Acquiring Cloud Storage Forensic Evidence though Android Smartphone

Aye Chan Ko, Wint Thida Zaw
University of Computer Studies, Mandalay
ayechanko.ucsm@gmail.com

Abstract

There is a growing shift towards the greater use of mobile devices which increasingly use cloud storage, as internal storage on each device is limited. Because of Cloud storage services are getting popular among individuals and organizations, it creates potentially conducive to security breaches and malicious activities. Therefore, challenges being raised to conduct a digital forensics investigation in cloud storage environment. Smartphone become a great provider of digital evidences in crimes.

In this paper, a proof of concept that smartphone device, which has accessed cloud storage service, can be used to present a partial view of the evidence contained in the cloud storage for cloud forensics investigation. This work conducts a preliminary investigation into the residual artifacts created on an Android device that has accessed cloud storage services. To evaluate the proposed proof of concept, series of analysis will be conducted with smartphone device, android operating system and cloud storage application.

Key words: Cloud Storage, Smart Phone, Mobile, Forensic Evidence

1. Introduction

With the trend, smart phones become a very popular and indispensable tool in daily life and work, because smart phone have a special feature, single-user feature. As popularity of the smart phones continues to grow, it changes the way of cyber crime. Due to its large storage, smart phones become a great provider of digital evidences in crimes. Smart phones provide users with the combined of several capabilities which will lead to the user information and be used as evidence in criminal cases. The availability of cloud storage has spread of cloud storage services.

Cloud storage services have been embraced by both individuals and organizations. This creates an environment that is potentially conducive to security breaches and malicious activities. The investigation of these cloud environments presents new challenges for the digital forensics community.

Cloud storage services such as Dropbox, Box and SugarSync have been embraced by both individuals and organizations. A press release from Dropbox reported that their customer base has surpassed 25 million users [2]. They also claim that over one billion files are saved every three days using its services [3].

2. Technical Background Information

In this Section some fundamental technical background information including cloud storage, Mobile forensics are discussed.

2.1 Cloud Storage

Cloud storage service is a business that maintains and manages its customers' data and makes that data accessible over a network, usually the Internet. Cloud storage can provide the benefits of greater accessibility and reliability; rapid deployment; strong protection for data backup, archival and disaster recovery purposes; and lower overall storage costs as a result of not having to purchase, manage and maintain expensive hardware.

There are four types of cloud storage: Personal, Public, Private and Hybrid cloud storage. Most popular cloud storage providers are Dropbox, Box, SugarSync, Go**o**gle Drive and Sky Drive.

Dropbox is a file hosting service that enables users to store and share files and folders. Dropbox allows users to create a special folder on each of their computers, which Dropbox then synchronizes so that it appears to be the same folder (with the same contents) regardless of which computer is used to view it. Files placed in this folder also are accessible through a website and mobile phone applications. The client software is available for Microsoft Windows operating system (OS), Apple Mac OSX, Linux, Apple iOS, Android, Blackberry and Windows Phone devices.

2.2. Mobile Forensics

Mobile phone forensics is the science of retrieving data from a mobile phone under forensically sound conditions. With the increased emphasis on social security issues, crime issue is considerable when it comes to the utilization of smart phone technologies, digital forensics provide the technical skills to collect evidences for the court to review and judge cases. Digital equipment has changed daily, people has pervasive use some common digital devices such as computers, Internet, mobile phones, digital cameras, hardware, storage devices, etc. Currently, digital forensics has widely used in the areas of network forensics, mobile forensics, computer forensics, and memory forensics, etc. According to NIST definition of mobile phone forensics process is collection, examination, analysis and reporting [9]. Mobile forensics processes are shown in Figure 1.

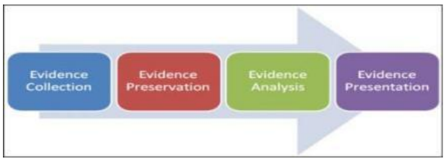


Figure 1. Mobile Forensics Processes

- **Collection:** This phase describe looking for possible evidence identified and collected.
- **Examination:** This phase examines eviden-ce acquire by using tools and preservation.
- **Analysis:** This phase extracts evidence that is significant to criminal investigation.
- **Reporting:** This phase is documenting the analyzing results and presenting the evidence.

