Google Drive Forensics

Dr. Digvijaysinh Rathod
Institute of Forensic Science, Gujarat Forensic Sciences University
digvijay.rathod@gfsu.edu.in

Abstract: File storage and synchronization cloud services receives great response from internet users and these services offers features through which users can store files on cloud, sync those data with pc / mobile device or share all kind of files or personal data publically or with specific person. Recently there are cases reported where cyber criminals used and/or targeted such cloud services to commit malicious activities such as identity theft, privacy issues, malware, sexual harassment and cyber terrorism etc. The retrieval of evidences from cloud storage services such as Google Drive, DropBox and OneDrive etc., have been identified as an emerging challenges for digital forensic researchers and examiners. There is a need for a sound digital forensic knowledge relating to the forensic analysis of cloud storage services to identify potential digital evidences. Google Drive is a popular cloud storage service and in this research paper, I did detail study of artifact left behind by Google Drive using Registry changes while installation or un-installation process; File system analysis while login or logout process, uploading, downloading or deletion of files; Analysis of Log and memory analysis to identify artifacts of forensic interest. During the research, the hash of the extracted data/artifacts on the cloud is checked with the original data/artifacts to establish the integrity. Timestamp information may be a crucial aspect of an investigation and therefore it is important to record the information available, and to understand the circumstances relating to a timestamp on a file.

KEYWORDS: Google Drive, Dropbox, OneDrive, RAM Forensics, Man-In-The-Cloud.

1.0 INTRODUCTION

Cloud computing is a form of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand [1]. Due to rapid development of technology related to internet, cloud computing and mobile device, people can access resources from anywhere and anytime. Cloud storage services such as Google Drive, DropBox and OneDrive etc. plays an important role in the information sharing [3] on internet because person can store data on cloud, sync those data with PC / mobile device or share all kind of data or personal data publically or with specific person.

According to the report [4] published by the Imperva Hacker Intelligence Initiative cyber security company and it shows that hackers may now easily get access to all users' files in cloud services such as Google Drive, Microsoft OneDrive, Dropbox [2], if they are able to get into the computer, on which the clients of these services are installed. Moreover, the hackers won't need the logins and passwords to access data in the users' accounts [5]. Moreover new type of attack called 'Man-In-The-Cloud' (MITC) that allows hackers to access cloud storage services without the need for a password [6]. Such cybercrime cases reported recently shows that cyber criminals used and/or targeted such cloud services to perform malicious activities.

Cloud storage services can be used to store, access and distribute data via remote infrastructure in overseas jurisdictions to avoid the scrutiny of law enforcement agencies [7]. Digital forensics of cloud storage services has always been emerging challenges for digital forensic researchers and examiners. In this research paper, using various digital forensic techniques artifacts were identified that are likely to be left by the Google Drive.

The rest of paper is organized as follows. In section 2, I discussed literature survey of existing related research work. I focused on methodology and preparation of research along with result analysis in section 3. Paper is concluded with research outcome comments in section 4.

2.0 Related Research work:

McClain discussed forensics of Dropbox installed on window 7 OS [8], Darren Quick discussed forensics of Dropbox installed on windows 7 OS and Apple iPhone [9], Chung conducted forensics on verities of cloud storage services installed on different OS [10], Darren Quick shown forensics of Microsoft SkyDrive installed on computer and iPhone [11], S. Mehreen discussed different digital forensics techniques to extract evidences from Dropbox running on Window 8 OS [12] and lastly Ming Sang Chang conducted forensics of Google Drive on windows XP, windows 7 and windows 8 [13].

All of the above mentioned research conducted on Dropbox and Google Drive and artifacts were collected using registry changes or installation or un-installation process. In this research paper artifacts left behind by the Google

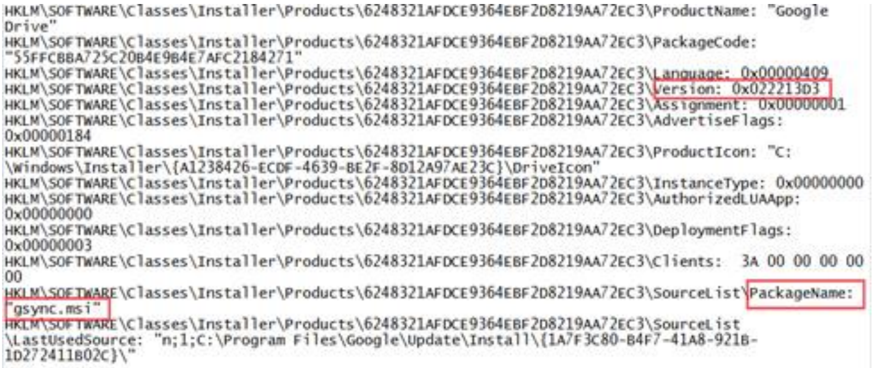
Drive were collected using Registry changes, File system analysis, log analysis and memory analysis in different scenario.

