Digital forensic investigation of Dropbox cloud storage service

Aye Chan Ko & Wint Thida Zaw
University of Computer Studies Mandalay, Myanmar
ayechankomm86@gmail.com

ABSTRACT: Nowadays, cloud storage services, a type of IaaS, are becoming a popular business paradigm for managing documents anytime and anywhere. It is possible for malicious users to abuse cloud storage services and the number of crime on them has increased rapidly. The investigation of these cloud storage services presents new challenges for the digital forensics community. Therefore procedures for forensic investigation of cloud storage services are necessary. This paper presents a process model for digital forensic investigation of cloud storage services and describes some important artifacts in PCs. Popular cloud storage service Dropbox is used as a case study; we document a series of digital forensic that they create experiments with the aim of providing forensic practitioners to undertake the cloud storage forensics.

Keywords: cloud storage, cyber crime, digital forensic investigation, Dropbox cloud storage service.

1 INTRODUCTION

In recent years, cloud computing has become popular as a cost-effective and efficient computing paradigm. Cloud storage is a popular option for users to store their data and be able to access it via a range of internet connected devices. Cloud storage services, a type of IaaS, provide users with storage space. There are a range of cloud storage hosting providers, and many offer free cloud storage services, such as Dropbox, Microsoft® SkyDrive®, and Google Drive. ICTs, such as personal computers, laptops, smartphones and tablets, are fundamental to modern society and open the door to increased productivity, faster communication capabilities, and immeasurable convenience.

However, it also changes the way criminals conduct their activities, and vulnerabilities in ICT infrastructure are fertile grounds for criminal exploitation. With the development of the cloud storage, the number of crime on them has increased rapidly [1, 2]. Therefore cloud storage has been identified as an emerging challenge to digital forensic researchers and practitioners. This paper will discuss the need for cloud storage forensics and presents the procedures for forensic investigation of cloud storage services. It will also attempt to discover what evidence can be gathered from Dropbox, including evidence that is located on the computer(s) with Dropbox installed on them as well as evidence that can be gathered from the web portal. Organization of the paper is as follows: Dropbox cloud storage and research questions for digital forensics are described in Section 2. Cloud Storage Forensics Framework is outlined in Section 3. Dropbox forensic investigation is discussed in Section 4. Section 5 draws conclusions from the work conducted.

2 DROPBOX CLOUD STORAGE FORENSIC AND RESEARCH QUESTIONS

2.1 *Dropbox cloud storage*

Dropbox [3] is the most frequently used and popular cloud storage service used by over 50 million people in the world that allows for users to backup files to the internet and to share them with other people. It has applications that run on Windows®, Mac, Linux, iPhone, Android and Blackberry. The Dropbox application creates artifacts on a system that may provide pertinent information. The Dropbox servers store many useful logs in regards to account history and a user's file history. Obtaining these artifacts and log files could provide an investigator with valuable evidence. Digital Forensics is a branch of forensic science that is used to encompassing the recovery and investigation of data in digital devices. Conventional digital forensic methods are insufficient for investigating cloud storage [4].

2.2 *Research questions for Dropbox Forensic*

- What artifacts are created during the Dropbox installation process?
- What artifacts are left behind after Dropbox is uninstalled?
- What artifacts are created in VM hard drives, database files and log files of Web Browsers during the accessing VMs?
- What artifacts are left behind in VM hard drives and Web Browsers after uploading and downloading files?
- What artifacts are left behind after Anti-Forensic software used?

3 FORENSIC FRAMEWORK

Our cloud storage forensic framework is based on the National Institute of Standards and Technology [5]. The framework is iterative, and a practitioner can start one or more iterative processes, while the overall investigation progresses. Our cloud storage forensic framework (Fig 1) comprises five phases; preparation, preservation, collection, examination and analysis, and documentation and presentation.

