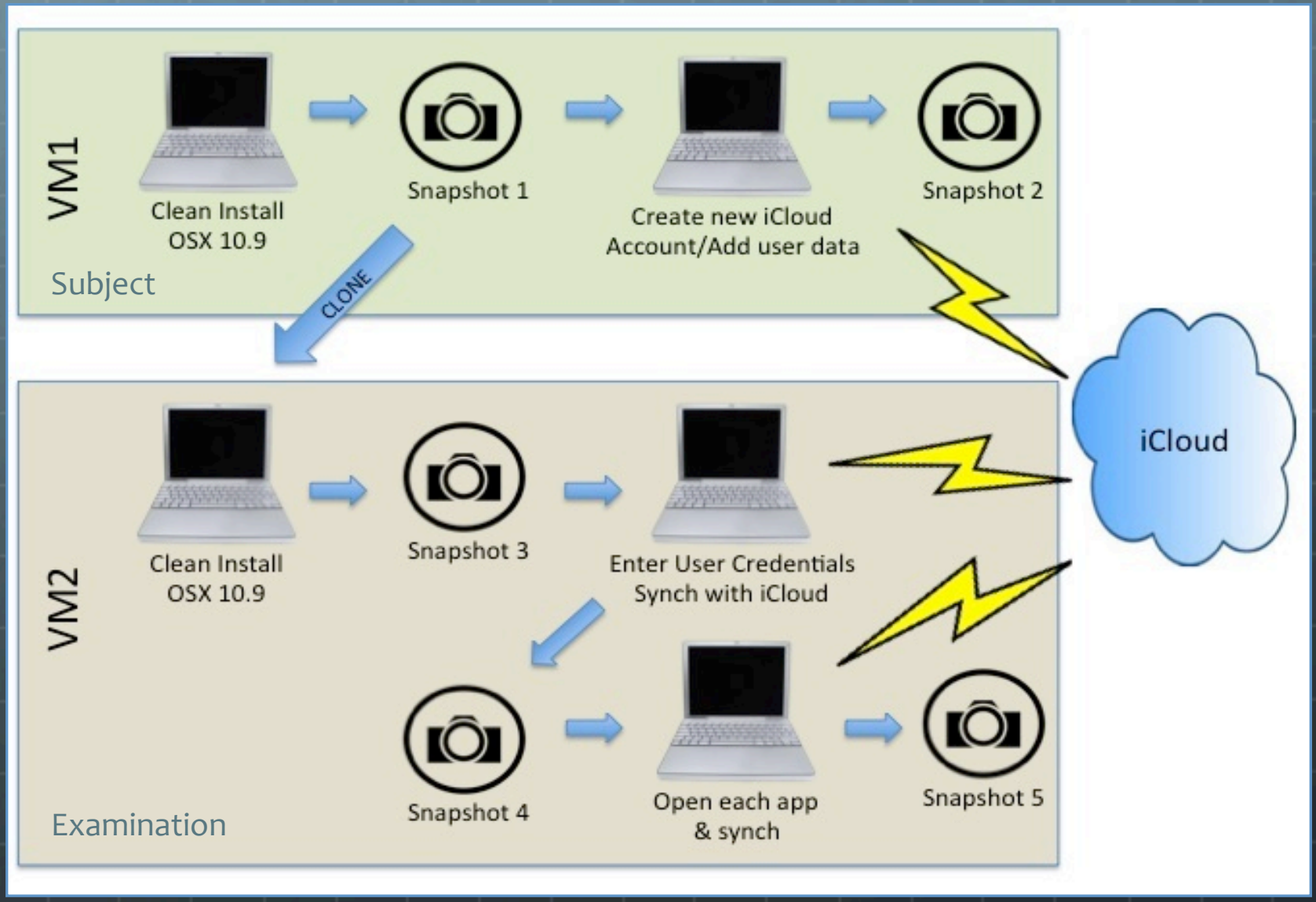
Methodology

- VMWare Fusion used to create two identical virtual machines representing subject computer and examination computer.
- Clean install of Mac OS X 10.9 along with iPhoto, Pages, Numbers, and Keynote applications.
- New iCloud account established, new iCloud data created on subject machine and synched with service.
- Snapshots taken at various times to locate iCloud artifacts on OS.
- Examination virtual machine used to synch newly created content.

Application Data Examined

Pre-installed	Non Pre-installed
Contacts	iPhoto
Mail	Pages
Calendar	Numbers
Reminders	Keynote
Safari	

VM Configuration



Initial Data Load

Application	Action
Contacts v.8.0 (1365)	New contact created with name and phone number
Mail v.7.0 (1822)	New email created, addressed to sender, and sent
Calendar v.7.0 (1835)	New event created
Reminders v.2.0 (187)	New reminder created
Safari v.7.0 (9537.71)	Safari web browser opened, typed URL: publicdomanpictures.net entered, page bookmarked, right-click on photo and saved to iPhoto.
iPhoto v.9.5.1 (902.17)	Automatically opened from Safari, downloaded picture selected and dragged to Photo Stream menu item.
Pages v.5.0.1 (1478)	New Pages document created and saved to iCloud
Numbers v.3.0.1 (1483)	New Numbers document created and saved to iCloud
Keynote v.6.0.1 (1486)	New Keynote document created and saved to iCloud.

