IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 4 Issue 8 August, 2016

Forensic Investigation of Google Drive on Android

Ming Sang Chang

Department of Information Management, Central Police University,Taoyuan City, 33304, Taiwan.

mschang@mail.cpu.edu.tw

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 aAndroid System. 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:GoogleDrive, Digital Forensics, Cloud Storage 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 smart phone with Android system. The rest of this paper is organized as follows. In section 2, we show the literature survey of existing related works. Methodologyis 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[13]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. Darren Quick[14]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. 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].

In this paper, we will discuss the identification of data remnants of a user activities related to Google Drive usage on an Android system.

3. METHODOLOGY

This research focus on what data remnants after a user has accessed, up-loaded, and downloaded data from Google Drive on an Android system. Our study uses the Google Drive client software and different browsers to test it. We use the popular browsers include Firefox, and Google Chrome on a smart phone. We use two browsers and Google Drive app in our research to determine any differences in the ability to retrieve data remnants. We want to find the username, password, files, contents within files, or the presence of the use of Google Drive. In addition, we also create circumstances to simulate a user running CCleaner to remove evidence of the activities of Google Drive.

The software of these experiments includes Android V4.2.2, Google Chrome V31.0.1650.59, Firefox V45.0.1, and Google Drive App V2.3.631.15.34. The forensic and analysis tools are AccessData FTK Imager V3.1.1.8, MANDIANT Memoryze V3.0, WinHex V18.5, SQLite V2.0.1, and CCleaner V1.13.50.

We use a smart phone, Taiwan Mobile Amazing A7, to gather the data in relation to the use of Google Drive for Android. We make multiple scenarios to explore the use of Google Drive withdifferent browsers. They include Google Chrome (GC) and Firefox (FF). The use of Google Drive App (GDA) is also a case to gather the data remnants. After finishing each experiment, the smart phone was restored to the original state.

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. For each scenario, three base images, GC-Base, FF-Base, and GDA-Base, were created. The Base image files were used as control media to determine the files created when user activity was undertaken in each scenario. All scenarios for Android are shown in table 1.

Table 1: All scenarios of experiments

Action	GC	FF	GDA
Base	GC-Base	FF-Base	GDA-Base
Upload	GC-Upload	FF-Upload	GDA-Upload
Access	GC-Access	FF-Access	GDA-Access
Download	GC-Download	FF-Download	GDA-Download
CCleaner	GC-CCleaner	FF-CCleaner	GDA- CCleaner

The details of our experiment are as follows.

1. We install different browser and client software in three separate Base scenarios. They are Google Chrome V31.0.1650.59, Firefox V45.0.1, and Google Drive App V2.3.631.15.34. After finishing the installation there are no operations on these experiments.
2. The test files are uploaded to Google Drive in three scenarios. They are GC-Upload, FF-Upload, and GDA-Upload. Then we delete test files from the smart phone. After we open the test files from Google Drive, we close the browser or Google Drive App.
3. In the Access scenarios, we use different browsers and app to log in Google Drive and only online open the test files which are uploaded previously. Then we log out and close the browser or Google Drive App.
4. In the Download scenarios, we use different browsers 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 smart phone. We open the download files. Then we log out and close the browser or client software.
5. We use CCleaner software to do anti-Forensics. We do the same action as download scenarios. Then CCleaner V1.13.50 was run to clear temporary files, test files, and browsing history.

4. RESULT AND ANALYSIS

After all the experiments, we use AccessData FTK Imager, SQLite, and WinHex to findthe data remnants of all scenarios. This research is to determine the data remnants on Android for the use of Google Drive.We try to find the artifacts of username, password, browser access, software access, and files stored within the account. We use keywords to search the data remnants.

There are five different kinds of experiments to be discussed.

(1) Base

There are three Base experiments, such as GC-Base, FF-Base, and GDA-Base. They have no data originally present relating to the sample test data. We Analyzethree control Base scenarios to confirm there was no data originally relating to Google Drive.

(2) Upload

There are threeUpload experiments, such as GC-Upload, FF-Upload, and GDA-Upload. The test files were uploaded to Google Drive. We use the keywords to find data remnants.The keywords include test account (wjl.test.one@gmail.com), password (zaqwsxcd), WiFi account (joeko), WiFi password (19750402), testfiles, and contents of test file. We only use GDA-Upload to be an example to show the findings. The filename, account, and time stamp can be found by SQLite as Figure 1. The filename also can be found by FTK Imager as Figure 2.