2.3 Android

Android is a Linux-based operating system for mobile devices such as smartphones and tablet computers. It is developed by the Open Handset Alliance, led by Google, and other companies. Android™ delivers a complete set of software for mobile devices: an operating system, middleware and key mobile applications. Android is the world's most popular mobile platform. Android devices are made by various manufacturers, and its operating system and applications are developed by enthusiasts all over the World. The main characteristic of Android devices is its source code availability.

3. Conceptual Architecture

The proposed conceptual architecture of “Acquiring Cloud Storage Forensic Evidence though Android Smartphone” consists of four components: Cloud Storage, Mobile Clients, Investigator and Generating documents and evidence. The conceptual architecture is shown in Figure 2.

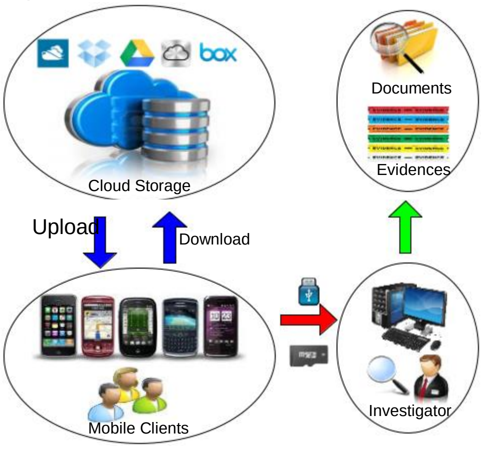


Figure 2. Conceptual Architecture

4. Experimental Design

We conduct the experiment based on the following stages.

- Installing Cloud Storage application on Smartphone
- Loading data set to cloud storage
- Connecting Cloud Storage and Smartphone
- Manipulating the files contained in Cloud Storage via Smartphone
- Performing recovery processes of Cloud Storage and Smartphone by using tools

4.1 Scope of the Experiment

This experiment was conducted by Global System of Mobile (GSM) and non GSM mobile devices were not considered. The cloud storage application selected for inclusion in this experiment. Rooted Android Smartphone device was used to conduct the experiment.

Android smartphone’s technical specification is shown in Table 1.

A pre-defined data set was created as shown in Table 2.

Table 1. Smartphone Device Feature

Mobile Device	Huawei G610-U100
Operating System	Android (Version 4.2.1)
Processor Speed	Quard Core 1.2 GHz
Internal Memory	4 GB
Networks	Wi-fi 802.11 b/g, GSM, WCDMA, GPS, Bluetooth

Table 2. Data Set

File name	Size (KB)	Manipulation
01.jpg	14	FV
02.jpg	10	FVD
03.mp4	21297	NP
04.mp4	22081	FV
05.pdf	14508	FOF
06.pdf	866	FV
07.mp3	5431	NP
08.mp3	4550	FVD
09.docx	913	FV
10.docx	17	FOF

FV= File viewed,
FOF= File viewed and saved for offline accessed,
NP=no manipulation,
FVD=file viewed and then deleted.

4.2 Detail Steps for Experiment

The following steps were undertaken to prepare device and to conduct the experiment.

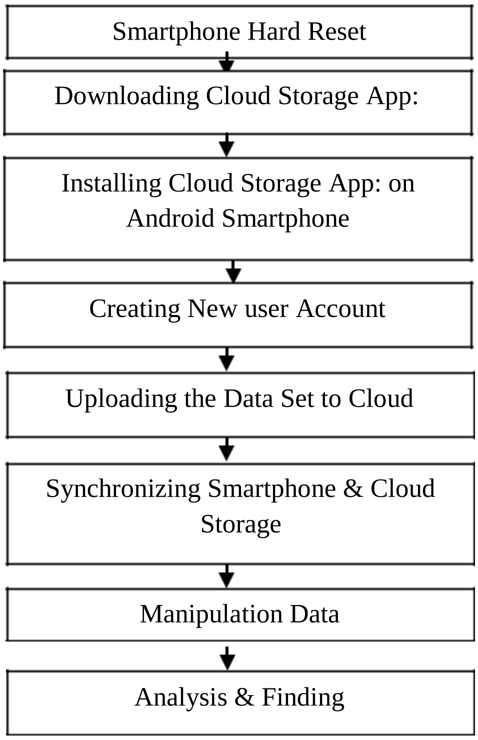

Smartphone Hard Reset
Downloading Cloud Storage App:
Installing Cloud Storage App: on Android Smartphone
Creating New user Account
Uploading the Data Set to Cloud
Synchronizing Smartphone & Cloud Storage
Manipulation Data
Analysis & Finding