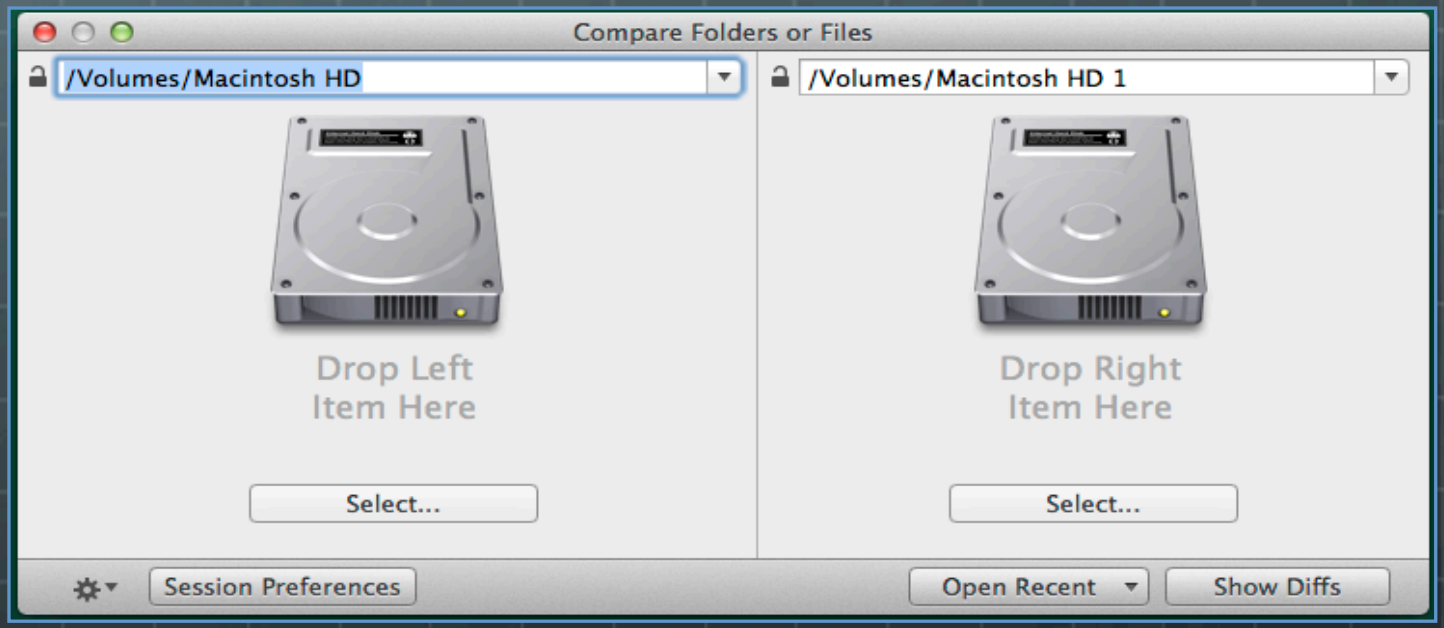
Data Collection

- Since live acquisition, virtual machine window was video recorded using screen capture software: Voila v.3.6
- Exam machine started, snapshot taken
- Exam machine logged into iCloud
- Some apps do not synch until opened so each application was opened and data allowed to synch.
- Virtual machine shutdown and snapshot taken.

