Forensics Analysis from Cloud Storage Client Application on Proprietary Operating System

Amirullah Amirullah
Universitas Islam Indonesia
Jl. Kaliurang KM 14,5
Yogyakarta, 55584

Imam Riadi
Universitas Ahmad Dahlan
Jl. Prof. Dr. Soepomo,
Yogyakarta, 55164

Ahmad Luthfi
Universitas Islam Indonesia
Jl. Kaliurang KM 14,5
Yogyakarta, 55584

ABSTRACT
Increased use of cloud storage services have become a necessity alternative that complements the main storage media in everyday activities because it offers ease of doing automatic backups, sharing files and photos and so forth on a variety of computing devices and smartphones. It is very possible loopholes for criminals to store illegal files or matters relating to such activities. There are various types of cloud services with each type having a different potential use in criminal activities. One area of difficulty is the identification and acquisition of potential data when different services can be exploited by criminals. Because geographically cloud servers scattered in various regions. This causes difficulties for digital forensic investigators will add time and expense, to contact all potential service providers to determine whether the data stored in the server cloud services. This paper presented at a target on the client side user application to help find the data renmant on the use of cloud storage applications of various service provider on the proprietary operating system focuses on the Windows 10 platform. Results from this research include a variety of state after the install, deleted and uninstall web browser and memory, in order to find digital evidence. Based on the test results the success index average was 82.63% and the remaining can not be analyzed, the results depend on various state, procedures and tools that are used, the research can be carried out smoothly.

General Terms
Digital investigation, Cloud storage, Application Forensics.

Keywords
Cloud, Storage, Forensics, Operating System, Windows 10.

1. INTRODUCTION
Fifth Annual Report of the Cisco ® Global Cloud Index (2014-2019), which was released October 28, 2015 forecasts that global cloud traffic will more than quadruple by the end of 2019, from 2.1 to 8.6 zettabytes (ZB), outpacing the growth of total global data center traffic, which is forecast to triple during the same time frame (from 3.4 to 10.4 ZB). Several factors are driving cloud traffic's accelerating growth and the transition to cloud services, including the personal cloud demands of an increasing number of mobile devices; the rapid growth in popularity of public cloud services for business, and the increased degree of virtualization in private clouds which is increasing the density of those workloads. The growth of machine-to-machine (M2M) connections also has the potential to drive more cloud traffic in the future [1].

Cisco GCI (Global Cloud Index) estimates that in 2019, more than half or 55 percent (2 billion) of the population of Internet consumers will use personal cloud storage, up from 42 percent (1.1 billion users) by 2014. as shown in the Fig 1.

Fig 1: Expansion Cloud Storage Consumer

Cisco GCI forecasts that global consumer cloud storage traffic will grow from 14 EB annually in 2014 to 39 EB by 2019 at a Compound Annual Grade Rate (CAGR) of 23 percent (Fig. 2). This growth translates to per-user traffic of 1.6 Gigabytes (GB) per month by 2019, compared to 992 MB per month in 2014 [2].

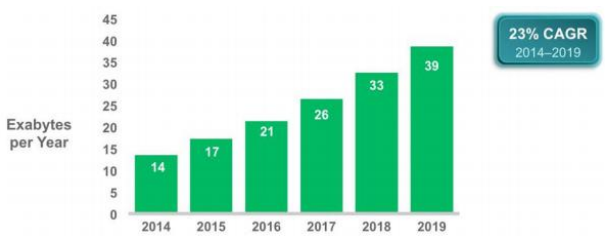

Fig 2: Consumer Cloud Storage Traffic

There are two things associated with cloud storage account. The first is related to the use of a web browser and the second is through a client application installed by the user's device. This research will conduct an analysis of several client applications and develop how to get the data. Previous research analysis applications on onedrive, google drive, and dropbox on windows 7 [3][4][5] and in Windows 8 [6][7], the research will be shown some of the client application that runs on Windows 10. to add differences and develop a different sample, the selected application is different from previous research. Then choose 3 cloud storage applications that Dropbox, Copy, and CloudMe. Specification of the three shown in Table 1 .

