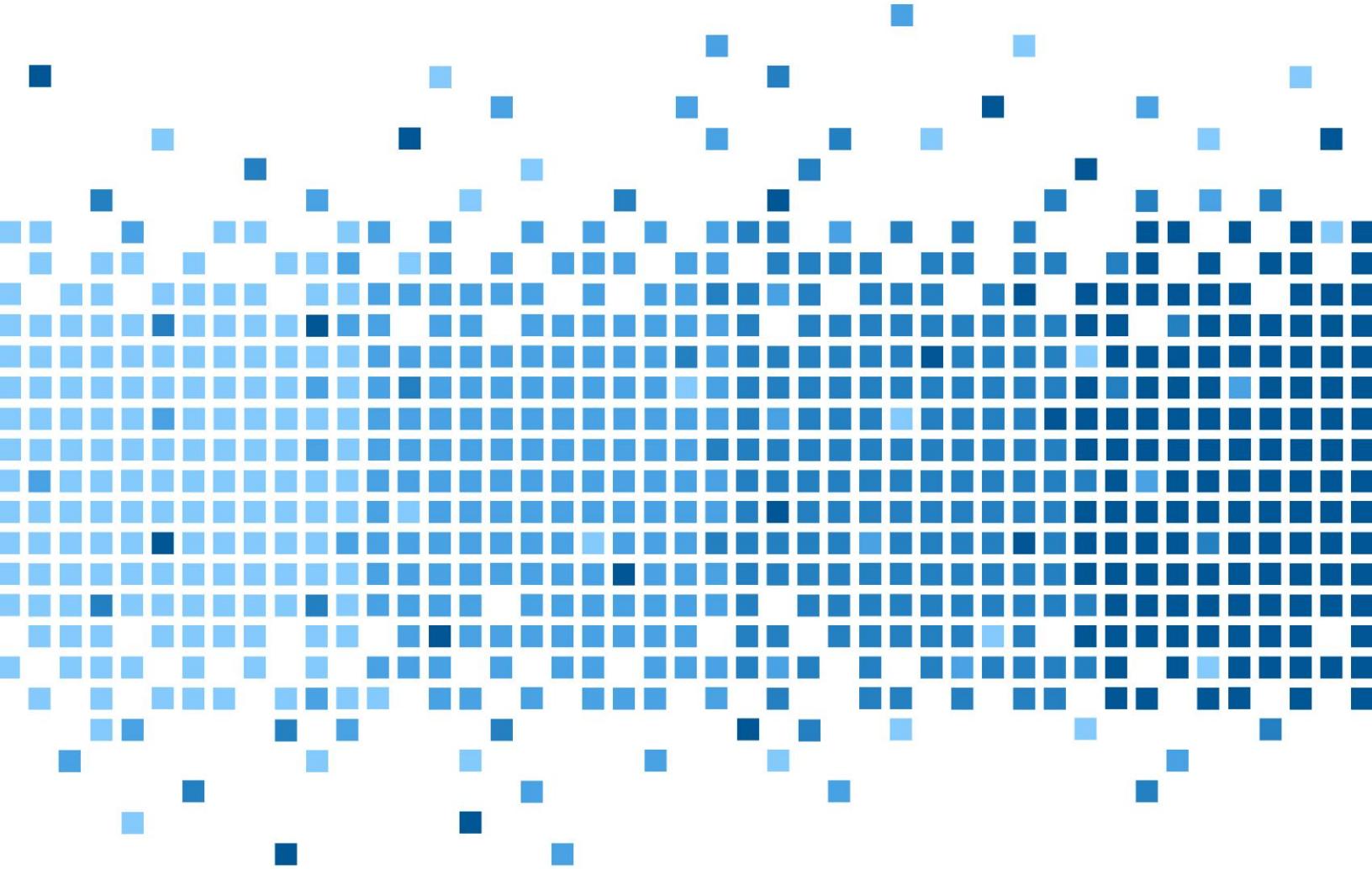
CHAMPLAIN COLLEGE | LCDI Leahy Center for Digital Investigation

[Investigation of Cloud Services]



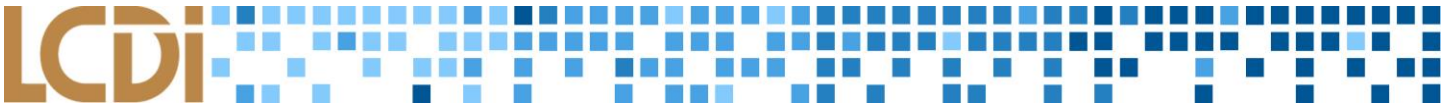
175 Lakeside Ave, Room 300A
Phone: (802)865-5744
Fax: (802)865-6446
http://www.lcdi.champlain.edu

04/27/2016

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents



Introduction

Cloud storage is a method of storing files and data within a server network by sending it over the Internet, where it is stored and will remain accessible through a dedicated application or browser client. Often, these servers are managed by cloud service providers, or companies that commercialize the use of the cloud to consumers. This means that data stored in the cloud can be retrieved from multiple devices without any transfer of physical storage. Cloud storage can be created privately and managed by corporations or high-level cloud providers that offer services exclusively to enterprises. Because of these conveniences, cloud storage has become a very popular choice of storage for both businesses and individuals. Over the course of this project, the LCDI seeks to investigate and explore some of the most popular consumer-level cloud services.

Background

The LCDI has conducted prior research regarding cloud services. The last report, released in November 2013, covered Google Drive, Dropbox, and Microsoft's SkyDrive (the precursor to OneDrive). Since then, cloud usage has increased dramatically: in 2013 there were an estimated 979 exabytes (or 979 billion gigabytes) of IP traffic to personal clouds, which is expected to double in 2016 (Statisa). Cloud service software has undergone immense improvements by their developers since the previous report was published, warranting a re-evaluation of the services. Additionally, the LCDI decided to include iCloud in this analysis because of its presence on all modern Mac computers by default.

Purpose and Scope

The purpose of this report is to serve as a digital forensic resource identifying the default locations of artifacts produced when cloud services interact with a machine running a Windows 7 operating system. The exception is iCloud, which was analyzed through OS X El Capitan as it comes preinstalled on that particular OS. The results of this research will be useful for digital forensic investigations where relevant information may be stored over the cloud. Reporting the artifacts created when using cloud services and their default locations assists in digital investigation, as our data indicates the potential locations of information that may be pertinent.

As of March 2016, Windows 7 is the most commonly used operating system on desktop machines worldwide, with current usage at almost 46% of all desktop computers (Stat Counter), leading the LCDI to limit the scope of this investigation to machines largely running Windows 7.

Research Questions

1) What artifacts are created or modified when the cloud storage application is installed?

2) Is there evidence of files after they have been deleted from the cloud storage application folder?

3) What changes are made to artifacts and metadata when a file is moved or copied from the base folder to another folder?

4) What artifacts remain after the cloud storage application has been unlinked and uninstalled?

Terminology

Acquisition – The process of copying data from a piece of evidence, to another location in a forensically sound manner so that the data may be analyzed at a later time. This is usually done by attaching some form of write blocking device to the storage media, and creating a copy of the data. The goal is to leave the original media intact while working on a copy of it. This allows for evidence to be verified at a later date. There are two different types of data acquisition methods: Physical and Logical.

Artifacts – Any data generated by user interaction that can be collected and examined. Any user data retrieved from the browser is considered an artifact, including cookies, caches, geolocation, search history, etc.

Cloud Storage – A computing model where data can be stored and accessed remotely. A Cloud Service provider usually manages multiple servers and locations to make their resources available to end users on the same network (the internet.)

Digital Forensics – Investigation and recovery of the data found on digital devices. This can include collecting data from a hard drive, verifying data collected, or analyzing such data. Evidence to be used in court must be collected through "sound" methods as nearly all digital evidence is circumstantial. An example of improving a piece of evidence's legitimacy is comparing the hash sum of the evidence to an image that is being worked with (The physical evidence is not usually touched in order to preserve it.)

Encase v7.10 - A suite of forensic software that can be used to acquire, process, and analyze data. The software offers functions such as MD5 hash verification, live imaging, and supports various different file formats such as .VMDK.

Forensic Toolkit (FTK) - A digital forensic tool suite made by AccessData. FTK allows users to acquire, process, and verify evidence. FTK supports many image formats. The current is Version 5.6. Version 5.5 is the version that the lab currently uses.

FTK Imager – is a free extension of FTK 4.1. This is a powerful imaging program that can be used to create forensic images of a drive, which can then be opened in most forensic software for examination. There are other functions that allow this program to take images of specific files in a storage device as well as floppy disks, CDs, DVDs, and zip disks.

Operating System (OS) – A suite of programs that controls signals to and from input devices (such as a mouse, keyboard, microphone), peripherals (hard disks, CD/DVD drives, printers, etc.), output devices (monitors, speakers, etc.) and performs the basic functions needed for a computer to operate. This entails input and output, memory allocation, file management, task scheduling, etc. Having an OS is essential to operate a computer, as applications utilize the OS to function.

Parse – The process of dividing a computer language statement into parts that can be made useful for the computer. A parser in a program compiler is a program that takes each program statement that a developer has written and divides it into parts (for example, the main command, options, target objects, their attributes, and so forth) that can then be used for developing further actions or for creating the instructions that form an executable program.

Virtual Machine (VM) – An emulation of a computer system that runs on software utilizing a host's resources. The virtual machine acts as a separate computer that is able to perform tasks and run applications.

VMDK Image File – Refers to a copy of a hard drive, or disk image, which is compressed into a series of files. This form of image is known as a logical image, which only acquires the parts of the hard drive that have active data, and dismisses the rest of the drive. The VMDK, means that the image was taken from a Virtual Machine's hard drive.

Methodology and Methods

Equipment Used

Table 1: Software

Software	Version
Guidance Software Encase v7.10 Forensic Software	7.10.05
Magnet Forensics Internet Evidence Finder	6.7.7.1515
VMWare vSphere	5.5
Microsoft OneDrive	17.3.6381.0405
Google Drive Client	1.29
Apple iCloud	5.1
Dropbox	3.14.7

Data Collection

During this stage of the project, the goal was to conduct a variety of actions that could be done within all of the cloud services. A total of 28 files were created for the investigation, which evenly consisted of four file types: .docx, .jpg, .mp3 and .pdf. Multiple instances of each file type were used. Each instance had a different set of operations performed on it, made in accordance with the data generation sheet. Operations performed include uploading, downloading, accessing, editing and deleting. For example, File 3 of each file type was to be deleted. By taking continuous snapshots throughout data collection, the information could be easily analyzed for changes that occur within the computer. All of the timestamps, steps and directions required to complete the data collection were written out in a data generation script.

