# A Forensically Robust Method For Acquisition Of iCloud Data

*By*

**Kurt Oestreicher**

*From the proceedings of*

The Digital Forensic Research Conference

**DFRWS 2014 USA**

Denver, CO (Aug 3rd - 6th)

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

# A forensically robust method for acquisition of iCloud data

Kurt Oestreicher*

*Champlain College, 163 South Willard Street, Burlington, VT 05401, USA*

*Keywords:*
Apple
iCloud
Cloud forensics
OS X 10.9
Mavericks
Mac forensics

## ABSTRACT

The acquisition of data stored on cloud services has become increasingly important to digital forensic investigations. Apple, Inc. continues to expand the capabilities of its cloud service, iCloud. As such, it is critical to determine an effective means for forensic acquisition of data from this service and its effect on the original file data and metadata.

This research examined files acquired from the iCloud service via the native Mac OS X system synchronization with the service. The goal was to determine the operating system locations of iCloud-synched files. Once located, the secondary goal was to determine if the file hash values match those of the original files and whether file metadata, particularly timestamps, are altered.

## Introduction

### *Research problem*

The acquisition of data stored on cloud services has become increasingly important to digital forensic investigations. Apple, Inc. continues to expand the capabilities of its cloud service, iCloud. As of June 2013, iCloud had 320 million user accounts with over 900 billion iMessages and 125 billion photo uploads (Kahn, 2013).

This is a tremendous source of data for digital investigators but the problem is establishing a forensically robust method for acquiring this data from iCloud. With the recent updates to both the iCloud service and the introduction of the newest Mac operating system, OS X 10.9 Mavericks, many of the data structures and their locations in the file system have changed. As a result, a method had to be developed not only for downloading this data to an examination computer and verifying the integrity of the acquired data, but also locating where the iCloud-synched files are stored in the file system.

For the purposes of this research, data integrity was established by comparing the MD5 hash values of the original files to those of the acquired files. Recent research addressing the retrieval of files and file metadata stored on similar providers: Dropbox, Google Drive, and Microsoft SkyDrive established that, while the MD5 hash values remained unchanged, the timestamp metadata was unreliable (Quick and Choo, 2013). Therefore, the research also compared the metadata of the original files to those of the acquired files to establish if and how the timestamps had been altered.

### *Field of research*

Apple, Inc. first introduced iCloud in October 2011 as a free cloud storage, synchronization, and computing service. The primary purpose of iCloud is to allow users of Apple's iPhone, iPad, and Mac computers to seamlessly synchronize their data between devices. At launch time, the following iCloud services were available:

- Users could synchronize their contacts, calendars, email and notes across devices as well as access the data through the iCloud.com web interface.

* Tel.: +1 860 532 0474; fax: +1 203 349 2425.
*E-mail address:* koestreicher@gmail.com.

http://dx.doi.org/10.1016/j.diin.2014.05.006

- Users could enable their devices to be backed up to iCloud. This backup included music, apps, books, Camera Roll (photos and videos), device settings, and app data
- Documents created through Apple's iWork software suite could be stored in iCloud and pushed to all devices. Third party developers that utilized the iCloud Storage application programming interface (API) could allow files from their applications to be stored on iCloud
- If enabled, a feature called Photo Stream would automatically upload up to 1000 photos from the user's device for storage and synchronization across platforms
- iTunes Match allowed for users to upload, store, and download up to 25,000 music titles for an additional fee of $24.99/year (Apple Inc., 2011).

Over the last two years, Apple has continued to expand the iCloud features. At the 2013 World Wide Developer Conference, Apple announced the introduction of the iWork suite of applications: Pages, Numbers, and Keynote as free, web-based productivity solutions (Mangalindan, 2013). This expands the previous capability of simply storing and synchronizing these documents by also allowing users to create and edit these documents with any web browser.

### *Research questions*

In order to solve the problem of developing a forensically sound method for acquiring the data from an iCloud user account, several questions have to be answered:

- 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?

### *Contributions*

The forensic integrity of recovered evidence is critical to investigators. Metadata such as timestamps could be essential to establishing a suspect's alibi or involvement in criminal activity. The primary intent of this research was to establish a best practice for acquiring iCloud data and determine how original user data or metadata was altered in the process.

Additionally, this research outlines where the iCloud user data is stored on the OS X 10.9 Mavericks file system. This will assist investigators not only with iCloud acquisitions but also with traditional dead-box analysis of OS X 10.9 systems. This is significant because Apple has recently changed the stored locations for these files.

