IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 8, August 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

Forensic Analysis of Google Drive on Windows

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. Google Drive is a popular service, providing users a cost-effective, and in some cases free, ability to access, store, collaborate, and disseminate data. 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 computer. We focus on exploring the cloud activities of Google 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: *Google 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 Google Drive in a variety of ways, and also undertaking anti-forensics to hide the use of cloud storage on a Windows 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

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 [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]. 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 [11]. Darren Quick discusses data remnants on user machines of using Microsoft SkyDrive. They use a computer and an iPhone to access Microsoft SkyDrive [12]. 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 [13]. 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 [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 not been done all of Windows XP, Windows 7, and Windows 8 on Google Drive. In this paper, we will discuss the identification of data remnants of a user activities related to Google Drive usage on Windows XP, Windows 7, and Windows 8.

3. Methodology and Research Preparation

This research focus on what data remnants after a user has accessed, up-loaded, and downloaded data from Google Drive. Our study uses the Google Drive client software and different browsers to test it. We use the popular browsers include Microsoft Internet Explorer, 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 CCleaner to remove evidence of using Google Drive.

We create 36 virtual machines to gather the data in relation to the use of Google Drive for Windows XP, 7, and 8. We make multiple scenarios to explore the use of Google Drive with a different browser. They include Internet Explorer (IE), 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 Google Drive, we create six sub-experiment systems for each browser. They are Base, Access, Download, Upload, Uninstall, and CCleaner.

Table 1: All Virtual Machine Files

VM	Windows XP	Windows 7	Windows 8
Base−VM	IEXP−Base, GCXP−Base	IE7−Base, GC7−Base	IE8−Base, GC8−Base
Access−VM	IEXP−Access, GCXP−Access	IE7−Access, GC7−Access	IE8−Access, GC8−Access
Download−VM	IEXP-Download, GCXP-Download	IE7−Download, GC7−Download	IE8-Download, GC8-Download
Upload−VM	IEXP−Upload, GCXP− Upload	IE7−Upload, GC7−Upload	IE8−Upload, GC8−Upload
Uninstall−VM	IEXP−Uninstall, GCXP− Uninstall	IE7−Uninstall, GC7−Uninstall	IE8−Uninstall, GC8−Uninstall
CCleaner−VM	IEXP−CCleaner, GCXP−CCleaner	IE7−CCleaner, GC7− CCleaner	IE8−CCleaner, GC8− CCleaner

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 8.0.4 to create virtual machine. For each browser scenario, a base image, Base-VM, was created. We install Windows XP, 7, 8 on a 15 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 XP, 7, 8 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 10 (IE10) on Windows 8, IE8 on Windows XP and 7, and Google Chrome (GC) version 29 on Windows XP, 7, and 8.
2. We make a copy of the Base-VM for each scenario of Google Drive. These 30 VMs are labeled IEXP-Access, IEXP-Download, IEXP-Upload, IEXP-Uninstall, IEXP-CCleaner, IE7-Access, IE7-Download, IE7-Upload, IE7-Uninstall, IE7-CCleaner, IE8-Access, IE8-Download, IE8-Upload, IE8-Uninstall, IE8-CCleaner, GCXP-Access, GCXP-Download, GCXP-Upload, GCXP-Uninstall, GCXP-CCleaner, GC7-Access, GC7-Download, GC7-Upload, GC7-Uninstall, GC7-

CCleaner, GC8-Access, GC8-Download, GC8-Upload, GC8-Uninstall, and GC8-CCleaner.

3. We use upload virtual machines to upload test files. The test files are uploaded to Google Drive. Then we delete test files from the virtual machines. After we open the test files from Google Drive, we close the browser and shut down the system.
4. In the Access-VM virtual machines, we use different browsers to log in Google Drive 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. In the Download-VM virtual machines, we use different browser or client software to log in Google Drive 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. In the Uninstall-VM virtual machines, we install Google Drive client software on them. We use Google Drive client software to log in Google Drive and upload the test files. Then we log out and close the client software, and uninstall the client software.
7. We use CCleaner software to do anti-Forensics. We do the same action as upload virtual machines. We run CCleaner v4.05 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 Windows XP, 7, and 8 PC for the use of Google Drive. We try to find username, password, browser access, software access, and files stored within the account. We use keywords to search the data remnants.

