CHAMPLAIN COLLEGE

LCDI

The Senator Patrick Leahy
Center for Digital Investigation

Cloud Forensics

Written & Researched by:
Maegan Katz & Ryan Montelbano

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

November 4, 2013

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 new technology that makes it possible for users to upload data to the web, allowing for instant accessibility and the ability to share data with others at any time. Cloud technology is creating a challenge for forensic investigators, as data can be uploaded or shared from one computer and opened on another computer without leaving a large amount of traceable evidence. Google Drive, Dropbox, and SkyDrive are a few examples of these cloud storage services that need to be investigated further.

Background

The use of cloud forensics is an emerging field that requires more attention than standard digital forensics. A large portion of the research done on cloud computing so far has dealt with the increasing legal troubles that law enforcement will face when attempting to seize or retrieve information in the cloud. Many organizations that are using cloud services may not have considered the legal issues that come with public clouds. According to Network World (Messmer, 2013), “any business that anticipates using cloud-based services should be asking the question: What can my cloud provider do for me in terms of providing digital forensics data in the event of any legal dispute, civil or criminal case, cyber-attack, or data breach?” Other studies have compared the actual providers themselves. Each cloud service provider is going to be different; this complicates cloud-based forensics because each company will have different rules, guidelines, and requirements. According to the IATAC (Scott Zimmerman, 2011), “to date, there has been very little research done on the current state of the tools, processes, and methodologies to obtain legally defensible digital evidence in the cloud.”

Purpose and Scope

The purpose of this research is to find key aspects of different cloud storage applications to aid forensic investigators and law enforcement. It is important to find any and all relevant artifacts that are created during the applications use, as well as any files or metadata of files being uploaded, whether or not they have been deleted.

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

Artifacts – A digital artifact is any undesired alteration in computer data. Hardware/software malfunctions, compression, deletion, and movement can all be possible causes.

Cloud Computing – Cloud computing is a “model for enabling convenient, on-demand network access to a shared pool of configurable computing resources, such as networks, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Linthicum, 2013).

Cloud Forensics – Cloud forensics is "the application of digital forensics in cloud computing as a subset of network forensics. It is a cross discipline between cloud computing and digital forensics" (Cruz, 2012).

CSV (Comma-separated value) – CSV files store rows and columns of data in plain-text form, much like and Excel document.

Digital Evidence – Digital evidence is "information of probative value that is stored or transmitted in a binary form" (NCFS, 2012). Digital evidence not only includes computers in the traditional sense, but also digital audio, video, and pictures.

Digital Forensics – The identification, examination, collection, preservation, and analysis of computer data and information.

DropBox – File hosting service operated by Dropbox, Inc. Dropbox offers cloud storage, file synchronization, and client software.

EnCase – EnCase is a suite of digital forensics tools created by Guidance Software. The software comes in several forms designed for forensic, cyber security, and e-discovery use. Data recovered by EnCase has been used successfully in various court systems around the world.

E01 – An E01 is the extension of an image file for EnCase.

FTK – Forensic Toolkit, or FTK, is computer forensics software made by AccessData. It scans a hard drive looking for data. It can, for example, locate deleted e-mails and scan a disk for text strings to use as a password dictionary to crack encryptions. The toolkit also includes a standalone disk imaging program called FTK Imager. It saves an image of a hard disk in one file or in segments that may be reconstructed. FTK Imager calculates MD5 hash values and confirms the integrity of the data before closing the files.

Google Drive – Google Drive is a file storage and synchronization service provided by Google. It provides cloud storage, file sharing, and collaborative editing. Files shared publicly on Google Drive can be searched for with web search engines.

Metadata – Metadata is data providing information about one or more aspects of the data such as: means of creation of the data, purpose of the data, time and date of creation, creator of the data, and the location where the data was created (NISO, 2004).

Microsoft SkyDrive – File hosting service that allows users to upload and sync files to a cloud storage and then access them from a Web browser or their local/mobile device. It is part of the Windows Live range of online services and allows users to keep the files private, share them with contacts, or make the files public. Publicly shared files do not require a Microsoft account for access.

Pagefile – A pagefile is a form of virtual memory that stores data that can't be held by RAM.

Unallocated Space – Unallocated space is where files or pieces of files that are temporary of deleted are stored.