### *Overview*

The primary purpose of this paper is to conduct quantitative research into the movement and storage of specific file types from the initial client, to the iCloud server, to a secondary client. The secondary client serves as the examination machine used by an examiner when collecting forensic data from the iCloud servers.

This paper first examines similar cloud research that has been conducted on other platforms and the results of that research. A methodology for acquiring and validating the iCloud acquisition process is then explained in detail. The results of the research are then discussed along with any conclusions made.

In October 2013, Apple introduced its new Mac operating system, OS X 10.9 Mavericks. Alongside this announcement, Apple also introduced changes to its iCloud service and the synchronization capabilities that it has with OS X 10.9. This resulted in application artifacts being relocated to different areas of the file system. It has also significantly changed the key file structures of its iWork applications: Pages, Numbers, and Keynote to provide more seamless synchronization across the Mac, iCloud, and iOS platforms (Heer, 2013). Therefore, in an attempt to provide the most up-to-date analysis possible, the research was conducted using the latest public releases of OS X 10.9, iCloud, and iWork applications as of December 5, 2013.

Like most cloud services, Apple's data storage centers are located in multiple jurisdictions, creating complications for investigators seeking authorization to access this data. Apple has data centers located in North Carolina, Oregon, and California with a fourth center under development in Nevada (Dilger, 2013). 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.

## Literature review

A review was conducted for peer-reviewed articles that are relevant to this research topic. A brief summary of the research methods, findings, limitations, and conclusions for each study is provided and any similar conclusions or conflicting findings are discussed.

Quick and Choo (2013) conducted research to determine if files uploaded, stored, and subsequently acquired from cloud storage providers: Dropbox, Google Drive, and Microsoft SkyDrive, were altered in any way. The researchers used data from the Enron corpus and created research account with the three service providers. For each service provider, they set up a virtual machine (VM), enabled Wireshark for tracking traffic between the VM and the provider, and used Microsoft Expression Encoder to record video of the entire process. The original files were hashed and timestamps recorded. Then in each case, the files were uploaded/downloaded to the providers using both the web browser interface as well as the providers' client application. After each of these instances was completed, the virtual machine was stopped and the image preserved for analysis with FTK, EnCase, and XRY.

The researchers determined that, in all cases, the hash values remained unchanged throughout. This indicated that the data in the files were unaltered. However, the timestamps were not reliable and were manipulated by each service. These stamps also varied depending on whether the native client application was used versus the web browser interface. The fact that the data was unaltered but that timestamps are unreliable is very important to investigations relying on this cloud data.

As part of their research, they identified several other providers that should be researched in the future to determine if files stored on their servers are altered in any way. Forensic reliability of data acquired from iCloud storage was identified as a future research area.

Dykstra and Sherman (2012) focused on the forensic reliability of data downloaded from Amazon Elastic Compute Cloud (EC2) servers. One of the main differences between EC2 and iCloud is that EC2 functions as an Infrastructure-as-a-Service (IaaS) solution. With IaaS providers, the consumer has direct control over the creation and usage of a virtual machine that installed on the host server. The nature of IaaS is such that a forensic investigator has the capability of uploading a traditional acquisition tool such as EnCase or FTK to the virtual machine and then creating a forensic image of the entire virtual machine that can then be analyzed through traditional stand-alone computer forensic techniques.

The researchers utilized several different techniques for acquiring the data off of the EC2 virtual machine. The first two techniques involved using the virtual machine to create a forensic image and then using EnCase Enterprise or FTK to analyze the image. These techniques are not relevant to iCloud forensic examination because there is no current iCloud capability for end-user creation of virtual machines.

The third technique is more relevant to iCloud data retrieval in that the researchers used the Amazon Web Service (AWS) to export the data. This process is similar to what might occur if the provider was issued a subpoena. Amazon exports the data requested to an external drive, maintains chain-of-custody, and ships the drive directly to the requestor. Along with the drive, Amazon also includes a report of the data exported that includes “date and time of the transfer, location on the storage device, MD5 checksum, and number of bytes” (Dykstra and Sherman, 2012).

Unlike the iCloud retrieval process, Amazon exports the files to a physical hard drive whereas iCloud files are downloaded via the Internet. However, the researchers concluded that the files that were exported from Amazon and shipped to them had the same hash values as the original files. This indicates that utilizing this technique the cloud data was unaltered. One possible avenue for future research would be to submit a request to Apple for iCloud data to be exported in this fashion to a physical drive that is shipped to the researcher. The data could then be analyzed to see if it had been altered from the initial uploaded files.

