Cloud based Storage Drive Forensics

Prashant Bhatt[1], Mr. Naresh Kumar Gardas[2], Ms. Shweta Chawla[3], Moin Khorajiya[4]

[1] PG Student, Network Security, GTU PG School, Ahmedabad, Gujarat, India
[2] Course-Coordinator, CDAC-ACTS, Pune, Maharashtra, India
[3]Head and Chief Investigator, S C Cyber Solutions, Pune, Maharashtra, India
[4] PG Student, Network Security, GTU PG School, Ahmedabad, Gujarat, India

ABSTRACT

Cloud Storage is recently as emerging topic in these eras. As the data are increasing, the storage become major issue for the people. There are different kind of Cloud Storage application such as One Drive, Sky Drive, Drop Box and Google Drive. Google Drive is gaining more popularity as it is user friendly than any other Cloud Storage Application. Google Drive is a Cloud Storage Application which allows user to store, share and edit the file in the cloud. In these paper, the authors will perform forensics of Google Drive via di1fferent technique such as using client software, Google Drive access via browser, Memory Analysis, Network Analysis and other techniques. From that the Authors will find, what type of data remnants can be found in user device.

Keyword: - *Cloud Storage, Google Drive, Forensics, Digital Forensic;*

1. Introduction

1.1 Cloud Storage

Cloud Storage is new hot topic for the modern era. As we know that all the application or user want to store their data at one place so that whenever they need such data they can easily access it. In Early Times, They have to take a backup by copying in a hard disk and any USB Devices or cloning such files. As such Technique is somehow costly and sometime, there is major issue i.e. loss of data can be also happen. To overcome these type of Problem, Cloud Storage comes into existence.

It is based on virtualized infrastructure which provides accessible interfaces near instant elasticity and scalability, multi-tenancy, and metered resources [6]. It can deployed off-premise or on-premise service and made up of many distributed resources, but it acts as a single storage [2].

There are many different consumer cloud storage provider are available in market, which provide or offering the free access of cloud storage such as Microsoft SkyDrive, One Drive, Drop Box and Google Drive, Sugar Sync. There are different way to access such as user can install client software on Personal Computer (PC) and access by web browser or mobile and laptop.

It is used to store the electronic data on internet or remote infrastructure rather than local storage which can be accessed by computer or electronic device [3].

1.2 Architecture of Cloud Storage

The Basic work of Cloud storage architectures delivering the storage on demand in multi-tenant way. It consist of a front end that gives an API which allow user to access the storage. In Traditional storage, this API is the SCSI protocol; but in cloud storage, these protocols are developed in which author find web server, file-based front ends. Behind that front end there is a layer called middleware and also known as storage logic. This layer includes a variety of features such as replication and data reduction, over the traditional one [5].

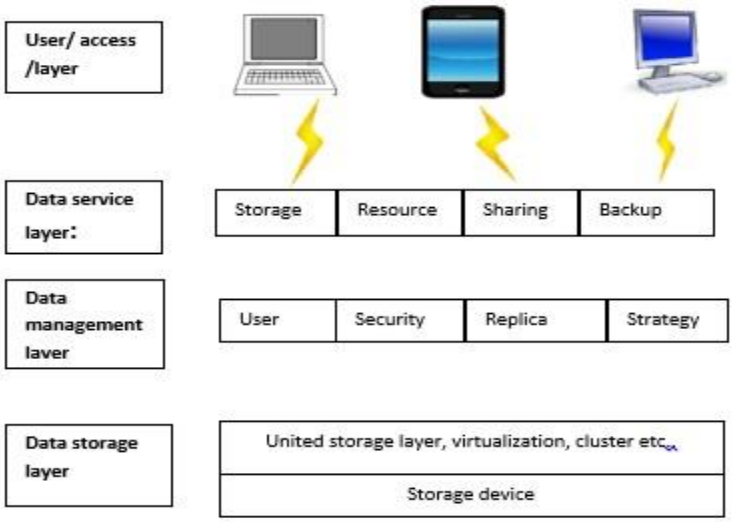

Fig. 1. Architecture of Cloud Storage

2. Digital Forensics

There are lots of digital forensics models have been propose by digital forensics investigators. These is a common forensic analysis framework to guide forensic investigations with future scope offering new services. These steps are generally accepted standards and procedures that digital forensic investigator examines and follow the four stage in their investigation:-

- Identification of Digital Evidence
- Preservation of Digital Evidence
- Analysis of Digital Evidence
- Presentation of Digital Evidence