Virtual Machine – A virtual machine is a software-based computer that executes and runs programs like a physical machine. A virtual machine supports the execution of a complete operating system. VMs usually emulate an existing architecture and are built with the purpose of either providing a platform to run programs where the real hardware is not available for use, or of having multiple instances of virtual machines. This leads to more efficient use of computing resources, both in terms of energy consumption and cost effectiveness (known as hardware virtualization).

Methodology and Methods

Before we began this project, we created a virtual machine (VM) for each of the three cloud services: Dropbox, SkyDrive, and Google Drive. We chose to create a 20GB Windows 7 VM for each cloud service and downloaded Sysinternals Process Monitor to record any and all changes/additions that the cloud services made during their use, from the installation to when the services were uninstalled.

Once we created the VMs and downloaded Process Monitor, we started Process Monitor, downloaded the cloud service, and started the installation process. Before continuing with the installation process, we filtered Process Monitor by the cloud service's setup Process Identifier (PID). We selected to only show results from file system activity and registry activity, as we are mainly looking for changes to the registry and files. We then continued with the installation of the cloud service. After the cloud service finished installing, we saved the results from Process Monitor and shutdown the VM. We then copied the VM to a new folder in order to preserve the original artifacts that were created during the installation process. For our subsequent research, we continued with the following: starting the VM, starting Process Monitor, filtering the process monitor results by the cloud service's PID(s), performing the required action for the step (setup, upload files, copy a file, move a file, open a file, delete a file, unlink the account, and uninstall), saved the results from process monitor, shutdown the VM, and copied the VM to a new folder.

The data set files that we deleted from SkyDrive were turtle.jpg and wildlife.wmv. GettingStarted.pdf and WinPcap_4_1_2.exe were deleted fromDropbox, and Plan.docx and WinPcap_4_1_2.exe were deleted from Google Drive.

After we finished creating the virtual machines, we used FTK Imager 3.1.0.1514 to create E01 files for each VM, which we imported into FTK 4.1.0.165 for analysis. In total, we had seven different images per cloud service to parse through and several dozen CSV files from Process Monitor to view changes made to the files and the registry.

Appendix A shows the steps taken with each of the cloud services.

Equipment Used

Table 1: Equipment and Software

Equipment/Software	Version	Details
VMware Workstation	*9.0.2*	*Used to create and run the Window 7 VMs*
Windows 7	*64-bit*	*Used to create the base VM for this project*
Process Monitor	*3.05*	*Used to monitor change made to the files and the registry*
Dropbox	*2.0.26*	*Cloud service used to generate data*
SkyDrive	*17.0.2015.0811*	*Cloud service used to generate data*

Google Drive	*1.11.4865.2530*	*Cloud service used to generate data*
FTK	*4.1.0.165*	*Used to analyze the images from the VM*
FTK Imager	*3.1.0.1514*	*Used to create E01 files for each VM*

Data Collection

The data we collected for this project included CSV files from Process Monitor, as well as files from searches made in FTK. Table 2 shows the number of unique artifacts found using Process Monitor for each of the cloud services. Appendix B shows all of the information related to the two deleted files in each cloud service.

Table 2: Total Number of Filtered Files

SkyDrive Process	# of unique paths	# of files with "SkyDrive" in the name	# of registry keys with "SkyDrive" in the name
Install	4959	171	69
Upload	6165	224	80
Move/Copy	179	20	0
Open	1	0	0
Delete	595	14	3
Unlink	1178	48	28
Uninstall	4689	217	56
Dropbox Process	**# of unique paths**	**# of files with "Dropbox" in the name**	**# of registry keys with "Dropbox" in the name**
Install	4163	39	52
Setup	87	60	10
Upload	212	36	2
Move/Copy	75	24	4
Open	106	5	0
Delete	127	17	1
Unlink	3000	19	12
Uninstall	1222	43	10
Google Drive Process	**# of unique paths**	**# of files with "GoogleDrive" in the name**	**# of registry keys with "GoogleDrive" in the name**
Install	9438	7	102
Upload	9449	4	101
Move/Copy	138	0	0
Delete	2767	1	1
Unlink	118	2	2
Uninstall	118	2	2

Analysis

All of our data for analysis came from the CSV files created by Process Monitor and search results from FTK. Process Monitor has the option to save results by path, folder, and extension. We chose to focus on the path results and filter those using Excel. We first separated the unique paths by file path and registry path. Then, we filtered the results further so that only the results containing the words *'Dropbox,' 'SkyDrive,'* or *'GoogleDrive'* were listed, to show the files or registry keys that are definitely related to the cloud service. Next, in FTK, we acquired the deleted, unlinked, and uninstalled images for each of the cloud services and performed a keyword search for the two deleted files from each cloud service. The deleted image is the image we took after deleting a few files from the cloud services. The unlink image is where we unlinked the user account from the application, and the uninstall image is where we uninstalled the application.