3.0 Methodology and Preparation of Research:

The aim and objective of the research is to collect artifacts form Google Drive once user has accessed it. Adopted methodology carry out during the entire research is divided in four phases 1. Registry changes analysis using RegShot 2. File system changes analysis using DiskPulse 3. Log analysis of Sync_log file 5. Ram analysis using FTK. I configured cloud storage Google Drive application on virtual machine with the configuration of windows 7, 18 GB HDD and 2 GB RAM. Following activities performed to make different situations,

1. Start RegShot and Save the first instance of it.
2. Install the cloud application and capture the 2nd instance using RegShot.
3. Compare both the instances to know the changes made in the registry.
4. Monitor the changes in the file system while uploading, updating and deleting the files using DiskPulse
5. Calculate the Hash of the files to verify integrity of the file
6. Uninstall the application and monitor the changes in the registry
7. Capture the memory of the virtual instance to understand the artifacts left in the Memory

Purpose behind creating such different situations is to know what kind of artifacts with their attributes and location left behind by the Google Drive in particular scenario. Research with verities of scenario helps digital forensic researchers or examiners to handle real time cases related to cloud storage services.



```
HKLM\SOFTWARE\Classes\Installer\Products\6248321AFDCE9364EBF2D8219AA72EC3\ProductName: "Google
Drive"
HKLM\SOFTWARE\Classes\Installer\Products\6248321AFDCE9364EBF2D8219AA72EC3\PackageCode:
"55FFCBBA725C20B4E9B4E7AFC2184271"
HKLM\SOFTWARE\Classes\Installer\Products\6248321AFDCE9364EBF2D8219AA72EC3\Language: 0x00000409
HKLM\SOFTWARE\Classes\Installer\Products\6248321AFDCE9364EBF2D8219AA72EC3\Version: 0x022213D3
HKLM\SOFTWARE\Classes\Installer\Products\6248321AFDCE9364EBF2D8219AA72EC3\Assignment: 0x00000001
HKLM\SOFTWARE\Classes\Installer\Products\6248321AFDCE9364EBF2D8219AA72EC3\AdvertiseFlags:
0x00000184
HKLM\SOFTWARE\Classes\Installer\Products\6248321AFDCE9364EBF2D8219AA72EC3\ProductIcon: "C:
\Windows\Installer\{A1238426-ECDF-4639-BE2F-8D12A97AE23C}\DriveIcon"
HKLM\SOFTWARE\Classes\Installer\Products\6248321AFDCE9364EBF2D8219AA72EC3\InstanceType: 0x00000000
HKLM\SOFTWARE\Classes\Installer\Products\6248321AFDCE9364EBF2D8219AA72EC3\AuthorizedLUAApp:
0x00000000
HKLM\SOFTWARE\Classes\Installer\Products\6248321AFDCE9364EBF2D8219AA72EC3\DeploymentFlags:
0x00000003
HKLM\SOFTWARE\Classes\Installer\Products\6248321AFDCE9364EBF2D8219AA72EC3\Clients:  3A 00 00 00 00
00
HKLM\SOFTWARE\Classes\Installer\Products\6248321AFDCE9364EBF2D8219AA72EC3\SourceList\PackageName:
"gsync.msi"
HKLM\SOFTWARE\Classes\Installer\Products\6248321AFDCE9364EBF2D8219AA72EC3\SourceList
\LastUsedSource: "n;1;C:\Program Files\Google\Update\Install\{1A7F3C80-B4F7-41A8-921B-
1D272411B02C}\"
```

Figure 1 Registry Artifacts (Install)

3.1 Registry changes analysis: After the installation of Google Drive in windows 7 machine, installation related artifacts (Figure 1) such as version and package was found from registry of windows 7. Registry instance taken using RegShot during the installation of Google Drive and it was found that while installation of Google Drive - 8 keys deleted, 596 keys added, 957 values deleted, 892 values added, 25 values modified and total changes was 2478.

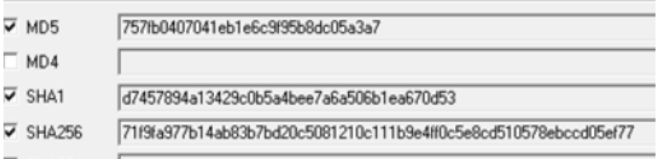
3.2 File system changes: To record the changes in the file system following sub-scenario was created and changes in the file system were observed using DiskPulse for every scenario,

3.2.1 User Login :

Whenever any login process is attempted there are various changes in the file system which was recorded by DiskPluse and it was observed that 42 NOEXT files, 12 Txt files, 5 DAT files, 3 PNG files, 2 GIF fiels, 2 LOG1 files, 1 LOG files and 1 DB-WAL files were created. It was also observed that during login process 45 files were modified, 19 files were created and 4 files were deleted.