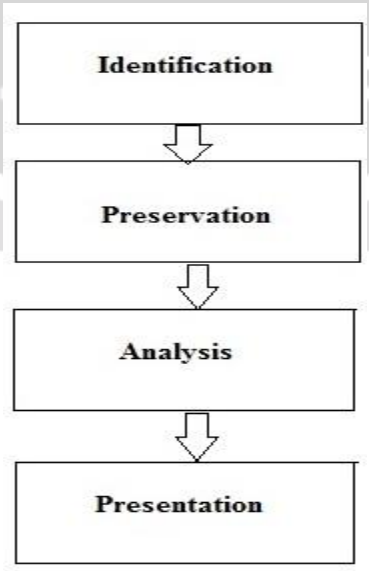

Fig. 2. Procedures of Digital Forensics

2.1 Identification of Digital Evidence

It is a first step of Digital Forensics Framework. In these Investigator identify what type of content is being useful for the investigator or useful content for further analyzing.

2.2 Preservation of Digital Evidence

In these step of Digital Forensics Framework. It will preserve the useful content by Forensics tool such as Access FTK Imager and it help for providing integrity, by checking the hash values of the file. In these phase, Chain of Custody plays an important role for preserving the data. It help to provide integrity.

2.3 Analysis of Digital Evidence

In these phase the analysis of such preserve data is to be done. Analysis can be done by different method such as Recycle Bin, Browser Analysis, Memory Analysis, Temp File analysis, Swap File analysis, Registry Analysis and Network Analysis.

2.4 Presentation of Digital Evidence

This is a last phase of Digital Evidence Framework, analysis of evidence is being presented in the Systematic manner and common man can also understand the analysis of such Digital Evidence.

3. CLOUD BASED DRIVE FORENSICS

As author discussed in early section, there are lots of Cloud based Drives found in market such as Dropbox, Google Drive, One box and Sugar Sync. In this work, Google Drive is being more focused on, because it is most popular drive and another reason is that there is no need to create another account for Google Drive as it uses Gmail or one simple Google account, which provide all google services.

Right Now, Cloud Forensics is an important domain for the Researchers and Forensics Investigators. As almost everything is slowly getting transferred to the Cloud environment. The users are now storing their important documents on Cloud Storage drive for ease of access at any time and at any place with use of Internet.

In this work, Cloud Storage Drive i.e. Google Drive is taken into consideration because it is user friendly as compared to any other Cloud Storage Application. Analysis of Google Drive from different platforms like Google Drive client Software, Recycle Bin, Browser Analysis, Memory Analysis and Network Analysis will be carried out [1].

3.1 Analyzing with Client Software

Whenever author run the executable file 'googledrivesync.exe', it will create the folder at 'C:\Program Files \Google\Drive\' in these author will find that 'googledrivesync32.dll' was created. Created in the users folder is a directory as follows: 'C:\Users\ [username]\AppData\Local \Google\Drive\ in these folder author will take only two file which are useful for us i.e. 'sync_config.db' and 'snapshot.db'. Both of these file are viewed by SQLite Browser as it is SQLite format 3 Database [1].

In sync_config.db, data stored in it include the total path of sync folder where files in the account are downloaded and synchronized and the user email used to access the Google Drive account. While 'snapshot.db', data stored in it include the file details which are store in Google Drive account. Information such as filenames, modified and created times, URL, Size, Resource ID, and a checksum value which matched the MD5 value for the associated file. When Google drive client software installed in system and if author ran it open automatically without prompting for a password. This will help forensic investigator to make forensic copy of hard drive. Analyzing such hard drive author can get username and password, which is already store in it [1].

3.2 Memory Analysis

Memory Analysis or Capturing the memory can be done by using X-ways and Encase tool. While capturing a memory, author search 'Google Drive' in VM memory files. The Google Drive username was located in memory capture files near text, <Email> and password are located in free text, it found near '&passwd= [password]' and '&passwdagain= [password]' [1].

3.3 Analyzing the Network

Network analysis can be done by Network Miner, Wireshark and Encase Tool. The Network Traffic is observed on Port no. 80 (HTTP) and Port no. 443 (HTTPS). Whenever user access the Drive account, it appear login session are established with Google using the different IP address with URLs of 'www.google.com' [1]. When accessing files or data in an account via a browser, the process of accessing IP's in the ranges previously mentioned for the client software were observed: (1) 'www.google.com', (2) 'VeriSign', (3) 'account. Google', (4) 'docs.google' [1].

