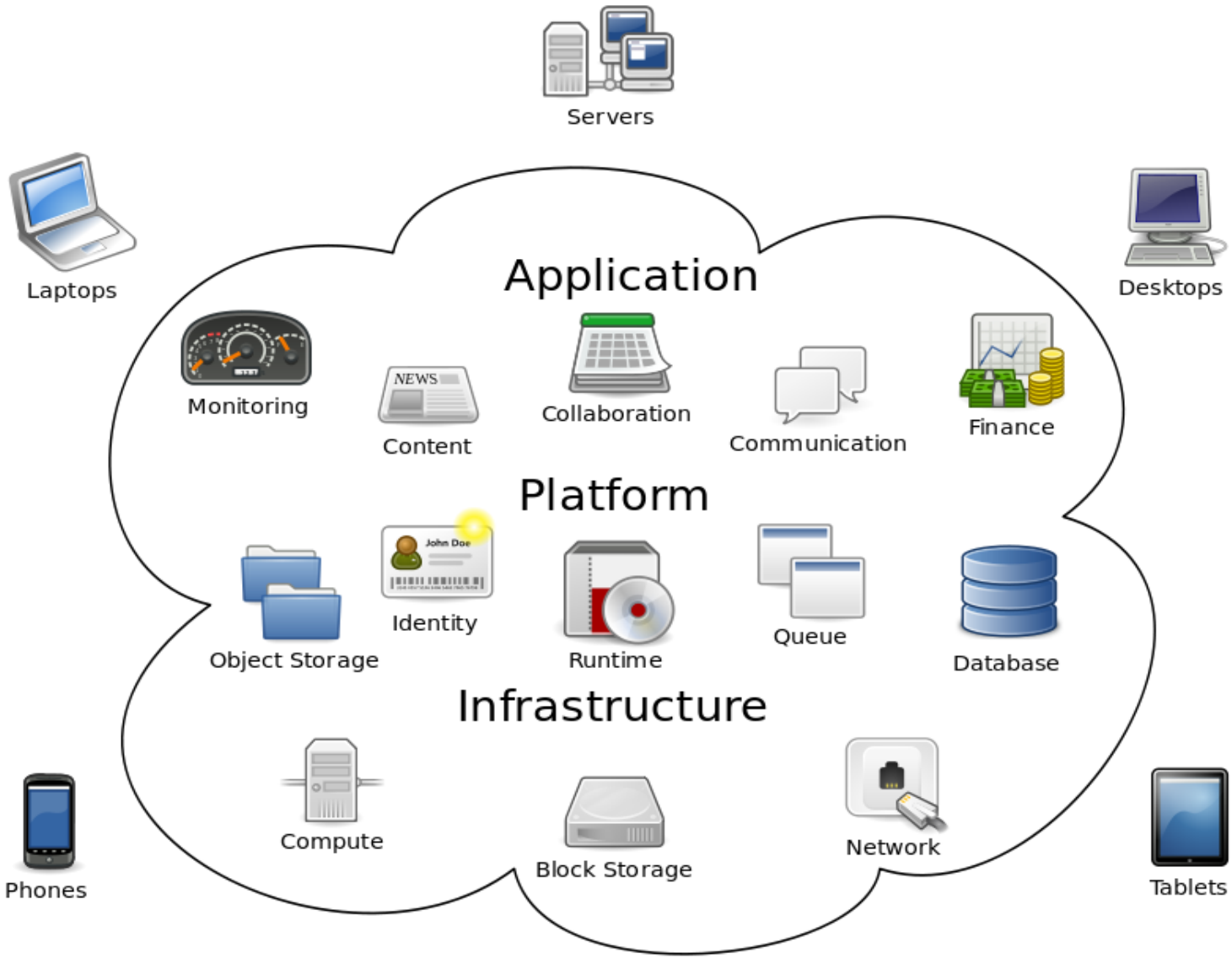
DIGITAL FORENSIC INVESTIGATION OF CLOUD STORAGE SERVICES

Hyunji Chung , Jungheum Park , Sangjin Lee , Cheulhoon Kang

Presented by: Abdiwahid Abubakar Ahmed, ID #201205820

OUTLINE

1. Introduction
2. Cloud storage services and digital forensics
3. Artifacts of cloud storage services (Windows and Mac)
4. Artifacts of cloud storage services (smartphones)
5. Case study of a cloud storage service
6. Discussion and conclusions



