

# Cloud based Storage Drive Forensics

Prashant Bhatt<sup>1</sup>, Mr. Naresh Kumar Gardas<sup>2</sup>, Ms. Shweta Chawla<sup>3</sup>, Moin Khorajiya<sup>4</sup>

<sup>1</sup> PG Student, Network Security, GTU PG School, Ahmedabad, Gujarat, India

<sup>2</sup> Course-Coordinator, CDAC-ACTS, Pune, Maharashtra, India

<sup>3</sup> Head and Chief Investigator, S C Cyber Solutions, Pune, Maharashtra, India

<sup>4</sup> 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 different 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<sup>[6]</sup>. It can deployed off-premise or on-premise service and made up of many distributed resources, but it acts as a single storage<sup>[2]</sup>.

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<sup>[5]</sup>.

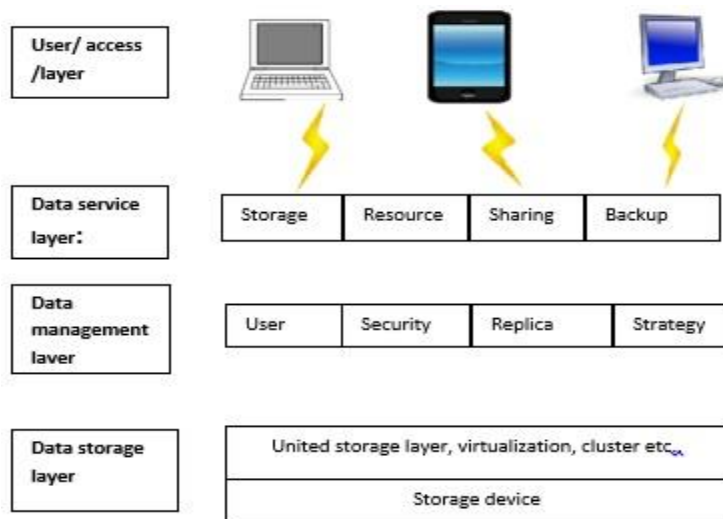


Fig. 1. Architecture of Cloud Storage

## 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

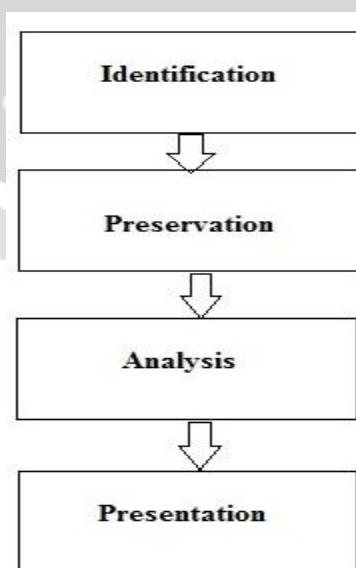


Fig. 2. Procedures of Digital Forensics

### 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<sup>[1]</sup>.

### 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<sup>[1]</sup>.

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 as 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<sup>[1]</sup>.