3.4 Analyzing Registry

Registry analysis can be done by tools such as Registry Analyzer or by default Windows tool i.e. Registry Editor. In Registry Editor, checking the hives HKEY_CURRENT_USER\Software\ Explorer\ComDlg32\OpenSavePidIMRU' display all the file format and check for the required file format such as doc, docx, exe and etc.

Another Method is checking hives 'HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentsDocs'

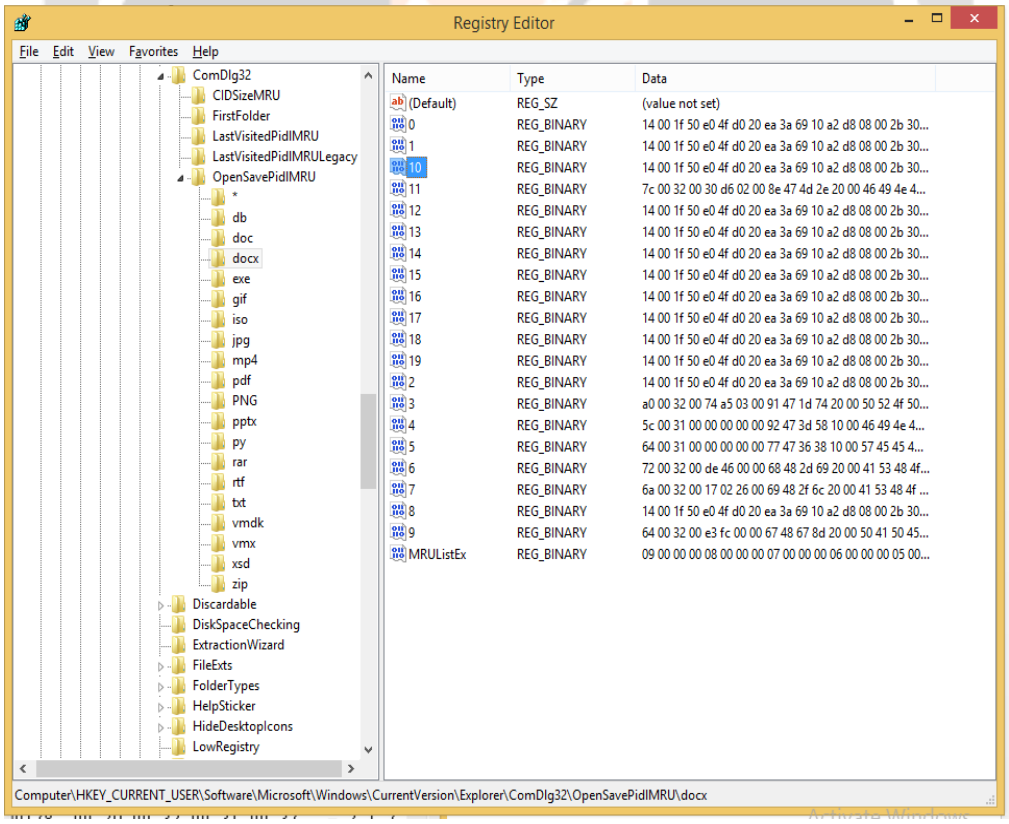

Fig. 3:.Registry Editor

3.5 Google Drive account when accessed via a browser

Whenever Author access the Google web account (via https:// drive.google.com/) will displays the username at the top right corner of the Browser. In this, information displayed also includes the last modified time. When Author download files from Google Drive via the browser, the folders and files are compressed into a ZIP file [1]. While analyzing the drives accessed via a browser, no artefacts or associated file is found. To solve this issue faced by investigator, author performs some experiments which will provide an artefacts of Google Drive documents in the system, which help investigator to find the artefacts and solve the issue.

4. EXPERIMENTAL WORK.

The Author is working with the issue of the artefacts not being found on the system. Experiments are carried out by the author using script to find the artefacts of Google Drive documents.

First, Win Hex tool is used to give some hint whether artifacts related documents are found in the system or not. Author created a Document in Google Docs with some unique words.