Tab1e 1. Comparation DropBox, Copy and CloudMe

Specifications			
Version	2.5.35	1.44	1.9.1
Operating Systems	WindowMacLinux	WindowMacLinux	WindowMacLinux
Storage	1 TB	250 GB	100 GB
Monthly Price	$9.99	$4.99	$9
Upload (Backup) Speed	Max (7.6 Mbps)	7.8 Mbps	1.8 Mbps
Download (Restore) Speed	Max (30 Mbps)	27 Mbps	74.7 Mbps
Features			
Automatic Backup	yes	yes	yes
Backup Any Folder	no	yes	yes
Backup to Local Drive	no	no	no
Free Trial	yes	yes	yes
Free Online Storage	2 GB	15 GB	3 GB
File Versioning	yes	yes	no
Keep Deleted Files	30 Days	30 Days	60 Days
Bandwidth Controls	yes	yes	yes
Public File Sharing	yes	yes	yes
NAS Backup	no	no	yes
Security			
Encrypted Storage	yes	yes	no
Encrypted Transfer	yes	yes	yes
Personal Encryption	no	no	no
Support			
Phone Support	yes	no	no
Email Support	yes	yes	yes
24/7 Support	no	no	no
Live Chat	no	no	no

Previously study about the features and security in the CloudMe, and Dropbox on research [8], examined the security mechanisms of cloud storage services identified four typical features of cloud storage services, the copy, backup, synchronization and file sharing feature. Examined [9] various cloud storage vendors provides data storage, space availability, scaling, sharing, secure transmission between. cloud storage medium. In the above table is a comparison of specifications, features, security and support [10], major difference with the other in file versioning, keep deleted files, and encrypted storage. it is to understand the depth of the object of study that will be discussed, and this is part of the preparation phase.

2. RELATED WORK

Reese [11]describes the process using a snapshot using Boot EBS volume within Amazon's cloud services where there is the ability to snapshot a system, however, this does not apply to service Cloud storage as this process is beyond the control of the user. Iswardani. A, [12] examined log for denial of service attack in cloud. Clark, [13] examined the image Exif metadata remnants on Microsoft SkyDrive, Windows Azure, and Flickr, with a focus on information in the picture to be openly shared, found that personal information is available in a lot of pictures along with the public, which could be relevant in investigations, such as global positioning information. D. Quick, B. Martini, and K.-K. R. Choo [3] Examining the various circumstances that included a variety of methods to store, upload, and access data in the cloud. Potential sources of information are identified including the client log file software, prefetch files, link files, network traffic and memory capture, On Dropbox, Microsoft SkyDrive and Google Drive on Windows 7 and Apple iPhone 3G. AK McCurdy, Researching monitoring system that can be deployed and used by system administrators to detect the use Dropbox on the network, and broswer At the Dropbox application and OS Windows XP. [14]. S. Mehreen and B. Aslam [6] Examine artifacts dropbox on Windows 8, using digital forensic methodology.M. Epiphany [4] examined the artifacts Cloud Cloud storage on Dropbox, SkyDrive, Google Drive, iCloud operating system Windows 7. Chung [15] developed a procedure for the investigation of devices such as PCs and smartphones on Amazon S3, Dropbox, Google Docs and Evernote on Windows 7. Malik [7] Windows 8.1 researching digital artifacts in ownCloud, Copy, and Dropbox.

3. METHODOLOGY

The methodology used is the digital forensics methodology, namely preparation, preservation, analysis and reporting. The analysis method to find out all the problems and needs required to undertake to do the research thesis titled cloud storage application forensic methods to be used to look for problems, responding to the problems encountered and the testing stage as well as all the necessities such as needs analysis software and analysis of hardware requirements. Additionally two methods to answer research questions first used, among others: Methods Dynamic on Storage used for processes that occur during the installation and uninstall, activity of hard disks by using the tools Diskpulse, Regshot, Procces Monitor, and Procces Explorer, thus easily find artifacts location of the file or directory and characteristics or behavior of the application client Cloud Storage and Static methods used in the analysis of web browser and client database applications by conducting inspections analysis directly on the database files using sqlite browser, log viewer, do recovey deleted files can thus find artifacts related to client Cloud Storage. Coverage area of research is shown in Fig 3 below.

