IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 6, June 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

Forensic investigation of Amazon Cloud Drive on Windows 10

Ming Sang Chang

Associate Professor, Department of Information Management, Central Police University,
Taoyuan City, 33304, Taiwan (R.O.C.)

Abstract

Cloud storage services are increasingly used by consumers, business, and government. These services are fairly easy to obtain. There are many cloud storage services, such as Amazon Cloud Drive, Google Drive, Dropbox, etc. These cloud services have their own characteristics, but the easiness of creating an account cause to crime and illegal activities. It is difficult to identify, acquire, and preserve the evidences when criminals use disparate services. This study was undertaken to determine the data remnants on a Windows 10 computer. We focus on exploring the cloud activities of Amazon Cloud Drive and try to obtain evidences that may be left under these activities, different Internet browsers. By determining the data remnants on client devices, we attempt to enhance the efficiency of the digital forensics and crime investigation.

Keywords: *Amazon Cloud Drive, Cloud Storage Forensics, Digital Forensics.*

1. Introduction

Due to the rapid development of Internet technology coupled with the mobile device, people can access to Internet anytime and anywhere. They can watch the video, browse the Web, access cloud storage and so on. Cloud computing is a model for enabling ubiquitous network access to a shared pool of configurable computing resources [1]. The users of cloud computing can alleviate big capital investments, replacing them with low cost and more flexible operational expenses, while taking advantage of its speed, agility, flexibility, infinite elasticity and more importantly mobility because services can be accessed anytime and anywhere [2]. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers [3].

According to a new forecast from International Data Corporation (IDC), public IT cloud services spending will grow to more than $149 billion in 2019 [4]. A study by Market Research Media found that the global cloud computing market is expected to grow at a compound annual growth rate of 30% reaching $270 billion by 2020 [5]. A recent study conducted by RightScale group on the adoption of cloud computing, concluded that 95 percent of organizations surveyed are running applications or experimenting with infrastructure-as-a-service in January 2016 [6]. It already has begun changing how IT delivers economic value to countries, cities, industries, and businesses. The availability of cloud storage services is becoming a popular option for consumers to store data.

Internet brings a lot of convenience for modern life, but also caused many emerging crime problems. Since the information technology and mobile networks developed, resulting in crime figures increase rapidly. It is also with diverse types of crime by different information services. The criminals may use cloud storage for criminal purpose. It adds to the challenge of digital evidence in cases under investigation. Cloud storage services can be used to store, access and distribute data via remote infrastructure in overseas jurisdictions to avoid the scrutiny of law enforcement agencies [7].

While criminals are scrutinized by law enforcement agencies, the Internet crimes are effectively suppressed. But it is still a security issue that can't be ignored. For computer crime investigators, set up a systematic investigation procedure and confirm each of digital evidence to prove the offense is very important. It is important to have a strict methodology and set of procedures for executing digital forensic investigations and examinations. In addition, it is also important to have a contemporary understanding of the location and type of data remains left behind by cloud storage users on the devices they use to access their data [8]. The identification of potential data stores is an area that can impede an investigation. If forensic examiners are not knowledgeable regarding the different types of cloud-based storage systems available and what artifacts each may leave behind, they could miss critical information during an investigation.

In this paper, we discuss the digital forensics, and conduct research into the data remnants of a user accessing Amazon Cloud Drive in a variety of ways, and also undertaking anti-forensics to hide the use of cloud storage on a Windows 10 PC. The rest of this paper is organized as follows. In section 2, we show the literature survey of existing related works. Methodology and research

preparation is presented in section 3. Result and analysis is presented in section 4. Section 5 is a conclusion.