DocumentView

id	Entry_id	title	owner	creationTime	lastModifiedTime
2	2	testwj1.jpg	wjl.test.one@gmail.com	1459102965828	1459102965828
3	3	testwd2.doc	wjl.test.one@gmail.com	1459102971495	1459102971495
4	4	testwm3.mp3	wjl.test.one@gmail.com	1459102982066	1459102982066
5	5	testwt4.txt	wjl.test.one@gmail.com	1459102987025	1459102987025
6	6	testwt4.txt	wjl.test.one@gmail.com	1459102995189	1459102995189
7	7	testwx5.xls	wjl.test.one@gmail.com	1459103003411	1459103003411
8	8	testwp6.pdf	wjl.test.one@gmail.com	1459103038913	1459103038913

Figure 1 The data remnants of GDA-Upload by SQLite

Figure 2 The data remnants of GDA-Uploadby FTK Imager

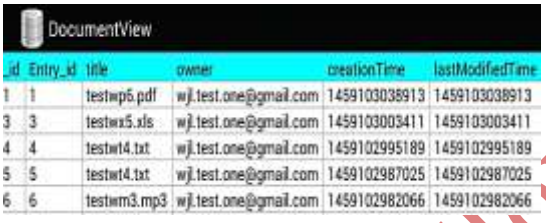
Table 2 The findings of Upload experiments

Remnants	GC-Upload	FF-Upload	GDA-Upload
Account	None	None	found
Password	None	None	None
WiFiaccout	None	None	None
WiFi password	None	None	None
Testfile	None	None	found
Contents	found	found	found

From these experiments, the test account,testfiles, contents of test file, and time stamp can be found by SQLite, and WinHex. The findings of remnant of GC-Upload and FF-Upload are less than GDA-Upload. The findings of experiments are shown as Table 2.

(3) Access

There are threeAccess experiments, such as GC-Access, FF-Access, and GDA-Access. We use different browsers or client software to log in Google Drive and only online open the test files which are uploaded previously. Then we log out and close the browsers or app. The keywords can be used to find data remnants. We only use GDA-Access to be an example to show the findings. The filename, account, and time stamp can be found by SQLite as Figure 3. The filename also can be found by FTK Imager.


DocumentView

_id	Entry_id	title	owner	creationTime	lastModifiedTime
1	1	testwp6.pdf	wjl.test.one@gmail.com	1459103038913	1459103038913
3	3	testwx5.xls	wjl.test.one@gmail.com	1459103003411	1459103003411
4	4	testwt4.txt	wjl.test.one@gmail.com	1459102995189	1459102995189
5	5	testwt4.txt	wjl.test.one@gmail.com	1459102987025	1459102987025
6	6	testwm3.mp3	wjl.test.one@gmail.com	1459102982066	1459102982066

Figure 3 The data remnants of GDA-Access by SQLite

From these experiments, the test account,testfiles, contents of test file, and time stamp can be found by SQLite, and WinHex. The remnants of GC-Access and FF-Access are less than GDA-Upload. The findings of experiments are the same as Table 2.

(4) Download

There are threeAccess experiments, such as GC-Download, FF-Download, and GDA-Download. We use different browsers or client software to log in Google Drive and download the test files which are uploaded previously. Then we log out and close the browsers or client software. The keywords can be used to find data remnants. We only use GDA-Download to be an example to show the findings. The filename, account, and time stamp can be found by SQLite. The filename also can be found by FTK Imager.

Table 3 The findings of Download experiments

Remnants	GC-Upload	FF-Upload	GDA-Upload
Account	None	None	found
Password	None	None	None
WiFiaccout	None	None	None
WiFi password	None	None	None
Testfile	found	found	found
Contents	found	found	found

From these experiments, the test account,testfiles, contents of test file, and time stamp can be found by SQLite, and WinHex. The findings of remnant of GC-Download and FF-Download are less than GDA-Download. The findings of experiments are shown in Table 3.

(5) CCleaner-VM

We do the same actions as Download scenarios. Then we uninstall browser or client softwareand runCCleaner to delete browser or client softwaredata remnants such as password, cookies, cache, history, etc. The keywords can be used to find data remnants. We only use GDA-CCleaner to be an example to show the findings. The file name,and time stamp can be found by SQLite as Figure 4. The filename also can be found by FTK Imager.

From these experiments, the testfiles, contents of test file, and time stamp can be found by SQLite, and WinHex. The findings of remnant of GC-CCleaner and FF-CCleaner are the same as GDA-CCleaner. The findings of experiments are shown in Table 4.


downloads

_id	hint	lastmod
41	file:///storage/sdcard0/Download/testwj1.jpg	1459105991628
44	file:///storage/sdcard0/Download/testwd2.doc	1459105992609
45	file:///storage/sdcard0/Download/testwm3.mp3	1459106000027
46	file:///storage/sdcard0/Download/testwt4.txt	1459106004429
47	file:///storage/sdcard0/Download/testwx5.xls	1459106009676
48	file:///storage/sdcard0/Download/testwp6.pdf	1459106019104

Figure 4 The data remnants of GDA-CCleaner by SQLit

Table 4 The findings of CCleaner experiments

Remnants	GC-Upload	FF-Upload	GDA-Upload
Account	None	None	None
Password	None	None	None
WiFiaccout	None	None	None
WiFi password	None	None	None
Testfile	found	found	found
Contents	found	found	found

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.

The remnants of cloud activity can be found on smart phone. It could be valuable for the forensic examiners. We found the remnants in these experiments. The username, the cache files, and log activity which helps in recovering the deleted files and data. We identify the account, file name, contents, and time stamp to determine user details and cloud storage information relating to use of Google Drive in our research.By determining the data remnants on client devices, we attempt to enhance the efficiency of the digital forensics and crime investigation

6. 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