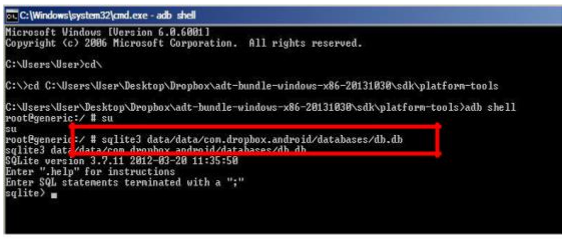
Figure 3. Detail Steps for Conducting Experiment

4.3 Analysis and Findings on and Smart-phone

An analysis of the Android memory dumps revealed that forensic artifacts can be recovered from both the smartphone itself and the SD memory card. Files and meta-data related to the applications stored in internal memory can be found in a subfolder under the location */data/data/*. The location of evidence on the SD card varies depending on the application being investigated. Application data stored in internal memory is generally saved in a subfolder under the location.

- JPEG image thumbnails: */android/data/com..android/cache/thumbs/*.
- Files saved for offline viewing and documents viewed and not deleted on the device: */Android/data/com..android/files/scratch*.

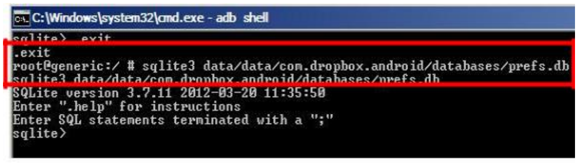
The majority of meta-data evidence can be found in two SQLite databases, ***db.db*** and ***prefs.db***. The meta-data related to the files currently stored in the service are contained in ***db.db.*** (Figure 4)



```
C:\Windows\system32\cmd.exe - adb  shell
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\User>cd\

C:\>cd C:\Users\User\Desktop\Dropbox\adt-bundle-windows-x86-20131030\sdk\platform-tools

C:\Users\User\Desktop\Dropbox\adt-bundle-windows-x86-20131030\sdk\platform-tools>adb shell
root@generic:/ # su
su
root@generic:/ # sqlite3 data/data/com.dropbox.android/databases/db.db
sqlite3 data/data/com.dropbox.android/databases/db.db
SQLite version 3.7.11 2012-03-20 11:35:50
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> _
```

Figure 4. Local Databases (db.db)

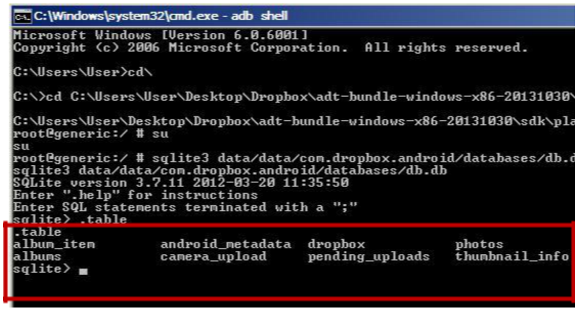
User-specific meta-data are contained in ***prefs.db***. **(Figure. 5)** This information is stored in a table called *AccountPrefs*. Clearing the cache of the application, removes the documents viewed and not deleted on the device which are stored in the *com..android/files/scratch* directory.



```
C:\Windows\system32\cmd.exe - adb  shell
sqlite> .exit
.exit
root@generic:/ # sqlite3 data/data/com.dropbox.android/databases/prefs.db
sqlite3 data/data/com.dropbox.android/databases/prefs.db
SQLite version 3.7.11 2012-03-20 11:35:50
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite>
```

Figure 5. Local Databases (***prefs.db***)

All the tables contained in ***db.db*** are listed as shown in Figure 6.