2. Related Works

McClain discusses Dropbox client software from a forensic perspective. He found some data remnants on the machine of cloud end user. He concluded that registry changes, updated files, web cache, and deleted files recovery are the major remnants found on Windows 7 [9]. Chung did a research on forensic remnants of cloud storage on different operating systems. They present methods for collecting and analyzing evidence about a variety of the cloud storage services [10]. Jason discusses the digital artifacts left behind after an Amazon Cloud Drive has been accessed from a computer. Methods available to a forensic examiner that can be used to determine file transfers that occurred to and from an Amazon Cloud Drive on a windows 7 computer [11]. Darren Quick discusses data remnants on end user devices of using Dropbox. They want to determine the data remnants on a Windows 7 computer and an Apple iPhone 3G when users use different methods to store, upload, and access data in the cloud [12]. Darren Quick discusses data remnants on user machines of using Google Drive. They use a computer and an iPhone to access Google Drive. They want to discover the remnants left on client devices. After a user accesses Google Drive, They examine the benefits of using a proposed framework to guide an investigation when undertaking forensic analysis of a cloud computing environment [13]. Darren Quick also discusses data remnants on user machines of using Microsoft SkyDrive. They use a computer and an iPhone to access Microsoft SkyDrive [14]. S. Mehreen discusses the identification of data remnants of a user activities related to Dropbox usage on Windows 8. They focused on the cloud end user and aimed at finding the data remnants of cloud storage activity, specifically Dropbox on Windows 8 platform [15].

All of the above mentioned research has been done on older versions of Windows i.e. Windows 8 or prior versions. Thus the cloud storage forensics on Windows 10 remains an area to be explored. In this paper, we will discuss the identification of data remnants of a user activities related to Amazon Cloud Drive usage on Windows 10.

3. Methodology and Research Preparation

This research focus on what data remnants after a user has accessed, up-loaded, and downloaded data from Amazon Cloud Drive. Our study uses the Amazon Cloud Drive client software and different browsers to test it. We use the popular browsers include Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome. We use these browsers in our research to determine any differences in the ability to retrieve data remnants. We want to find username, password, files, text within files, or the presence of client software. In addition, we also create circumstances to simulate a user running BleachBit to remove evidence of using Amazon Cloud Drive.

We create 18 virtual machines to gather the data in relation to the use of Amazon Cloud Drive for Windows 10. We make multiple scenarios to explore the use of Amazon Cloud Drive with a different browser. They include Internet Explorer (IE), Mozilla Firefox (MF), and Google Chrome (GC). We create Virtual Machines for each browser to replicate different circumstance of usage. This represents different physical computer systems available for analysis, with different circumstances and data remnants available for analysis on each VM. According to the operation of Amazon Cloud Drive, we create five sub-experiment systems for each browser. They are Base, Access, Download, Upload, and BleachBit.

Table 1: All Virtual Machine Files

Apps / VM	Internet Explorer	Mozilla Firefox	Google Chrome	Application
Base-VM	IE-Base	MF-Base	GC-Base	ACDD-Base
Upload-VM	IE-Upload	MF-Upload	GC-Upload	ACDD-Upload
Access-VM	IE-Access	MF-Access	GC-Access	None
Download-VM	IE-Download	MF-Download	GC-Download	ACDD-Download
BleachBit-VM	IE-BleachBit	MF-BleachBit	GC-BleachBit	None

We use the base image files to compare the subsequent image files to determine the changes made. It is possible to observe the changes of file systems. We use VMware Workstation 10.0.0 to create virtual machine. For each browser scenario, a base image, Base-VM, was created. We install Windows 10（Build 9841）on a 20 GB virtual hard drive with 1 GB RAM. The Base-VM files were used as control media to determine the files created when user activity was undertaken in each scenario. All scenarios for Windows 10 are shown in table 1.

We describe the details of our experiment as follows.

1. We install different browser software into separate Base-VMs. They are Internet Explorer (IE) v11.0.10011, Mozilla Firefox (MF) v31.0, and Google Chrome (GC)

v39.0.2171. We also install client software, Amazon Cloud Drive Desktop (ACDD) v2.3, into separate Base-VM. These four base VMs are labeled IE-Base, MF-Base, GC-Base, and ACDD -Base,