Locate Artifacts

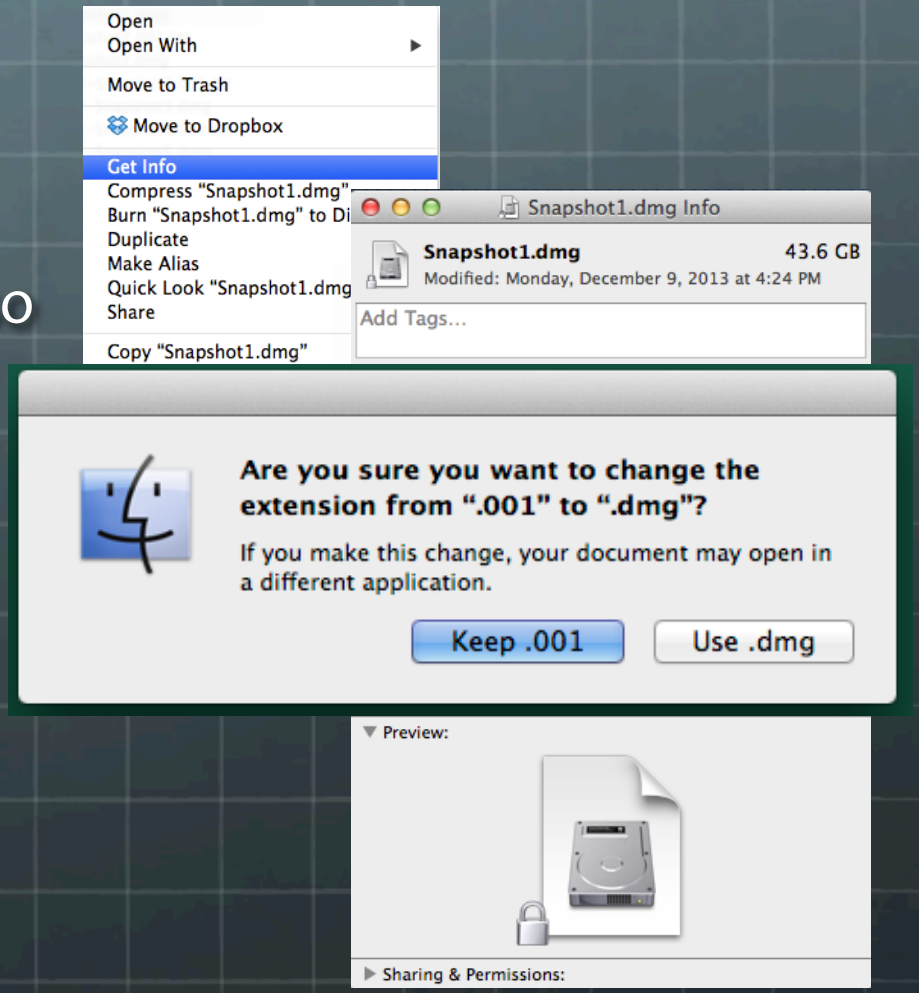
VisualDiffer v.1.5.7 used to take two volumes and compare based on file timestamps and sizes to determine changes between snapshots.

Problem: *VMWare Fusion snapshots stored as .vmdk. VisualDiffer requires images to be mounted.*