Analysis

As we began our data generation, it was important for us as a group to make sure we covered all of our bases. For this project, we made sure we created, modified, and deleted various file types. For all cloud services except for iCloud, we decided to use Windows 7 virtual machines, and for iCloud we used a MacOS virtual machine, running OS X El Capitan. Using the same data generation script, each group went through and made the changes to various files, to ensure that finding artifacts and comparing them would be easier. In this section we will cover each cloud service's analysis, explaining what was done on each machine, as well as any complications that were encountered during the course of our analysis..

OneDrive

We conducted our analysis of OneDrive with Encase v7.10; we wanted to see which files were created, deleted, or modified and in what directories they were stored, being cognizant of the scope of our investigation. We verified this by looking at a log file which updates when a user completes certain actions. We found these logs in the directory *C:/Users/lcdicloud/AppData/Local/Microsoft/OneDrive/log.*

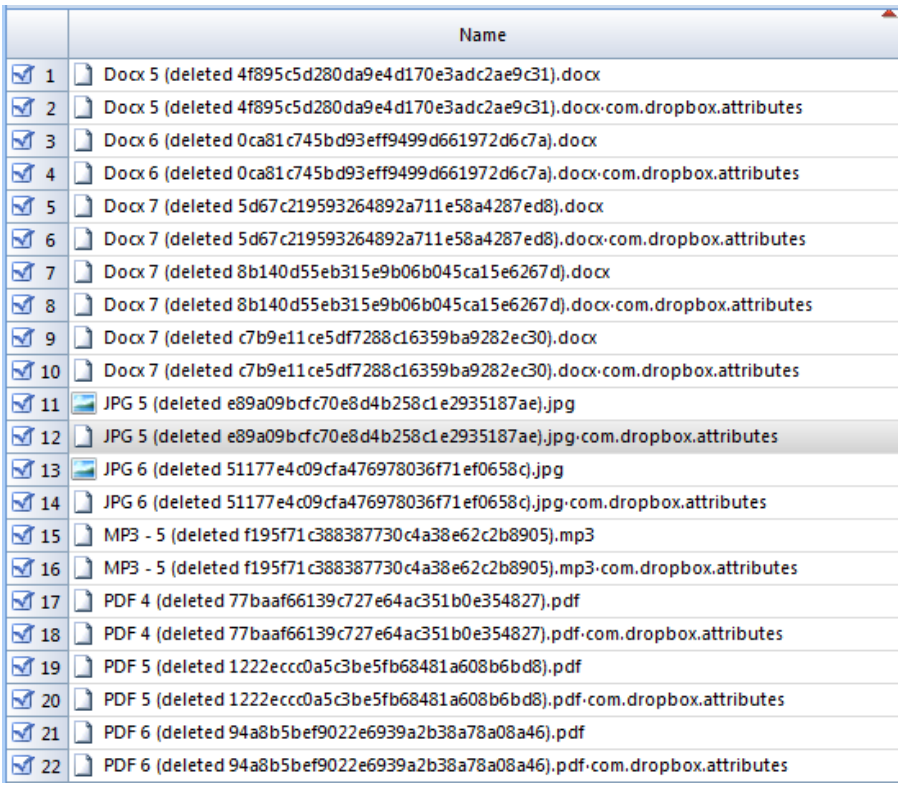
We found that log files contained a history of downloaded, deleted and modified files under two different file names: *C:/Users/lcdicloud/Appdata/Local/Microsoft/OneDrive/logs/Personal/SyncEngine-2016-2-25-924.2464.2.odl* and *C:/Users/lcdicloud/AppData/Local/Microsoft/OneDrive/log/SyncEngine-2016-2-26-98.2852.4.odl.* This occurred because the data generation took place over a two day period. Additionally, once we deleted a file it would be automatically put into the recycling bin whether deleted on the client or the browser. We also found that OneDrive creates a folder with a directory path of *C:/Users/lcdicloud/OneDrive* that contains all of the user's files.

We analyzed some of our registry data in Encase v7.10. Using the tool RegRipper 2.8, we parsed the registry files into a more comprehensible format. We found OneDrive artifacts in the *SYSTEM, NTUSER,* and *SOFTWARE* registries. In our analysis of the *SOFTWARE* directory we found that OneDrive created five registry subkeys, which corresponded with the scope of our investigation. In the *SYSTEM* directory we found a very important file, *OneDriveSetup.exe*, with the path *C:\Users\lcdicloud\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\V6P2WFBV\.* This helped us analyze and find other artifacts by showing that OneDrive data had been accessed through Internet Explorer. Since we used Internet Explorer to access OneDrive, we found two files that had been downloaded: *docx04.docx* and *mp306(PF).mp3* through Internet Explorer. We were able to view our deleted files in the *$Recycle Bin* directory.

Dropbox

The directory *C:\Users\%USERNAME%\AppData\Local\Dropbox\instance1* contains many of Dropbox's configuration files as well as all of the databases for each Dropbox installation on the computer. For older versions of Windows, there is a standalone tool made by Magnet Forensics, the tool allows for the decryption of Dropbox .dbx files. Unfortunately we were not able to decrypt any of the databases except for *filecache.dbx*, an encrypted database which contains a listing of all of the files which are stored in the users Dropbox.

Using Encase v7.10, we were able to go into the Dropbox directory under the user's profile, where we identified a folder named *.dropbox.filecache*. This file contained a folder which was named with a date that corresponded with when we deleted the files from the Dropbox web app. Inside this folder was a full copy of every file which had been deleted using the Dropbox web application.



	Name
1	Docx 5 (deleted 4f895c5d280da9e4d170e3adc2ae9c31).docx
2	Docx 5 (deleted 4f895c5d280da9e4d170e3adc2ae9c31).docx·com.dropbox.attributes
3	Docx 6 (deleted 0ca81c745bd93eff9499d661972d6c7a).docx
4	Docx 6 (deleted 0ca81c745bd93eff9499d661972d6c7a).docx·com.dropbox.attributes
5	Docx 7 (deleted 5d67c219593264892a711e58a4287ed8).docx
6	Docx 7 (deleted 5d67c219593264892a711e58a4287ed8).docx·com.dropbox.attributes
7	Docx 7 (deleted 8b140d55eb315e9b06b045ca15e6267d).docx
8	Docx 7 (deleted 8b140d55eb315e9b06b045ca15e6267d).docx·com.dropbox.attributes
9	Docx 7 (deleted c7b9e11ce5df7288c16359ba9282ec30).docx
10	Docx 7 (deleted c7b9e11ce5df7288c16359ba9282ec30).docx·com.dropbox.attributes
11	JPG 5 (deleted e89a09bcfc70e8d4b258c1e2935187ae).jpg
12	JPG 5 (deleted e89a09bcfc70e8d4b258c1e2935187ae).jpg·com.dropbox.attributes
13	JPG 6 (deleted 51177e4c09cfa476978036f71ef0658c).jpg
14	JPG 6 (deleted 51177e4c09cfa476978036f71ef0658c).jpg·com.dropbox.attributes
15	MP3 - 5 (deleted f195f71c388387730c4a38e62c2b8905).mp3
16	MP3 - 5 (deleted f195f71c388387730c4a38e62c2b8905).mp3·com.dropbox.attributes
17	PDF 4 (deleted 77baaf66139c727e64ac351b0e354827).pdf
18	PDF 4 (deleted 77baaf66139c727e64ac351b0e354827).pdf·com.dropbox.attributes
19	PDF 5 (deleted 1222eccc0a5c3be5fb68481a608b6bd8).pdf
20	PDF 5 (deleted 1222eccc0a5c3be5fb68481a608b6bd8).pdf·com.dropbox.attributes
21	PDF 6 (deleted 94a8b5bef9022e6939a2b38a78a08a46).pdf
22	PDF 6 (deleted 94a8b5bef9022e6939a2b38a78a08a46).pdf·com.dropbox.attributes

*Figure 1: Items in the **.dropbox.filecache** directory*

It is interesting to note that the files that we found in this folder had data appended to their names. In every case it was the word deleted followed by 16 hexadecimal bytes which we suspect to be a hash of the file as well as a timestamp. At this time we have not been able to prove or disprove this fact, however we can confirm that it is not an MD5 or SHA1 hash of the original file.

In addition, Encase v7.10 shows that each of these files in the cached folder have an alternate data stream. For all files except for .jpg files, the alternate data stream was 83 bytes in size. The first two bytes of the files matched that of an artifact compressed with Zlib. Using the "zlib.decompress()" function in Python, the data streams were able to be decompressed, revealing what appears to be identifying information about the files. For example, the file named *Docx 5 (deleted 4f895c5d280da9e4d170e3adc2ae9c31).docx-+com.dropbox.attributes* contained compressed text, shown in Figure 2 below:

```
xœ«VJ)É/HÉ¯^OËÌIÍL‰ÏÉONÌQ²R¨VÉMLÎÈÌ↳%%–"¶…R↑K↑⇵%ã*₀Ó°âdoC"D·¶ç€,¯€ô,Œ@[[¥ÚÚZ ¿Ó;
```

*Figure 2: A compressed **.attributes** file*

When decompressed, shown below (Figure 3):

```
{"dropbox_fileid_local": {"machineid_attr": {"data": "3z85VscK14aHdCPpJPgphQ=="}}}
```

*Figure 3: A decompressed **.attributes** file*

These appear to be identifiers for each file.

Google Drive

The Google Drive desktop app is almost entirely linked to the Drive browser client. When the application is installed on a machine, a directory is created in **C:/Users/<USER>/AppData/Local/Google/Drive**. To associate a Google account with the app, a window opens to a standard browser login screen, and then creates a new folder in the user directory where the account's Drive contents are automatically synchronized to. When a file is accessed through this folder, it opens the default browser and directs the user to the file through Google Drive's website. If one of these shortcuts get deleted, the corresponding file is moved to the user's Trash folder in the browser. The trashed file can be recovered, but is lost if the Trash folder is emptied. If a desktop shortcut is moved from the sync folder, the shortcut still exists and works as normal; if a file is downloaded to the desktop from the browser, this file is now independent of any changes made to the original document in Drive.