Chung et al. (2012) focused on four popular cloud service providers: Amazon S3, Dropbox, Google Docs, and Evernote. Rather than focus on the data stored on the servers themselves, the researchers examine the system artifacts left on the client computers of Mac and Windows computers when the services are accessed.

These artifacts that are created by accessing the cloud services can have significant forensic value. All of the services researched can be accessed via a web browser so the researchers looked at the artifacts created by two popular browsers, Internet Explorer and Firefox. While there are definitely some useful artifacts left behind while using web browser access, most of the data resides in the temporary Internet files and Internet history areas. These artifacts are typically limited to indicating which sites were accessed and at what times.

Several of the providers, however, have native applications that can be installed on the client computers. These applications create various artifacts that are much more useful to forensic investigations. For example, Dropbox and Evernote synchronize the files stored on the cloud server with the client computer hard drive. As a result, an investigator should be able to obtain all of the actual documents and associated metadata from the client device itself. The researchers conducted a case study in which files from System A were uploaded to Dropbox and subsequently located on System B after having been synchronized with the cloud server.

One potential problem with the above study is that the researchers simply tracked the file names rather than create hashes of the files at each phase to indicate that the original file was not altered in any way.

The research is useful and can be applied to studies involving iCloud. The iCloud service installs various files on the client operating system, which are synchronized versions of those same files on the iCloud server. A study of these artifacts may be incorporated as part of this research topic regarding iCloud file acquisition. However, cryptographic hashes should be used to ensure that the files are identical in all cases.

Martini and Choo (2012) focused on the framework for conducting investigations involving cloud computing. As such, it is essentially a discussion of the authors' theory on how cloud investigations differ from conventional computer forensic investigations. No research is discussed as to the reliability of data files extracted from specific cloud services.

The article is relevant to cloud research because it details specific concerns that occur with the acquisition of cloud data versus other types of data acquisition. The authors believe that unlike traditional frameworks, evidence source identification and preservation are the first and primary concern followed by acquisition. They also state that, while IaaS services may have the capability of exporting an image of a virtual hard disk, Software as a Service (SaaS) providers may only permit downloading of individual data files.

The authors also compare acquisition of cloud data to that of live forensics. However, they state that the acquisition of cloud data is more susceptible to legal issues because the data must often be acquired by a third party and not by the investigators themselves. The researchers also point out that the preservation of file metadata is often critical to investigations and that the absence of valid metadata may render the recovered data inadmissible in court.

## Methodology and methods

### *Overarching methodology*

To conduct this research, two identical virtual machines representing the subject computer and examination computer were created with a clean install of Mac OS X 10.9 along with the Pages, Numbers, and Keynote applications. Throughout the process, snapshots were taken at various stages and then compared so as to locate the artifacts created by the iCloud service. A new iCloud account was established, new iCloud data was created on the subject machine, and the data was synchronized with the cloud service.

The second virtual machine was started and synchronized with the newly created iCloud account. This represented an examiner performing a live acquisition of the data. Analysis was then performed to locate the iCloud artifacts created on the system. The downloaded files were compared with the original files to determine if the files and metadata were the same and, if not, what the differences were.

### *Initial configuration*

The host computer used to conduct this research consisted of a mid-2012 MacBook Pro with retina display, configured with a 2.3 GHz Intel Core i7 processor and 8 GB 1600 MHz DDR3 memory. The host operating system was running Mac OS X 10.9 (13A603) (Apple Inc.).

A new virtual machine (VM1), representing the subject's computer, was created using VMware Fusion Professional Version 6.0.2 (1398658) and a clean install of OS X 10.9 (13A603) (VMware). The following applications where then installed on VM1: Pages, Numbers, and Keynote. The virtual machine was then shutdown and a snapshot taken (Snapshot 1). A clone of this snapshot was created for the examiner's machine (VM2) (Fig. 1).

VM1 was then restarted and the researcher signed up for a new iCloud account through the system settings application. Once the signup was complete, documents and data were created in the various iCloud enabled applications (Table 1). Once the data was populated, VM1 was shutdown and a second snapshot (Snapshot 2) was taken.

### *Data collection*

Since this was a live acquisition and cloud based services can be changed at any time, the virtual machine window was video recorded using the screen capture software Voila v.3.6 (Global Delight Technologies Pvt. Ltd.).