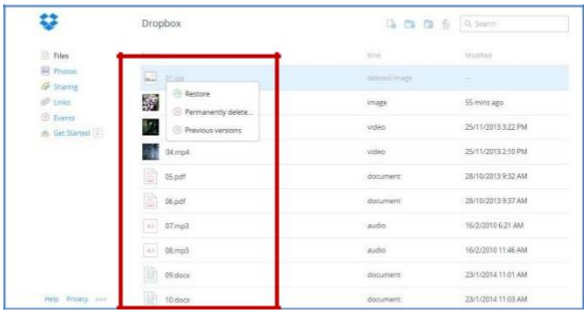


```
C:\Windows\system32\cmd.exe - adb  shell
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\User>cd\

C:\>cd C:\Users\User\Desktop\Dropbox\adt-bundle-windows-x86-20131030\

C:\Users\User\Desktop\Dropbox\adt-bundle-windows-x86-20131030\sdk\pla
root@generic:/ # su
su
root@generic:/ # sqlite3 data/data/com.dropbox.android/databases/db.d
sqlite3 data/data/com.dropbox.android/databases/db.db
SQLite version 3.7.11 2012-03-20 11:35:50
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .table
.table
album_item         android_metadata  dropbox            photos
albums             camera_upload     pending_uploads    thumbnail_info
sqlite> _
```

Figure 6. All Tables Contained in ***db.db***

In android side, we can check and investigate the files after synchronizing with the cloud with the smartphone. The files contained in the remain in the local database in app in android device. Even if smartphone is offline from the cloud, we can get all the files in the   by accessing local database. During synchronizing, all the   files contained in are stored in the local database.

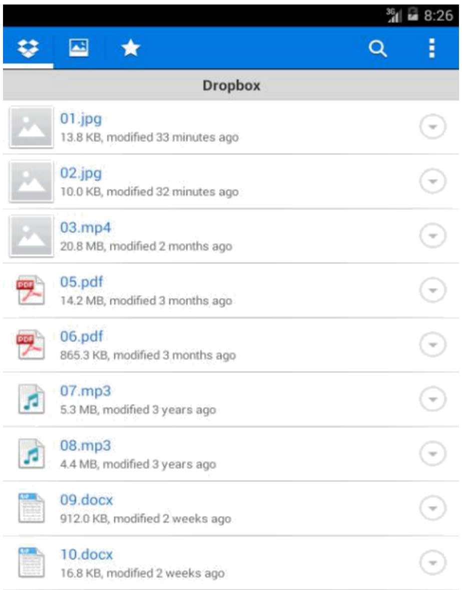
All the files uploaded in   cloud storage which are used for experiment can be seen in Figure 7.



	Kind	Modified
01.jpg	deleted image	--
	image	55 mins ago
	video	25/11/2013 3:22 PM
04.mp4	video	25/11/2013 2:10 PM
05.pdf	document	28/10/2013 9:32 AM
06.pdf	document	28/10/2013 9:37 AM
07.mp3	audio	16/2/2010 6:21 AM
08.mp3	audio	16/2/2010 11:46 AM
09.docx	document	23/1/2014 11:01 AM
10.docx	document	23/1/2014 11:03 AM

Figure 7. All Files Contained in Dropbox

Uploaded data used for experiment can be seen from Smartphone device is shown in Figure 8.