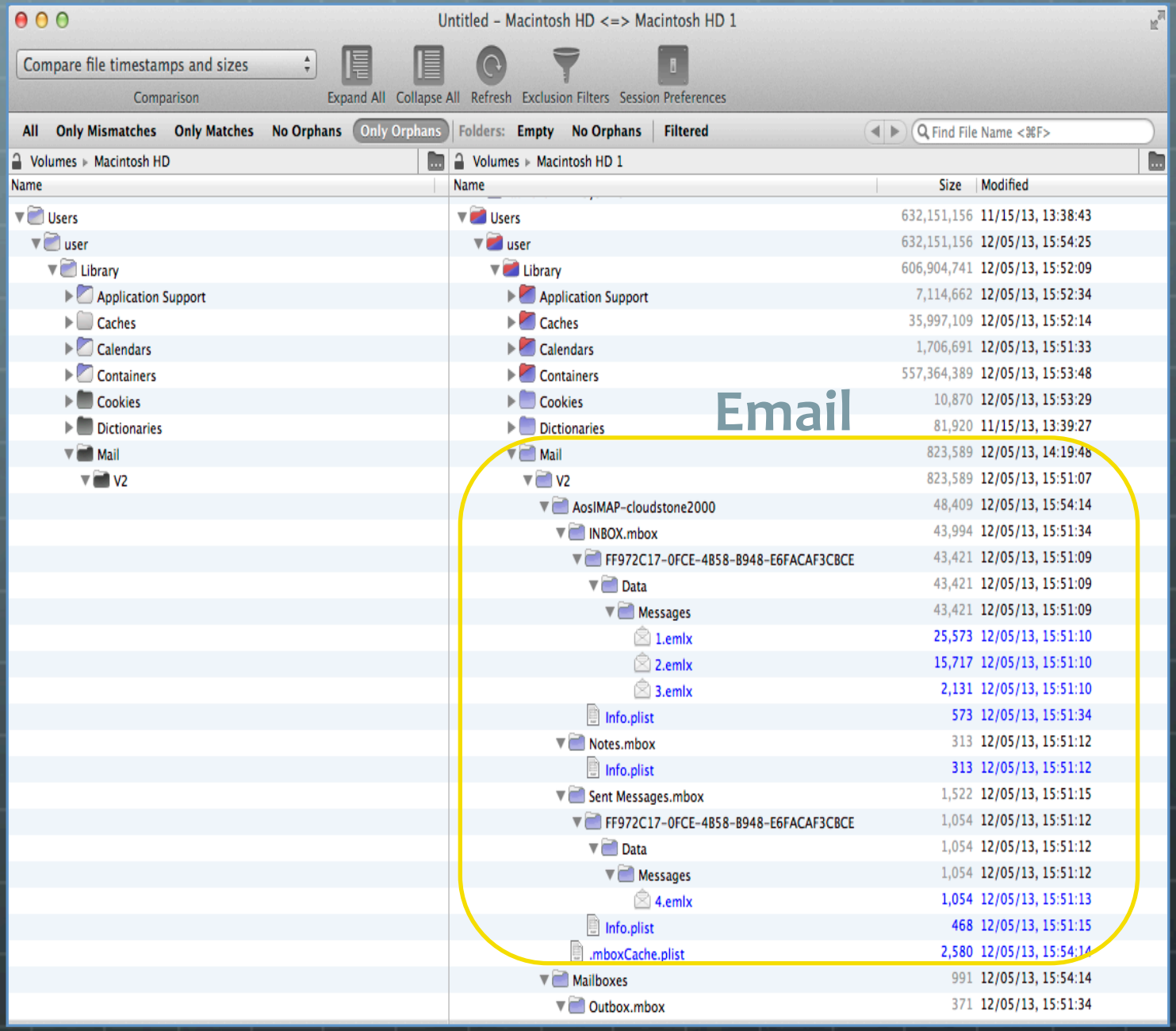


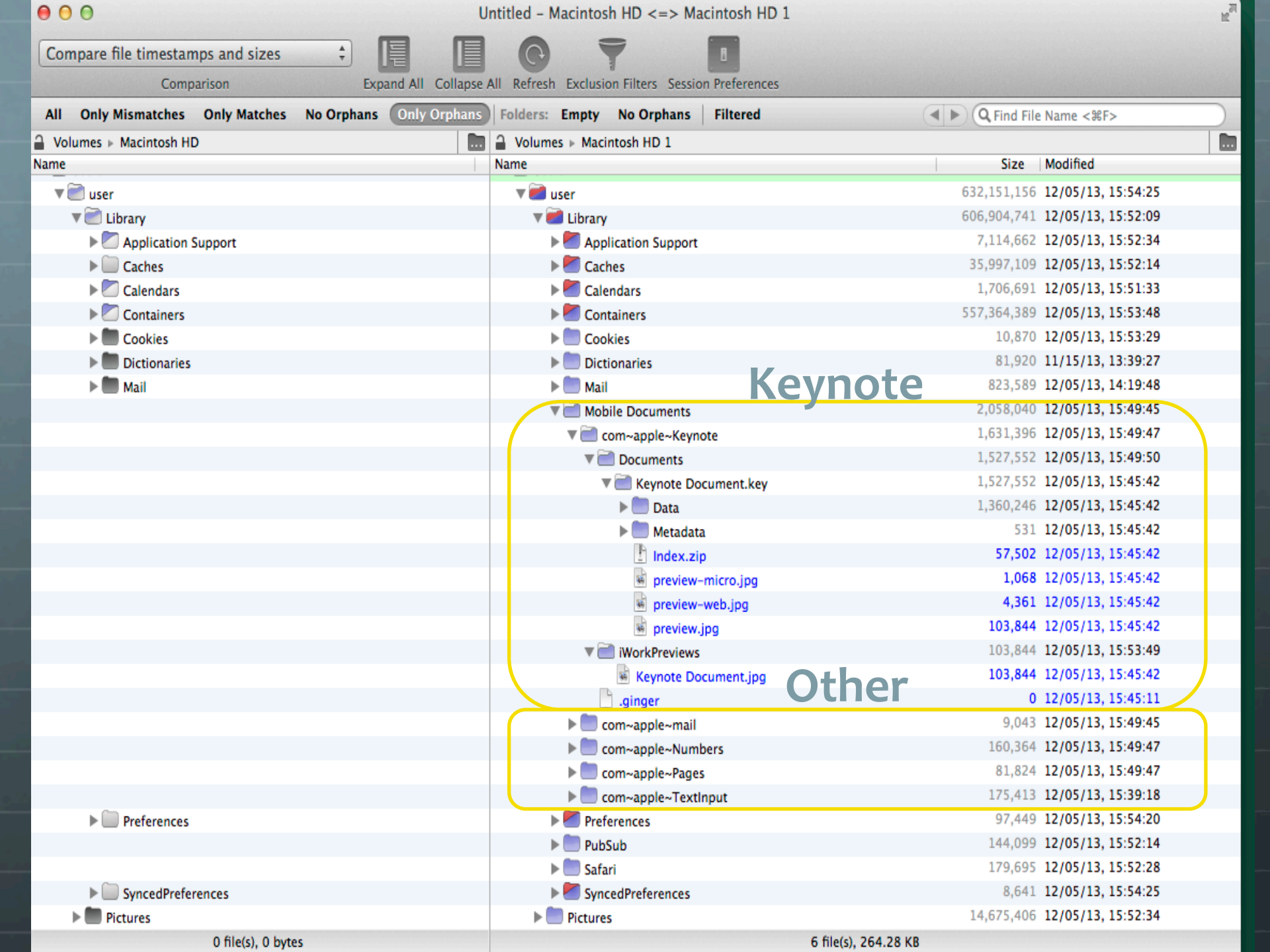
Mounting the Snapshots

- FTK Imager used to create RAW image from .vmdk
- After RAW file created, extension changed to .dmg so image could be mounted.
- .dmg made read-only:
  - Right-click on file
  - Select “Get Info”
  - Check the “Locked” option.