An analysis of the Drive directory shows a single predominant artifact: a very large file named **synclog.log**. All other files in the directory were either unrelated or indiscernible. This file logs all communication between the desktop application and the main Drive browser client, making it a prime source of information regarding actions taken while utilizing Google Drive.

iCloud

Overall, the investigation of iCloud was successful. The data that was received from the analysis shows what data is created after the initial login of iCloud; this is shown below in the results section. The data also shows any changes in location when files were moved from the iCloud folder after logging out of the active account or disabling the service entirely. Along with the results, screenshots are provided that show the file paths of artifacts that reveal information such as the username of the account currently logged into iCloud. Each screenshot was taken to show the instances of when files were created, moved, edited, and deleted on the hard drive. Using the pictures provided, the data found within the hard drive can be compared with snapshots of the VM captured before, during, and data generation actions were completed.

After the completing the data generation procedure, some of the files' timestamps from within the hard drive of the VM were found to not be in sync with the time recorded during datagen. After creating the documents, the timestamps were checked from within the computer, where it was first noted that the computer's clock was 3 hours off. The problem was identified as a possible incompatibility between the operating system and the VM software, with the VM's date and time not updating each time it is accessed. Every time the VM was not in use, the software would put the VM into a suspension mode, which essentially freezes the current state of the VM, including the time. So every time the VM was turned back on, the clock would remain at the same time from the previous session. During the analysis, another group of researchers used the same VM, thus the clock was always changing. Although this may have possibly contributed to the error, it could not be linked to the direct cause. After collaborating with another investigation of a different cloud service, in which a Windows 7 VM was used, the error did not take place, and in fact the time remained accurate whenever logging in and out. This error could have been avoided had the investigation been done on a computer with the sole purpose for this investigation, thus excluding any possibility of contamination from other investigations taking place. Also, had the data generation sheet completed in a single session and not over the span of several days, the time would have never been interrupted. A solution that was implemented during the investigation was to manually re-adjust the clock every time the user logged in, which required administrator access to complete. An error of this caliber could potentially hinder investigators by not being able to validate whether certain data was in a given location at a given time.

Another major complication arose while analyzing the hard drive images of the VM. Once all of the images were ready to be uploaded into Encase, the image containing the pre-datagen data was the only one that could be processed. The other images were empty, but should have contained the changes in the data on the hard drive of the VM. The problem was that each time a snapshot of the VM was taken, the .vmdk file – which contained the entirety of the VM's file system - was split into multiple files. A solution was found online to be able to piece together the VM image. vSphere has a unique set of features, one of which allows a user to combine two parts of a VM's image. After the process was complete, the same was done for the remaining images, and finally the images were uploaded to Encase v7.10 for analysis.

Results

OneDrive

When perusing our virtual image, most of our results came from different locations in various directories. A large amount of pertinent data was found with in log files, temporary internet files and the Windows registry. OneDrive logs with all information pertaining to the data generation were found under *C:\Users\Lcdicloud\AppData\Local\Microsoft\Onedrive\Logs\Personal.* This directory contained 18 separate sync logs that we scanned through. Most of the data from our results came from *SyncEngine-2016-2-25-924.2464.2.odl and SyncEngine-2016-2-26-98.2852.4.odl*. These are *.odl* files, which are used with the Microsoft Visual Development environment with applications that are written in the C/C++ programming language. We had two separate days of log files because our data generation was carried out over two days. The timestamps themselves were off because the date and time within VM time inaccurate when we started and we didn't notice until after our analysis. When looking at the results from our we found our files under the file path *C:/Users/lcdicloud/OneDrive***.** It contained all of our files that we utilized for the data generation.

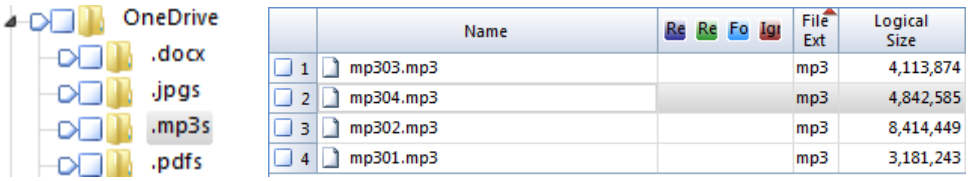


Figure 4: The OneDrive directory and its contents

Looking at our results in Encase v7.10 we found OneDrive artifacts in the *SYSTEM, NTUSER, SOFTWARE* registry. In the *SYSTEM* directory we found the file *OneDriveSetup.exe* The file path is *C:\Users\lcdicloud\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\V6P2WFBV\OneDriveSetup.exe***.**

This verified that OneDrive data had been accessed through Internet Explorer. Since we used Internet Explorer to access OneDrive, we located two files that had been downloaded: *docx04.docx* and *mp306(PF).mp3* through Internet Explorer (Figure 5). The browser then attaches an alternate data stream to the file downloaded. The alternate data stream Zone Identifier is the name used by Internet Explorer. This verifies that it was downloaded from a trusted browser by the operating system (Figure 6).

Figure 5: Items in the Internet Explorer directory

edownloader.cpp EnclosureDownloader::StartDownload
6089890299B0D363!231 }K>> enclosuredownloader.cpp. EnclosureDownloader::Execute
NextDownloadStep 6089890299B0D363!231 jpg04.jpg
3b15be84aff20b322a93c0b9aaa62e25 6089890299B0D363!231.0 TransferBlocks }K>> enc

4 }K>> 49 localchanges.cpp handleLocalRemoveFile 6089890299B0D363!258 %MountPoin
t%\.pdfs\pdf06.pdf }K>> localchanges.cppb startLocalChangeHash %MountPoint%\
.pdfs\pdf06.pdf }K>> localchanges.cppm handleLocalChanges
LC_HASH 10 }K>> localchanges.cpp handleLocalChangeHash %MountPoint%\.pdfs\
pdf06.pdf }K>> localchanges.cppm handleLocalChanges LC_DELETE_FILE
4 }K>> 49 localchanges.cpp handleLocalRemoveFile 6089890299B0D363!258 %MountPoin
t%\.pdfs\pdf06.pdf }K>> 4| localchanges.cpp doFileRemove %MountPoint%\.pdfs\
pdf06.pdf X }K>> 4w watcher.cpp Watcher::Monitor X

Figure 6: Information in the alternate data stream

Once the files were deleted they could be viewed in the *$Recycling Bin (S-1-5-21-3232094785-1753034976-2445384379-1000)* through Encase 7.10 (Figure 7).

	Name	Re Re Fo Igr	File Ext	Logical Size
14	jpg05.jpg		jpg	114,635
15	$IJS243Y.jpg		jpg	544
16	$I1ALKHM.mp3		mp3	544
17	mp306(PF).mp3		mp3	6,623,299
18	mp305(Hope).mp3		mp3	3,798,830
19	$IX5TY6C.mp3		mp3	544
20	pdf05.pdf		pdf	373,591
21	pdf06.pdf		pdf	29,127
22	pdf03.pdf		pdf	5,150,626
23	$I5SRA0B.pdf		pdf	544
24	$IM15JQO.pdf		pdf	544
25	$I75A0AD.pdf		pdf	544

*Figure 7: Items in the **Recycle Bin***

We found that OneDrive created five registry sub keys coinciding with its initial execution through Internet Explorer on February 25th, 2016. Since the date and time inside the VM was not in sync with the workstation it was difficult to verify the exact time that user actions occurred in the datagen (Figure 8).

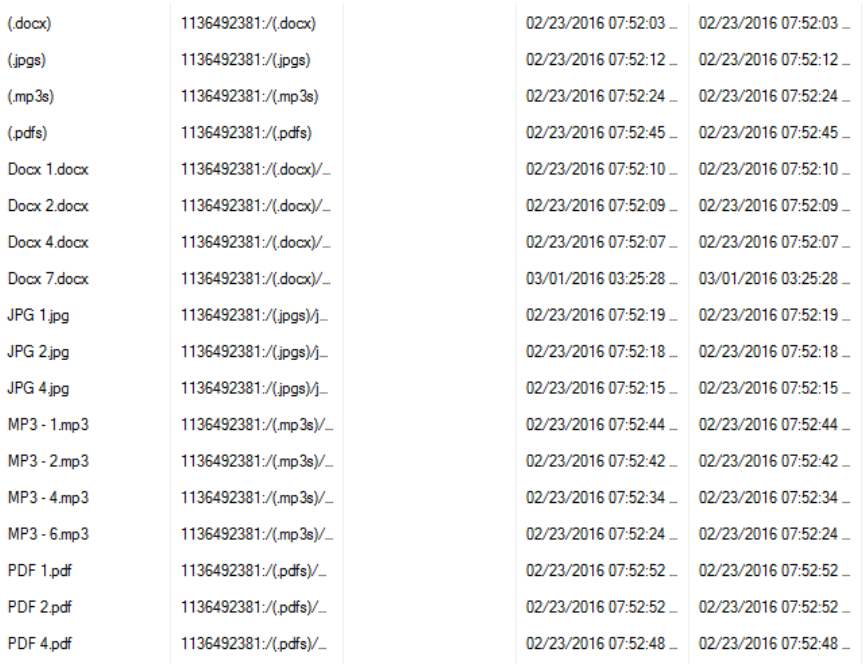
```
shelloverlay
Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
LastWrite Time Thu Feb 25 09:19:44 2016 (UTC)

Thu Feb 25 09:19:44 2016 Z
   OneDrive1  {BBACC218-34EA-4666-9D7A-C78F2274A524}
   OneDrive2  {5AB7172C-9C11-405C-8DD5-AF20F3606282}
   OneDrive3  {A78ED123-AB77-406B-9962-2A5D9D2F7F30}
   OneDrive4  {F241C880-6982-4CE5-8CF7-7085BA96DA5A}
   OneDrive5  {A0396A93-DC06-4AEF-BEE9-95FFCCAEF20E}
```

*Figure 8: Changes made in the **Software Registry***

Dropbox

Our analysis was originally hindered while trying to decrypt Dropbox's database files. These files are encrypted SQLite databases, which are secured using the password of the local account password. The software that we attempted to use to decrypt the files were incompatible with the Windows 7 system data. Our next tool was IEF 6.7's Dropbox artifact module, which required us to enter the user's local account password in order to be able to decrypt the *filecache.dbx* file located in *C:\Users\%USERNAME%\AppData\Local\Dropbox\instance1* (Figure 9).