Results

SkyDrive

4959 artifacts were created or modified when SkyDrive was installed. 171 of those were file paths that contained the word "SkyDrive," and 69 of those were registry paths that contained the word "SkyDrive." 6165 artifacts were created or modified when files were uploaded to SkyDrive. 224 of those were file paths that contained the word "SkyDrive," and 80 of those were registry paths that contained the word "SkyDrive." 179 artifacts were created or modified when files had been moved or copied within SkyDrive. 20 of those were file paths that contained the word "SkyDrive." Additionally, we were able to find evidence of turtle.jpg and wildlife.wmv in unallocated space, a number of $Recycle.Bin CSV files, pagefile.sys, and the AppData folder. There were 24 files related to turtle.jpg and 19 files related to wildlife.wmv that remained after SkyDrive had been unlinked and uninstalled. In total, 1178 unique artifacts were affected when SkyDrive was unlinked and 4689 unique artifacts when SkyDrive was uninstalled.

Dropbox

4163 artifacts were created or modified when Dropbox was installed. 39 of those were files paths that contained the word "Dropbox," and 52 of those were registry paths that contained the word "Dropbox." 212 artifacts were created or modified when files were uploaded to Dropbox. 36 of those were file paths that contained the word "Dropbox," and 2 of those were registry paths that contained the word "Dropbox." 75 artifacts were created or modified when files were moved or copied within Dropbox. 24 of those were file paths that contained the word "Dropbox," and 4 of those were registry paths that contained the word "Dropbox." We were unable to find evidence of GettingStarted.pdf, but we were able to find a renamed deleted version of GettingStarted.pdf [Getting Started (deleted e8e9f5e1ecea9b19af69596f25b4fb39).pdf] in pagefile.sys. We were able to find evidence of WinPcap_4_1_2.exe in unallocated space, as well as in pagefile.sys. There were 2 files related to GettingStarted.pdf and 1 file related to WinPcap_4_1_2.exe that remained after Dropbox had been unlinked and uninstalled. In total, 3000 unique artifacts were affected when Dropbox was unlinked and 1222 unique artifacts when Dropbox was uninstalled.

Google Drive

9438 artifacts were created or modified when Google Drive was installed. 7 of those were file paths that contained the word "GoogleDrive," and 102 of those were registry paths that contained the word "GoogleDrive." 9449 artifacts were created or modified when files were uploaded to Google Drive. Four of those were file paths that contained the word "GoogleDrive," and 101 of those were registry paths that contained the word "GoogleDrive." 138 artifacts were created or modified when files had been moved or copied within Google Drive. We were also able to find evidence of Plan.docx and WinPcap_4_1_2.exe in unallocated space, a number of $Recycle.Bin CSV files, and pagefile.sys. Additionally, we found evidence of Plan.docx in a configuration file. There are 13 files related to WinPcap_4_1_2.exe and 12 files related to Plan.docx that remained after Google Drive had been unlinked and uninstalled. In total, 118 unique artifacts were affected when Google Drive was unlinked and 118 unique artifacts when Google Drive was uninstalled.

Conclusion

Our results show that a number of artifacts are left behind after the deletion, unlinking, and uninstalling of SkyDrive, Dropbox, and Google Drive. We found that evidence of the files could be located in unallocated space for each application, along with $Recylce.Bin CSV files, and pagefile.sys. The number of artifacts that were affected upon creation, deletion, uploading, and moving within each application varied. All three cloud services left behind trace evidence of our target files after being unlinked and uninstalled. With each application, the amount of the evidence found was different, but it was still present in some form.

Further Work

Within the field of cloud forensics, more research and planning needs to be done, along with the implementation of industry standard law practices. Currently, rules, regulations, guidelines, and standard practices can vary greatly from provider to provider. This makes it increasingly difficult for forensic technicians to work.