Snapshots Compared




Untitled – Macintosh HD <=> Macintosh HD 1
Compare file timestamps and sizes
Comparison
Expand All
Collapse All
Refresh
Exclusion Filters
Session Preferences
All
Only Mismatches
Only Matches
No Orphans
Only Orphans
Folders:
Empty
No Orphans
Filtered
Find File Name <⌘F>
Volumes ▸ Macintosh HD
Volumes ▸ Macintosh HD 1
Name
Size
Modified
user
Library
Application Support
Caches
Calendars
Containers
Cookies
Dictionaries
Mail
Mobile Documents
com~apple~Keynote
Documents
Keynote Document.key
Data
Metadata
Index.zip
preview-micro.jpg
preview-web.jpg
preview.jpg
iWorkPreviews
Keynote Document.jpg
.ginger
com~apple~mail
com~apple~Numbers
com~apple~Pages
com~apple~TextInput
Preferences
PubSub
Safari
SyncedPreferences
Pictures
632,151,156 12/05/13, 15:54:25
606,904,741 12/05/13, 15:52:09
7,114,662 12/05/13, 15:52:34
35,997,109 12/05/13, 15:52:14
1,706,691 12/05/13, 15:51:33
557,364,389 12/05/13, 15:53:48
10,870 12/05/13, 15:53:29
81,920 11/15/13, 13:39:27
823,589 12/05/13, 14:19:48
2,058,040 12/05/13, 15:49:45
1,631,396 12/05/13, 15:49:47
1,527,552 12/05/13, 15:49:50
1,527,552 12/05/13, 15:45:42
1,360,246 12/05/13, 15:45:42
531 12/05/13, 15:45:42
57,502 12/05/13, 15:45:42
1,068 12/05/13, 15:45:42
4,361 12/05/13, 15:45:42
103,844 12/05/13, 15:45:42
103,844 12/05/13, 15:53:49
103,844 12/05/13, 15:45:42
0 12/05/13, 15:45:11
9,043 12/05/13, 15:49:45
160,364 12/05/13, 15:49:47
81,824 12/05/13, 15:49:47
175,413 12/05/13, 15:39:18
97,449 12/05/13, 15:54:20
144,099 12/05/13, 15:52:14
179,695 12/05/13, 15:52:28
8,641 12/05/13, 15:54:25
14,675,406 12/05/13, 15:52:34
Keynote
Other
0 file(s), 0 bytes
6 file(s), 264.28 KB

Application Data File Paths

Application	Data File Path
Contacts	/Users/user/Library/Application Support/AddressBook/Sources/
Mail	/Users/user/Library/Mail/
Calendar	/Users/user/Library/Calendars/
Reminders	/Users/user/Library/Calendars/
Safari	/Users/user/Library/Safari/
iPhoto	/Users/user/Pictures/iPhoto Library.photolibrary/
Pages	/Users/user/Library/Mobile Documents/com~apple~Pages/Documents/
Numbers	/Users/user/Library/Mobile Documents/com~apple~Numbers/
Keynote	/Users/user/Library/Mobile Documents/com~apple~Keynote/