There are three different Windows operating system and five different kind experiments to be discussed.

4.1 Windows XP

(1) Base-VM

There are two Base-VM hard drives, such as IEXP-Base, and GCXP-Base. They have no data originally present relating to the sample test data. We Analyze this two control Base-VM hard disc drives to confirm there was no data originally relating to Google Drive.

(2) Access-VM

In these virtual machines, IEXP-Access, and GCXP-Access, we use different browser to log in Google Drive 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 account name in different locations. In IE cache, we find it on cookies and Unallocated Clusters. In GC cache, we find the account name on Cache, Unallocated Clusters, and C:\ Documents and Setting\Administrator\Local Setting\Application Data\Google\Chrome\User Data\. All the other remnants of activities of these virtual machines will be shown in Table 2.

(3) Upload-VM

We use upload virtual machines to upload test files. We find the account name in different directories. In IE and GC, we find it on cookies, Unallocated Clusters, $MFT, and $LogFile. All the other remnants of activities of these virtual machines will be shown in Table 2.

(4) Download-VM

We use download virtual machines to download test files. We find the account name in different directories. In IE and GC, we find it on cookies, and Unallocated Clusters. All the other remnants of activities of these virtual machines will be shown in Table 2.

(5) Uninstall-VM

We use Uninstall-VM virtual machines to upload files. Then we uninstall client software. We find the account name in different directories. In IE and GC, we find it on cookies, Unallocated Clusters, $MFT, and $LogFile. All the other remnants of activities of these virtual machines will be shown in Table 2.

(6) CCleaner-VM

We do the same actions as Upload-VM. Then we run CCleaner 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. In IE, the account name can't be found. In GC, we find the account name on $LogFile and pagefile.sys. All the other remnants of activities of these virtual machines will be shown in Table 2. We find data remnants of the keyword Google, account name, and test files because EnCase can recover delete files. A lot of evidences can be found in system log files and Unallocated Clusters in these experiments. It means we did the deleted operation before.

4.2 Windows 7

(1) Base-VM

There are two Base-VM hard drives, such as IE7-Base, and GC7-Base. They have no data originally present relating to the sample test data. We Analyze this two control Base-VM hard disc drives to confirm there was no data originally relating to Google Drive.

(2) Access-VM

In these virtual machines, IE7-Access, and GC7-Access, we use different browser to log in Google Drive 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 account name in different locations. In IE cache, we find it on cookies and Unallocated Clusters. In GC cache, we find the account name on Unallocated Clusters, and Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State. All the other remnants of activities of these virtual machines will be shown in Table 3.

(3) Upload-VM

We use upload virtual machines to upload test files. We find the account name in different directories. In IE, we find it on pagefile.sys, $MFT, $LogFile. In GC, we find it on $MFT, $LogFile, and Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State. All the other remnants of activities of these virtual machines will be shown in Table 3.

(4) Download-VM

We use download virtual machines to download test files. We find the account name in different directories. In IE, we find it on Cookies, and Unallocated Clusters. In GC, we find it on Unallocated Clusters, and Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State. All the other remnants of activities of these virtual machines will be shown in Table 3.

(5) Uninstall-VM

We use Uninstall-VM virtual machines to upload files. Then we uninstall client software. We find the account name in different directories. In IE, we find it on pagefile.sys, $MFT, and $LogFile. In GC, we find it on Cache, $LogFile, Unallocated Clusters, and Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State. All the other remnants of activities of these virtual machines will be shown in Table 3.

(6) CCleaner-VM

We do the same actions as Upload-VM. Then we run CCleaner 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. In IE, the account name on pagefile.sys. In GC, we find the account name on pagefile.sys, and Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State. All the other remnants of activities of these virtual machines will be shown in Table 3. We find data remnants of the keyword Google, account name, and test files because EnCase can recover delete files. A lot of evidences can be found in system log files and Unallocated Clusters in these experiments. It means we did the deleted operation before.