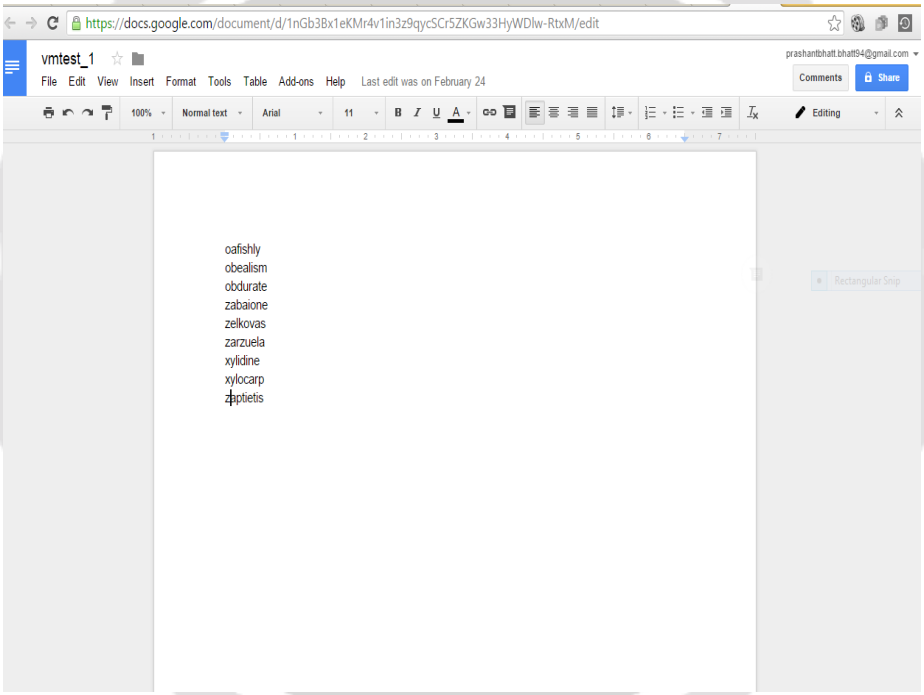

Fig. 5. Google Docs File

In this, word oafishly is being searched and it will display the file name where it exist (See Figure 6). It will display the file, which can be beneficial to the investigator.

Another search of particular word or file is done by using FTK Imager tool. When the FTK Imager tool is used, it captures the memory of system and found the word 'oafishly' by analyzing it (See Figure 7).