2. We make a copy of the Base-VM for each browser and Amazon Cloud Drive. These 14 VMs are labeled IE-Access, IE-Download, IE-Upload, IE-BleachBit, MF-Access, MF-Download, MF-Upload, MF-BleachBit, GC-Access, GC-Download, GC-Upload, GC-BleachBit, ACDD-Download, and ACDD-Upload.
3. We use upload virtual machines to upload test files. These upload virtual machines are IE-Upload, MF-Upload, GC-Upload, and ACDD-Upload. The test files are uploaded to Amazon Cloud Storage. Then we delete test files from the virtual machines. After we open the test files from Amazon Cloud Storage, we close the browser or client software, then shuts down the system.
4. In these virtual machines, IE-Access, MF-Access, and GC-Access, we use different browser to log in Amazon Cloud Storage and only online open the test files which are uploaded previously. Then we log out and close the browser, and shut down the system.
5. The download virtual machines are IE-Download, MF-Download, GC-Download, and ACDD- Download. We use different browser or client software to log in Amazon Cloud Storage and only online open the test files which are uploaded previously. Then we download the test files on the desktop of virtual machines. We open the download files. Then we log out and close the browser or client software, and shut down the system.
6. We use BleachBit 1.6 software to do anti-Forensics. These anti-Forensics virtual machines are IE-BleachBit, MF-BleachBit, and GC-BleachBit. We do the same action as download virtual machines. Then the downloaded test files are deleted. We run BleachBit 1.6 software to clear temporary files, test files, and browsing history.

4. Result and Analysis

After all the experiments, we use Guidance EnCase v7.04 to analyze VMDK files of all virtual machines. This research is to determine the data remnants on a Windows 10 PC for the use of Amazon Cloud Storage. We try to find username, password, browser access, software access, and files stored within the account. We use keywords to search the data remnants. They include Amazon, account name (testforensic2014), account password (test123456789), test files (1.bmp, 1.jpg, 1.doc, 1.xls, 1.ppt), and the text within the test files (This is Microsoft word, This is Microsoft excel, This is Microsoft PowerPoint).

There are five different kind experiments to be discussed.

Base-VM

There are four Base-VM hard drives, such as IE-Base, MF-Base, GC-Base, and ACDD-Base. They have no data originally present relating to the sample test data and Amazon Cloud Storage files. We Analyze this four control Base-VM hard disc drives to confirm there was no data originally relating to Amazon Cloud Storage.

Access-VM

In these virtual machines, IE-Access, MF-Access, and GC-Access, we use different browser to log in Amazon Cloud Storage and only online open the test files which are uploaded previously. Then we log out and close the browser, and shut down the system. We find the remnants by EnCase. We find the keyword Amazon in different directories. In IE cache, we find it on C\Users\[username]\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat. In MF cache, we find the keyword Amazon on C\Users\[username]\AppData\Local\Mozilla\Firefox\Profiles\wz1g2ln3.default\cache2\. In GC cache, we find the keyword Amazon on C\Users\[username]\AppData\Local\Google\Chrome\User Data\Default\Cache\. In GC history, we find it on C\Users\[username]\AppData\Local\Google\Chrome\User Data\Default\History. We also find the keyword on the C\Unallocated Clusters and C\pagefile.sys. in IE-Access, MF-Access, and GC-Access. About account name, we find it on the C\$MFT, C\hiberfil.sys, C\pagefile.sys, and C\Unallocated Clusters in IE-Access, MF-Access, and GC-Access. We can't find the password because it was not stored on the file of disc. We find the action of opening the test files online that have no data remnants on the browser's cache. Table 2 shows the remnants of Access-VMs.

Upload-VM

We use upload virtual machines to upload test files. These upload virtual machines are IE-Upload, MF-Upload, GC-Upload, and ACDD-Upload. In this paragraph we just discuss IE-Upload, MF-Upload, and GC-Upload. We will discuss ACDD-Upload in different paragraph of this section. We find the keyword Amazon, test account name, and password in the same directories as Access-VM. About test files, we find data remnants on C\$MFT, and C\pagefile.sys in IE-Upload, and MF-Upload. We also find data remnants on C\$MFT, C\$Extend\$UsnJrnl·$J, and C\$LogFile in GC-Upload. About text in files, it is different from Access-VM. We can find data remnants on C\Unallocated Clusters in IE-Upload, MF-Upload, and GC-Upload.