Analysis

Application Name/File Path	Created	Accessed	Modified	MD5
Contacts				
/Users/user/Library/Application Support/AddressBook/Sources/BDC8A8D1-4D5E-46D3-8746-CF9DC4D39AC4/AddressBook-v22.abcddb-wal	12/5/2013 3:38:28 PM	12/5/2013 3:40:41 PM	12/5/2013 3:40:41 PM	f9dea3d92ec684cbbb1fd62ccd787312
/Users/user/Library/Application Support/AddressBook/Sources/D2907400-687E-4FDE-B8F4-4B27C0E49878/AddressBook-v22.abcddb-wal	12/5/2013 3:49:39 PM	12/5/2013 3:51:31 PM	12/5/2013 3:51:24 PM	a8051b97be968ffd9c54dd0866b135a4
Mail - Inbox				
/Users/user/Library/Mail/V2/AosIMAP-cloudstone2000/INBOX.mbox/BA27AA0A-C69C-4AC7- B8A8-C517FF666DB3/Data/Messages/4.emlx	12/5/2013 3:39:41 PM	12/5/2013 3:39:41 PM	12/5/2013 3:39:41 PM	6cc2cb1018d246483bc343361172d548
/Users/user/Library/Mail/V2/AosIMAP-cloudstone2000/INBOX.mbox/FF972C17-0FCE-4B58- B948-E6FACAF3CBCE/Data/Messages/3.emlx	12/5/2013 3:51:09 PM	12/5/2013 3:51:09 PM	12/5/2013 3:51:09 PM	6cc2cb1018d246483bc343361172d548
Mail - Sent				
/Users/user/Library/Mail/V2/AosIMAP-cloudstone2000/Sent Messages.mbox/BA27AA0A-C69C- 4AC7-B8A8-C517FF666DB3/Data/Messages/5.emlx	12/5/2013 3:39:41 PM	12/5/2013 3:39:41 PM	12/5/2013 3:39:41 PM	fe10c6d7a33829c2af5d6f800edddf7f
/Users/user/Library/Mail/V2/AosIMAP-cloudstone2000/Sent Messages.mbox/FF972C17-0FCE-4B58-B948-E6FACAF3CBCE/Data/Messages/4.emlx	12/5/2013 3:51:12 PM	12/5/2013 3:51:12 PM	12/5/2013 3:51:12 PM	89a5aea52c9afda1164106a816a87336
Calendar (Individual Events)				
/Users/user/Library/Calendars/F87CD4FA-5B1D-4E6E-B5D7-3F0AB61E5C50.caldav/A8F3EBFA-F7FC-4026-86E3-5DD05FD96E9E.calendar/Events/93F37727-B90B-4B04-90CF-36082DE392F3.ics	12/5/2013 3:40:50 PM	12/5/2013 3:40:50 PM	12/5/2013 3:41:01 PM	5a23a8f5a48ba07ff801950c0e6e9ee2
/Users/user/Library/Calendars/74FA4B91-AA8C-4F7C-A84D-8028C1588220.caldav/E4F71911-C68F-488F-A6FC-817A31EB4DBF.calendar/Events/93F37727-B90B-4B04-90CF-36082DE392F3.ics	12/5/2013 3:49:49 PM	12/5/2013 3:49:49 PM	12/5/2013 3:49:49 PM	5921e1be2cb51bf9d65ddb41c16e1310
Reminders				
/Users/user/Library/Calendars/F87CD4FA-5B1D-4E6E-B5D7-3F0AB61E5C50.caldav/5EA1CEE1-7ECB-47B3-9F5E-86EF7BC8BD71.calendar/Events/AD6FD050-9ECE-43D2-978F-C33DEB8B83D5.ics	12/5/2013 3:41:21 PM	12/5/2013 3:41:21 PM	12/5/2013 3:41:22 PM	4591c02173038908a63e9c8ec4af42dd
/Users/user/Library/Calendars/74FA4B91-AA8C-4F7C-A84D-8028C1588220.caldav/9E61D143-8996-465D-8751-F65BAC2C0C9D.calendar/Events/AD6FD050-9ECE-43D2-978F-C33DEB8B83D5.ics	12/5/2013 3:49:50 PM	12/5/2013 3:49:50 PM	12/5/2013 3:49:50 PM	4591c02173038908a63e9c8ec4af42dd
Safari Bookmarks				
/Users/user/Library/Safari/Bookmarks.plist	12/5/2013 3:42:40 PM	12/5/2013 3:42:40 PM	12/5/2013 3:42:40 PM	3528cc9800bb14b8b8fdfd0d036ada06
/Users/user/Library/Safari/Bookmarks.plist	12/5/2013 3:49:43 PM	12/5/2013 3:49:43 PM	12/5/2013 3:49:43 PM	91df269b4e48b4d8dca41369c1f06429
iPhoto				
/Users/user/Pictures/iPhoto Library.photolibrary/Masters/2013/12/05/20131205-154255/red-rosebud.jpg	12/5/2013 3:42:47 PM	12/5/2013 3:42:47 PM	12/5/2013 3:42:47 PM	0641687b2f509ab4fdc6ca7b506077a1
/Users/user/Pictures/iPhoto Library.photolibrary/Masters/2013/12/05/20131205-155248/red-rosebud.jpg	12/5/2013 3:42:47 PM	12/5/2013 3:52:48 PM	12/5/2013 3:42:47 PM	0641687b2f509ab4fdc6ca7b506077a1
Pages				
/Users/user/Library/Mobile Documents/com~apple~Pages/Documents/Pages Document.pages/Index.zip	12/5/2013 3:44:20 PM	12/5/2013 3:44:22 PM	12/5/2013 3:44:20 PM	a7237ea6a0e8ca28c7a372db8cf5c08e
/Users/user/Library/Mobile Documents/com~apple~Pages/Documents/Pages Document.pages/Index.zip	12/5/2013 3:44:20 PM	12/5/2013 3:44:20 PM	12/5/2013 3:44:20 PM	a7237ea6a0e8ca28c7a372db8cf5c08e
Numbers				
/Users/user/Library/Mobile Documents/com~apple~Numbers/Documents/Numbers Document.numbers/Index.zip	12/5/2013 3:45:00 PM	12/5/2013 3:45:03 PM	12/5/2013 3:45:00 PM	3154d40656fc4042be20e99e65525755
/Users/user/Library/Mobile Documents/com~apple~Numbers/Documents/Numbers Document.numbers/Index.zip	12/5/2013 3:45:00 PM	12/5/2013 3:45:00 PM	12/5/2013 3:45:00 PM	3154d40656fc4042be20e99e65525755
Keynote				
/Users/user/Library/Mobile Documents/com~apple~Keynote/Documents/Keynote Document.key/Index.zip	12/5/2013 3:45:41 PM	12/5/2013 3:45:45 PM	12/5/2013 3:45:42 PM	2e95e189841ae61771b2ecd98bfb32ed
/Users/user/Library/Mobile Documents/com~apple~Keynote/Documents/Keynote Document.key/Index.zip	12/5/2013 3:45:42 PM	12/5/2013 3:45:42 PM	12/5/2013 3:45:42 PM	2e95e189841ae61771b2ecd98bfb32ed