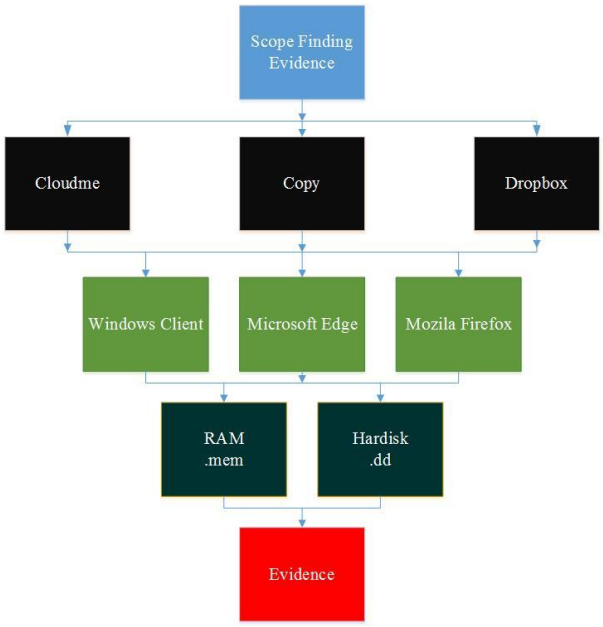

Fig 3: Block diagram of Research

In the picture above is a diagram of the research consists of three objects research is CloudMe, Copy, and Dropbox third Cloud Storage is accessed through the Windows client, Microsoft Edge, and Mozilla Firefox then performed phase of preservation to obtain an image of the hard disk and RAM then taken to the next process for phase of analysis.

4. TOOLS AND SETUP

Software is the object of the research are shown in Table 2 below [16][17][18]. This is research limitation, any prior

version of software may have difference outcomes, and subsequent changes to software my result in difference findings.

Table 2. Software Test

Software	Version
Windows OS	10 Pro
Microsoft Edge	20.10240.16384.0
Mozila Firefox	41.0.2
Dropbox Client	3.10.7
Copy Client	3.2.01.0481
CloudMe Client	1.9.1

The sample scenario deleted files uploaded and shown in Table 3.

Table 3. Sample File

File Name	File Size (Bytes)	Deleted
1.jpg	879394	1MF
2.jpg	845941	2MF
3.mp4	39624188	3MF
4.jpg	595284	1ME
5.jpg	707105	2ME
6.xlsx	118272	3ME
7.docx	491330	1CP
8.mp3	5411654	2CM
9.xlx	198144	3DB
10.pdf	8124477	-
11.jpg	48852	-

Notes:
1*=Copy 2*=CloudMe 3*=Drobpox *MF=Mozila Firefox *ME=Microsoft Edge *CM=Client CloudMe *CP=Client Copy *DB=Client Dropbox

There are eleven uploaded file on each server cloud, then given the elimination of the different circumstances in each file in a web browser and client-side applications, it's aiming to distinguish whether the synchronization process is going well. Also to simplify the process of finding evidence of the result of the elimination of those files.

5. RESULT

5.1 Web Browser Analysis

5.1.1 Mozilla Firefox

Web browser analysis is a process Analysis of the use of a web browser then that becomes the source of the evidence can be found in several databases. Mozilla Firefox can be found on a file folder \img_cloudtest1.dd\Users\cloudtest2015\AppData\Roaming\ Mozilla\Firefox\Profiles\p662qtt.default.

In Table 4 is shown the names of the database on Mozilla Firefox and its Description.

Table 4. File database Mozilla Firefox

Name Database	Description
content-prefs.sqlite	Individual settings for pages.
cookies.sqlite	Cookies
formhistory.sqlite	Saved form data
healthreport.sqlite	For all bugs involving collection, submission, analysis and user-facing features (about:healthreport) as part of the Firefox Health Report product
permissions.sqlite	Permission database for cookies, pop-up blocking, image loading and add-ons installation.
places.sqlite	Bookmarks, browsing and download history

Browser use Mozilla Firefox on cookiess.sqlite database stores information such as the base domain visited cloudme.com, copy.com and dropbox.com, saving time start of a connection, hostname, time expired, the time and the time the connection is terminated. Formhistory database stores information form field such as access login password, name, address and others. Places.sqlite database stores information about bookmarks, history of visits, information download the file name, storage location, connection time, hostname and favicons. File key3.db store information related to the encryption password database to decrypt the password can use firepasswordviewer from securityexploded.com.