Table 2: The remnants of Access-VM

Keyword	IE	Firefox	Chrome
Amazon	•C\Users\[username]\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat •C\Unallocated Clusters •C\pagefile.sys	•C\Users\[username]\AppData\Local\Mozilla\Firefox\Profiles\wz1g2ln3.default\cache2\ •C\Unallocated Clusters •C\pagefile.sys	•C\Users\[username]\AppData\Local\Google\Chrome\UserData\Default\History •C\Unallocated Clusters •C\pagefile.sys
testforensic2014 (account name)	•C\$MFT •C\hiberfil.sys •C\pagefile.sys •C\Unallocated Clusters	•C\$MFT •C\hiberfil.sys •C\pagefile.sys •C\Unallocated Clusters	•C\$MFT •C\hiberfil.sys •C\pagefile.sys •C\Unallocated Clusters
test123456789 (password)	none	none	none
1.doc, (test files)	none	none	none
This is Microsoft word. (text in the 1.doc)	none	none	none

Download-VM

We use download virtual machines to download test files. These download virtual machines are IE-Download, MF-Download, GC-Download, and ACDD-Download. In this paragraph we just discuss IE-Upload, MF-Upload, and GC-Upload. We will discuss ACDD-Upload in different paragraph. We find data remnants of the keyword Amazon, test account name, and password in the same directories as Access-VM. About test files, we find data remnants on C\$MFT in IE-Upload. In MF-Upload, we find data remnants on C\$MFT, C\Users\[username]\Desktop\, C\swapfile.sys, and C\Unallocated Clusters. We also find data remnants on C\$MFT, C\Users\[username]\Desktop\, C\hiberfil.sys, and C\pagefile.sys in GC-Upload. About text in files, we can find data remnants on C\Unallocated Clusters, and C\Users\[username]\Desktop\, in IE-Upload, MF-Upload, and GC-Upload. And we can only find data remnants on C\Users\[username]\AppData\Local\Google\Chrome\User Data\Default\Cache\ in GC-Download.

BleachBit-VM

We do the same actions as Download-VM. Then we run BleachBit to delete browser data remnants such as password, cookies, cache, history, etc. We also delete the history of the Windows Explorer such as most recently used files list, image cache, Recycle Bin, Scrapbook, etc. We find data remnants of the keyword Amazon, test account name, and password in the same directories as Access-VM. About test files, we find data remnants on C\$MFT, C\hiberfil.sys, and C\$Recycle.Bin\ in IE-BleachBit. In MF-BleachBit we find data remnants on C\$MFT, C\pagefile.sys, C\Users\[username]\Desktop\, and C\Unallocated Clusters. We also find data remnants on C\$MFT, C\hiberfil.sys, C\$Extend\$UsnJrnl·$J, C\$LogFile, C\$Recycle.Bin, and C\Unallocated Clusters in GC-BleachBit. About text in files, we can find data remnants on C\$Recycle.Bin\ and C\Unallocated Clusters in IE-BleachBit and MF-BleachBit. We also find data remnants on C\Users\[username]\AppData\Local\Google\Chrome\User Data\Default\Cache\, C\Unallocated Clusters, and C\pagefile.sys in GC-BleachBit.

We find data remnants of the keyword Amazon, test account name, and password in the same directories as Access-VM because EnCase can recover delete files. A lot of evidences can be found in system log files and Recycle Bin in this experiment. It means we did the deleted operation before.

Client Software

We install Amazon Cloud Drive Desktop v2.3 on virtual machine. There are three virtual machines name ACDD-Base, ACDD-Upload, and ACDD-Download. We log in and upload and download files. Then we find data remnants of the keyword Amazon on C\$Extend\$UsnJrnl·$J, C\hiberfil.sys, Unallocated Clusters, and C\Users\[username]\AppData\Local\Amazon\Cloud Drive\ in ACDD-Upload and ACDD-Download. We find data remnants of the account name on C\hiberfil.sys, C\Unallocated Clusters, C\$MFT, and C\pagefile.sys in ACDD-Upload and ACDD-Download.

About test files, we find data remnants on C\$MFT, C\$Extend\$UsnJrnl·$J, C\$LogFile, and C\Users\testf\AppData\Local\Amazon Cloud Drive\Logs\ in ACDD-Upload. In ACDD-Download, we find data remnants only on C\$MFT. About text in files, we can find data remnants on C\Unallocated Clusters in ACDD-Upload and ACDD-Download. The remnants of using Client software show as table 3.