Color Key

- Original
- Examiner Download
- MD5 Mismatch
- Match
- Examiner-Side Time Variation
- Original-Side Time Variation

Non-preinstalled Application MD5

Application Name/File Path	Created	Accessed	Modified	MD5
iPhoto				
/Users/user/Pictures/iPhoto Library.photolibrary/Masters/2013/12/05/20131205-154255/red-rosebud.jpg	12/5/2013 3:42:47 PM	12/5/2013 3:42:47 PM	12/5/2013 3:42:47 PM	0641687b2f509ab4fdc6ca7b506077a1
/Users/user/Pictures/iPhoto Library.photolibrary/Masters/2013/12/05/20131205-155248/red-rosebud.jpg	12/5/2013 3:42:47 PM	12/5/2013 3:52:48 PM	12/5/2013 3:42:47 PM	0641687b2f509ab4fdc6ca7b506077a1
Pages				
/Users/user/Library/Mobile Documents/com~apple~Pages/Documents/Pages Document.pages/Index.zip	12/5/2013 3:44:20 PM	12/5/2013 3:44:22 PM	12/5/2013 3:44:20 PM	a7237ea6a0e8ca28c7a372db8cf5c08e
/Users/user/Library/Mobile Documents/com~apple~Pages/Documents/Pages Document.pages/Index.zip	12/5/2013 3:44:20 PM	12/5/2013 3:44:20 PM	12/5/2013 3:44:20 PM	a7237ea6a0e8ca28c7a372db8cf5c08e
Numbers				
/Users/user/Library/Mobile Documents/com~apple~Numbers/Documents/Numbers Document.numbers/Index.zip	12/5/2013 3:45:00 PM	12/5/2013 3:45:03 PM	12/5/2013 3:45:00 PM	3154d40656fc4042be20e99e65525755
/Users/user/Library/Mobile Documents/com~apple~Numbers/Documents/Numbers Document.numbers/Index.zip	12/5/2013 3:45:00 PM	12/5/2013 3:45:00 PM	12/5/2013 3:45:00 PM	3154d40656fc4042be20e99e65525755
Keynote				
/Users/user/Library/Mobile Documents/com~apple~Keynote/Documents/Keynote Document.key/Index.zip	12/5/2013 3:45:41 PM	12/5/2013 3:45:45 PM	12/5/2013 3:45:42 PM	2e95e189841ae61771b2ecd98bfb32ed
/Users/user/Library/Mobile Documents/com~apple~Keynote/Documents/Keynote Document.key/Index.zip	12/5/2013 3:45:42 PM	12/5/2013 3:45:42 PM	12/5/2013 3:45:42 PM	2e95e189841ae61771b2ecd98bfb32ed