Cloud Computing

CLOUD COMPUTING:

- Computing resources delivered as a service over a network
- The name comes from the cloud-shaped

source: *http://en.wikipedia.org/wiki/Cloud_computing*

1. INTRODUCTION

- Cloud computing was expanded:
  - Development of an information technology infrastructure
  - Availability of free software
  - and advanced virtualization technology
- CC services divisions (in terms of resources provided):
  - SaaS (software as a service)
  - PaaS (platform as a service)
  - IaaS (infrastructure as a service).

SaaS (SOFTWARE as a SERVICE)

software delivery model in which software and associated data are centrally hosted on the cloud typically accessed via a web browser.

PaaS (PLATFORM as a SERVICE)

The provider provides the networks, servers, storage and as a service. The consumer creates the software, deployment and make configuration.

IaaS (INFRASTRUCTURE as a SERVICE)

- Providers offer computers and other resources on-demand.
- Users install operating-system images and their applications infrastructure, patch and maintain the OS and the softwares.

CLOUD STORAGE

- A type of IaaS, provide users with virtual space which allows users to store data such as documents, images, and music files.
- It also offers additional services such as editing, player, and email-sending capacity.
- Accessible from PC or a smartphone and this helped the expansion of cloud storage.

WHERE WE CAN FIND DF INFORMATION

- hosting companies keep confidentiality.
- We can analyze traces stored in user's device.
- conventional digital forensic methods are insufficient.
- We combine conventional computer forensics with mobile forensics to get useful information.

McClain, 2011

- Dropbox traces Windows
  - installation directory
  - registry changes on installation
  - network activity
  - database files
  - log files, and
  - uninstallation data
- Dropbox can be accessed via a smartphone

- what kind of data exists
- how they can be utilized to investigate
- did not explain specifically Dropbox traces in smartphones

HOW IS THIS PAPER ORGANIZED

- It looks traces left in local devices (PC and smartphones).
- All devices for a single user's cloud storage must be examined when conducting digital forensics
- It presents methods for collecting and analyzing evidence about a variety of the cloud storage services currently available.

HOW IS THIS PAPER ORGANIZED

- ***Section 2*** discusses methods for forensic investigation of cloud storage services, and important factors that should be considered in a forensic investigation.
- ***Section 3*** deals with the traces that are created with a Windows and Mac system.
- ***Section 4*** deals with the traces that are left when iOS and Android OS for smartphone are used

HOW IS THIS PAPER ORGANIZED

- ***Section 5*** presents a crime scenario involving a cloudstorage service and describes an investigation method.
- ***Section 6*** presents the conclusions

2. CLOUD STORAGE SERVICES AND DIGITAL FORENSICS

- Cloud storage services
  - A type of IaaS
  - Their use is increasing
  - can be accessed through a Web browser
  - Available in different platforms
  - The artifacts in PCs and smartphones differ due to different services

Services demonstrated in this paper: Amazon S3, Google Docs,Dropbox, and Evernote.

COMMON WAY TO USE		Type of service	Public services
PC (Windows, Mac)	Smartphone (iOS, android)	Data storage	Amazon S3, Dropbox, Sugarsync, and so on
Web browser or Client program	Application	Office suite + data storage	Google Docs, SkyDrive
		Note storage + data storage	Evernote, Awesome Note

2.1. PROCEDURE FOR DIGITAL INVESTIGATION OF CLOUD STORAGE SERVICES

The investigator collects and analyzes data from all devices that a user has used to access a cloud storage service. Such devices include PCs, smartphones, tablet PCs, and PDAs, but this paper covers only PCs and smartphones, which are the mostly widely used devices.