(.docx)	1136492381:/(.docx)		02/23/2016 07:52:03 ...	02/23/2016 07:52:03 ...
(.jpgs)	1136492381:/(.jpgs)		02/23/2016 07:52:12 ...	02/23/2016 07:52:12 ...
(.mp3s)	1136492381:/(.mp3s)		02/23/2016 07:52:24 ...	02/23/2016 07:52:24 ...
(.pdfs)	1136492381:/(.pdfs)		02/23/2016 07:52:45 ...	02/23/2016 07:52:45 ...
Docx 1.docx	1136492381:/(.docx)/...		02/23/2016 07:52:10 ...	02/23/2016 07:52:10 ...
Docx 2.docx	1136492381:/(.docx)/...		02/23/2016 07:52:09 ...	02/23/2016 07:52:09 ...
Docx 4.docx	1136492381:/(.docx)/...		02/23/2016 07:52:07 ...	02/23/2016 07:52:07 ...
Docx 7.docx	1136492381:/(.docx)/...		03/01/2016 03:25:28 ...	03/01/2016 03:25:28 ...
JPG 1.jpg	1136492381:/(.jpgs)/j...		02/23/2016 07:52:19 ...	02/23/2016 07:52:19 ...
JPG 2.jpg	1136492381:/(.jpgs)/j...		02/23/2016 07:52:18 ...	02/23/2016 07:52:18 ...
JPG 4.jpg	1136492381:/(.jpgs)/j...		02/23/2016 07:52:15 ...	02/23/2016 07:52:15 ...
MP3 - 1.mp3	1136492381:/(.mp3s)/...		02/23/2016 07:52:44 ...	02/23/2016 07:52:44 ...
MP3 - 2.mp3	1136492381:/(.mp3s)/...		02/23/2016 07:52:42 ...	02/23/2016 07:52:42 ...
MP3 - 4.mp3	1136492381:/(.mp3s)/...		02/23/2016 07:52:34 ...	02/23/2016 07:52:34 ...
MP3 - 6.mp3	1136492381:/(.mp3s)/...		02/23/2016 07:52:24 ...	02/23/2016 07:52:24 ...
PDF 1.pdf	1136492381:/(.pdfs)/...		02/23/2016 07:52:52 ...	02/23/2016 07:52:52 ...
PDF 2.pdf	1136492381:/(.pdfs)/...		02/23/2016 07:52:52 ...	02/23/2016 07:52:52 ...
PDF 4.pdf	1136492381:/(.pdfs)/...		02/23/2016 07:52:48 ...	02/23/2016 07:52:48 ...

*Figure 9: Items found in **filecache.dbx***

After our analysis of the image using Encase v7.10 we were successfully able to retrieve a copy of every file in the user's Dropbox folder except the one that was permanently deleted from the client computer during the data generation (Figure 10).

File	Recovered?
Doc1.docx	✓
Doc 2.docx	✓
Doc3.docx	✗

Doc4.docx	✓
Doc5.docx	✓
Doc6.docx	✓
Doc7.docx	✓

Figure 10: Word documents recovered

Google Drive

Although the synchronization log documents every single action performed while the user is accessing the service - resulting in thousands of lines of text - there is no real encryption besides unique identifiers (UIDs), so there were few obstacles in terms of finding relevant data. Something we noticed right away was that actions made to documents through the desktop shortcuts are articulated in the log, enclosed with plenty of useful information. This is shown in Figure 11 below:

```
2016-02-29 06:19:36,371 -0500 INFO pid=2236 2804:Worker-1
common.workers:194 Worker successfully completed
[ImmutableChange(Direction.DOWNLOAD, Action.MOVE, ino=1125899906902254,
name=Docx 4.docx,
route=[ImmutableCloudEntry(doc_id=0B1352biCAKVQc2FDZlZPNVF2NTA,filename=(,docx),
modified=1456771139,created=1456771141,acl_role=owner,doc_type=DocType.FOLDER,re
moved=False,parent_doc_ids=frozenset(['root']),child_doc_ids=frozenset(['0B1352b
iCAKVQSEo3bUdneWZ1ajg', '0B1352biCAKVQdU1nWWNVbUpiLVU',
'0B1352biCAKVQa2RvdWFGRGhIM00', '0B1352biCAKVQWmNGb0t3LXdPYmc',
'0B1352biCAKVQTk5LaDNtT090RFU', '1DEunG74vnfamj8IhgCIHpHjcla_JOumYmUE27GYo9gA',
'0B1352biCAKVQQjVxRnUzTDYzVGM']),size=0,checksum=None,change_stamp=543,server_mo
d_time=1456773521,is_zombie=False,shared=False,recursive_size=None,resource_type
=folder,version=None),ImmutableCloudEntry(doc_id=1DEunG74vnfamj8IhgCIHpHjcla_JOu
mYmUE27GYo9gA,filename=Docx
4.docx,modified=1456773521,created=1456773520,acl_role=owner,doc_type=DocType.DO
CUMENT,removed=False,parent_doc_ids=frozenset(['0B1352biCAKVQc2FDZlZPNVF2NTA']),
child_doc_ids=frozenset([]),size=0,checksum=None,change_stamp=547,server_mod_tim
e=1456773525,is_zombie=False,shared=False,recursive_size=None,resource_type=docu
ment,version=None)], rid=1DEunG74vnfamj8IhgCIHpHjcla_JOumYmUE27GYo9gA,
parent_ino=1970324837033273, is_folder=False, unparents_shared=False,
old_parent_ino=1970324837033273, shared=False, is_cancelled=False,
doc_type=DocType.DOCUMENT, hash=-1791727862, _constructor_called=True)]
```

*Figure 11: Information in **synclog.log***

Each documented action is attached with a plaintext timestamp, a description of the action performed, the name of the document, and epoch timestamps (created, modified) associated with the specified file. At the beginning of the log, the timestamps were accurate with the information documented in the script during data generation. Similar examples were gathered from other actions made through the desktop app during the datagen process, such as synchronization to the Drive desktop folder, downloading files, and edits in progress.

Unfortunately, at some point the timestamps switched to a completely different timeframe, shown below:

```
2016-02-29 13:42:54,184 -0500 INFO pid=3920 3924:MainThread
common.sync_app:1767 Repr caching stats: <class
'common.worker.worker_event.WorkerCreateCloudEvent'>:
 max hits: 1
 mean hits: 1.0
 max miss: 0
 mean miss: 0.0
<class 'common.delivery.ImmutableChange'>:
 max hits: 3
 mean hits: 3.0
 max miss: 0
 mean miss: 0.0
<class 'common.raw_event.ImmutableRawEvent'>:
 max hits: 7
 mean hits: 5.51428571429
 max miss: 0
 mean miss: 0.0
2016-02-29 06:15:06,934 -0500 INFO pid=2236 2252:MainThread    logging:1627
OS: Windows/6.1-SP1
2016-02-29 06:15:06,934 -0500 INFO pid=2236 2252:MainThread    logging:1627
Google Drive (build 1.27.1227.2094)
2016-02-29 06:15:06,934 -0500 INFO pid=2236 2252:MainThread    logging:1627
SSL: OpenSSL 1.0.1p 9 Jul 2015
2016-02-29 06:15:06,934 -0500 INFO pid=2236 2252:MainThread
common.multi_account.migration:60 Skipping upgrade (already performed).
```

*Figure 12: The timestamp in **synclog.log** has changed.*

We believe this discrepancy comes from an internal time issue within the VM used for data generation, and are doubtful that an issue of this nature would replicate itself on a personal computer that receives its internal time from the Internet.

Despite the wealth of information contained in the synchronization log, the files' actual destination is not accessible.

iCloud

There are a series of files and folders that are created simply by signing into iCloud. All Apple devices come pre-installed with iCloud, and also requires a login with a valid Apple or iCloud account. Once logged in, the iCloud folder will be created in the path *Users/(USERNAME)/Library/Application Support/* (Figure 13). This folder contains another created folder, */Accounts/,* whose contents include a file with the username of the iCloud account logged on to the computer. However, these were not the only paths created by iCloud.

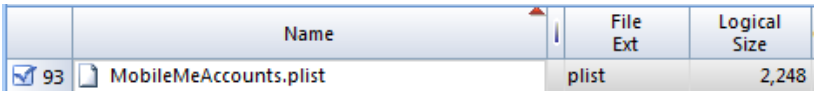
	Name
1	10142266693
2	lcdi.cloudforensics@gmail.com

*Figure 13: Items in the **Accounts** directory*

In the path *Users/(USERNAME)/Library/Preferences/,* two files were also created after logging into iCloud: *MobileMeAccounts.plist* and *com.apple.icloud.fmfd.notbackedup.plist* - both of which are binary plists, and cannot be read by a regular text editor, such as Notepad++ (used to read .plists up to this point in the project). These plists are shown below (Figures 14 and 15).

	Name	File Ext	Logical Size
34	com.apple.iChat.Yahoo.plist	plist	96
35	com.apple.icloud.fmfd.notbackedup.plist	plist	928
36	com.apple.icloud.fmfd.plist	plist	1,024

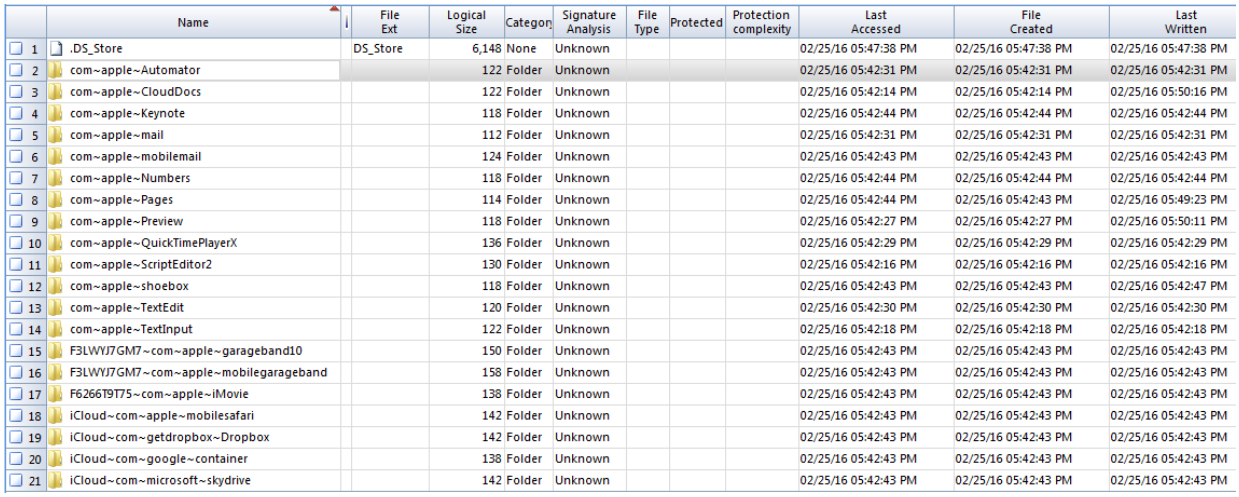
Figure 14: Binary plists



	Name	File Ext	Logical Size
93	MobileMeAccounts.plist	plist	2,248

Figure 15: MobileMeAccounts plist

One of the most important created artifacts is found in *Users/(USERNAME)/Library/Mobile Documents/* (Figure 16). This folder acts as a directory on the hard drive, holding data for all of the files that are stored on iCloud. In other words, all of the data available on the iCloud, when being viewed in a web browser, can also be viewed within this folder.