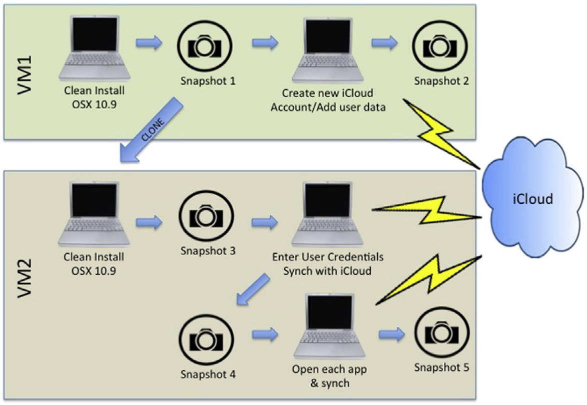


**Fig. 1.** Virtual machine configuration.

**Table 1**
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. |

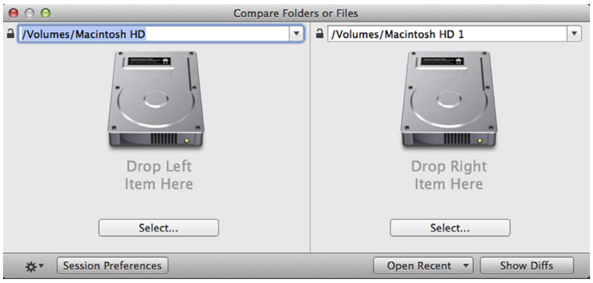
The examination machine (VM2) was started and an initial snapshot (Snapshot 3) was taken. The researcher then logged into iCloud through the system settings using the previously created iCloud credentials. Once the configuration was complete, another snapshot (Snapshot 4) was taken without shutting down the virtual machine. Since some apps do not synch until they are first opened, each of the previous applications was opened and data allowed to synch. The virtual machine was then shutdown and a final snapshot (Snapshot 5) was taken.

### *Results*

Both of the virtual machines were closed and the host machine was then used to conduct the analysis. The first step was to determine what files were added or changed between each snapshot. This allowed the researcher to discover the locations of file locations from the various iCloud applications and also to locate any other iCloud artifacts.

VisualDiffer v.1.5.7 for Mac can take two volumes and compare them based on file timestamps and sizes to determine what has changed between two snapshots (Ficano) (Fig. 2). Since VMware Fusion Snapshots are stored as .vmdk files, they had to be converted to be used with this tool. AccessData's Forensic Toolkit (FTK) Imager has the ability to take a .vmdk snapshot and create a RAW image file from it (AccessData Group). Each of the snapshots was loaded into FTK Imager and RAW files were created.

After the RAW files were created, the extension was changed to .dmg so that the images could be mounted in OS X and used with VisualDiffer. This was accomplished by right clicking on the RAW file and selecting “Get Info”. This opens a dialog box where the extensions were changed to .dmg and the option to lock the file was checked. Locking the files makes it a read-only file and ignores any other permission. The end result was a read-only, .dmg file for



Compare Folders or Files

/Volumes/Macintosh HD

/Volumes/Macintosh HD 1

**Fig. 2.** VisualDiffer volume selection.

each snapshot. Double clicking on these .dmg snapshots mounts them in OS X. At this point, they could be loaded into VisualDiffer for comparison. One convenient feature of VisualDiffer is the option to only show mismatched files. This option allowed the examiner to quickly narrow the results to show only those files that were added or changed since the previous snapshot.

Using this method, Snapshot 2 was compared to Snapshot 1. This displayed all changes or additions that were created on the file system as a result of signing up for iCloud and creating the various data entries. Files that changed since the previous snapshot are colored in red. Files that were added since the previous snapshot are colored in blue (Fig. 3).