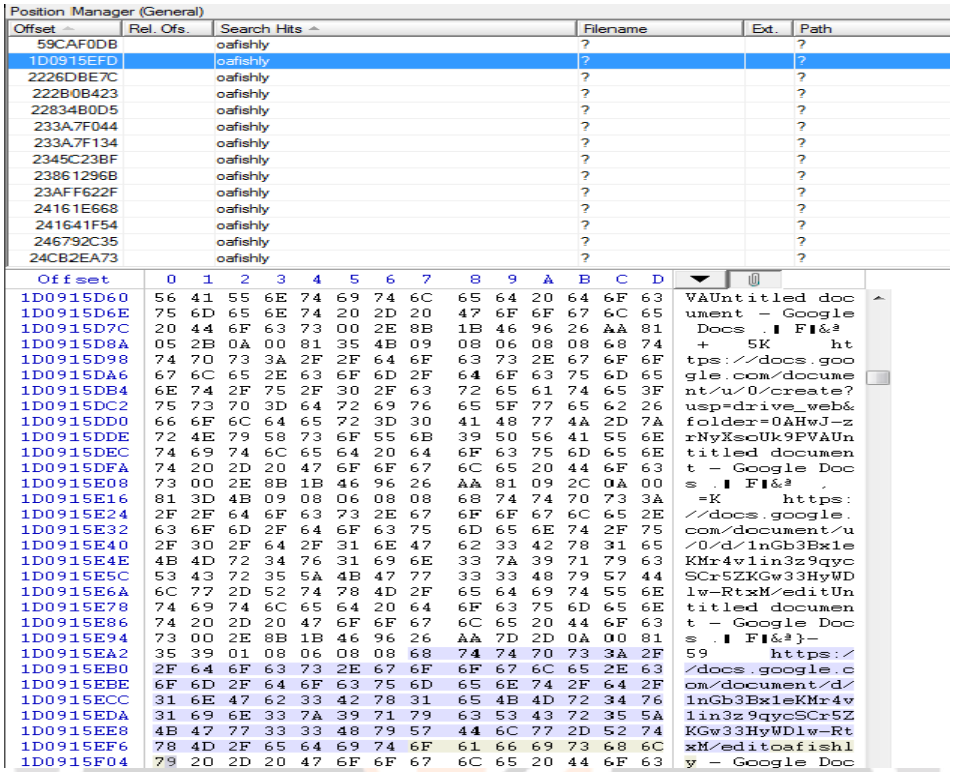

Fig. 6. Showing the Docs File

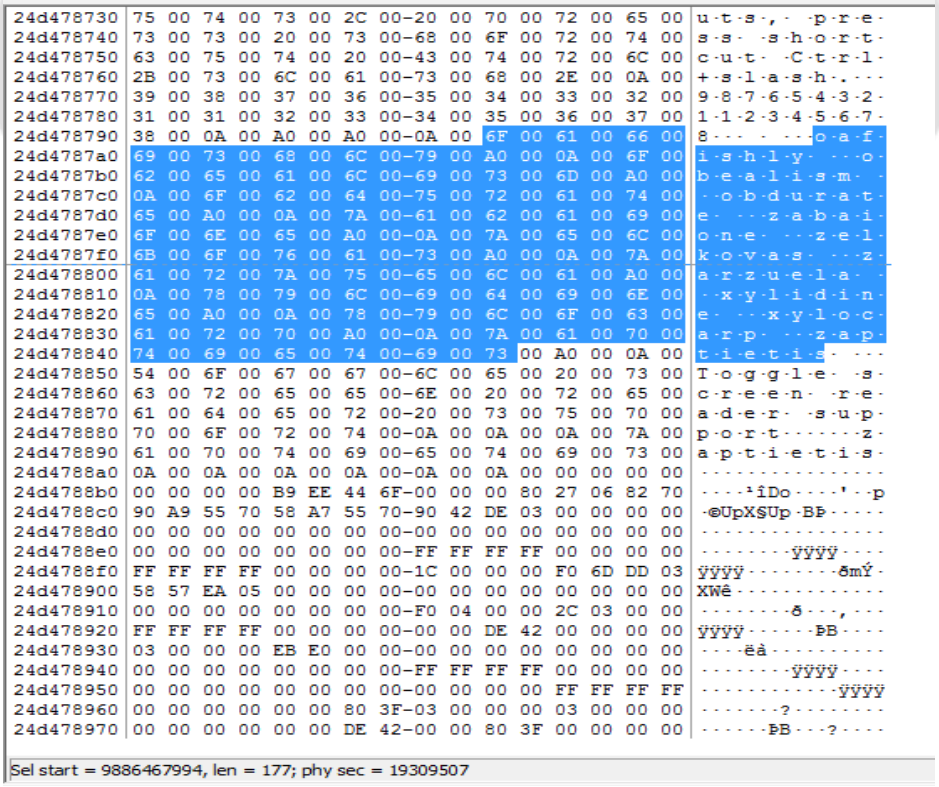

Fig. 7. FTK Imager

5 Conclusion

Whenever any storage of data using Cloud service provider is investigated, the initial stage is Identification of Cloud Service and user account detail. This will aid investigator to examine and identify the location of data and respond in order to secure the data. Examination of the Google Drive account by taking some keywords and common file location to locate useful information.

Author can also determine Google Drive username and Password from the preserved forensic image. It was great thing that Google Drive Password were some instance found as Plaintext in I.E. (Internet Explorer) and some other old Browser. But right now, such thing as being patched by such Browser. Recently, Author can only find Google Drive URL and which file they were accessing and Password remains in encrypted Form.

In Future Work, Author will prepare the Script which directly extract the Specific URL from the System. It help Investigator to solve the Drawbacks of Existing System

Acknowledgment. The trademarks, products name, Company name, Screenshot refereed in these paper are acknowledge to their respective owners.

6. REFERENCES

1. Darren Quick and Kim-Kwang Raymond Choo.: Google Drive: Forensic analysis of data remnants. Journal of Network and Computer Applications, (2014)

2. Google Drive: https://en.wikipedia.org/wiki/Google_Drive

3. Darren Quick and Kim-Kwang Raymond Choo: Forensic collection of cloud storage data: Does the act of Collection result in changes to the data or its metadata?, Digital Investigation, 2013

4. Cloud Storage: https://en.wikipedia.org/wiki/Cloud_Storage

5. Kulkarni, Gurudatt, Rani Waghmare, Rajnikant Palwe, Vidya Waykule, Hemant Bankar and Kundlik Koli : Cloud Storage Architecture, 7th International Conference on Telecommunication System Services and Applications (TSSA), 2012

6. Cloud Storage Architecture: https://www.hpcmicrosystems.net