4.3 Windows 8

(1) Base-VM

There are two Base-VM hard drives, such as IE7-Base, and GC7-Base. They have no data originally present relating to the sample test data. We Analyze this two control Base-VM hard disc drives to confirm there was no data originally relating to Google Drive.

(2) Access-VM

In these virtual machines, IE7-Access, and GC7-Access, we use different browser to log in Google Drive 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 account name in different locations. In IE cache, we find it on cookies and Unallocated Clusters. In GC cache, we find the account name on Unallocated Clusters, and Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State. All the other remnants of activities of these virtual machines will be shown in Table 4.

(3) Upload-VM

We use upload virtual machines to upload test files. We find the account name in different directories. In IE, we find it on pagefile.sys, $MFT, $LogFile. In GC, we find it on $MFT, $LogFile, and Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State. All the other remnants of activities of these virtual machines will be shown in Table 4.

(4) Download-VM

We use download virtual machines to download test files. We find the account name in different directories. In IE, we find it on Cookies, and Unallocated Clusters. In GC, we find it on Unallocated Clusters, and Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State. All the other remnants of activities of these virtual machines will be shown in Table 4.

(5) Uninstall-VM

We use Uninstall-VM virtual machines to upload files. Then we uninstall client software. We find the account name in different directories. In IE, we find it on pagefile.sys, $MFT, and $LogFile. In GC, we find it on Cache, $LogFile, Unallocated Clusters, and Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State. All the other remnants of activities of these virtual machines will be shown in Table 4.

(6) CCleaner-VM

We do the same actions as Upload-VM. Then we run CCleaner 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. In IE, the account name on pagefile.sys. In GC, we find the account name on pagefile.sys, and

Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State. All the other remnants of activities of these virtual machines will be shown in Table 4. We find data remnants of the keyword Google, account name, and test files because EnCase can recover delete files. A lot of evidences can be found in system log files and Unallocated Clusters in these experiments. It means we did the deleted operation before.

Table 2 The remnants of Windows XP

VM	Renmants	IE8	Google Chrome
Base	Account Password	None None	None None
Access	Account	Cookies, Unallocated Clusters	Cache, Unallocated Clusters, C:\ Documents and Setting\Administrator \ Local Setting\Application Data\Google\ Chrome \User Data\
	Password	None	None
	Locations	Cache, Cookie, history, pagefile.sys, Unallocated Clusters	Cache, Cookie, history, pagefile.sys, Unallocated Clusters
	Test files	Cache	Cache
	Keyword	Cookies, Unallocated Clusters, history, Cache	Cookies, Unallocated Clusters, history, Cache
Download	Account	Cookies, Unallocated Clusters	Cookies, Unallocated Clusters, Pagefile.sys
	Password	None	None
	Location	Cache, Cookie, history, pagefile.sys, Unallocated Clusters	Cache, Cookie, history, pagefile.sys, Unallocated Clusters
	Test files	Cache, $MFT, $LogFile, index.dat, Cookies、	$MFT, $LogFile, index.dat, pagefile.sys, Unallocated Clusters
	Keyword	Cookies, Unallocated Clusters, history, Cache	Cookies, Unallocated Clusters, history, Cache
Upload and Uninstall	Account	Cookies, Unallocated Clusters, $MFT, $LogFile	Cookies, Unallocated Clusters, $MFT, $LogFile pagefile.sys, sync_log
	Password	None	None
	Client software	C:\Program Files\Google\Drive\ google- drivesync.exe	C:\Program Files\Google\Drive\ google-drivesync.exe
	Locations	C:\ Documents and Setting\Administrator \ Local Setting\Application Data\Google\ Drive\	C:\ Documents and Setting\Administrator \ Local Setting\Application Data\Google\ Drive\
	Test files	Cache, Cookie, history, pagefile.sys, Unallocated Clusters	Cache, Cookie, history, pagefile.sys, Unallocated Clusters
	Keyword	Cookies, Unallocated Clusters, history	Cookies, Unallocated Clusters, history
CCleaner	Account	None	$LogFile, pagefile.sys, SyncData.sqlite3
	Password	None	None
	Locations	None	None
	Test files	None	Unallocated Clusters, NTUSER.DAT
	Keyword	Cookies, Unallocated Clusters, history	Cookies, Unallocated Clusters, history