For this project, we only used common or popular cloud services. These are services that have been around for a number of years, giving them time to grow and understand the industry that they are working with and have helped create. Additionally, some cloud services are accompanied by a mobile application, which we feel should be researched. To our team, it is important to know if the mobile application also leaves behind artifacts after it is unlinked and uninstalled. We were able to find that there are still remnants of files after they have been deleted, as well. Our next step would be to see if these files are actually recoverable in their original state.

Appendix A

SkyDrive

Time	Action/Variable
7/17/13 11:00	Powered on VM
11:01	Filtered Process Monitor by the SkyDrive PIDs
11:02	Used Chrome to navigate to SkyDrive download
11:03	Downloaded SkyDrive and started installed
11:06	Saved log files from Process Monitor
11:06	Shut down VM
11:07	Copied VM to next folder
7/22/13 10:19	Powered on VM

10:21	Copied “DataSet” to VM desktop
10:23	Filtered Process Monitor by the SkyDrive PIDs
10:24	Started SkyDrive > Prompted to create account
10:35	Added MP3, Zip, PDF, RTF, and EXE through desktop version of SkyDrive * Dragged into SkyDrive > automatically removed files from “DataSet” folder
10:40	Navigated to SkyDrive website
10:44	Uploaded XLS, DOCX, JPEG, and WMV through website version of SkyDrive * Did not remove files from “DataSet” folder like with the desktop version
10:50	Saved log files from Process Monitor
10:53	Shut down VM
10:53	Copied VM to next folder
8/2/13 11:49	Powered on VM
11:52	Filtered Process Monitor by the SkyDrive PIDs
12:02	Created folder “CloudStuff”
12:03	Moved RTF to folder
12:07	Copied DOCX to folder
12:10	Saved log files from Process Monitor
12:12	Shut down VM
12:16	Copied VM to next folder
12:44	Powered on VM
12:54	Filtered Process Monitor by the SkyDrive PIDs
12:55	Opened JPG
12:56	Opened RTF
12:58	Saved log files from Process Monitor
13:00	Shut down VM
13:04	Copied VM to next folder
8/5/13 13:41	Powered on VM
13:44	Filtered Process Monitor by the SkyDrive PIDs
13:53	Deleted WMV file via application
13:54	Navigated to SkyDrive website
13:56	Deleted JPG via SkyDrive website
14:00	Saved log files from Process Monitor
14:03	Shut down VM
14:04	Copied VM to next folder
15:01	Powered on VM

15:03	Filtered Process Monitor by the SkyDrive PIDs
15:06	Unlinked Account
15:07	Saved log files from Process Monitor
15:09	Shut down VM
15:09	Copied VM to next folder
16:04	Powered on VM
16:05	Filtered Process Monitor by the SkyDrive PIDs
16:08	Uninstalled Account
16:11	Saved log files from Process Monitor
16:13	Shut down VM

Dropbox

Time	Action/Variable
7/16/13 9:45	Powered on VM
9:50	Downloaded Dropbox
9:51	Ran Process Monitor
9:51	Ran Dropbox setup
9:53	Filtered Process Monitor by the Dropbox PIDs
9:56	Went through Dropbox installer
9:58	Dropbox finished installing and I closed the window
10:01	Saved the results from Process Monitor
10:04	Shutdown VM
7/22/13 8:39	Powered on VM
8:41	Started process monitor and filtered by the Dropbox process PID
8:50	Going through Dropbox set up
8:51	Clicked next->next->install->next->skip tour->finish
9:04	Shutdown VM
7/26/13 8:18	Powered on VM
8:25	Logged into Dropbox application
8:26	Started process monitor and filtered by the Dropbox process PID
8:06	Copied the dataset files to the VM
8:32	Moved 5 files from the dataset folder to the Dropbox folder
8:38	Saved log files from Process Monitor

8:38	Opened Chrome
8:39	Went to dropbox.com
8:39	Logged in
8:43	Dragged 4 files from the data set folder to the browser
8:45	Saved Process Monitor logs
8:47	Shut down VM
7/29/13 8:07	Powered on VM
8:08	Started process monitor and filtered by the Dropbox process PID
8:18	Created “cm folder” on Dropbox
8:39	Moved “Turtle.jpg” to “cm folder”
8:44	Copied “Plan.docx” to “cm folder”
9:27	Shut down VM
9:34	Powered on VM
9:36	Started process monitor and filtered by the Dropbox process PID
9:40	Opened “wildlife.wmv” in Dropbox folder
9:43	Shut down VM
9:53	Powered on VM
9:56	Started process monitor and filtered by the Dropbox process PID
10:05	Deleted “WinPcap_4_1_2.exe” from dropbox folder
10:09	Deleted “Getting Started.pdf” from dropbox.com
10:31	Shut down VM
11:00	Powered on VM
11:05	Started process monitor and filtered by the Dropbox process PID
11:19	Unlinked Dropbox account through application
11:36	Shut down VM
12:56	Powered on VM
13:00	Started process monitor and filtered by the Dropbox process PID
13:04	Uninstalling Dropbox
13:04	Dropbox uninstalled
13:06	Shut down VM