### 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’

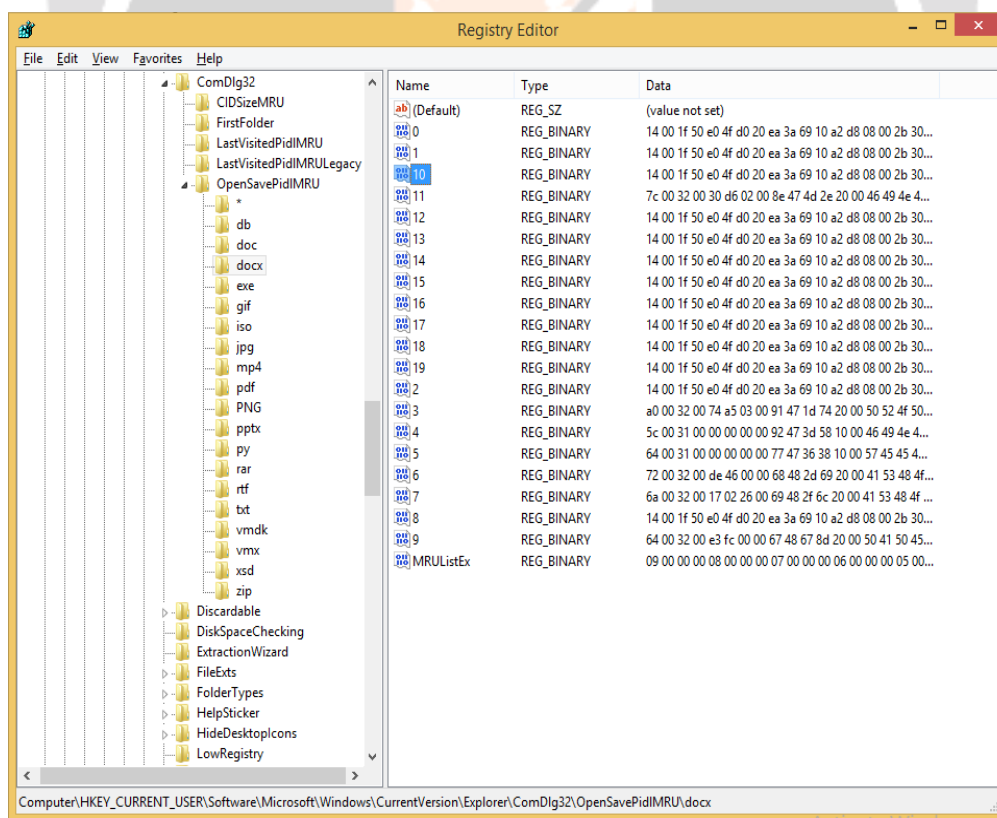


Fig. 3:Registry Editor

### 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 <sup>[1]</sup>. 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.

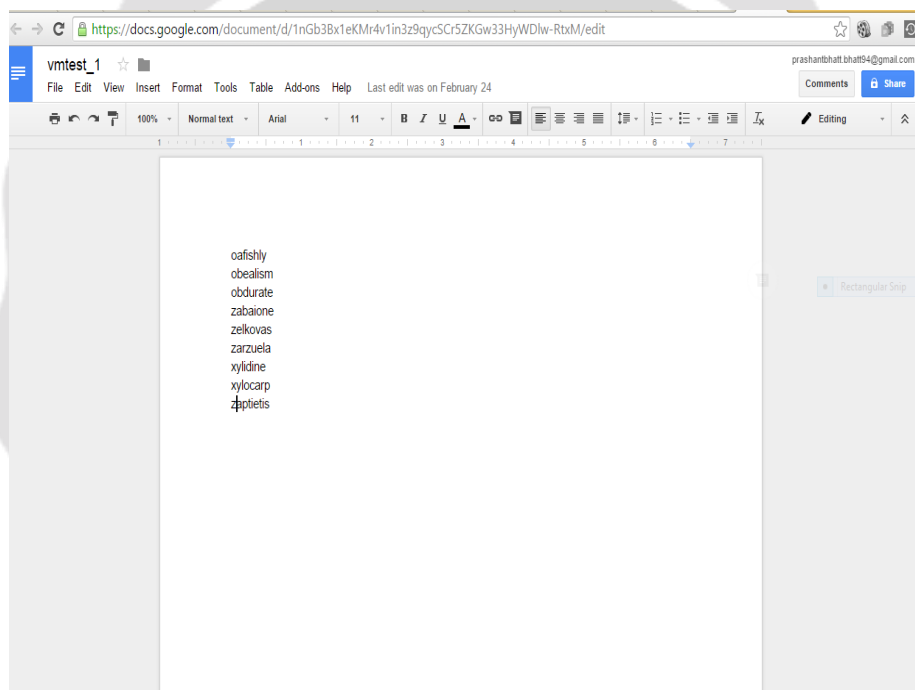


Fig. 5. Google Docs File

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).

Offset	Rel. ofs	Search Hits	Filename	Ext.	Path
59CAF0DB		oafishly	?		?
1D0915EFD		oafishly	?		?
2226DBE7C		oafishly	?		?
22280B423		oafishly	?		?
2283480D5		oafishly	?		?
233A7F044		oafishly	?		?
233A7F134		oafishly	?		?
2345C23BF		oafishly	?		?
238612968		oafishly	?		?
23AFF622F		oafishly	?		?
24161E668		oafishly	?		?
241641F54		oafishly	?		?
246792C35		oafishly	?		?
24CB2EA73		oafishly	?		?