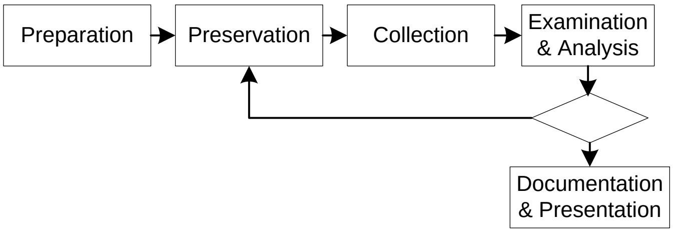


Figure 1. Cloud storage forensic framework

Preparation: This phase is concerned with preparation of tools, techniques, training, equipment acquisition, search warrants and monitoring authorisation and management support.

Preservation: This phase is concerned with isolation, securing and preserving the state of physical and digital evidence.

Collection: This phase is concerned with recording the physical scene and duplicating digital evidence using standardized and accepted procedures.

Examination and analysis: This phase is concerned with the examination and analysis of digital evidence. Examination is an in-depth systematic search of evidence relating to the suspected crime and focuses on identifying and locating potential evidence. Analysis determines importance and probative value to the case of the examined product.

Documentation and Presentation: This phase is concerned with completely and accurately reporting steps of findings and the results of the analysis of the digital evidence examination. Documentation is an ongoing process throughout the examination.

4 FORENSIC INVESTIGATION

4.1 *Preparation Phase*

To gather the artifacts in relation to the use of Dropbox created in Pcs, we created 18 VMs as shown in Fig 2. We examine and analyze a variety of circumstances of user accessing Dropbox by Windows client software and different Web browsers.

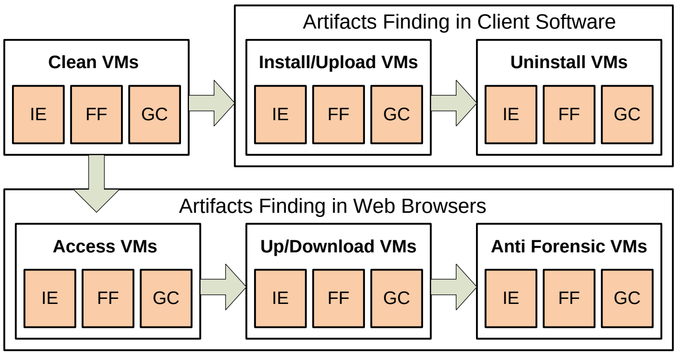


Figure 2. VMs creation for experiment

Testing environment and summary configurations of VMs are described in Table 1 and 2.

Table 1. Testing Environment

Environment	System Specification
Hosts	Intel® Core™ i7- 2600 CPU @ 3.40GHz, 4GB RAM, 1TB HD, 1Gigabit Ethernet
VMs	1024MB RAM, 50GB, HardDisk (SCSI)
Software	VMware®Workstation 9.0, Windows 7, CCleaner 4.19, Dropbox Client 2.10.30
Web Browsers	Internet Explorer 9, Mozilla FireFox 33.0, Google Chrome 38.0
EDRM File Format Dataset	consists of 381 files covering 200 file formats [6]. Key files: AFTER.doc, LEAR.pdf, piñata.png, Getting Started.pdf

Table 2. Summary Configuration of VMs

VMs	Software Components
3 Clean VMs	Win 8, Browsers (IE,FF,GC)
3 Install/Upload VMs	Win 8, Browsers(IE,FF,GC), Dataset, Dropbox client S/W
3 Uninstall VMs	
3 Access VMs	Win 8, Browsers (IE,FF,GC), Data Set
3 Up/Download VMs	
3 Anti-Forensic VMs	Win 8, Browsers (IE,FF,GC), Dataset, CClearner

4.2 *Preservation phase*

A digital forensic investigation is the ability to conduct analysis on a forensic copy, rather than interacting with or altering the original source. At the preservation stage, the physical items are examined and details documented, such as hard drive manufacturer, serial numbers, model numbers, and other information. Data is copied in a forensic manner, using write-protection and creating a bit-for-bit copy, verified with an MD5 and/or SHA hash algorithm.

4.3 *Collection phase*

Secure collection of evidence is important to guarantee the evidential integrity and security of information. In order to do analysis, we collect the digital evidence by using disk imaging tool. In this research, a forensic copy of virtual hard drive and each memory file are created by using AccessData FTK Imager [8]. MD5 hash value of each file is calculated and verified with each forensic copy.