01.jpg
13.8 KB, modified 33 minutes ago

02.jpg
10.0 KB, modified 32 minutes ago

03.mp4
20.8 MB, modified 2 months ago

05.pdf
14.2 MB, modified 3 months ago

06.pdf
865.3 KB, modified 3 months ago

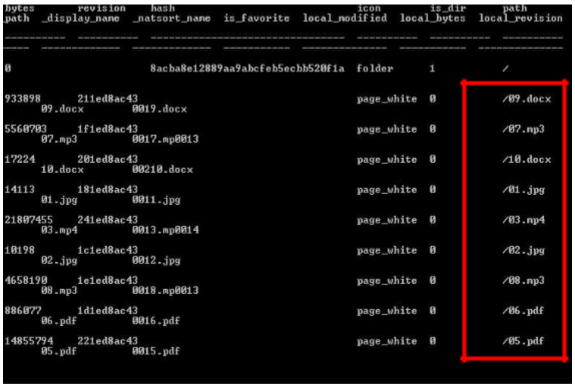
07.mp3
5.3 MB, modified 3 years ago

08.mp3
4.4 MB, modified 3 years ago

09.docx
912.0 KB, modified 2 weeks ago

10.docx
16.8 KB, modified 2 weeks ago

Figure 8: All the Files Contained in Dropbox are Displayed in Android Screen

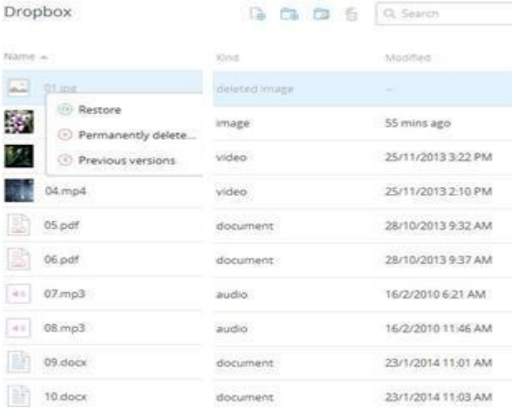


```
bytes       revision     hash                              icon        is_dir      path
path  _display_name  _natsort_name  is_favorite  local_modified  local_bytes  local_revision
---------- ---------- ------------------------------- ---------- ---------- ----------
----- ------------- ------------- ----------- -------------- ----------- --------------
0                        8acba8e12889aa9abcfeb5ecbb520f1a  folder      1           /

933898      211ed8ac43                                    page_white  0           /09.docx
      09.docx          0019.docx
5560703     1f1ed8ac43                                    page_white  0           /07.mp3
      07.mp3           0017.mp0013
17224       201ed8ac43                                    page_white  0           /10.docx
      10.docx          00210.docx
14113       181ed8ac43                                    page_white  0           /01.jpg
      01.jpg           0011.jpg
21807455    241ed8ac43                                    page_white  0           /03.mp4
      03.mp4           0013.mp0014
10198       1c1ed8ac43                                    page_white  0           /02.jpg
      02.jpg           0012.jpg
4658190     1e1ed8ac43                                    page_white  0           /08.mp3
      08.mp3           0018.mp0013
886077      1d1ed8ac43                                    page_white  0           /06.pdf
      06.pdf           0016.pdf
14855794    221ed8ac43                                    page_white  0           /05.pdf
      05.pdf           0015.pdf
```

Figure 9. All the File Name Stored in Smartphone

4.4 File Recovery

We conducted the experiment by deleting the file from Dropbox and Smartphone. In this experiment, we deleted a file (01.jpg) contained in the cloud and then restored the deleted file again. Restoring the file from Dropbox is shown in Figure 10.

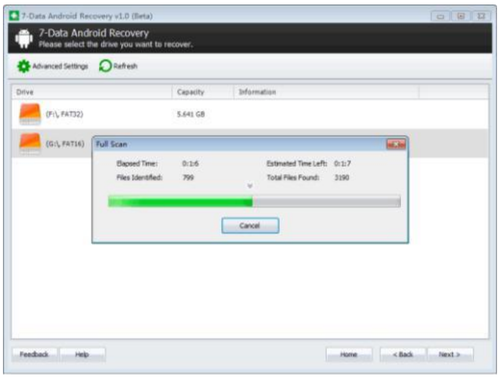


Name ▲	Kind	Modified
01.jpg	deleted image	--
	image	55 mins ago
	video	25/11/2013 3:22 PM
04.mp4	video	25/11/2013 2:10 PM
05.pdf	document	28/10/2013 9:32 AM
06.pdf	document	28/10/2013 9:37 AM
07.mp3	audio	16/2/2010 6:21 AM
08.mp3	audio	16/2/2010 11:46 AM
09.docx	document	23/1/2014 11:01 AM
10.docx	document	23/1/2014 11:03 AM

Figure 10.Recovering Deleted File from Dropbox

To recover the deleted file from android smartphone, 7-Data Android Recovery software [8] is installed on personal computer. 7-Data Android Recovery software is specially designed for Android system used by mobile phones and tablets/pads and SD card in Android devices. 7-Data Android Recovery effectively recovers photos, pictures, video, audio, documents, emails and other files from various Android devices on Windows PC. The following steps are performed for file recovery. The recovering deleted file from smartphone is shown in Figure 11.