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	
1D0915D60	56	41	55	6E	74	69	74	6C	65	64	20	64	6F	63	VAUntitled docu
1D0915D6E	75	6D	65	6E	74	20	2D	20	47	6F	6F	67	6C	65	ment - Google
1D0915D7C	20	44	6F	63	73	00	2E	8B	1B	46	96	26	AA	81	Docs   F!&#
1D0915D8A	05	2B	0A	00	81	35	4B	09	08	06	08	08	68	74	+ 5K ht
1D0915D98	74	70	73	3A	2F	2F	64	6F	63	73	2E	67	6F	6F	tps://docs.goo
1D0915DA6	67	6C	65	2E	63	6F	6D	2F	64	6F	63	75	6D	65	gle.com/docume
1D0915DBA	6E	74	2F	75	2F	30	2F	63	72	65	61	74	65	3F	nt/u/0/create?
1D0915DC2	75	73	70	3D	64	72	69	76	65	5F	77	65	62	26	usp=drive_web&
1D0915DD0	66	6F	6C	64	65	72	3D	30	41	48	77	4A	2D	7A	folder=0AHvJ-z
1D0915DDE	72	4E	79	58	73	6F	55	6B	39	50	56	41	55	6E	rNyXsoUk9PVAUn
1D0915DEC	74	69	74	6C	65	64	20	64	6F	63	75	6D	65	6E	itled documen
1D0915E08	74	20	2D	20	47	6F	6F	67	6C	65	20	44	6F	63	t - Google Doc
1D0915E16	73	00	2E	8B	1B	46	96	26	AA	81	09	2C	0A	00	s   F!&#
1D0915E24	81	3D	4B	09	08	06	08	08	68	74	74	70	73	3A	=K https:
1D0915E32	2F	2F	64	6F	63	73	2E	67	6F	6F	67	6C	65	2E	//docs.google.
1D0915E40	63	6F	6D	2F	64	6F	63	75	6D	65	6E	74	2F	75	com/document/u
1D0915E4E	2F	30	2F	64	2F	31	6E	47	62	33	42	78	31	65	/0/d/lnGb3Bx1e
1D0915E54	4B	4D	72	34	76	31	69	6E	33	7A	39	71	79	63	KMr4vlin3z9qyc
1D0915E5C	53	43	72	35	5A	4B	47	77	33	33	48	79	57	44	ScR5ZKGw33HyWD
1D0915E6A	6C	77	2D	52	74	78	4D	2F	65	64	69	74	55	6E	lw-RtxM/editUn
1D0915E78	74	69	74	6C	65	64	20	64	6F	63	75	6D	65	6E	itled documen
1D0915E86	74	20	2D	20	47	6F	6F	67	6C	65	20	44	6F	63	t - Google Doc
1D0915E94	73	00	2E	8B	1B	46	96	26	AA	7D	2D	0A	00	81	s   F!&#
1D0915EA2	35	39	01	08	06	08	08	68	74	74	70	73	3A	2F	59 https://
1D0915EA9	2F	64	6F	63	73	2E	67	6F	6F	67	6C	65	2E	63	/docs.google.c
1D0915EBE	6F	6D	2F	64	6F	63	75	6D	65	6E	74	2F	64	2F	om/document/d/
1D0915ECC	31	6E	47	62	33	42	78	31	65	4B	4D	72	34	76	lnGb3Bx1eKMr4v
1D0915EDA	31	69	6E	33	7A	39	71	79	63	53	43	72	35	5A	lin3z9qycScR5Z
1D0915EE8	4B	47	77	33	33	48	79	57	44	6C	77	2D	52	74	KGw33HyWDlw-Rt
1D0915EF6	78	4D	2F	65	64	69	74	6F	61	66	69	73	68	6C	xM/editoafishl
1D0915F04	79	20	2D	20	47	6F	6F	67	6C	65	20	44	6F	63	y - Google Doc