4.4 *Examination and analysis phase*

In this phase, forensic copies of the VM hard drives, memory captures were examined and analyzed by using forensic tools [8]. Dropbox cloud storage is a Web-based service and Internet browsing history is important for forensics investigation. In this research, we examined and analyzed the artifacts of Windows client software and Web browsers stored in PCs. We installed the client dropbox software and Dataset used for testing on "Install/Upload VMs" then examined and analyzed. The artifacts found in that VMs are listed in Table 3.

Table 3. Important paths of Dropbox client software

Folder/File	Paths
Installe Folder	"%AppData%\Dropbox
Sync Folder	C:\Users\<username>\Dropbox
Default file	Getting Started.pdf .dropbox (DROPBOX File)

Link Files	C:\Users\<username>\Desktop\Dropbox.lnk
	C:\Users\<username>\Links\Dropbox.lnk

Executable & libraries	C:\Users\<username>\AppData\Roaming\Dropbox\bin
Prefetch Files	C:\Windows\Prefetch\DROPBOX N.N.NN.EXE-NNNNNNNN.pf C:\Windows\Prefetch\DROPBOX N.N.NN.EXE-NNNNNNNN.pf
Database Files	%AppData%\Dropbox\host.dbx, host.db, unlink.db %AppData%\Dropbox\instance1\aggregation.dbx, config.dbx, photo.dbx, unlink.db deleted.dbx, sigstore.dbx, filecache.dbx, notifications.dbx,

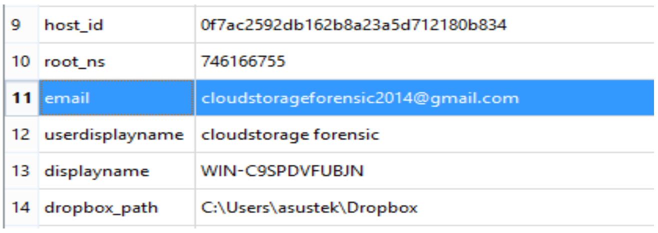
To examine the result of user uninstalling the client software, we created Uninstall VMs and did the experiment. We found that Dropbox sync folder and file contents remained on the hard drive and was not affected. Only host.dbx file remain in "%AppData%\Dropbox" and other files are removed. All database files are removed form "%AppData%\Dropbox\instance1\".

The majority of Dropbox's configuration and user info are stored in SQLite database files. Dropbox® Decryptor from Magnet Forensics Tools [9] and SQLite DB Browser [10] are used to decrypt the Dropbox encrypted SQLite databases and to view the contents of the DB file. The important artifacts of Dropbox databases are shown in Table 4.

Table 4. Important artifacts of Dropbox databases

config.dbx	
Host_id	Signature value of the Host's ID
Email	DropBox user's email
Displayname	PC Display Name
Userdiaplayname	Dropbox User's name
Dropbox_path	Location of Dropbox User folder
filecache.dbx (file_journal)	
id	File's ID assign by DropBox
Server_path	The path of the stored file
Local_filename	The name of the stored file
Local_size	The size of the stored file
Local_mtime	File modification time(UNIX Time)
Local_ctime	File creation time (UNIX Time)
User_id	Dropbox User ID
sigstore.dbx	
hash	The hash value of the stored file
size	The size of the stored file
deleted.dbx (File Table)	
cache_path	Path of cache file
origin_path	Path of deleted filename in sync folder
Date_added	Deleted date
Size	The size of the stored file
mtime	modification time

The information contain in config.dbx, filecache.dbx, sigstore.dbx and delete.dbx are shown in Fig 3, 4, 5 and 6.