- Step 1. Connect the Android device with a USB cable
- Step 2. Start scanning for recoverable files.
- Step 3. Preview recovered files.
- Step 4. Save recovered files.



Please select the drive you want to recover.

Drive	Capacity	Information
(F:\, FAT32)	5.641 GB	
(G:\, FAT16)		

Elapsed Time: 0:1:6
Files Identified: 799
Estimated Time Left: 0:1:7
Total Files Found: 3190

Figure 11. Recovering Deleted File from Smartphone

4.5 Analysis Summary

The Section summarizes the analysis of experiment.

(i) smartphone devices which access cloud storage service can potentially contain the data and can be used as cloud storage forensic evidence.

(ii) it is possible to recover files from the Dropbox.

(iii) Data can be recovered from a smartphone device which has accessed a cloud storage service.

5. Related Work

For acquiring evidence from a variety of cloud providers and services, researchers have proposed methods [1, 4]. The authors [1] proposed the idea of isolating a cloud instance for further investigation and several methods. None of these methods were empirically validated nor is it clear how a forensic image of the instance under investigation is obtained from the proposed techniques.

Grispos, et al., [5] described how digital forensic models and techniques used for investigating computer systems could prove ineffective in a cloud computing environment. Furthermore, they identified several challenges for forensic investigators including: creating adequate forensic images, the recovery of segregated evidence and large data storage management.

The authors [7] conducted digital forensic investigations in cloud computing environment. They provided an initial assessment on cloud storage data on client-side devices and they highlighted smartphones can be used as proxy for forensic evidence contained in cloud storage services.

6. Conclusion

The demand for cloud computing is increasing and conducting digital forensic investigations is challenging. Among cloud computing services, cloud storage services are popular because of various additional functions and mass storage. It is easy to access cloud storage services using smartphones. With increasing utilization, it is possible for malicious users to abuse cloud storage services. Therefore a study on a preliminary investigation into the residual artifacts created on an Android device that has accessed cloud storage service. Detail experiments are presented. According to the experiments we found that smartphone devices which access cloud storage service can potentially contain the data and can be used as cloud storage forensic evidence. As a future work, we will analyse the artifacts of all accessible divices such as Windows system, Mac system, iPhone, and Android smartphone.

References

[1] W. Delport, M.S. Olivier and M. Kohn, “Isolating a Cloud Instance for a Digital Forensic Investigation”, 2011 Information Security for South Africa, 2011

[2] Dropbox Raises $250 Million in Series B Funding, https://www.dropbox.com/news/20111018.

[3] Dropbox Reveals Tremendous Growth With Over 200 Million Files Saved Daily by More Than 25 Million People, https://www.dropbox.com/news/20110418

[4] J. Dykstra, and A. T. Sherman, “Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing”, Exploring and Evaluating Tools, Trust, and Techniques, Digital Forensic Research Workshop (DFRWS), 2012

[5] G. Grispos, T. Storer and W. B. Glisson, “Calm before the Storm: The Challenges of Cloud Computing in Digital Forensics”, International Journal of Digital Crime and Forensics, 4(2), 2012,pp. 28-48.

[6] S. George, H. S. Venter and F. Thomas,” Digital Forensic Framework for a cloud environment.”,IST-Africa 2012 Conference Proceedings, 2012

[7] G. Grispos, W.B. Glisson, and T. Storer, “Using Smartphones as a Proxy for Forensic Evidence contained in Cloud Storage Services*”,* Hawaii International Conference on System Sciences, pp. 1-10, 2013 46th Hawaii International Conference on System Sciences, 2013.

[8] http://7datarecovery.com/android-data-recovery/

[9] B. Martini and K-KR Choo. An Integrated Conceptual Digital Forensic Framework for Cloud Computing. Elsevier- Digital Investigation, volume XXX, pp. 1-10, 2012