Pre-installed Application MD5

Application Name/File Path	Created	Accessed	Modified	MD5
Contacts				
/Users/user/Library/Application Support/AddressBook/Sources/BDC8A8D1-4D5E-46D3-8746-CF9DC4D39AC4/AddressBook-v22.abcddb-wal	12/5/2013 3:38:28 PM	12/5/2013 3:40:41 PM	12/5/2013 3:40:41 PM	f9dea3d92ec684cbbb1fd62ccd787312
/Users/user/Library/Application Support/AddressBook/Sources/D2907400-687E-4FDE-B8F4-4B27C0E49878/AddressBook-v22.abcddb-wal	12/5/2013 3:49:39 PM	12/5/2013 3:51:31 PM	12/5/2013 3:51:24 PM	a8051b97be968ffd9c54dd0866b135a4
Mail - Inbox				
/Users/user/Library/Mail/V2/AosIMAP-cloudstone2000/INBOX.mbox/BA27AA0A-C69C-4AC7- B8A8-C517FF666DB3/Data/Messages/4.emlx	12/5/2013 3:39:41 PM	12/5/2013 3:39:41 PM	12/5/2013 3:39:41 PM	6cc2cb1018d246483bc343361172d548
/Users/user/Library/Mail/V2/AosIMAP-cloudstone2000/INBOX.mbox/FF972C17-0FCE-4B58- B948-E6FACAF3CBCE/Data/Messages/3.emlx	12/5/2013 3:51:09 PM	12/5/2013 3:51:09 PM	12/5/2013 3:51:09 PM	6cc2cb1018d246483bc343361172d548
Mail - Sent				
/Users/user/Library/Mail/V2/AosIMAP-cloudstone2000/Sent Messages.mbox/BA27AA0A-C69C- 4AC7-B8A8-C517FF666DB3/Data/Messages/5.emlx	12/5/2013 3:39:41 PM	12/5/2013 3:39:41 PM	12/5/2013 3:39:41 PM	fe10c6d7a33829c2af5d6f800edddf7f
/Users/user/Library/Mail/V2/AosIMAP-cloudstone2000/Sent Messages.mbox/FF972C17-0FCE-4B58-B948-E6FACAF3CBCE/Data/Messages/4.emlx	12/5/2013 3:51:12 PM	12/5/2013 3:51:12 PM	12/5/2013 3:51:12 PM	89a5aea52c9afda1164106a816a87336
Calendar (Individual Events)				
/Users/user/Library/Calendars/F87CD4FA-5B1D-4E6E-B5D7-3F0AB61E5C50.caldav/A8F3EBFA-F7FC-4026-86E3-5DD05FD96E9E.calendar/Events/93F37727-B90B-4B04-90CF-36082DE392F3.ics	12/5/2013 3:40:50 PM	12/5/2013 3:40:50 PM	12/5/2013 3:41:01 PM	5a23a8f5a48ba07ff801950c0e6e9ee2
/Users/user/Library/Calendars/74FA4B91-AA8C-4F7C-A84D-8028C1588220.caldav/E4F71911-C68F-488F-A6FC-817A31EB4DBF.calendar/Events/93F37727-B90B-4B04-90CF-36082DE392F3.ics	12/5/2013 3:49:49 PM	12/5/2013 3:49:49 PM	12/5/2013 3:49:49 PM	5921e1be2cb51bf9d65ddb41c16e1310
Reminders				
/Users/user/Library/Calendars/F87CD4FA-5B1D-4E6E-B5D7-3F0AB61E5C50.caldav/5EA1CEE1-7ECB-47B3-9F5E-86EF7BC8BD71.calendar/Events/AD6FD050-9ECE-43D2-978F-C33DEB8B83D5.ics	12/5/2013 3:41:21 PM	12/5/2013 3:41:21 PM	12/5/2013 3:41:22 PM	4591c02173038908a63e9c8ec4af42dd
/Users/user/Library/Calendars/74FA4B91-AA8C-4F7C-A84D-8028C1588220.caldav/9E61D143-8996-465D-8751-F65BAC2C0C9D.calendar/Events/AD6FD050-9ECE-43D2-978F-C33DEB8B83D5.ics	12/5/2013 3:49:50 PM	12/5/2013 3:49:50 PM	12/5/2013 3:49:50 PM	4591c02173038908a63e9c8ec4af42dd
Safari Bookmarks				
/Users/user/Library/Safari/Bookmarks.plist	12/5/2013 3:42:40 PM	12/5/2013 3:42:40 PM	12/5/2013 3:42:40 PM	3528cc9800bb14b8b8fdfd0d036ada06
/Users/user/Library/Safari/Bookmarks.plist	12/5/2013 3:49:43 PM	12/5/2013 3:49:43 PM	12/5/2013 3:49:43 PM	91df269b4e48b4d8dca41369c1f06429

Non-preinstalled Application Timestamp Analysis

Application	Version	Created	Accessed	Modified
iPhoto	Original	12/5/2013 3:42:47 PM	12/5/2013 3:42:47 PM	12/5/2013 3:42:47 PM
	Acquired	12/5/2013 3:42:47 PM	12/5/2013 3:52:48 PM	12/5/2013 3:42:47 PM
Pages	Original	12/5/2013 3:44:20 PM	12/5/2013 3:44:22 PM	12/5/2013 3:44:20 PM
	Acquired	12/5/2013 3:44:20 PM	12/5/2013 3:44:20 PM	12/5/2013 3:44:20 PM
Numbers	Original	12/5/2013 3:45:00 PM	12/5/2013 3:45:03 PM	12/5/2013 3:45:00 PM
	Acquired	12/5/2013 3:45:00 PM	12/5/2013 3:45:00 PM	12/5/2013 3:45:00 PM
Keynote	Original	12/5/2013 3:45:41 PM	12/5/2013 3:45:45 PM	12/5/2013 3:45:42 PM
	Acquired	12/5/2013 3:45:42 PM	12/5/2013 3:45:42 PM	12/5/2013 3:45:42 PM

Conclusions

- Same workflow can be used to identify artifacts in future versions of OS X or iCloud (i.e. Yosemite).
- Video recording of live acquisition essential to meeting the documentation requirement.
- Non-preinstalled application data: MD5 hash and timestamps establish data integrity – Forensically Sound
- Pre-installed application data requires more study.
  - Textual content of the documents were unchanged.
  - Differing MD5 values may present a challenge when attempting to satisfy courts of data integrity.

Further Work

- Research was limited to Mac OS X 10.9 synch with iCloud
- Do same results occur between different Mac computer models or different versions of OS X ?
- Effect of iCloud synchronization with iOS devices (iPhone, iPad, iPod Touch)
- What is causing the MD5 values to differ for certain files?
- Why do some timestamps differ by 1-3 seconds?

Questions ?