9	host_id	0f7ac2592db162b8a23a5d712180b834
10	root_ns	746166755
11	email	cloudstorageforensic2014@gmail.com
12	userdisplayname	cloudstorage forensic
13	displayname	WIN-C9SPDVFUBJN
14	dropbox_path	C:\Users\asustek\Dropbox

Figure 3. config.dbx

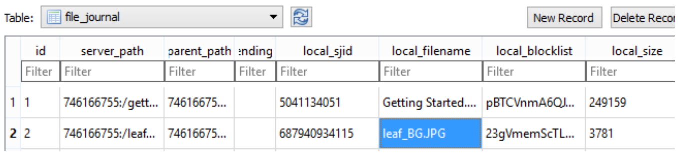


Table: file_journal

	id	server_path	parent_path	nding	local_sjid	local_filename	local_blocklist	local_size
1	1	746166755:/gett...	74616675...		5041134051	Getting Started....	pBTCVnmA6QJ...	249159
2	2	746166755:/leaf...	74616675...		687940934115	leaf_BG.JPG	23gVmemScTL...	3781

Figure 4. filecache.dbx

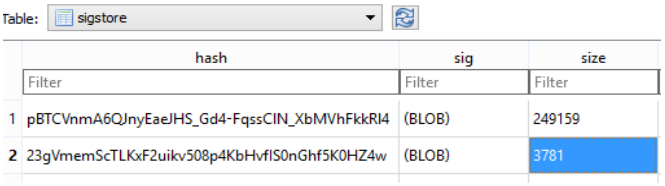
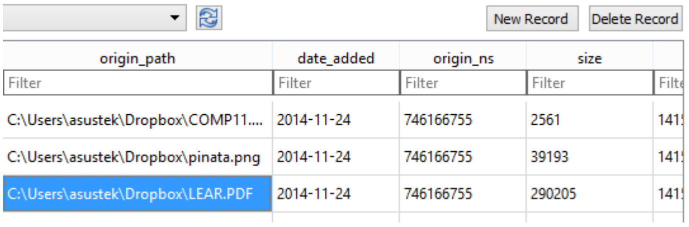


Table: sigstore

	hash	sig	size
1	pBTCVnmA6QJnyEaeJHS_Gd4-FqssCIN_XbMVhFkkRl4	(BLOB)	249159
2	23gVmemScTLKxF2uikv508p4KbHvflS0nGhf5K0HZ4w	(BLOB)	3781

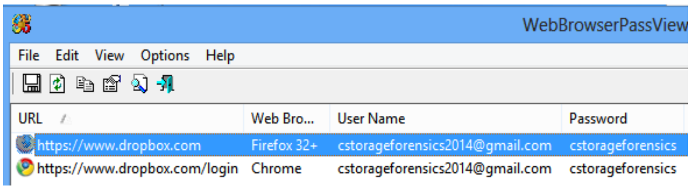
Figure 5. sigstore.dbx



origin_path	date_added	origin_ns	size	
C:\Users\asustek\Dropbox\COMP11....	2014-11-24	746166755	2561	141
C:\Users\asustek\Dropbox\pinata.png	2014-11-24	746166755	39193	141
C:\Users\asustek\Dropbox\LEAR.PDF	2014-11-24	746166755	290205	141

Figure 6. deleted.dbx

To view the user names and passwords stored by Web browsers (Fig. 7), we used PasswordFox, password recovery tool [11].



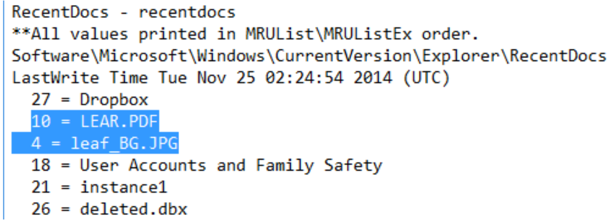
URL	Web Bro...	User Name	Password
https://www.dropbox.com	Firefox 32+	cstorageforensics2014@gmail.com	cstorageforensics
https://www.dropbox.com/login	Chrome	cstorageforensics2014@gmail.com	cstorageforensics