5.1.2 Microsoft Edge

Analysis of the use of a web browser then that becomes the source of the evidence can be found in a file databases. At Microsoft Edge can be found on a file \img_cloudtest1.dd\Users\cloudtest2015\AppData\Local\Micr osoft\ Windows\webcache\WebCacheV01.dat

In Table 5 is shown the names of the database on Mozilla Firefox and its Description.

Table 5. Table File ESE Microsoft Edge

Name Table	Description
Content	Temporary internet Files
Cookies	Cookies
Doomstore	WebStore
History	URL History
Iedownload	Downloaded files
MSHist01YYYYMMDD	Time span of URL History

In Table 5, Table Content contains information about temporary internet file consists of several containerid contained how much data is stored is stored, containerid could not a fixed value but can be capricious or random, tables cookies store information cookies stored on some containers, as well as the history table containing information browsing history and ieDownload information about the location of the downloaded file, the possibility of users use the browser to download files from the Microsoft edge CloudMe, Copy or Dropbox account. The password can descrypt using iepassview from nirsoft.com.

5.2 Client Application Analysis

5.2.1 CloudMe

CloudMe client during the installation and running of applications using the Disk pulse and Prosess Monitor easily find where the main file CloudMe stored during the analysis found important files related or could be evidence.

The main database file contained in the CloudMe /img_cloudtest1.dd/Users/cloudtest2015/AppData/Local/CloudMe/Sync/cache.db

Fig 4 is shown the location on the path to the directory where the log files and database CloudMe.

Tag	File
cloudme	/img_cloudtest1.dd/Users/cloudtest2015/AppData/Local/CloudMe/Sync/cache.db
cloudme	/img_cloudtest1.dd/Users/cloudtest2015/AppData/Local/CloudMe/Sync/logs/2015-11-13.txt

Fig 4: Location File of CloudMe

In Table 6 is shown the names of the database and log on CloudMe and its Description.

Table 6. File Analysis of CloudMe

Name File	Description
Cache.db	This database store user name information (username), a local directory path that stores information about files stored in CloudMe, information about the names, size, and other metadata.
YYYY-MM-DD.txt	This file log Shows the login time information to connect to the Internet, connections problem, and control error other and etc.

5.2.2 Copy

Copy client during the installation and running of applications using the Diskpulse and Process monitor easily find where the main file Copy stored during the analysis found important files related or could be evidence.

Fig 5 is shown the location on the path to the directory where the log files and database copy.

Tag	File
copy	/img_cloudtest1.dd/Users/cloudtest2015/AppData/Roaming/Copy/synclog.txt
copy	/img_cloudtest1.dd/Users/cloudtest2015/AppData/Roaming/Copy/trace.txt
copy	/img_cloudtest1.dd/Users/cloudtest2015/AppData/Roaming/Copy/copy mir968659@gmail.com.db
copy	/img_cloudtest1.dd/Users/cloudtest2015/AppData/Roaming/Copy/config.db

Fig 5: Location File of Copy

In Table 7 is shown the name of the database and log files on Copy and its description.

Table 7. File Analysis of Copy

Name File	Description
config.db:	File database saving settings such as the user email, first name, last name, and user ID, ClientID. It also contains the path root and the cache root directory of Copy's, client version and other settings.
trace.txt:	File log file's entries contain information related the hosting machine (operating system, host information, etc.), the client application, and the server.
synclog.txt	This files log store information related to the operations types. Some operations are authentication attempts and file manipulation (such as upload, download, modification, and deletion).
copy <User_Email>.db	This file database is very interesting for a investigator this point it contains the list of files and metadata stored in the root directory of Copy. (in our case the name of the file is mir968659@gmail.com.db)

5.2.3 Dropbox

Dropbox application to open the database file must use tools dropboxdescrytor to be able to read this tool database file can be downloaded at magnetforensics.com

Fig 6 is shown the location on the path to the directory where the log files and database Dropbox.