	Name	File Ext	Logical Size	Categor	Signature Analysis	File Type	Protected	Protection complexity	Last Accessed	File Created	Last Written
1	.DS_Store	DS_Store	6,148	None	Unknown				02/25/16 05:47:38 PM	02/25/16 05:47:38 PM	02/25/16 05:47:38 PM
2	com~apple~Automator		122	Folder	Unknown				02/25/16 05:42:31 PM	02/25/16 05:42:31 PM	02/25/16 05:42:31 PM
3	com~apple~CloudDocs		122	Folder	Unknown				02/25/16 05:42:14 PM	02/25/16 05:42:14 PM	02/25/16 05:50:16 PM
4	com~apple~Keynote		118	Folder	Unknown				02/25/16 05:42:44 PM	02/25/16 05:42:44 PM	02/25/16 05:42:44 PM
5	com~apple~mail		112	Folder	Unknown				02/25/16 05:42:31 PM	02/25/16 05:42:31 PM	02/25/16 05:42:31 PM
6	com~apple~mobilemail		124	Folder	Unknown				02/25/16 05:42:43 PM	02/25/16 05:42:43 PM	02/25/16 05:42:43 PM
7	com~apple~Numbers		118	Folder	Unknown				02/25/16 05:42:44 PM	02/25/16 05:42:44 PM	02/25/16 05:42:44 PM
8	com~apple~Pages		114	Folder	Unknown				02/25/16 05:42:44 PM	02/25/16 05:42:43 PM	02/25/16 05:49:23 PM
9	com~apple~Preview		118	Folder	Unknown				02/25/16 05:42:27 PM	02/25/16 05:42:27 PM	02/25/16 05:50:11 PM
10	com~apple~QuickTimePlayerX		136	Folder	Unknown				02/25/16 05:42:29 PM	02/25/16 05:42:29 PM	02/25/16 05:42:29 PM
11	com~apple~ScriptEditor2		130	Folder	Unknown				02/25/16 05:42:16 PM	02/25/16 05:42:16 PM	02/25/16 05:42:16 PM
12	com~apple~shoebox		118	Folder	Unknown				02/25/16 05:42:43 PM	02/25/16 05:42:43 PM	02/25/16 05:42:47 PM
13	com~apple~TextEdit		120	Folder	Unknown				02/25/16 05:42:30 PM	02/25/16 05:42:30 PM	02/25/16 05:42:30 PM
14	com~apple~TextInput		122	Folder	Unknown				02/25/16 05:42:18 PM	02/25/16 05:42:18 PM	02/25/16 05:42:18 PM
15	F3LWYJ7GM7~com~apple~garageband10		150	Folder	Unknown				02/25/16 05:42:43 PM	02/25/16 05:42:43 PM	02/25/16 05:42:43 PM
16	F3LWYJ7GM7~com~apple~mobilegarageband		158	Folder	Unknown				02/25/16 05:42:43 PM	02/25/16 05:42:43 PM	02/25/16 05:42:43 PM
17	F6266T9T75~com~apple~iMovie		138	Folder	Unknown				02/25/16 05:42:43 PM	02/25/16 05:42:43 PM	02/25/16 05:42:43 PM
18	iCloud~com~apple~mobilesafari		142	Folder	Unknown				02/25/16 05:42:43 PM	02/25/16 05:42:43 PM	02/25/16 05:42:43 PM
19	iCloud~com~getdropbox~Dropbox		142	Folder	Unknown				02/25/16 05:42:43 PM	02/25/16 05:42:43 PM	02/25/16 05:42:43 PM
20	iCloud~com~google~container		138	Folder	Unknown				02/25/16 05:42:43 PM	02/25/16 05:42:43 PM	02/25/16 05:42:43 PM
21	iCloud~com~microsoft~skydrive		142	Folder	Unknown				02/25/16 05:42:43 PM	02/25/16 05:42:43 PM	02/25/16 05:42:43 PM

*Figure 16: Items in the **Mobile Documents** directory*

With further analysis, the data also serves to help find evidence of files after they had been deleted from the cloud storage application folder. The first place to look is in the Trash (the recycling bin of MacOS). Content deleted from the iCloud folder is sent to the Trash and stays until manually emptied/deleted. Once deleted, the actual file couldn't be found. However, with some searching, a path was found that contained thumbnails of all files ever held within the iCloud folder, located in *\private\var\folders\2n\584mlx0s09zdgxsry9qg597r0000gn\C\com.apple.QuickLook.thumbnailcache\thumbnails.data* (Figure 17)

	Name	Re	Re	Fo	Ig	File Ext	Logical Size	Category	Signature Analysis	File Type
1	JPG 5.jpg.bmp					bmp	16,438	Picture	Match	Microsoft Bitm...
2	JPG 5.jpg.4321					4321	136	None	Unknown	
3	JPG 6.jpg.bmp					bmp	16,438	Picture	Match	Microsoft Bitm...
4	JPG 6.jpg.4321					4321	136	None	Unknown	
5	JPG 2.jpg.bmp					bmp	16,438	Picture	Match	Microsoft Bitm...
6	JPG 2.jpg.4321					4321	136	None	Unknown	
7	JPG 4.jpg.bmp					bmp	16,438	Picture	Match	Microsoft Bitm...
8	JPG 4.jpg.4321					4321	136	None	Unknown	
9	JPG 3.jpg.bmp					bmp	16,438	Picture	Match	Microsoft Bitm...
10	JPG 3.jpg.4321					4321	136	None	Unknown	
11	JPG 1.jpg.bmp					bmp	16,438	Picture	Match	Microsoft Bitm...
12	JPG 1.jpg.4321					4321	136	None	Unknown	
13	PDF 6.pdf.bmp					bmp	16,438	Picture	Match	Microsoft Bitm...
14	PDF 6.pdf.4321					4321	160	None	Unknown	
15	PDF 4.pdf.bmp					bmp	16,438	Picture	Match	Microsoft Bitm...
16	PDF 4.pdf.4321					4321	160	None	Unknown	
17	PDF 5.pdf.bmp					bmp	16,438	Picture	Match	Microsoft Bitm...

*Figure 17: Items in **thumbnails.data***

This folder contains .bmp files - a thumbnail of each file - as well as unknown files with the extension .4321. When iCloud is logged out, many of the files created were also deleted off the machine; however these files remained untouched. The content of the files in thumbnail form cannot be read, due to the resolution of the pictures being too small; however, the existence of these files alone, could be evidence enough link files to an iCloud account.

In the same location as the thumbnails there is another file that is very important: *\private\var\folders\2n\584mlx0s09zdgxsry9qg597r0000gn\C\com.apple.QuickLook.thumbnailcache\index.sqlite* (Figure 18). This file is a sqlite database file that shows the location of the files that were found within the iCloud, as well as their file paths on the hard drive. This data helps determine the new location of a file, every time a file is moved.

	folder	file_name	fs_id
	Filter	Filter	Filter
19	/Users/lcdicf/Library/Mobile Documents/com~apple~Pages/Documents	Pages Doc 6.pages	/.file/id=6571367.436376/
20	/Users/lcdicf/Library/Mobile Documents/com~apple~CloudDocs/MP3	MP3 - 5.mp3	/.file/id=6571367.435399
21	/Users/lcdicf/Library/Mobile Documents/com~apple~CloudDocs/MP3	MP3 - 4.mp3	/.file/id=6571367.435382
22	/Users/lcdicf/Library/Mobile Documents/com~apple~CloudDocs/MP3	MP3 - 2.mp3	/.file/id=6571367.435396
23	/Users/lcdicf/Library/Mobile Documents/com~apple~CloudDocs/MP3	MP3 - 1.mp3	/.file/id=6571367.435389
24	/Users/lcdicf/Library/Mobile Documents/com~apple~CloudDocs/PDF	PDF 1.pdf	/.file/id=6571367.435381
25	/Users/lcdicf/Library/Mobile Documents/com~apple~CloudDocs/PDF	PDF 2.pdf	/.file/id=6571367.435392
26	/Users/lcdicf/Desktop	Untitled 1.odt	/.file/id=6571367.453108
27	/Users/lcdicf/Desktop/docs	doc 2.2.odt	/.file/id=6571367.453457
28	/Users/lcdicf/Library/Mobile Documents/com~apple~Pages/Documents	doc 2.2.odt	/.file/id=6571367.453457
29	/Users/lcdicf/Downloads	Pages Doc 4.pages	/.file/id=6571367.453726/

*Figure 18: Items found in **index.sqlite***

Conclusion

Cloud services are far from identical; therefore each analysis produced very results. From some services, such as Dropbox and OneDrive, full documents were able to be recovered, whereas services like Google Drive and iCloud were not. The artifacts that have been found during this investigation are new, and can therefore be helpful in aiding law enforcement investigations involving laptop and desktop computers. That being said, some of these artifacts have already identified. This does not mean that the artifacts have lost their value - in fact it is imperative that forensic artifacts taken from cloud services are often revisited to keep up with rapid update cycles.

The gathered results show that every time an action is taken with a file - whether it is created, deleted, modified, or accessing - there are artifacts left behind to some capacity. Evidence shows that when files are deleted, they may have only moved to a recycling or trash bin. Certain logs record when there is a change in the data or the file is moved. Depending where the data was found, sometimes the document would give exact details as to what happened to the document. For example it would provide what happened to the file, followed by where it was located, as well as the name of the document. Overall the goal, of artificially creating artifacts and locating evidence of this, was completed successfully.