Figure 7. User name and password

Table 5. Important files and paths of Web Browsers

Mozilla Firefox 33.0.2	
Data	Path
Cache	%LocalAppData%\Mozilla\Firefox\profile\xxxxx.default\cache2\entries
History	%AppData%\Mozilla\Firefox\profile\ xxxxx.default\places.sqlite %AppData%\Mozilla\Firefox\profile\ xxxxx.default\formhistory.sqlite
Cookie	%AppData%\Mozilla\Firefox\profile\ xxxxx.default\cookies.sqlite %AppData%\Mozilla\Firefox\profile\ xxxxx.default\ permissions.sqlite
IE 9.10.9200.16384	
Cache	%LocalAppData%\Microsoft\Windows\ TemporaryInternet Files\Low
History	%LocalAppData%\Microsoft\ Internet Explorer
Cookie	%LocalAppData%\Microsoft\Windows\ cookies
Google Chrome 38.0.2125.111 m	
Cache	%LocalAppData%\Google\Chrome\ user data\default\cache
History	%LocalAppData%\Google\Chrome\ user data\default\history
Cookie	%LocalAppData%\Google\Chrome\ user data\default\cookie

We examined and analyzed the registry files of all VMS, created for doing experiment, using Windows Registry data extraction and correlation tool, RegRipper [12]. There were references to the Dropbox URL, Dropbox Software files and folders, Dropbox default files and EDRM File Format Dataset test files in Install/Upload VMs, Access VMs and Download VMs but not in Clean VMs. Dropbox username is not provided in registry file. NTUSER.dat file is a registry file which contains a unique documents folder, custom settings, desktop properties and browsing history. Sample RegRipper output is listed in Fig 8.



```
RecentDocs - recentdocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Tue Nov 25 02:24:54 2014 (UTC)
  27 = Dropbox
  10 = LEAR.PDF
   4 = leaf_BG.JPG
  18 = User Accounts and Family Safety
  21 = instance1
  26 = deleted.dbx
```

Figure 8. Sample RegRipper output of NTUSER.DAT

Analysis of the 3 anti-forensic VMs, we observed that the references to the file names were removed when all options were used for CCleaner [7].

4.5 *Documentation and presentation phase*

According to the experiment, we found that a variety of data remnants were located when user used Dropbox to access and store data. The important files, paths, artifacts of Dropbox cloud storage service are documented as shown in above tables. This information enables a practitioner to conduct forensic analysis and will assist to determine if Dropbox client software has been used.

5 CONCLUSION

Cloud storage services are becoming more prevalent, and not just for businesses – end- and home-users are taking advantage of opportunities to automate backups, make files available offline or from any computer, share files and photos, and so on. It is possible for malicious users to abuse cloud storage services and the number of crime on them has increased rapidly. In this paper, cloud storage forensic framework is presented and popular cloud storage service Dropbox is used as a case study. We conducted the experiment on Dropbox cloud storage and highlighted a lot of useful information that can be found by analyzing artifacts left by Cloud Storage clients. This methodology is helpful in the investigation of cloud storage services.

6 REFERENCES

[1] D. Quick, B. Martini and R. Choo, (2013), Cloud Storage Forensics, 1st Edition, ISBN: 9780124199705, Syngress

[2] H.Chung, J. Park, S. Lee, & C.Kang, (2012), Digital forensic investigation of cloud storage services. *Digital investigation*, *9*(2), 81-95.

[3] B. Martini and K-KR Choo, (2012), An integrated conceptual digital forensic framework for cloud computing. Elsevier- Digital Investigation, volume 9(2), pp. 71-80, 2012.

[4] Dropbox: www.dropbox.com

[5] K. Kent, S. Chevalier, T. Grance, & H. Dang, (2006), Guide to Integrating Forensic Techniques into Incident Response. SP800-86, Gaithersburg: U.S. Department of Commerce

[6] EDRM File Format Data Set: http://www.edrm.net/ resources/data-sets/edrm-file-format-data-set

[7] CCleaner:http://www.piriform.com/ccleaner

[8] FTKImager:http://accessdata.com/solutions/ digital-forensics/forensic-toolkit-ftk

[9] DropboxDecryptor:http://www.magnetforensics.com

[10] SQLiteDB Browser: http://sqlitebrowser.org

[11] Password Recovery: http://www.nirsoft.net

[12] RegRipper: http://regripper.wordpress.com

https://my.pcloud.com/#page=register&invite=xlyLZuuCxgy