Tag	File
dropbox	/img_cloudtest1.dd/Users/cloudtest2015/AppData/Roaming/Dropbox/host.db
dropbox	/img_cloudtest1.dd/Users/cloudtest2015/AppData/Roaming/Dropbox/host.dbx
dropbox	/img_cloudtest1.dd/Users/cloudtest2015/AppData/Roaming/Dropbox/instance_db/instance.dbx
dropbox	/img_cloudtest1.dd/Users/cloudtest2015/AppData/Roaming/Dropbox/instance1/checker.dbx
dropbox	/img_cloudtest1.dd/Users/cloudtest2015/AppData/Roaming/Dropbox/instance1/config.db
dropbox	/img_cloudtest1.dd/Users/cloudtest2015/AppData/Roaming/Dropbox/instance1/deleted.dbx
dropbox	/img_cloudtest1.dd/Users/cloudtest2015/AppData/Roaming/Dropbox/instance1/filecache.dbx
dropbox	/img_cloudtest1.dd/Users/cloudtest2015/AppData/Roaming/Dropbox/instance1/photo.dbx
dropbox	/img_cloudtest1.dd/Users/cloudtest2015/AppData/Roaming/Dropbox/instance1/sigstore.dbx

Fig 6: Location File of Dropbox

In Table 8 is shown the names of the database on Dropbox and its Description.

Table 8. File Analysis of Dropbox

Name File	Description
config.dbx	This files database at the table config stores the host IDs, the user's email, user information, host_id, root folder paths, among other settings. This file is one of the encrypted files, and after it has been decrypted with magnet forensics dropbox decryptor it is possible to see it.
filecache.dbx	This file database contains the server paths, the files lists and the files names, the sizes of the files, the modification and creation times in the table file_journal. The table deleted_fileids contain metadata file has been deleted.

5.3 Memory Analysis

Memory analysis using Belkasoft Evidence Finder and a search keywords used in the file .mem. in memory there is a lot of information that can be used and proof. However memory analysis is not always possible, and therefore the possibility of memory can not be analyzed during digital forensic investigations. If possible, the memory should be acquired. Digital evidence can be found in memory, among others include, user information, user details, a list of files and information files, accessing files and folders, process information, procces instruction, host names, libraries are loaded, libraries are loaded via the server, temporary files, accessing database files and log files, authentication, artifact using web browser also found in ram such as cookies, URL history and other in Fig. 7 shows the result of analysis using WinHex.

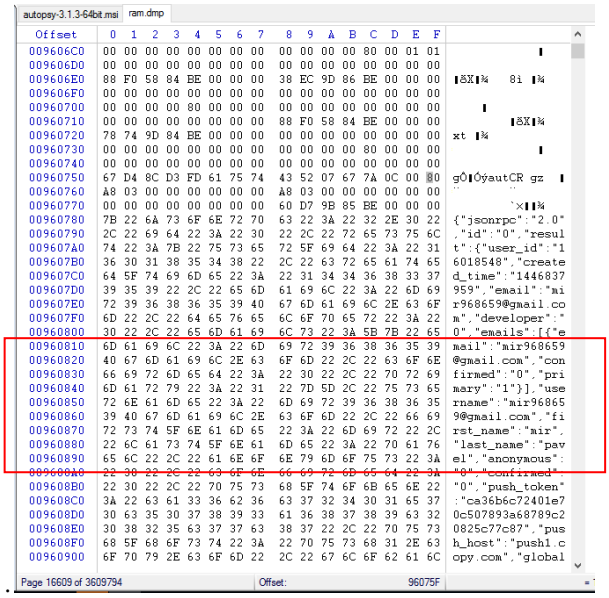

Fig 7: Analysis RAM using WinHex

In the picture above is based on analyzes using WinHex looks username, email, user information and other.