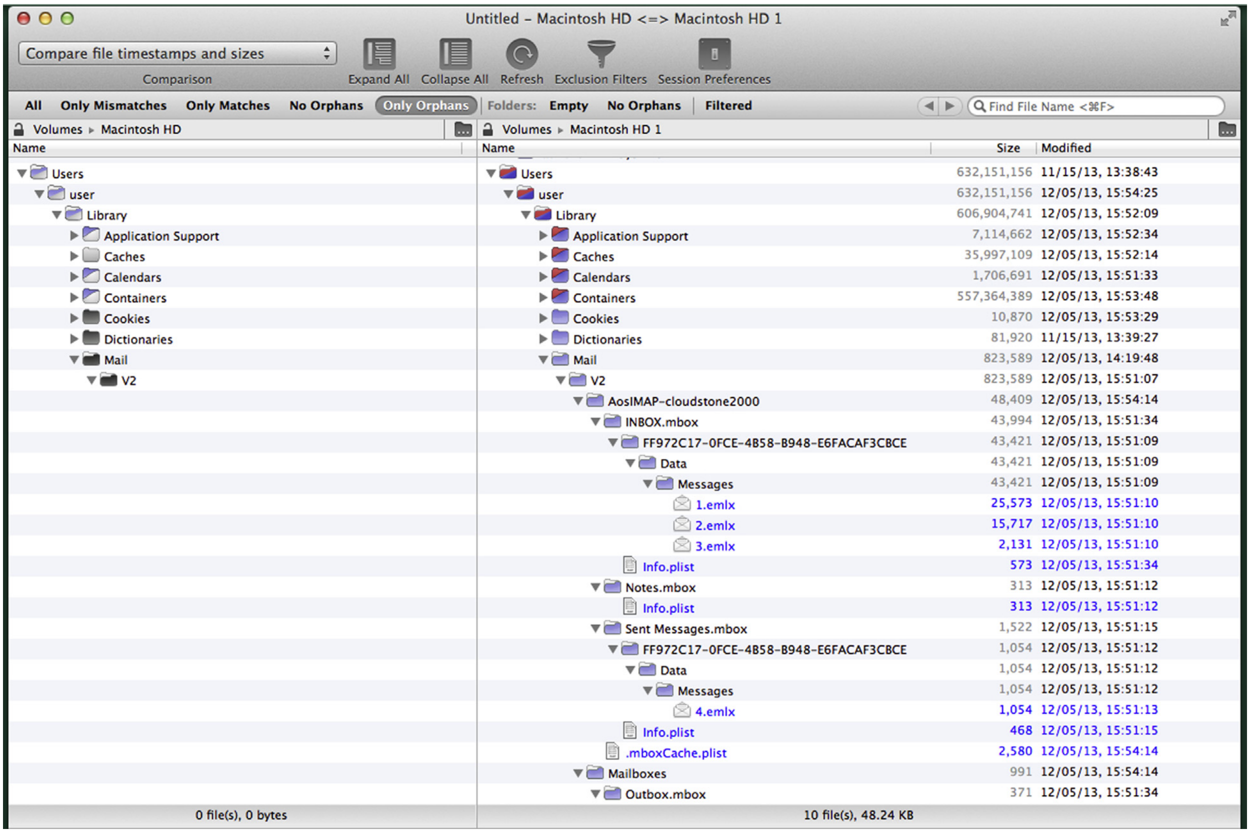
Once these files and their locations were recorded, the next phase was to compare the files from the original snapshot (Snapshot 2) to the examiner-downloaded snapshot (Snapshot 5) to determine if they matched. The images for Snapshots 2 and 5 were then added as evidence to FTK 4.2.2 for further analysis. Each of the iCloud data files was analyzed and the associated MD5 hash values and timestamps were compared.

Fig. 4 illustrates the discovered file locations and paths, along with the timestamps and MD5 hash values. Each application data file is listed and color-coded according to the associated snapshot.

## Analysis

### *File locations*

As a result of the snapshot comparison, it appears that all of the iCloud-synched user documents are located in various subfolders within the/Users/user/Library/folder (Table 2). The standard applications that are part of the Mac OS 10.9 distribution; Contacts, Mail, Calendar, Reminder, and Safari; all have their own unique subfolders directly under the/Users/user/Library/parent folder. Non-preinstalled application data; such as Pages, Number, and Keynote; are all contained in the subfolder/Users/user/Library/Mobile Documents/. The exception to this is iPhoto