PROCEDURE FOR INVESTIGATION OF A CLOUD STORAGE SERVICE

Figure 1, page 3

2.2.IMPORTANT FACTORS IN AN INVESTIGATION

2.2.1. Log files of web browsers

- Internet Explorer and Firefox log files in profile directory.
  - Cache - images, icons, text, HTML, XML files, download URLs, download times, and data sizes
  - History - visited URLs, titles of Web pages, the times of visits, and the number of visits
  - Cookie - hosts, paths, cookie modification & expiration times, names, and values
  - and download - local paths of downloaded files, download URLs, file sizes, download times, and status

This paper focuses on log files of Internet Explorer and Firefox

2.2.2. ARTIFACTS OF CLIENT APPLICATIONS IN PC

- Left traces in the registry, and log files and database files.
- Logins status
- Used or denied services & synchronization

2.2.3. ARTIFACTS IN SMARTPHONES

Database files, XML files, and plist files.

2.2.4. Physical memory

Information about users (IDs and passwords)

Collecting physical memory is possible when doing live forensics. This is beyond the focus of this paper

3. ARTIFACTS OF CLOUD STORAGE SERVICES (WINDOWS AND MAC)

- 3.1. AMAZON S3
  - Amazon S3 is a Web-based cloud storage service and provides various APIs. Many cloud storage services are built using APIs.

3.1.1. WINDOWS [IE 8.0]

Appendix A. Artifacts of Cloud Storage Service (Windows).

Service	File system path		File name	Details
	XP	Vista/7		
Amazon S3	%UserProfile%\Application Data\Microsoft\Office\Recent	%UserProfile%\Roaming\Microsoft\Office\Recent	*File name* on s3 amazonaws.com.lnk	- MS Office Files that are downloaded and opened
	%UserProfile%\Local Settings\Temporary Internet Files\Content.IE5	%UserProfile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5	*Log file name*[n].txt	- API that user requests - Time at which user requests API - Name of bucket that accessed Windows system - User's canonical ID
Dropbox	%UserProfile%\Application Data\Dropbox	%UserProfile%\AppData\Roaming\Dropbox	config.db	- E-mail address for login - Files that has been accessed most recently (At most five)
			filecache.db	- Synced file name and path of cloud server - Creation Time - Modification Time
Evernote	%UserProfile%\Local Settings\ApplicationData\Evernote\Evernote\Databases	%UserProfile%\AppData\Local\Evernote\Evernote\Databases	userID.exb	- Location that user created note - Flag that represents deletion of note - Type of smartphone operating system - Creation Time - Modification Time - Information about attached file
			userID.exb.thumbnails	- Combination of PNG files that take a snapshot of note
	%UserProfile%\Local Settings\ApplicationData\Evernote\Evernote\Logs	%UserProfile%\AppData\Local\Evernote\Evernote\Logs	AppLog_Date.txt	- Authentication information - Account ID - History of user's behavior
			enclipper_Date.txt	- Time at which Evernote started

3.1.1. WINDOWS [IE 8.0]

- The first and second fields in this file are the user's canonical ID and bucket name
- The third field is the time at which the user performed the action.
- The seventh field describes the user's action.
- The eighth field is the name of the file on which the user acted.
- The last field is the HTTP user-agent value

[Canonical user ID] [Bucket Name] [06/Jan/2012:08:42:20 +0000] [10.186.158.41] [Canonical user ID] [F9ECC0485160EBC5]
[REST.DELETE.OBJECT] [File Name] ["DELETE /Bucket Name/File Name HTTP/1.1"] [204] [-] [-] [42277] [21] [-]["-"]"[S3Console/0.4]"

3.1.2. MAC [Firefox 9.0.1]

- Possibility of uploading, downloading files & logging
- General forensic tools are needed for investigation
- The artifacts of Amazon S3 are deleted when browser is closed. EnCase can be used to restore.