5.4 Deleted Analysis & Uninstall Analysis

One thing that is important to conduct digital investigations, is recovering from a deleted file. For the recovering deleted files from cloud storage accounts, perform recovery from the server side and the client side. Copy the client application has a feature known as undelete. This feature can restore a deleted file either locally or on a server.

CloudMe and Dropbox does not have a similar feature, but it can be done, restore deleted files or files that are modified, which account can only be accessed via a web browser is not through the application as well as on Copy. And differences keep deleted files in days. Dropbox can also delete files permanently.

Using tools Autopsy, File (allocated space) is still visible in recyble bin, and point to the directory of origin, before dideleted. The files can still be recovered. And if the file has been deleted in recyble bin (unallocated space) still can be recovered, using tools Foremost, SCAPEL, and PhotoRec TSK toolkit.

The uninstall process on CloudMe, the main folder to store database and log files in the folder C:\user\cloudtest2015\ AppData\Local\CloudMe\Sync still visible as well as files synchronization is still contained in the folder C:\user/ cloudtest2015\CloudMe, use Scanreg can find registry files related to the use of applications CloudMe.

After doing the uninstall process, the main folder of the Copy also includes files that are inside the folder C:\user/ cloudtest2015\AppData\Roaming\Copy also still there, while the database and log files have been deleted. This means that we can not see the user usage activity. using RegScanner we can use string-based search using the copy, it is possible to find some registry keys were left behind when the application has been deleted and uninstalled.

During the uninstall process of the dropbox, dropbox folder is still visible on the hard disk, it also still contains the files. the folder C:\Users\cloudtest2015\AppData\Roaming\Dropbox is also still there, while the files are encrypted database has been deleted. There are many registry key from dropbox and can be traced remaining data during the installation process, it can be used as evidence of the use of client applications.

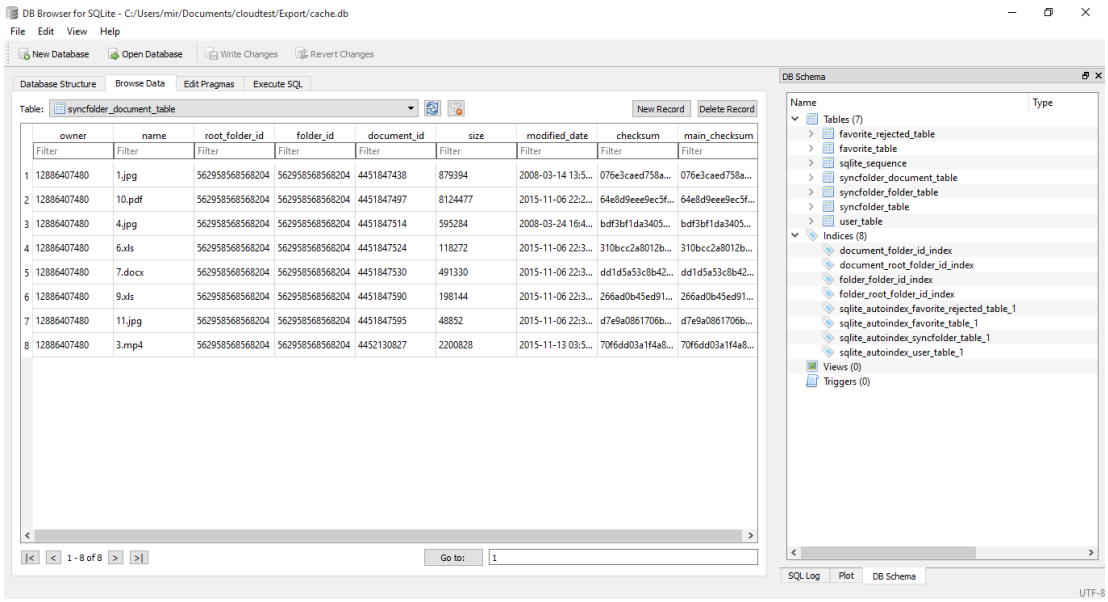

Fig 8: Table syncfolder_document_file in database Cache.db of CloudMe Application

In Fig.8 is the content of a database file from an application cache.db CloudMe, shows the remaining files, and files that have been deleted does not appear in the table syncfolder_document_tabel that file 2.jpg, and file 8.mp3 5.jpg file.