Table 3 The remnants of Windows 7

VM	Renmants	IE8	Google Chrome
Base	Account Password	None None	None None
Access	Account	Unallocated Clusters	Unallocated Clusters, Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State
	Password	None	None
	Locations	Cache, Cookie, $MFT, Unallocated Clusters	Cache, Cookie, $MFT, Unallocated Clusters
	Test files	Cache	Cache

	Keyword	Cookies, Unallocated Clusters, history, Cache	Cookies, Unallocated Clusters, history, Cache
Download	Account	Cookies, Unallocated Clusters	Unallocated Clusters, Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State
	Password	None	None
	Location	Cache, Cookie, history, pagefile.sys, Unallocated Clusters	Cache, Cookie, history, pagefile.sys, Unallocated Clusters
	Test files	Cache, $LogFile, Cookies	$MFT, $LogFile, NTUSER.DAT
	Keyword	Cookies, Unallocated Clusters, history, Cache	Cookies, Unallocated Clusters, history, Cache
Upload	Account	pagefile.sys, $MFT, $LogFile	$MFT, $LogFile, Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State
	Password	\AppData\Local\Microsoft\Internet Explorer\Recovery\Last Active\{FC4656}.dat	Search by &Email= and &Passwd= and &PasswdAgain=
	Client software	$LogFile, $MFT, $UsnJrnl, hiberfil.sys, pagefile.sys	$LogFile, $MFT, $UsnJrnl, hiberfil.sys, pagefile.sys
	Locations	Cache, Cookie, $MFT	Cache, Cookie, Program Files\Google \Chrome\Application\30.0.1599.69\Locales\
	Test files	Cache, Cookie, history, pagefile.sys	Cache, Cookie, history, pagefile.sys,
	Keyword	Cookies, Unallocated Clusters, history	Cookies, Unallocated Clusters, history
Uninstall	Account	pagefile. sys, $MFT, $LogFile	Cache,$LogFile,Unallocated Clusters, Users\Administrator\AppData\Local\Google \Chrome\User Data\Local State
	Password	\AppData\Local\Microsoft\Internet Explorer\Recovery\Last Active\{FC4656}.dat	Search by &Email= and &Passwd= and &PasswdAgain=
	Client software	Windows\Installer\44726.msi	System Volume Information
	Locations	Cache, Cookie, pagefile.sys	Cache, Cookie, history, Unallocated Clusters
	Test files	Cache, Cookie, history, pagefile.sys, Unallocated Clusters	Cache, Cookie, history, pagefile.sys, Unallocated Clusters
	Keyword	Cookies, Unallocated Clusters, history	Cookies, Unallocated Clusters, history
CCleaner	Account	pagefile. sys	pagefile.sys, Users\Administrator\AppData\Local\Google \Chrome\User Data\Local State
	Password	None	None
	Locations	Unallocated Clusters, pagefile.sys	Unallocated Clusters, pagefile.sys, history
	Test files	pagefile.sys, NTUSER.DAT	pagefile.sys, NTUSER.DAT
	Keyword	Cookies, Unallocated Clusters, history	Cookies, Unallocated Clusters, history

Table 4 The remnants of Windows 8

VM	Renmants	IE10	Google Chrome
Base	Account Password	None None	None None
Access	Account	None	Unallocated Clusters, Users\Administrator\AppData\Local\Google \Chrome\User Data\Local State
	Password	None	None
	Locations	Cache, Cookie, $MFT, WebCacheV01.dat	Cache, Cookie, $MFT, Unallocated Clusters
	Test files	WebCacheV01.dat	\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3
	Keyword	Cookies, Unallocated Clusters, history, Cache	Cookies, Unallocated Clusters, history, Cache