Further Work

Cloud forensics is an ever growing field and more research will be done in the future. The team only looked at four common cloud services and there are many more being used. Cloud services have been around for a while now, and more people, and businesses use them each day. We have just scratched the surface, there is much more to be done with cloud storage, including mobile cloud applications. Cloud forensics will keep gaining more popularity, making it a key resource to use for forensic investigators.

Appendix

OneDrive: Data Generation Sheet

OneDrive	User Action	Directions
DATE/TIME	**NAME**	
	Prior to Data Gen	
2/25/2016 11:09:00	Start VMware vSphere	Open VMware Sphere, the VM should load automatically. Hit the play button to unsuspend
2/25/2016 11:09:00	Capture snapshot of VM	Click "Add Snapshot" along the taskbar. Name snapshot "Drive pre-data gen".

2/25/2016 11:10:00	Copy vmdk file	Copy vmdk file of VM to folder on resource drive called ".vmdks for onedrive", and place inside and title "Fresh Install"
2/25/2016 11:50:00	Download and install onedrive (Desktop)	Navigate to "https://onedrive.live.com/about/en-us/download/" and install normal onedrive
2/25/2016 11:56:00	Copy vmdk file	Copy vmdk file of VM to folder on resource drive called ".vmdks for onedrive", and place inside and title"after onedrives installed"
2/25/2016 12:27:00	Log in to onedrive Desktop client	Start onedrive Desktop client. onedrive credentials located on Secret Server.
2/25/2016 12:30:00	Log in to onedrive web client	Start Internet Explorer, navigate to onedrive.com. Login using credentials located on Secret Server.
2/25/2016 12:33:00	Put files into onedrive	Take all the files (.DOCx, JPG, MP3, PDF) from Google Drive, and insert them into the onedrive account.
	File Type: .Docx	
2/26/2016 11:13:00	Ignore < .Docx 1>	DO NOT TOUCH <.Docx 1>
2/26/2016 11:13:00	Access < .Docx 2>	Access onedrive on desktop and open < .Docx 2> (just open)
2/262016 11:18:00	Delete < .Docx 3>	Access the onedrive on desktop and delete < .Docx 3>
2/26/2016 11:20:00	Download < .Docx 4>	Open onedrive in Internet Explorer, navigate to and download < .Docx 4> to the downloads folder
2/26/2016 11:21:00	delete < .Docx 5>	Open onedrive in Internet Explorer, delete < .Docx 5>
2/26/2016 11:22:00	Access and delete < .Docx 6>	Access < .Docx 6> online and delete from onedrive (online)
2/26/2016 11:27:00	edit < .Docx 7>	Access onedrive on desktop and edit < .Docx 7> Then using onedrive in Internet Explorer delete < .Docx 7>
	File Type: JPG	
2/26/2016 11:43:00	Ignore <JPG 1>	DO NOT TOUCH <JPG 1>

2/26/2016 11:43:00	Access <JPG 2>	Access onedrive on Desktop and open <JPG 2> (just open)
2/26/2016 11:44:00	Delete <JPG 3>	Access onedrive on desktop and delete <JPG 3>
2/26/2016 11:45:00	Download <JPG 4>	Open onedrive in Internet Explorer, download <JPG 4> to the downloads folder
2/26/2016 11:47:00	Delete Online <JPG 5>	Access onedrive on desktop and delete <JPG 5>
2/26/2016 11:47:00	Access and delete <JPG 6>	Access onedrive in internet explorer and open <JPG 6>. Then using onedrive online delete <JPG 6>
	File Type: MP3-	
2/26/2016 11:50:00	Ignore <MP3 - 1>	DO NOT TOUCH <MP3 - 1>
2/26/2016 11:50:00	Access <MP3 - 2>	Access onedrive on desktop and open <MP3 - 2>. (just open)
2/26/2016 11:51:00	Delete <MP3 - 3>	Access onedrive on desktop and delete <MP3 - 3>
2/26/2016 11:53:00	Download <MP3 - 4>	Open onedrive in Internet Explorer, download <MP3 - 4> to the downloads folder
2/26/2016 11:55:00	Delete Online <MP3 - 5>	Open onedrive in internet explorer, delete <MP3 - 5>
2/26/2016 11:55:00	Access and delete <MP3 - 6>	Access onedrive in internet explorer and open <MP3 - 6>. Then using onedrive online delete <MP3 - 6>
	File Type: PDF	
2/26/2016 11:59:00	Ignore <PDF 1>	DO NOT TOUCH <PDF 1>
2/26/2016 12:00:00	Access <PDF 2>	Access onedrive on desktop and open <PDF 2>. (just open)
2/26/2016 12:10:00	Delete <PDF 3>	Access onedrive on desktop and delete <PDF 3>

2/26/2016 12:01:00	Download <PDF 4>	Open onedrive in Internet Explorer, download <PDF 4> to the downloads folder
2/26/2016 12:04:00	Delete Online<PDF 5>	Open onedrive in internet explorer, delete <PDF 5>
2/26/2016 12:05:00	Access and delete <PDF 6>	Access onedrive in internet explorer and open <PDF 6>. Then using onedrive online delete <PDF 6>
	Desync Online	
3/22/2016	Create Word Document Online.	Open Internet Explorer 10. In URL bar search "onedrive". Login with account credentials. When the OneDrive webpage is loaded select New > Word Document > Doc_1 3.22.2016
	After DataGen	
2/26/2016 12:20:00	Copy VMDK file	Copy vmdk file of VM to folder on resource drive called ".vmdks for onedrive", and place inside and title "After DataGen"

Dropbox: Data Generation Sheet

Date/Time	Data Gen Action	Directions
XX:XX:XX XX/XX/2016	Name	
	Pre-DataGen	
	Noah Siddall	
2/24/2016 16:34:00	Start VMware vSphere Client	Open VMware vSphere Client C:\Program Files (x86)\VMware\Infrastructure\Virtual Infrastructure Client\Launcher\
2/24/2016 16:34:00	Sign In to Virtual Windows 7 Machine	Enter "192.168.1.2" for IP address, check "Use Windows session credentials" then press "Login" Ignore SSL certificate warnings
2/24/2016 16:35:00	Power Up Windows 7 Machine	Select "Hosts and Clusters." Expand the dropdown menus on the left (vCenter.research.lcdi > LCDI > 192.168.1.20 > Cloud Forensics VM) select "Cloud Forensics VM: onedrive." Power up the machine by pressing the green arrow and launch the virtual machine console by selecting the icon with the desktop and green arrow in it.
2/24/2016 16:37:00	Sign In	Sign in to the user "lcdicloud" password on secret server
2/24/2016 16:38:00	Create Snapshot of the "fresh" machine.	Select "Take a Snapshot of this Virtual Machine" before performing any actions
2/24/2016 16:40:00	Open Time/Date Settings	Right click time/date in the bottom left of the desktop, select "Adjust date/time".
2/24/2016 16:42:00	Edit Time/Date Settings	Select "Internet Time" time. Select "Change Settings". Check "Synchronize with an Internet time server". Select "time.nist.gov" from the dropdown menu and select "Update now."
3/1/2016 11:25:48	Get first image	Directions needed for this step.
3/1/2016 14:42:00	Download & Install Dropbox desktop application	Open Internet Explorer and search "Dropbox" in the omnibox; access https://www.dropbox.com/downloading?src=index. If the install file does not automatically download, click "restart the download". If needed, direct the download to C:\Users\username\Downloads Close Internet Explorer. Go to the location of the install file, and open the install file. Allow Dropbox to make changes to the computer.
3/1/2016 14:55:00	Get second image	Directions needed for this step.
3/1/2016 15:09:00	Time synced with server.	
3/1/2016 15:13:00	Log in to Dropbox client	Open Dropbox if it is not open already. Enter username and password. Click through the
	File Type: DOCS	

3/1/2016 15:16:00	Ignore < .Docx 1>	
3/1/2016 15:17:00	Access < .Docx 2>	Access the local Dropbox folder and open <.Docx 2>
3/1/2016 15:18:00	Delete < .Docx 3>	Access the local Dropbox folder and delete <.Docx 3>
3/1/2016 15:20:00	Download < .Docx 4>	Open Dropbox in Internet Explorer, navigate to and download < .Docx 4>
3/1/2016 15:21:00	delete < .Docx 5>	Open Dropbox in Internet Explorer, delete < .Docx 5>
3/1/2016 15:21:00	Access and delete < .Docx 6>	Access < .Docx 6> In Internet Explorer and delete from Dropbox online
3/1/2016 15:25:00	edit < .Docx 7>	Access Dropbox on desktop and edit < .Docx7>. Sync Dropbox. Then using Dropbox in Internet Explorer delete < .Docx 7>
	File Type: JPG	
3/1/2016 15:26:00	Ignore <JPG 1>	
3/1/2016 15:27:00	Access <JPG 2>	Access the local Dropbox folder and open <.JPG 2>
3/1/2016 15:32:00	Delete <JPG 3>	Access the local Dropbox folder and delete <.JPG 3>
3/1/2016 15:35:00	Download <JPG 4>	Open Dropbox in Internet Explorer, navigate to and download < .JPG 4>
3/1/2016 15:36:00	Delete Online <JPG 5>	Open Dropbox in Internet Explorer, delete < .JPG 5>
3/1/2016 15:37:00	Access and delete <JPG 6>	Access < .JPG 6> In Internet Explorer and delete from Dropbox online
	File Type: MP3	
3/1/2016 15:52:00	Ignore <MP3 - 1>	
3/1/2016 15:56:00	Access <MP3 - 2>	Access the local Dropbox folder and open <.MP3 - 2>
3/1/2016 16:06:00	Delete <MP3 - 3>	Access the local Dropbox folder and delete <.MP3 - 3>
3/1/2016 16:10:00	Download <MP3 - 4>	Open Dropbox in Internet Explorer, navigate to and download < .MP3 - 4>
3/1/2016 16:15:00	Delete Online <MP3 - 5>	Open Dropbox in Internet Explorer, delete < .MP3 - 5>
3/1/2016 16:16:00	Access and delete <MP3 - 6>	Access < .MP3 - 6> In Internet Explorer and delete from Dropbox online