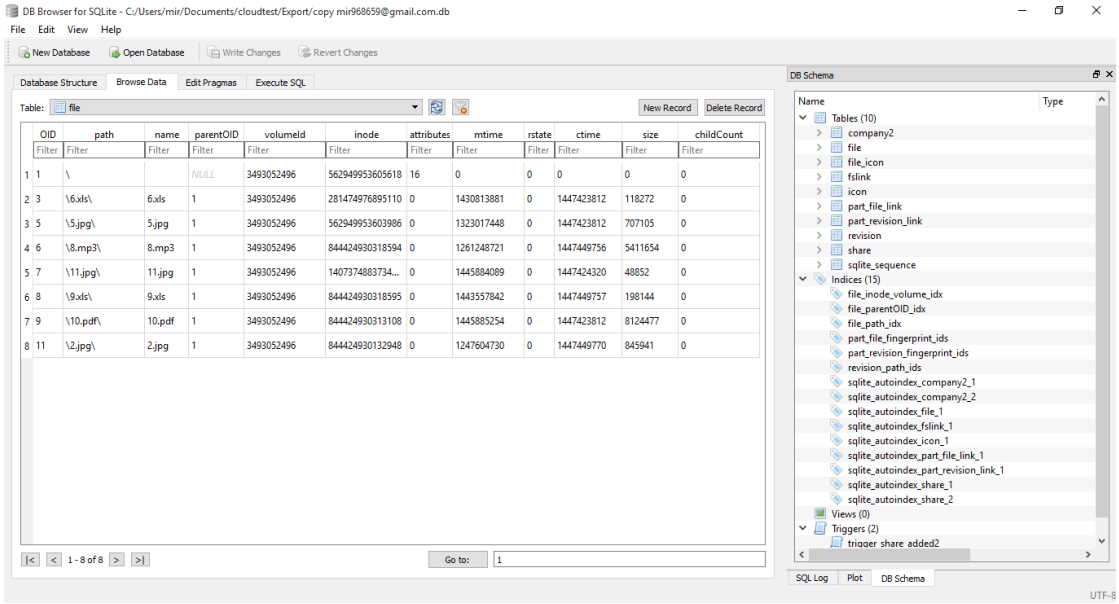

Fig 9: Table file in database mir968659@gmail.com.db of Copy Application

In Fig.9 is a database file contents of the database mir968659 @ gmail.com.db of application Copy, shows the remaining files, and files that have been deleted does not appear in the table file namely 1.jpg file, file 4.jpg and file 7.docx.