Download	Account	$MFT, hiberfil.sys, pagefile.sys, swapflies.sys, Unallocated Clusters	Unallocated Clusters, Users\Administrator\AppData\Local\Google \Chrome\User Data\Local State
	Password	None	hiberfil.sys
	Location	Cache, Cookie, history, pagefile.sys, Unallocated Clusters	Cache, Cookie, history, pagefile.sys, Unallocated Clusters
	Test files	NTUSER.DAT, Shortcuts, UserClass.dat	Cache, automaticDestinations-ms, NTUSER.DAT, Unallocated Clusters
	Keyword	Cookies, Unallocated Clusters, history, Cache	Cookies, Unallocated Clusters, history, Cache
Upload	Account	pagefile.sys, $MFT, $LogFile, swapflies.sys, Shortcuts, Unallocated Clusters	automaticDestinations-ms, hiberfil.sys, Shortcuts
	Password	\AppData\Local\Microsoft\Internet Explorer\Recovery\Last Active\{FC4656}.dat	pagefile.sys
	Client software	Program Files\Google\ Drive\ google drivesync.exe	$LogFile, $MFT, $UsnJrnl, hiberfil.sys, pagefile.sys
	Locations	Cache, Cookie, $MFT	pagefile.sys, Program Files\Google \Chrome\Application\30.0.1750.154\Locales\
	Test files	Cache, Cookie, history, pagefile.sys	Cache, automaticDestinations-ms, NTUSER.DAT, pagefile.sys,
	Keyword	Cookies, Unallocated Clusters, history	Cookies, Unallocated Clusters, history
Uninstall	Account	pagefile. sys, $MFT, $LogFile, swapflies.sys, Unallocated Clusters	pagefile. sys, $MFT, $LogFile, swapflies.sys, Unallocated Clusters
	Password	None	None
	Client software	Windows\Installer\44726.msi \AppData\Local\Microsoft\Internet Explorer\Recovery\Last Active\{FC4656}.dat	None
	Locations	$MFT, Cache, Cookie, pagefile.sys	Cache, hiberfil.sys, Unallocated Clusters
	Test files	Cache, Cookie, history, pagefile.sys, Unallocated Clusters	pagefile.sys, UsrClass.dat, snapshot.db-wal, pagefile.sys, automaticDestinations-ms, NTUSER.DAT
	Keyword	Cookies, Unallocated Clusters, history	Cookies, Unallocated Clusters, history
CCleaner	Account	$MFT, $LogFile, pagefile.sys, swapflies.sys, Unallocated Clusters	$MFT, $LogFile, pagefile.sys, swapflies.sys, Unallocated Clusters
	Password	None	None
	Locations	None	Unallocated Clusters, hiberfil.sys, Program Files\Google \Chrome\Application\ 30.0.1750.154\Locales\
	Test files	pagefile.sys, NTUSER.DAT	Unallocated Clusters, NTUSER.DAT
	Keyword	Cookies, Unallocated Clusters, history	Cookies, Unallocated Clusters, history

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 Google 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 Google 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 Jul 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 Jul 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] D. Quick and K.-K. R. Choo, Dropbox analysis: Data remnants on user machines. Digital Investigation. 2013;10(1): 3-18.
[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] McClain, F. Dropbox Forensics. 2011; https://articles.forensicfocus.com/2011/07/24/dropbox-forensics/ (Access on Jul 20, 2016).
[12] Darren Quick, Kim-Kwang Raymond Choo, "Digital droplets: Microsoft SkyDrive forensic data remnants," Future Generation Computer Systems. 2013;29(6):1378-1394.
[13] Hale, Jason. Amazon Cloud Drive Forensic Analysis. Digital Investigation. 2013;10(3): 259- 265.
[14] 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.
[15] S. Mehreen, B. Aslam. Windows 8 Cloud Storage Analysis: Dropbox Forensics. International Bhurban Conference on Applied Sciences & Technology. 2015;312-317