	File Type: PDF	
3/1/2016 16:20:00	Ignore <PDF 1>	
3/1/2016 16:33:00	Download and Installed Adobe Reader	
3/1/2016 16:35:00	Access <PDF 2>	Access the local Dropbox folder and open <.PDF 2>
3/1/2016 16:36:00	Delete <PDF 3>	Access the local Dropbox folder and delete <.PDF 3>
3/1/2016 16:39:00	Download <PDF 4>	Open Dropbox in Internet Explorer, navigate to and download < .PDF 4>
3/1/2016 16:40:00	Delete Online<PDF 5>	Open Dropbox in Internet Explorer, delete < .PDF 5>
3/1/2016 16:43:00	Access and delete <PDF 6>	Access < .PDF 6> In Internet Explorer and delete from Dropbox online
16:44	**SHUDOWN**	
	Post-DataGen	

Google Drive: Data Generation Sheet

Google	Data Gen Action	Directions
DATE/TIME(EST)	**Name**	
2/23/2016 18:19	Clean the Google Drive Account	Sign in to the account on a local machine and delete all files permanently
2/23/2016 18:22	Start VMware vSphere Client	Open VMware vSphere Client C:\Program Files (x86)\VMware\Infrastructure\Virtual Infrastructure Client\Launcher\
2/23/2016 18:22	Sign In to Virtual Windows 7 Machine	Enter "192.168.1.2" for IP address, check "Use Windows session credentials" then press "Login" Ignore SSL certificate warnings
2/23/2016 18:25	Power Up Windows 7 Machine	Select "Hosts and Clusters." Expand the dropdown menus on the left (vCenter.research.lcdi > LCDI > 192.168.1.20 > Cloud Forensics VM) select "Cloud Forensics VM: Google Drive." Power up the machine by pressing the green arrow
2/23/2016 18:27	Launch the virtual machine console	Selecting the icon with the desktop and green arrow in it.
2/23/2016 18:27	Sign In	Sign in to the user "lcdicloud"
2/23/2016 18:46	Create Virtual Machine Snapshot	Select "Take a snapshot of this virtual machine" in vSphere client
Started 3/8/2016 16:45 Finished 3/8/2016 17:03	Download vmdk of "fresh" machine	Using VMWare vCenter Converter Standalone connect to the ESXI server (192.168.1.2) and use the Convert machine tool.
2/24/2016 16:02	Power the Windows 7 Machine Back On	Press the green arrow
2/29/2016 13:38	Open Time/Date Settings	Right click time/date in the bottom left of the desktop, select "Adjust date/time". Leave time zone as "Eastern Time"
2/29/2016 13:38	Edit Time/Date Settings	Select "Internet Time" time. Select "Change Settings". Check "Synchronize with an Internet time server". Select "time.nist.gov" from the dropdown menu and select "Update now."
2/29/2016 13:30	Download Google Drive Desktop Client	Open Internet Explorer and browse to "https://www.google.com/drive/download/", Click "Download for PC", then click "Accept and Install"

2/29/2016 13:31	Install Google Drive Desktop Client	Run "googledrivesync.exe", select "Run" when prompted whether or not you want to run the file, and select "Yes" when prompted "Do you want to allow the following program to make changes to this computer?"
2/29/2016 13:35	Log in to Google Drive client	Start Google Drive for Desktop. Enter the Google Account information provided on the secret server to Login.
2/29/2016 13:35	Open Internet Explorer	Click the icon in the bottom left corner
2/29/2016 13:37	Log in to Drive using Internet Explorer	Browse to drive.google.com Enter account information provided on secret server.
2/29/2016 13:39	Download All Files for Use	Browse to https://goo.gl/loCrwB using Internet Explorer and Download the file using Dropbox. when prompted to sign up select "No thanks."(goo.gl used as a link shortner)
2/29/2016 13:39	Import Files to Googe Drive	Open the .zip file and drag all folders (.docx, .jpgs, .mp3s, .pdfs) into the Google Drive folder. Allow Google Drive to import all files.
2/29/2016 13:41	Create Virtual Machine Snapshot	Select "Take a snapshot of this virtual machine" in vSphere client. Allow the process to complete then power off the machine.
Started 3/8/2016 16:27 Finished 3/8/2016 16:41	Download vmdk of Machine with client installed and files synced.	Using VMWare vCenter Converter Standalone connect to the ESXI server (192.168.1.2) and use the Convert machine tool.
	File Type: docx	
2/29/2016 14:17	Ignore < Docx 1>	
2/29/2016 14:18	Access < Docx 2>	Access the local Google Drive folder and open <.Docx 2>
2/29/2016 14:18	Delete < Docx 3>	Access the local Google Drive folder and delete <.Docx 3>
2/29/2016 14:19	Download < Docx 4>	Open Google Drive in Internet Explorer, navigate to and download < .Docx 4>
2/29/2016 14:19	delete < Docx 5>	Open Google Drive in Internet Explorer, delete < .Docx 5>
2/29/2016 14:20	Access and delete < Docx 6>	Access < .Docx 6> In Internet Explorer and delete from Google Drive online
2/29/2016 14:24	Edit < Docx 7>	Access Google Drive on desktop and edit < .Docx7>. Sync Google Drive. Then using Google Drive in Internet Explorer delete < .Docx 7>
	File Type: JPG	

2/29/2016 14:25	Ignore <JPG 1>	
2/29/2016 14:26	Access <JPG 2>	Access the local Google Drive folder and open <JPG 2>
2/29/2016 14:26	Delete <JPG 3>	Access the local Google Drive folder and delete <JPG 3>
2/29/2016 14:25	Download <JPG 4>	Open Google Drive in Internet Explorer, download <JPG 4>
2/29/2016 14:25	Delete Online <JPG 5>	Open Google Drive in Internet Explorer and delete <JPG 5>
2/29/2016 14:25	Access and delete <JPG 6>	Access Google Drive online and open <JPG 6>. Then using Google Drive online delete <JPG 6>
	File Type: MP3	
2/29/2016 14:26	Ignore <MP3 - 1>	
2/29/2016 14:26	Access <MP3 - 2>	Access the local Google Drive folder and open <MP3 - 2>
2/29/2016 14:26	Delete <MP3 - 3>	Access the local Google Drive folder and delete <MP3 - 3>
2/29/2016 14:26	Download <MP3 - 4>	Open Google Drive in Internet Explorer, download <MP3 - 4>
2/29/2016 14:27	Delete Online <MP3 - 5>	Open Google Drive online delete <MP3 - 5>
2/29/2016 14:27	Access and delete <MP3 - 6>	Access Google Drive online and open <MP3 - 6>. Then using Google Drive online delete <MP3 - 6>
	File Type: PDF	
2/29/2016 14:31	Ignore <PDF 1>	
2/29/2016 14:31	Access <PDF 2>	Access the local Google Drive folder and select <PDF 2>.
2/29/2016 14:31	Delete <PDF 3>	Access the local Google Drive folder and delete <PDF 3>
2/29/2016 14:32	Download <PDF 4>	Open Google Drive in Internet Explorer, download <PDF 4>
2/29/2016 14:32	Delete Online<PDF 5>	Open Google Drive online delete <PDF 5>
2/29/2016 14:32	Access and delete <PDF 6>	Access Google Drive online and open <PDF 6>. Then using Google Drive online delete <PDF 6>
2/29/2016 14:34	Create Virtual Machine Snapshot then power off.	Select "Take a snapshot of this virtual machine" in vSphere client. Then power off the machine using vSphere

Started 3/8/2016 16:10 Finished 3/8/2016 16:23	**Download vmdk of machine**	Using VMWare vCenter Converter Standalone connect to the ESXI server (192.168.1.2) and use the Convert machine tool.
	Differences When Performing Actions While Signed Out (Client running)	
3/21/2016 13:57	Power on VM to Snapshop (Final)	Use vSphere for this
3/21/2016 14:04	Disconect The Assosciated Account	Open the local Google Drive Client and select "Disconect Account"
3/21/2016 14:52	Open Google Drive In Internet Explorer	Browse to drive.google.com
3/21/2016 14:54	Access <Docx 1>	Open <Docx1> through Google Drive on Internet Explorer
3/21/2016 14:57	Create new file Using Drive <Docx 91>	Using Drive through Internet Explorer create a new doc file. Name this doc file "Docx 91"
3/21/2016 15:03	Create a new file using notepad <Docx 92>	Using the notepad client on the Desktop create the file save as "Docx 92" to Desktop
3/21/2016 15:05	Manually upload <Docx 92> to Drive Account	Open Google Drive in Internet Explorer and upload <Docx 92>
3/21/2016 15:07	Create a new file using notepad <Docx 93>	Using the notepad client on the Desktop create the file saved as "Docx 93" to Desktop
3/21/2016 15:14	Manually upload <Docx 93> to Drive Account	Open Google Drive in Internet Explorer and upload <Docx 93>
3/21/2016 15:17	Delete <Docx 93> from Drive Account	Open Google Drive in Internet Explorer and delete <Docx 93>
3/21/2016 15:35	Create Virtual Machine Snapshot	Select "Take a snapshot of this virtual machine" in vSphere client. Allow the process to complete then power off the machine.
3/21/2016 37	Download vmdk of Machine with client installed and files synced.	Using VMWare vCenter Converter Standalone connect to the ESXI server (192.168.1.2) and use the Convert machine tool.
	Post Datagen	