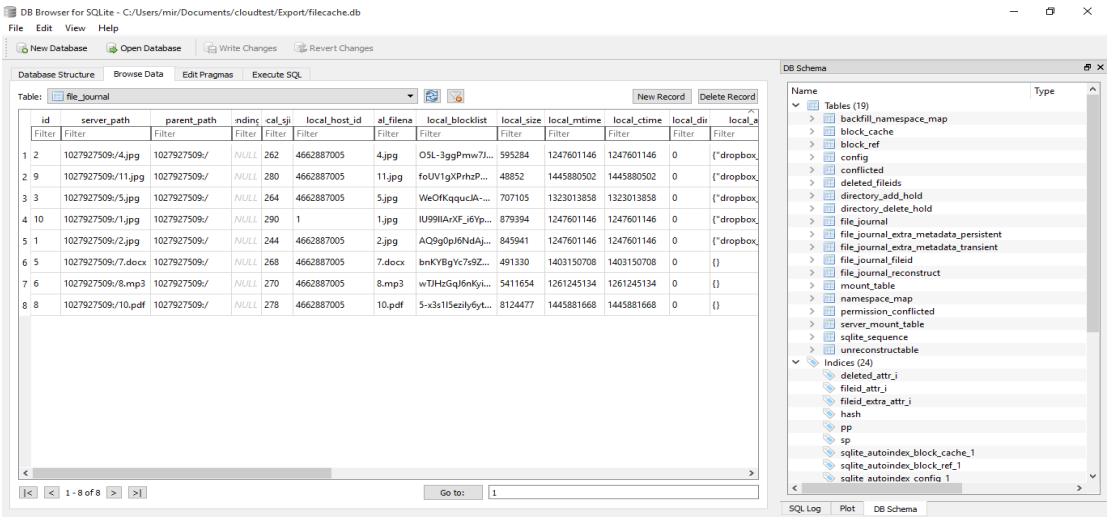

Fig 10: Table file_journal in filecache.db of Dropbox Application

In Fig.10 is a file from the contents of the application Dropbox filecache.db database, shows the remaining files, and files that have been deleted does not appear in the table file_journal namely 3.mp4 file, file 6.xls and file 9.xls

6. CONCLUCION

In this paper presented that it is possible of getting digital evidence that related to the use of cloud storage client on Windows 10 platform. Digital evidence can be found in the database and log files created by applications, on the web browser, in memory and the registry. This study contributes to the problems of the cloud in particular helps forensic investigators in mapping the area that became a source of digital evidence. Based on the test results success rate average is 82,63% and the remaining can not be analyzed, the results depend on various state, procedures and tools that are used, the research can be carried out smoothly.

7. REFERENCES

[1] Cisco.com, "No Title," 2015. [Online]. Available: a) http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1724918. [Accessed: 01-Nov-2015].

[2] Cisco, "Cisco Global Cloud Index: Forecast and Methodology, 2014–2019," *Cisco Press*, 2015. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf. [Accessed: 01-Nov-2015].

[3] D. Quick, B. Martini, and K.-K. R. Choo, *Cloud Storage Forensics*. 2014.

[4] M. Epifani, "Cloud Storage Forensics," in *SANS Eurupean Digital Forensics Summit 2013*, 2013.

[5] J. Chung, H., Park and C. Lee, S., Kang, "Digital Forensic Investigation of Cloud Storage Services, Digital Investigation," 2012.

[6] S. Mehreen and B. Aslam, "Windows 8 cloud storage analysis: Dropbox forensics," in *2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 2015, pp. 312–317.

[7] R. Malik, "Analysis of Evidence in Cloud Storage Client Applications on the Windows Platform," *Int'l Conf. Secur. Manag.*, 2015.

[8] M. Borgmann, T. Hahn, M. Herfert, T. Kunz, M. Richter, U. Viebeg, and S. Vowé, *On the Security of Cloud Storage Services*. Fraunhofer Verlag; Stuttgart, Germany: Fraunhofer Institute for Secure Information Technology SIT, 2012.

[9] T. Prasath and S. Karthikeyan, "Cloud Storage Vendors Wide Support and Security Key Features for Shifting Towards Business Perspective," *Int. J. Cloud Comput. Serv. Sci.*, vol. 2, no. 6, pp. 421–426, 2013.

[10] M. Lohnash and G. Akerlund, "Online Backup Comparison," 2015. [Online]. Available: http://www.backupreview.com/online-comp-provider/. [Accessed: 01-Nov-2015].

[11] G. Reese, "Cloud Forensics Using Ebs Boot Volumes," *Oreilly.com*, 2010.

[12] A. Iswardani and I. Riadi, "Denial of service log analysis using density k-means method," *J. Theor. Appl. Inf. Technol.*, vol. 83, no. 2, p. 2, 2016.

[13] P. . Clark, "Digital Forensics Tool Testing–Image Metadata in the Cloud', Department of Computer Science and Media Technology," *Gjøvik Univ. Coll.*, 2011.

[14] A. K. Mccurdy, "Dropbox : Forensic Detection the requirements of Edinburgh Napier University," 2013.

[15] H. Chung, J. Park, S. Lee, and C. Kang, "Digital forensic investigation of cloud storage services," *Digit. Investig.*, vol. 9, no. 2, pp. 81–95, 2012.

[16] Www.dropbox.com, "No Title." [Online]. Available: http://www.dropbox.com.

[17] Copy.com, "No Title." [Online]. Available: http://www.copy.com.

[18] Www.cloudme.com, "No Title." [Online]. Available: http://www.cloudme.com.