Untitled – Macintosh HD <=> Macintosh HD 1

Compare file timestamps and sizes

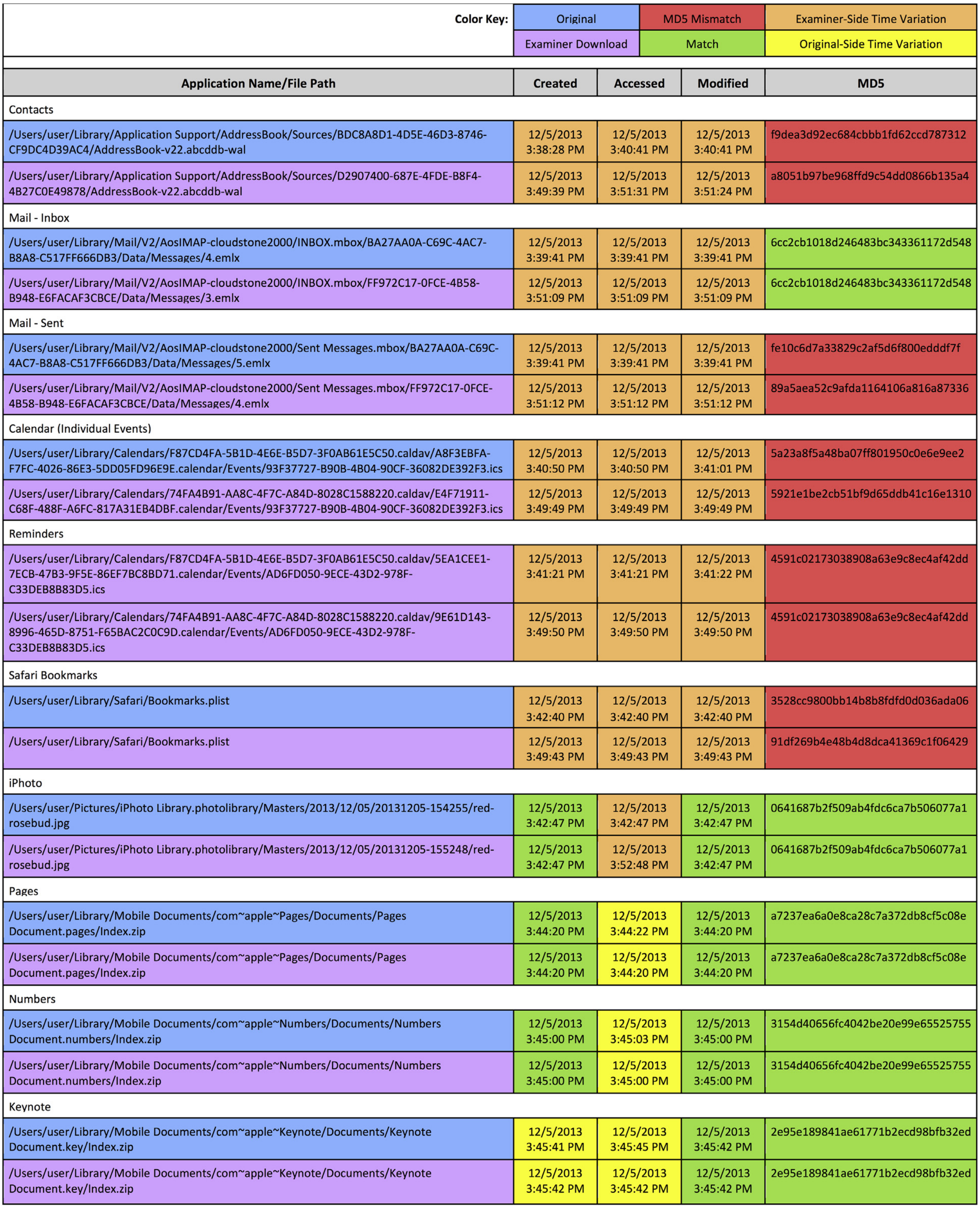
```
Volumes ▸ Macintosh HD
Name
▼ Users
  ▼ user
    ▼ Library
      ▶ Application Support
      ▶ Caches
      ▶ Calendars
      ▶ Containers
      ▶ Cookies
      ▶ Dictionaries
      ▼ Mail
        ▼ V2

0 file(s), 0 bytes
```

```
Volumes ▸ Macintosh HD 1
Name                                                   Size  Modified
▼ Users                                         632,151,156  11/15/13, 13:38:43
  ▼ user                                        632,151,156  12/05/13, 15:54:25
    ▼ Library                                   606,904,741  12/05/13, 15:52:09
      ▶ Application Support                       7,114,662  12/05/13, 15:52:34
      ▶ Caches                                   35,997,109  12/05/13, 15:52:14
      ▶ Calendars                                 1,706,691  12/05/13, 15:51:33
      ▶ Containers                              557,364,389  12/05/13, 15:53:48
      ▶ Cookies                                      10,870  12/05/13, 15:53:29
      ▶ Dictionaries                                 81,920  11/15/13, 13:39:27
      ▼ Mail                                        823,589  12/05/13, 14:19:48
        ▼ V2                                        823,589  12/05/13, 15:51:07
          ▼ AosIMAP-cloudstone2000                   48,409  12/05/13, 15:54:14
            ▼ INBOX.mbox                             43,994  12/05/13, 15:51:34
              ▼ FF972C17-0FCE-4B58-B948-E6FACAF3CBCE 43,421  12/05/13, 15:51:09
                ▼ Data                               43,421  12/05/13, 15:51:09
                  ▼ Messages                         43,421  12/05/13, 15:51:09
                      1.emlx                         25,573  12/05/13, 15:51:10
                      2.emlx                         15,717  12/05/13, 15:51:10
                      3.emlx                          2,131  12/05/13, 15:51:10
              Info.plist                                573  12/05/13, 15:51:34
            ▼ Notes.mbox                                313  12/05/13, 15:51:12
              Info.plist                                313  12/05/13, 15:51:12
            ▼ Sent Messages.mbox                      1,522  12/05/13, 15:51:15
              ▼ FF972C17-0FCE-4B58-B948-E6FACAF3CBCE  1,054  12/05/13, 15:51:12
                ▼ Data                                1,054  12/05/13, 15:51:12
                  ▼ Messages                          1,054  12/05/13, 15:51:12
                      4.emlx                          1,054  12/05/13, 15:51:13
              Info.plist                                468  12/05/13, 15:51:15
            .mboxCache.plist                          2,580  12/05/13, 15:54:14
          ▼ Mailboxes                                   991  12/05/13, 15:54:14
            ▼ Outbox.mbox                               371  12/05/13, 15:51:34

10 file(s), 48.24 KB
```