Google Drive

Time	Action/Variable

7/16/13 14:02	Downloaded Google Drive
14:03	Ran Process Monitor
14:03	Ran Google Drive setup
14:04	Started process monitor and filtered by the Google Drive process PID
14:05	Google Drive finished installing
14:13	Saved the results from Process Monitor
14:15	Shutdown VM
7/30/13 9:32	Powered on VM
9:33	Started Google Drive
9:34	Signed into Google Drive
9:36	Started process monitor and filtered by the Google Drive process PID
9:37	Clicked next->start sync
9:38	Dropbox synced
9:56	Copied over dataset to VM
10:28	Copied 5 files from the dataset folder to the Google Drive folder locate under my username.
10:52	Saved log files from Process Monitor
10:55	Opened Chrome
10:56	Went to drive.google.com and logged in
10:59	Dragged 4 files from the data set folder to the browser
11:18	Shut down VM
7/31/13 9:01	Powered on VM
9:02	Started process monitor and filtered by the Google Drive process PID
9:07	Created a “cm folder” on Google Drive
9:08	Moved “cloudservices.rtf” to “cm folder”
9:18	Copied a “blogs.zip” to “cm folder”
9:28	Shutdown VM
9:52	Powered on VM
9:53	Started process monitor and filtered by the Google Drive process PID
10:15	Opened “Best Coast – The Only Place.mp3” in GD folder
10:23	Opened “wildlife.wmv” in GD folder
10:24	Shut down VM
10:31	Powered on VM
10:33	Started process monitor and filtered by the Google Drive process PID
10:35	Deleted “WinPcap_4_1_2.exe” from GD folder

10:40	Deleted “Plan.docx” from GD.com
10:42	Shut down VM
11:04	Started VM
11:06	Started process monitor and filtered by the Google Drive process PID
11:06	Unlinked Google Drive account through application
11:11	Shut down VM
11:26	Powered on VM
11:28	Started process monitor and filtered by the Google Drive process PID
11:29	Uninstalling Google Drive
11:29	Google Drive uninstalled
11:32	Shut down VM

Appendix B

SkyDrive

Turtle.jpg

- Found in unallocated space
    - 0071049
- Found in allocated space
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RUDSTO2.csv
    - pagefile.sys
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RI4LWB8.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RHH9I59.csv
    - Users/nmurray/AppData/Local/Microsoft/SkyDrive/logs/WIN-0BEK5AK8E2S.dev=0.2013-07-22.1023.1532-1.log
    - Users/nmurray/AppData/Local/Microsoft/SkyDrive/logs/WIN-0BEK5AK8E2S.dev=0.2013-08-05.1342.1452-1.log
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RVZ9NEN.csv
    - $MFT
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RAKFFNG.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RF88HZX.csv
    - Users/nmurray/AppData/Local/Google/Chrome/User Data/Default/Cache/data_1
    - Users/nmurray/AppData/Local/Google/Chrome/User Data/Default/Cache/data_3
    - Users/nmurray/AppData/Local/Microsoft/SkyDrive/logs/SyncDiagnostics.log
    - Users/nmurray/AppData/Roaming/Microsoft/Windows/Recent/Turtle.lnk
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R7KXHV3.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R9QC4XQ.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RDR8Y57.csv

- $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RPCUJNQ.csv
- $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RT2O978.csv
- $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RWIWU17.csv
- Users/nmurray/AppData/Local/Microsoft/History/History.IE5/index.dat
- Users/nmurray/AppData/Local/Microsoft/History/History.IE5/MSHist012013080220130803/index.dat
- Users/nmurray/AppData/Local/Microsoft/History/History.IE5/index.dat/entry #00045
- Users/nmurray/AppData/Local/Microsoft/History/History.IE5/MSHist012013080220130803/index.dat/entry #00000