3.2. DROPBOX

- A frequently used cloud storage service.
- Allows sync and the user can access their storage using Windows, Mac, iPhones, and Android

Dropbox

3.2.1. WINDOWS

Appendix A. Artifacts of Cloud Storage Service (Windows).

Service	File system path		File name	Details
	XP	Vista/7		
Amazon S3	%UserProfile% \Application Data \Microsoft\Office\Recent	%UserProfile% \Roaming\Microsoft \Office\Recent	*File name* on s3 amazonaws.com.lnk	- MS Office Files that are downloaded and opened
	%UserProfile% \Local Settings \Temporary Internet Files\Content.IE5	%UserProfile%\AppData \Local\Microsoft\Windows \Temporary Internet Files \Content.IE5	*Log file name*[n].txt	- API that user requests - Time at which user requests API - Name of bucket that accessed Windows system - User's canonical ID
Dropbox	%UserProfile% \Application Data \Dropbox	%UserProfile%\AppData \Roaming\Dropbox	config.db	- E-mail address for login - Files that has been accessed most recently (At most five)
			filecache.db	- Synced file name and path of cloud server - Creation Time - Modification Time
Evernote	%UserProfile% \Local Settings \ApplicationData \Evernote\Evernote \Databases	%UserProfile%\AppData \Local\Evernote \Evernote\Databases	userID.exb	- Location that user created note - Flag that represents deletion of note - Type of smartphone operating system - Creation Time - Modification Time - Information about attached file
			userID.exb.thumbnails	- Combination of PNG files that take a snapshot of note
	%UserProfile% \Local Settings \ApplicationData \Evernote\Evernote\Logs	%UserProfile%\AppData \Local\Evernote \Evernote\Logs	AppLog_Date.txt	- Authentication information - Account ID - History of user's behavior
			enclipper_Date.txt	- Time at which Evernote started

Table 6
config.db.

Key	Value
dropbox_path	%UserProfile%\AppData\Roaming\Dropbox
email	foryou7187@yahoo.co.kr
recently_changed3	(lp1 (V41248546:/**paper101.doc** 100 tp2 a(V41248546:/**Digital Forensic of Cloud.pdf** Ntp3 a(V41248546:/**Lecture1.pdf** Ntp4 a(V41248546:/**Hello.ppt** Ntp5 a(V41248546:/**snort.pdf** Ntp6 a.

The investigator can find the suspect's dropbox_path by copying config.db to that PC, and then places config.db in the same path as the suspect's dropbox_path.

Table 7
filecache.db.

Server_path	Local_filename	Local_mtime	Local_ctime
37288970:/Hello	Hello	1307405626	1302685077

3.3. EVERNOTE

Evernote allows a user to store an idea anywhere and anytime. Evernote synchronizes notes every time they are saved. Accessible through Windows, Mac, iPhones, and Android smartphones.

EVERNOTE®

3.3.1. WINDOWS

Title	**Date_created**	Date_updated	is_deleted	Source	Latitude	**Longitude**
Evernote test	733700.33961805 6	733700.34945601 9	1	Mobile.android	37.321429	-122.015791

Table 8 [userID].exb.

3.2.1. WINDOWS

Appendix A. Artifacts of Cloud Storage Service (Windows).