Table 3: The remnants of using Client software

Keyword	Download	Upload

Amazon	•C\$Extend\$UsnJrnl•$J •C\hiberfil.sys •C\Unallocated Clusters •C\Users\[username]\AppData\Local\Amazon\Cloud Drive\	•C\$Extend\$UsnJrnl•$J •C\hiberfil.sys •C\Unallocated Clusters •C\Users\[username]\AppData\Local\Amazon\Cloud Drive\
testforensic2014 (account name)	•C\$MFT •C\hiberfil.sys •C\pagefile.sys •C\Unallocated Clusters	•C\$MFT •C\hiberfil.sys •C\pagefile.sys •C\Unallocated Clusters
test123456789 (password)	none	none
1.doc, (testfile)	•C\$MFT	•C\$MFT •C\$Extend\$UsnJrnl•$J •C\$LogFile •C\Users\testf\AppData\Local\Amazon Cloud Drive\Logs\
This is Microsoft word. (text in the 1.doc)	•C\Unallocated Clusters	•C\Unallocated Clusters

5. Conclusions

When we investigate the using of cloud storage, the initial stages include the identification of a cloud service and user account. This may enable investigators to identify the location of data. In this research, we find that an investigator can identify Amazon Cloud Drive account use by undertaking keyword searches and examine test files locations to locate relevant information.

The remnants of cloud activity can be found on local machines. It could be valuable for the forensic examiners. We found the remnants in local folders. The username, the cache files, and log activity which helps in recovering the deleted files and data. We identify the locations of data and files to determine user details and cloud storage information relating to use of Amazon Cloud Drive in our research.

References

[1] Mell, P & Grance, T. The Nist Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-145. 2011.

[2] Ameer Pichan, Mihai Lazarescu, Sie Teng Soh. Cloud forensics: Technical challenges, solutions and comparative analysis. Digital Investigation 2015;13:38-57.

[3] Haghighat, M., Zonouz, S., & Abdel-Mottaleb, M. CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification. Expert Systems with Applications, 2015;42(21):7905–7916.

[4] IDC: Worldwide Public Cloud Services Spending Forecast. 2016; https://www.idc.com/getdoc.jsp?containerId=prUS40960516 (Access on May 20, 2016)

[5] Zawaod S, Hasan R. Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. Distributed, Parallel, and Cluster Computing. 2013;arXiv:1302.6312.

[6] RightScale 2016 State of the Cloud Report. http://www.mcit.gov.eg/Upcont/Documents/Reports%20and%20Documents_1252016000_RightScale-2016-State-of-the-Cloud-Report.pdf (Access on May 20, 2016).

[7] Biggs, S & Vidalis, S. Cloud Computing: The Impact on Digital Forensic Investigations. Proceedings of IEEE International Conference for Internet Technology and Secured Transactions. 2009;1–6.

[8] Guo, H, Shang, T & Jin, B. Forensic Investigations in Cloud Environments. IEEE International Conference on Computer Science and Information Processing. 2012;248-251.

[9] McClain, F. Dropbox Forensics. 2011; https://articles.forensicfocus.com/2011/07/24/dropbox-forensics/ (Access on May 20, 2016).

[10] Chung, H, Park, J, Lee, S & Kang, C (2012), Digital Forensic Investigation of Cloud Storage Services, Digital Investigation. 2012; 9(2): 81–95.

[11] Hale, Jason. Amazon Cloud Drive Forensic Analysis. Digital Investigation. 2013;10(3): 259- 265.

[12] D. Quick and K.-K. R. Choo, Dropbox analysis: Data remnants on user machines. Digital Investigation. 2013;10(1): 3-18.

[13] Darren Quick, Kim-Kwang Raymond Choo, "Google Drive: forensic analysis of cloud storage data remnants," Journal of Network and Computer Applications. 2014;40:179-193.

[14] Darren Quick, Kim-Kwang Raymond Choo, "Digital droplets: Microsoft SkyDrive forensic data remnants," Future Generation Computer Systems. 2013;29(6):1378-1394.

[15] S. Mehreen, B. Aslam. Windows 8 Cloud Storage Analysis: Dropbox Forensics. International Bhurban Conference on Applied Sciences & Technology. 2015;312-317