Wildlife.wmv

-Found in unallocated space

    - 0071049

- Found in allocated space
    - pagefile.sys
    - Users/nmurray/AppData/Local/Microsoft/SkyDrive/logs/WIN-0BEK5AK8E2S.dev=0.2013-07-22.1023.1532-1.log
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RI4LWB8.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RHH9I59.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RUDSTO2.csv
    - Users/nmurray/AppData/Local/Microsoft/SkyDrive/logs/WIN-0BEK5AK8E2S.dev=0.2013-08-05.1342.1452-1.log
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RVZ9NEN.csv
    - $MFT
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RAKFFNG.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RF88HZX.csv
    - Users/nmurray/AppData/Local/Microsoft/SkyDrive/logs/SyncDiagnostics.log
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R7KXHV3.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R9QC4XQ.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RDR8Y57.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RPCUJNQ.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RT2O978.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RWIWU17.csv
    - Users/nmurray/AppData/Local/Google/Chrome/User Data/Default/Cache/data_1
    - Users/nmurray/AppData/Local/Google/Chrome/User Data/Default/Cache/data_3

Dropbox

GettingStarted.pdf

- None found in unallocated space
- None found directly in allocated space
    - For GettingStarted.pdf it said that it was deleted, but I was still able to view the pdf. The name of the document was now Getting Started (deleted e8e9f5e1ecea9b19af69596f25b4fb39).pdf
    - pagefile.sys

WinPcap_4_1_2.exe

- Found in unallocated space
    - 1400229 (Deleted Image Only)
    - 0042851 (Unlinked Image Only)
    - 1988814 (Uninstalled Image Only)
- Found in allocated space
    - pagefile.sys

Google Drive

WinPcap_4_1_2.exe

- Found in unallocated space
    - 2527568 (Uninstalled Image Only)
    - 3444093
    - 0012438, 0807322, 3462303 (Unlinked Image Only)
    - 0163109 (Deleted Image Only)
    - /Users/nmyrray/AppData/Local/Microsoft/Media Player/Sync Playlist/en-US/00157A1/08_Video_rated_at_4_or_5_starts.wpl.FileSlack
    - Users/nmurray/AppData/Local/Temp/_MEI16762/wxmsw294u_webview.vc90.dll.FileSlack
- Found in allocated space
    - pagefile.sys
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RBT82LG.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R38TOPG.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R0J80YI.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R71YJQD.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R9CQ29T.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R0J80YI.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R7L7OVL.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RR0Qy8M.csv
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RZMADBD.csv
    - Users/nmurray/AppData/Local/Microsoft/Windows/UsrClass.dat

Plan.docx

- Found in unallocated space
    - 0050263, 2527568 (Uninstalled Image Only)
    - 0163109 (Deleted Image Only)
    - 0207322 (Unlinked Image Only)
    - 3444093, 3462303

    -Users/nmurray/AppData/Local/Temp/_MEI16762/wxmsw294u_webview.vc90.dll.FileSlack
- Found in allocated space
    - pagefile.sys
    - Config.Msi/24091.rbf
    - $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RBT82LG.csv

- $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R38TOPG.csv
- $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R0J80YI.csv
- $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R71YJQD.csv
- $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R9CQ29T.csv
- $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R0J80YI.csv
- $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$R7L7OVL.csv
- $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RR0Qy8M.csv
- $Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/$RZMADBD.csv

References

Cruz, X. (2012, November 5). The Basics of Cloud Forensics. *CloudTimes*. Retrieved from http://cloudtimes.org/2012/11/05/the-basics-of-cloud-forensics/

Digital evidence. (2012). *NCFS*. Retrieved from http://www.ncfs.org/digital_evd.html

Linthicum, D. (2013, March 15). The ticking time bomb known as cloud forensics. *InfoWorld*. Retrieved from http://www.infoworld.com/d/cloud-computing/the-ticking-time-bomb-known-cloud-forensics-214229

Messmer, E. (2013, March 6). Cloud forensics: In a lawsuit, can your cloud provider get key evidence you need? *Network World*. Retrieved from http://www.networkworld.com/news/2013/030613-cloud-forensics-267447.html

Understanding metadata [PDF]. (2004). Bethesda, MD: NISO Press.

Zimmerman, S., & Glavach, D. (2011, Winter). Cyber forensics in the cloud. *IAnewsletter*, *14*, 4-7.