Service	File system path		File name	Details
	XP	Vista/7		
Amazon S3	%UserProfile% \Application Data \Microsoft\Office\Recent	%UserProfile% \Roaming\Microsoft \Office\Recent	*File name* on s3 amazonaws.com.lnk	- MS Office Files that are downloaded and opened
	%UserProfile% \Local Settings \Temporary Internet Files\Content.IE5	%UserProfile%\AppData \Local\Microsoft\Windows \Temporary Internet Files \Content.IE5	*Log file name*[n].txt	- API that user requests - Time at which user requests API - Name of bucket that accessed Windows system - User's canonical ID
Dropbox	%UserProfile% \Application Data \Dropbox	%UserProfile%\AppData \Roaming\Dropbox	config.db	- E-mail address for login - Files that has been accessed most recently (At most five)
			filecache.db	- Synced file name and path of cloud server - Creation Time - Modification Time
Evernote	%UserProfile% \Local Settings \ApplicationData \Evernote\Evernote \Databases	%UserProfile%\AppData \Local\Evernote \Evernote\Databases	userID.exb	- Location that user created note - Flag that represents deletion of note - Type of smartphone operating system - Creation Time - Modification Time - Information about attached file
			userID.exb.thumbnails	- Combination of PNG files that take a snapshot of note
	%UserProfile% \Local Settings \ApplicationData \Evernote\Evernote\Logs	%UserProfile%\AppData \Local\Evernote \Evernote\Logs	AppLog_Date.txt	- Authentication information - Account ID - History of user's behavior
			enclipper_Date.txt	- Time at which Evernote started

```
45 4E 54 30 D9 00 00 00 40 00 00 00 16 74 14 06   ENTOÙ...@....t..
6D CE 04 00 01 00 00 00 89 50 4E 47 0D 0A 1A 0A   mÎ......‰PNG....
                        ......                          ...
22 43 00 00 01 00 00 00 89 50 4E 47 0D 0A 1A 0A   "C......‰PNG....
00 00 00 0D 49 48 44 52 00 00 03 20 00 00 02 2A   ....IHDR... ...*
                        ......                          ...
```

Fig. 3. [*userID*].exb.thumbnails.

The file [userID].exb.thumbnails is a combination of PNG files that take a snapshot of the note at every synchronization.

```
Log opened on 2011/06/01 10:24:21 (UTC+9:00)

10:24:21 [4900] Client info: Evernote Windows/131509; Windows/6.1.7601 Service Pack 1;
10:24:21 [4900] * link: "C: \Users \dodochung \AppData \Roaming \Microsoft \Windows \SendTo \Evernote.lnk"
10:24:53 [3036] 0% Authenticating user "hjhjhjhj"
10:24:55 [3036] 0% Session terminated abnormally, elapsed time: 2s
10:24:57 [3036] 0% Authenticating user "dodochung"
10:25:02 [4900] Opened database: C:\Users\dodochung\AppData\Local\Evernote\Evernote\Databases\dodochung.exb (1.6MB Fixed)
10:27:01 [5764] AutoUpdate: selected update with revision 144118
```

Fig. 4. AppLog_[*Date*].txt.

- AppLog_[Date].txt is created once a day when Evernote starts.
- Inside it is the authentication information, the account ID, and start and end time.
- enclipper_[Date].txt is created once a day, like AppLog_[Date].txt. It includes application start time.

3.3.2. MAC

Important four files in Appendix B are Evernote.sql, fullscreenThumbnail.png, thumbnail.png, and Evernote.log.

Appendix B. Artifacts of Cloud Storage Service (Mac).

Service	File system path	File name	Details
Dropbox	/Users/[user name]/.dropbox	config.db	- E-mail address for login - Files that has been accessed most recently (At most five)
		filecache.db	- Synced file name and path of cloud server - Creation Time - Modification Time
Evernote	/Users/[user name]/Library/Application Support/Evernote/data	Evernote.sql	- Location that user created note - Flag that represents deletion of note - Type of smartphone operating system - Creation Time - Modification Time - Information about attached file
	/Users/[user name]/Library/Application Support /Evernote/data/Contents	fullscreenThumbnail.png	- Full screenshot of note
	/Users/[user name]/Library /Application Support/Evernote/logs	thumbnail.png	- Snapshot of content in note
		Evernote.log	- Authentication information - Account ID - History of user's behavior
Google Docs	/Users/[user name]/Library/Caches /Firefox/Profiles/[random 8 digits].default /Cache	PNG file	- Each page of uploaded file (ppt, pptx, pdf) in image
	/Users/[user name]/Library/Caches /Firefox/Profiles/[random 8 digits].default /Cache	HTML file	- Part of contents of ppt, pptx when editing it

3.4. GOOGLE DOCS

Web-based service that offers flexibility to be productive from one's desk, on the road, at home and on a mobile phone.