**Fig. 3.** Changes to file system.



| Color Key: | | | |
|---|---|---|---|
| | Original | MD5 Mismatch | Examiner-Side Time Variation |
| | Examiner Download | Match | Original-Side Time Variation |

| 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 |

**Fig. 4.** File comparison – original versus examiner download.

**Table 2**
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/ |

which, although it is not a preinstalled application, has its data folder directly under the parent/Users/user/Library/.

For the preinstalled applications; Contacts, Mail, Calendar, and Reminders; the operating system generates a folder with a Globally Unique Identifier (GUID) to house the individual user documents.

Although this is normal operating system behavior, when using this technique for downloading iCloud data, investigators will first need to determine the unique GUID subfolder names in order to locate the underlying files (Table 3). Within the calendar folders, a subfolder named "Events" contains the individual calendar entries. For this research, the individual event MD5 hash values were compared and found to not match the originals.

### *MD5 hash values*

The MD5 hash value analysis had mixed results with some data having matching hashes and others being mismatched. All of the non-preinstalled application data files; iPhoto, Pages, Numbers, and Keynote; had matching MD5 hashes between the original and the acquired files. The preinstalled Reminders application had mismatched MD5 hash values but the Mail application inbox files had matching MD5 hash values. Although it is appears that the operating system generates unique names for inbox files as they are downloaded, the matching hash values indicate that no changes were made to the file data as a result of the synchronization process.

The other preinstalled applications, however, had different MD5 hash values for the file data. When these differences were discovered, each of the files was examined in FTK to examine the contents of the file data. The textual data had been created by the researcher for each application was identical between the original and the acquire versions of the files. This leads the researcher to hypothesize that some underlying data is changed as a result of the synchronization schema for built-in applications.

**Table 3**
Subfolder GUID name differences.

| Snapshot | Subfolder |
|---|---|
| Snapshot 2 | /Users/user/Library/Calendars/F87CD4FA-5B1D-4E6E-B5D7-3F0AB61E5C50.caldav/ |
| Snapshot 5 | /Users/user/Library/Calendars/74FA4B91-AA8C-4F7C-A84D-8028C1588220.caldav/ |

### *Metadata*

There were significant differences between the metadata handling of the non-preinstalled applications versus the preinstalled applications. For that reason, discussion of the metadata analysis will be divided between these two types.

#### *Non-preinstalled applications (iPhoto, Keynote, Pages, Numbers)*

Metadata analysis of the data resulted in similar findings. The non-preinstalled applications all had matching Modified timestamps (Table 4). With the exception of Keynote, they also had matching Created timestamps. The Keynote Created timestamp for the acquired data was 1 s later than the timestamp of the original. There was also a difference between the Accessed timestamps on all the iWork applications. For Pages, Numbers, and Keynote; all of the Accessed timestamps on the acquired data was 2–3 s earlier than that of the original data. The Accessed timestamps for iPhoto also did not match with the timestamp of the acquired file. The Accessed timestamp on the acquired photo correlates to when iPhoto was opened on the examiners machine for synching.