3/8/2016 17:00	**Copy vmdk files to Z: Drive**	Copy all vmdk files to the Network Drive
	EnCase Analysis	
3/8/2016 16:40	Create a new case in EnCase 7.10	Create a New case point Base case folder and Primary EvidenceCache to resource drive
3/8/2016 16:10	Add vmdk files as evidence	The vmdk files can simply be click and dragged into EnCase
3/1/2016 16:54	Acquire and Verify Evidence using EnCase	Select to "Acquire Evidence" on each raw vmdk file and allow the process to run
3/8/2016 17:20	Acquire vmdk (Final)	Encase Evidence file created using EnCase's acquire tool.
3/8/2016 17:20	Acquire vmdk (Fresh Install)	Encase Evidence file created using EnCase's acquire tool.
3/8/2016 17:20	Acquire vmdk (Synced)	Encase Evidence file created using EnCase's acquire tool.
3/21/2016 17:05	Acquire vmdk (Sign out)	Encase Evidence file created using EnCase's acquire tool.
3/21/2016 13:20	Process (Final) evidence file	Default settings used to process
3/21/2016 13:20	Process (Synced) evidence file	Default settings used to process
3/21/2016 13:20	Process (Fresh) evidence file	Default settings used to process
3/21/2016 17:05	Process (Sign out) evidence file	Default settings used to process

iCloud: Data Generation Sheet

iCloud	Data Gen Action	Directions
DATE (m/d/y)	**Prior to Data Gen**	**Directions**
2/18/16 (1:00PM)	Start VMfusion	Open VMFusion, the VM should load automatically. Hit the play button to unsuspend
2/24/16 (1:38PM)	Capture snapshot of VM	Click "Add Snapshot" along the taskbar. Name snapshot "Drive pre-data gen".
2/24/16 (1:44PM)	Copy vmdk file	Copy vmdk file of VM to folder on desktop titled "iCloud Project", and place inside "vmdk files" title "Fresh Install"
2/24/16 (2:05PM)	Put files into iCloud	Take all the files (JPG, MP3, and PDF) from Cloud Drive, and insert them into the iCloud account. Create Pages in lou of Docs
2/24/16 (2:09PM)	Create <Pages Doc 1>	Using the Pages application within Safari, create a new Page Document and Label it <Pages Doc 1>
2/24/16 (2:11PM)	Create <Pages Doc 2>	Using the Pages application within Safari, create a new Page Document and Label it <Pages Doc 2>
2/24/16 (2:18PM)	Create <Pages Doc 3>	Using the Pages application within Safari, create a new Page Document and Label it <Pages Doc 3>
2/24/16 (2:20PM)	Create <Pages Doc 4>	Using the Pages application within Safari, create a new Page Document and Label it <Pages Doc 4>
2/24/16 (2:21PM)	Create <Pages Doc 5>	Using the Pages application within Safari, create a new Page Document and Label it <Pages Doc 5>
2/24/16 (2:23PM)	Create <Pages Doc 6>	Using the Pages application within Safari, create a new Page Document and Label it <Pages Doc 6>
2/24/16 (2:23PM)	Create <Pages Doc 7>	Using the Pages application within Safari, create a new Page Document and Label it <Pages Doc 7>
2/25/16 (5:42PM)	Start iCloud application	Open Safari and navigate to https://support.apple.com/en-us/HT204283 and click on download button. (if not installed)
2/25/16 (5:42PM)	Log in to iCloud Desktop client	Start iCloud Desktop client. Apple credentials located on Secret Server.
2/25/16 (5:46PM)	Log in to iCloud web client	Start Safari, and navigate to iCloud.com. Login using credentials located on Secret Server.
2/25/16 (5:49PM)	Sync iCloud	Open iCloud Desktop client, by navigating to the Folder Directory(Finder), and opening iCloud
2/25/16 (5:50PM)	Capture snapshot of VM	Click "Add Snapshot" along the taskbar. Name snapshot "All Documents in iCloud".
2/25/16 (6:23PM)	Copy vmdk file	Copy vmdk file of VM to folder on desktop titled "iCloud Project", and place inside "vmdk files" title “After Data Sync"
DATE (m/d/y)	**File Type: Pages & .odt files (Libre Office)**	**Directions**

2/25/16 (6:25-6:30PM)	Download Libre Office	Open Safari, navigate to libreoffice.org and click the download button
2/26/16 (6:31PM)	Ignore <Pages Doc 1>	Make sure to place <Pages Doc 1> in iCloud drive, but do nothing else with it
2/29/16 (4:17PM)	Access <Pages Doc 2>	Access the iCloud Folder Directory created by iCloud and open <Pages Doc 2>
2/29/16 (4:20PM)	Access <Pages Doc 2>	Access the iCloud using safari and open <Pages Doc 2>
2/29/16 (4:29PM)	Create and save <doc 2.2.odt>	Using Libre application, create a new Document and Label it <doc 2.2.odt> save to desktop: Folder: "docs"
2/29/16 (4:32PM)	Upload <doc 2.2.odt>	Upload doc 2.2.odt to the iCloud using the iCloud Folder Directory
2/29/16 (4:34PM)	Access <Pages Doc 2.2>	Access the iCloud Folder Directory created by iCloud and open <doc 2.2.odt>
2/29/16 (4:35PM)	Delete <Pages Doc 3>	Access the iCloud Folder Directory and delete <Pages Doc 3>
2/29/16 (4:39PM)	Download <Pages Doc 4>	Open iCloud in Safari, navigate to and download <Pages Doc 4>
2/29/16 (4:41-42PM)	Download and delete <Pages Doc 5>	Open iCloud in Safari, download <Pages Doc 5> and then delete <Pages Doc 5> using iCloud in Safari
2/29/16 (4:52PM)	Access <Pages Doc 6>	Access the iCloud using safari and open <Pages Doc 6>
2/29/16 (4:56PM)	Create and save <doc 6.6.odt>	Using Libre application, create a new Document and Label it <doc 6.6.odt> save to desktop: Folder: "docs"
2/29/16 (5:05PM)	Upload <doc 6.6.odt>	Upload doc 6.6.odt to the iCloud folder "pages" using the iCloud Folder Directory
2/29/16 (5:06-07PM)	Edit and save <doc 6.6.odt>	Using the iCloud Folder Directory and open <doc6.6.odt>. Make edits to the contents of the document. Save and close document
DATE (m/d/y)	**File Type: JPG**	**Directions**
2/29/16 (5:47PM)	Ignore <JPG 1>	Make sure to place <JPG 1> in iCloud drive, but do nothing else with it.
2/29/16 (5:47PM)	Access <JPG 2>	Access the Folder Directory created by iCloud and select <JPG 2>.
2/29/16 (5:49PM)	Delete <JPG 3>	Access iCloud In Folder Directory and delete <JPG 3>
2/29/16 (5:52-53PM)	Download and delete <JPG 5>	Open iCloud in Safari, download <JPG 5> and delete <JPG 5> from iCloud using Safari
2/29/16 (5:54PM)	Download <JPG 4>	Open iCloud in Safari, download <JPG 4>
2/29/16 (5:55-57PM)	Access and delete <JPG 6>	Access iCloud In Folder Directory and open <JPG 6>. Then using Safari delete <JPG 6>

DATE (m/d/y)	File Type: MP3-	Directions
2/29/16 (6:06PM)	Ignore <MP3 - 1>	Make sure to place <MP3 - 1> in iCloud drive, but do nothing else with it.
2/29/16 (6:07PM)	Access <MP3 - 2>	Access the Folder Directory created by iCloud and select <MP3 - 2>.
2/29/16 (6:08PM)	Delete <MP3 - 3>	Access iCloud In Folder Directory and delete <MP3 - 3>
2/29/16 (6:09PM)	Download <MP3 - 4>	Open iCloud in Safari, download <MP3 - 4>
2/29/16 (6:10PM)	Download and delete <MP3 - 5>	Open iCloud in Safari, download <MP3 - 5> and delete <MP3 - 5> from iCloud using Safari
2/29/16 (6:11PM)	Access and delete <MP3 - 6>	Access iCloud In Folder Directory and open <MP3 - 9>. Then using Safari delete <MP3 - 9>
DATE (m/d/y)	**File Type: PDF**	**Directions**
2/29/16 (6:11PM)	Ignore <PDF 1>	Make sure to place <PDF 1> in iCloud drive, but do nothing else with it.
2/29/16 (6:13PM)	Access <PDF 2>	Access the Folder Directory created by iCloud and select <PDF 2>.
2/29/16 (6:14PM)	Delete <PDF 3>	Access iCloud In Folder Directory and delete <PDF 3>
2/29/16 (6:15PM)	Download <PDF 4>	Open iCloud in Safari, download <PDF 4>
2/29/16 (6:16PM)	Download and delete <PDF 5>	Open iCloud in Safari, download <PDF 5> and delete <PDF 5> from iCloud using Safari
2/29/16 (6:16PM)	Access and delete <PDF 6>	Access iCloud In Folder Directory and open <PDF 9>. Then using Safari delete <PDF 9>
DATE (m/d/y)	**Processes after Data Gen Completion**	**Directions**
2/29/16 (6:17PM)	Capture snapshot of VM	Click "Add Snapshot" along the taskbar. Name snapshot "Data Gen complete"
2/29/16 (6:20PM)	Copy vmdk file	Copy vmdk file of VM to folder on desktop titled "iCloud Project", and place inside "vmdk files" title "Data Gen complete"
DATE (m/d/y)	**Differences When Performing Actions While Signed Out (Client running)**	**Directions**
3/23/16 (12:45PM)	Power on VM to Snapshot (Final)	Use VMware
3/23/16 (12:48PM)	Disconnect The Associated Account	Open iCloud options, and Disconnect Account
3/23/16 (12:49PM)	Open iCloud in Safari	Browse to iCloud.com
3/23/16 (12:50PM)	Access <Pages Doc 1>	Open <Pages Doc 1> through iCloud on Safari

3/23/16 (12:53PM)	Create new file Using iCloud <pages doc 91>	Using iCloud through Safari create a new Pages doc file. Name this doc file <Pages Doc 1>
3/23/16 (1:02PM)	Delete <Doc 2.2> from iCloud	Open iCloud in Safari and delete <Doc 93>
3/23/16 (1:03PM)	Create Virtual Machine Snapshot	Select "Take a snapshot of this virtual machine" in VMware Label image as "iCloud signed out"
3/23/16 (1:05PM)	Copy vmdk file	Copy vmdk file of snapshot to the network drive & External

References

StatCounter. "Top 7 Desktop OSs from Mar 2015 to Mar 2016." StatCounter GlobalStats. StatCounter, Apr. 2016. Web. 21 Apr. 2016.

Statisa. "Number of Personal Cloud Storage Users from 2014 to 2019 (in Millions)." Statista. Statista, Inc., 2016. Web. 21 Apr. 2016.

"What Is VMware ESXi Server? - Definition from Techopedia." Techopedia.com. Techopedia, n.d. Web. 19 Apr. 2016.

Murray, Nick. "Internet Evidence Finder Report." Web log post. Senator Patrick Leahy Center for Digital Investigation, July 2013. Web. 19 Apr. 2016.

"How to Open and Convert Files with .ODL File Extension." *ODL File Extension*. N.p., n.d. Web. 28 Apr. 2016.

"5.6.1 Zone.Identifier Stream Name." *Internet Explorer Zone Identifier*. Microsoft Developer Network, n.d. Web. 28 Apr. 2016.