Originaly classified as a SaaS

Recently begun to support mobile access by iPhone and Android.

3.4.1. Windows

Table 9
Artifacts of Internet Explorer on Windows.

Behavior	Type of document	Artifacts
Accessing Google Docs	–	docs_google_com[n].htm
Browsing created document	Document	edit[n].htm
	Presentation	
	Spreadsheet	ccc[n].htm
Browsing uploaded document	PDF	viewer[n].htm
		viewer[n].txt
	PDF, ppt	viewer[n].png
Editing document	Document	edit[n].htm
	ppt	
	txt	
	Spreadsheet	ccc[n].htm

4. Artifacts of cloud storage services (smartphones)

4.1.1. Amazon S3

Appendix C. Artifacts of Cloud Storage Service (iOS).

Service	File full path	File type	Details
Amazon S3	Library/Preferences/com.moninnovations.iAwsManager.plist	plist	- User's name - User's access Key ID - User's secret access Key
	Document/iAwsManager/iAwsManager.3.0.db	SQLite	- Path, eTag, name and size of downloaded file - Name of bucket that accessed iPhone - Time at which file was downloaded
Dropbox	Library/Preferences/com.getdropbox.Dropbox.plist	plist	- E-mail address for login - The first login time
	Documents/Dropbox.sqlite	SQLite	- Time at which user browsed folder or file - Name and path of file that user browsed
	Documents/Uploads.sqlite		- Time at which file was uploaded - Name and path of uploaded file
Evernote	Documents/www.evernote.com/User/applog.txt	Text	- Beginning and end of service access - Beginning and end of synchronization time - connection status (Wi-Fi, 3G)
	Library/Preferences/com.evernote.iPhone.Evernote.plist	plist	- ccount ID
	Documents/www.evernote.com/User/Evernote2.sqlite	SQLite	- Time at which user created and modified note - Location that user created note - Flag that represents deletion of note

(*continued on next page*)

(*continued*)

Service	File full path	File type	Details
			- Type of smartphone operating system - Information about attached file - Title and contents of note
	Documents/www.evernote.com/User/Evernote2.sqlite.md	XML	- The latest synchronization time
Google Docs	Library/Preferences/com.jade.iGoogDocs.plist	plist	- Value for auto login that can be true or false - User's Google Docs ID - User's Google Docs Password (when auto login is true)
	Documents/[Title of Document].txt	html	- Contents of created text file

5. CASE STUDY OF A CLOUD STORAGE SERVICE

5.1. Case overview

- In 2011, documents containing designs for a new product had been leaked to a competitor. The file name is “A_design.pdf”.
- prime suspect was a Mr. K, credential files manager.
- After checking data logs there were no trace remained
- Mr. K PC and Android became target devices.
- The PC and smartphone were seized for forensic examination. PC was Windows 7 and the mobile was Android.

5.2. Objective

- judge whether or not Mr. K had leaked a secret file by investigating his PC and smartphone.

5.3. Method

- The investigation started with Mr. K's PC. The leaked file was not detected.
- issued a search and seizure warrant.
- The investigator realized that the suspect used Dropbox
- The suspect found

5.4. RESULTS

- Confidential file using Dropbox. Further examining the prime suspect’s PC and smartphone together, more precise investigation was possible.

6. DISCUSSION AND CONCLUSIONS

- The availability of cloud storage has spread of cloud storage services.
- possible for malicious users to abuse cloud storage services
- Until now, artifact examination can be done only in PCs.
- This method fails to provide information not available in the PC.
- This paper has proposed a process model

6. DISCUSSION AND CONCLUSIONS

- For forensic investigation of cloud storage services
- It described some important elements of an investigation.
- It also described a previously unknown method for forensic analysis of cloud storage services.
- This methodology is helpful in the investigation of cloud storage services.

THANK YOU

Q & A