What is interesting to note is that for all of the iWork applications; Pages, Numbers, and Keynote; the Created, Accessed, and Modified timestamps of the acquired files were identical to the Modified timestamps of the originals.

#### *Preinstalled applications (Contacts, Mail, Calendar, Reminders, Safari)*

Metadata analysis of the preinstalled applications established that none of the timestamp data from the acquired files matched those of the originals. In all cases, the timestamps of the acquired files correlated to when those files were downloaded to the examiner machine (Snapshot 5).

## Conclusion

While it was originally anticipated that there would be variations in the timestamps based on the results of research on other cloud providers, it was not thought that MD5 hash values would not match for some of the data files.

In conducting live acquisition from any cloud service, the first issue that must be addressed is ensuring that the process is "forensically sound". Casey (2011) defines forensically sound as follows:

> From a forensic standpoint, the acquisition process should change the original evidence as little as possible and any changes should be documented and assessed in the context of the final analytical results. Provided the acquisition process preserves a complete and accurate representation of the original data, and its authenticity and integrity can be validated, it is generally considered forensically sound.

**Table 4**
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 |

Based on this definition, the results of this research indicate that data downloaded from iCloud using the above-described method is forensically sound for applications that use the iCloud synching service. The video recording of the live acquisition process is important to meeting to the documentation requirement. For the non-preinstalled applications researched, the MD5 hash values and the timestamps on the acquired data correlated with those of the originals, establishing data integrity.

To meet the forensic soundness criteria for the preinstalled applications, however, there are questions that must be answered about the differences in the MD5 hash values. Although the research showed that the textual content of these documents was unchanged, it may be more challenging for an investigator to prove the files are sufficiently similar to satisfy the courts.

## Further work

This research was limited to the examination of files transferred from a Mac OS X 10.9 machine to the iCloud server, and then acquired on a secondary Mac OS X 10.9 machine. Additional research would need to be conducted to determine if the same results occur between different models of Mac computers or using different versions of OS X. This paper also does not explore the incorporation of iOS devices such as the Apple iPhone or iPad in the iCloud synchronization schema and any effects that iCloud has on files synched across these devices.

There is obviously some part of the iCloud synchronization schema that results in changes to the data files for preinstalled OS X applications. Further research into this synchronization schema and what changes are made to these files would be helpful for investigators attempting to establish the authenticity of documents acquired from iCloud.

Although the timestamps in the non-preinstalled applications are essentially the same to the original files, there is a difference of 1–3 seconds that this research has not explained. Although it is hypothesized that all the timestamps of the acquired files reflect the modified timestamps from the original, further analysis needs to be conducted to examine why this anomaly exists.

## References

AccessData Group, LLC. Forensic toolkit. Accessdata.com; n.d.
Apple, Inc. Apple – OS X Mavericks; n.d.
Apple, Inc. Apple introduces iCloud. Apple.com; 2011.
Casey E. Digital evidence and computer crime. 3rd ed. Waltham, MA: Elsevier, Inc; 2011.
Chung H, Park J, Lee S, Kang C. Digital forensic investigation of cloud storage services. Digit Investig 2012;9:81–95.
Dilger DE. Apple's iCloud reigning over the greenest data centers on the planet. Appleinsider.com; 2013.
Dykstra J, Sherman AT. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques. Digit Investig 2012;9:S90–8.
Ficano D. VisualDiffer; n.d.
Global Delight Technologies Pvt. Ltd. Voila; n.d.
Heer N. Exploring the new iWork for Mac file formats, Pixel Envy; 2013.
Kahn J. Apple at Q3 call: iCloud reaches 320M accounts, 900B iMessages, 125B photo uploads. 9to5mac.com; 2013.
Mangalindan JP. Apple WWDC 2013 liveblog – Fortune Tech. Tech.Fortune.Cnn.com; 2013.
Martini Ben, Choo K-KR. An integrated conceptual digital forensic framework for cloud computing. Digit Investig 2012;9:71–80.
Quick D, Choo K-KR. Forensic collection of cloud storage data: does the act of collection result in changes to the data or its metadata? Digit Investig; 2013.
VMware, Inc. Windows for Mac Desktop Virtualization; n.d.