Fig. 6. Showing the Docs File

24d478730	75	00	74	00	73	00	2C	00-20	00	70	00	72	00	65	00	u-t-s., . p-r-e-
24d478740	73	00	73	00	20	00	73	00-68	00	6F	00	72	00	74	00	s-s- s-h-o-r-t
24d478750	63	00	75	00	74	00	20	00-43	00	74	00	72	00	6C	00	c-u-t- C-t-r-l
24d478760	2B	00	73	00	6C	00	61	00-73	00	68	00	2E	00	0A	00	+s-l-a-s-h-...
24d478770	39	00	38	00	37	00	36	00-35	00	34	00	33	00	32	00	9-8-7-6-5-4-3-2
24d478780	31	00	31	00	32	00	33	00-34	00	35	00	36	00	37	00	1-1-2-3-4-5-6-7
24d478790	38	00	0A	00	A0	00	A0	00-0A	00	6F	00	61	00	66	00	8-... -...o-a-f
24d4787a0	69	00	73	00	68	00	6C	00-79	00	A0	00	0A	00	6F	00	i-s-h-l-y-...o-
24d4787b0	62	00	65	00	61	00	6C	00-69	00	73	00	6D	00	A0	00	b-e-a-l-i-s-m-
24d4787c0	0A	00	6F	00	62	00	64	00-75	00	72	00	61	00	74	00	-o-b-d-u-r-a-t
24d4787d0	65	00	A0	00	0A	00	7A	00-61	00	62	00	61	00	69	00	e-...z-a-b-a-i-
24d4787e0	6F	00	6E	00	65	00	A0	00-0A	00	7A	00	65	00	6C	00	o-n-e-...z-e-l
24d4787f0	6B	00	6F	00	76	00	61	00-73	00	A0	00	0A	00	7A	00	k-o-v-a-s-...z-
24d478800	61	00	72	00	7A	00	75	00-65	00	6C	00	61	00	A0	00	a-r-z-u-e-l-a-
24d478810	0A	00	78	00	79	00	6C	00-69	00	64	00	69	00	6E	00	-x-y-l-i-d-i-n
24d478820	65	00	A0	00	0A	00	78	00-79	00	6C	00	6F	00	63	00	e-...x-y-l-o-c
24d478830	61	00	72	00	70	00	A0	00-0A	00	7A	00	61	00	70	00	a-r-p-...z-a-p-
24d478840	74	00	69	00	65	00	74	00-69	00	73	00	A0	00	0A	00	t-i-e-t-i-s-...
24d478850	54	00	6F	00	67	00	67	00-6C	00	65	00	20	00	73	00	T-o-g-g-l-e-...s
24d478860	63	00	72	00	65	00	65	00-6E	00	20	00	72	00	65	00	c-r-e-e-n-...r-e-
24d478870	61	00	64	00	65	00	72	00-20	00	73	00	75	00	70	00	a-d-e-r-...s-up-
24d478880	70	00	6F	00	72	00	74	00-0A	00	0A	00	0A	00	7A	00	p-o-r-t-...z-
24d478890	61	00	70	00	74	00	69	00-65	00	74	00	69	00	73	00	a-p-t-i-e-t-i-s-
24d4788a0	0A	00	0A	00	0A	00	0A	00-0A	00	0A	00	00	00	00	00	.....
24d4788b0	00	00	00	00	B9	EE	44	6F-00	00	00	80	27	06	82	70	...iDo-...-p
24d4788c0	90	A9	55	70	58	A7	55	70-90	42	DE	03	00	00	00	00	@UpX\$Up-BB-...
24d4788d0	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00	.....
24d4788e0	00	00	00	00	00	00	00	00-FF	FF	FF	FF	FF	00	00	00	.....yyyy
24d4788f0	FF	FF	FF	FF	00	00	00	00-1C	00	00	00	00	F0	6D	DD	yyyy-...-5mY-
24d478900	58	57	EA	05	00	00	00	00-00	00	00	00	00	00	00	00	XWe-.....
24d478910	00	00	00	00	00	00	00	00-F0	04	00	00	2C	03	00	00	.....8-...
24d478920	FF	FF	FF	FF	00	00	00	00-00	00	DE	42	00	00	00	00	yyyy-...-BB-...
24d478930	03	00	00	00	EB	E0	00	00-00	00	00	00	00	00	00	00	...-e-...
24d478940	00	00	00	00	00	00	00	00-FF	FF	FF	FF	FF	00	00	00	.....yyyy
24d478950	00	00	00	00	00	00	00	00-00	00	00	00	FF	FF	FF	FF	.....yyyy
24d478960	00	00	00	00	00	80	3F-03	00	00	00	00	03	00	00	00	.....-?-...
24d478970	00	00	00	00	00	DE	42-00	00	80	3F	00	00	00	00	00	.....BB-?-...

Sel start = 9886467994, len = 177; phy sec = 19309507

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](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](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>