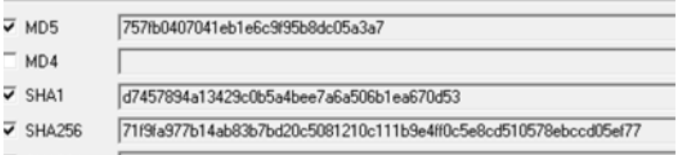
3.2.2 File upload:

The File “Digital-Evidence.jpg” was uploaded in Google Drive, after the file was uploaded the hash value of both the source file and the file uploaded on the cloud was calculated (Figure 2, 3) to verify its integrity. It was observed that during file upload, 27 NOEXT files, 21 DAT files, 11 TMP files, 8 LOG1 files, 5 DB-JOURNAL files, 4 Log files, 4 PNG files, 3 DB-WAL files and 9 other files were created. It was also observed that 172 files were modified, 30 files were created, 14 were deleted and 8 files were renamed.



☑ MD5 757fb0407041eb1e6c9f95b8dc05a3a7
☐ MD4
☑ SHA1 d7457894a13429c0b5a4bee7a6a506b1ea670d53
☑ SHA256 71f9fa977b14ab83b7bd20c5081210c111b9e4ff0c5e8cd510578ebccd05ef77

Figure 3 Hash value of image before uploading image

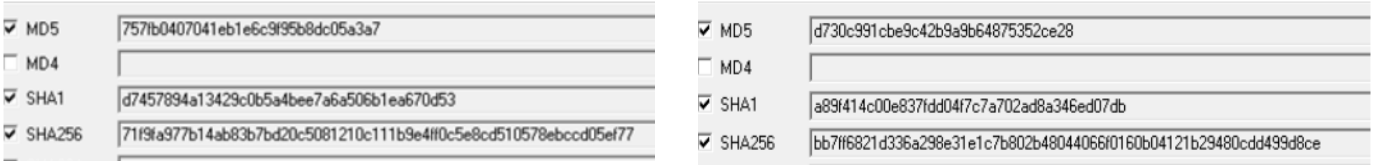


☑ MD5 757fb0407041eb1e6c9f95b8dc05a3a7
☐ MD4
☑ SHA1 d7457894a13429c0b5a4bee7a6a506b1ea670d53
☑ SHA256 71f9fa977b14ab83b7bd20c5081210c111b9e4ff0c5e8cd510578ebccd05ef77

Figure 2 Hash value of image after uploading image

3.2.3 Update and Delete file:

The file named "Digital-Evidence.jpg" which was uploaded on Google drive; was updated and changes in the file system were observed. Hash value (Figure 4) was calculated to see that image was changed or not. After the update, It was observed that 11 NOEXT , 10 JPG files, 5 LOG1 files, 5 DB-WAL files, 5 DAT files, 2 AUTOMATICDESTINATIONS-MS, DRIVEDOWNLOAD files, 1 PF files were affected. After a deletion of image file 7 NOEXT files, 5 LOG1 files, 4 DAT files, 2 DB-WAL files and 1 JPG file were changed



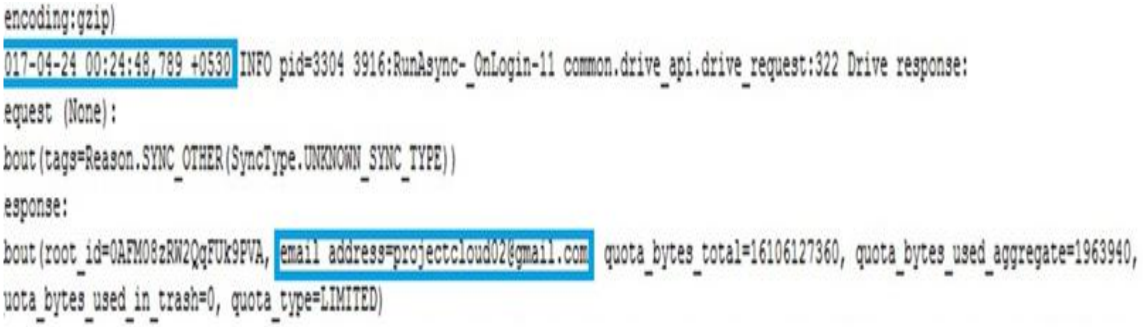
☑ MD5 757fb0407041eb1e6c9f95b8dc05a3a7
☐ MD4
☑ SHA1 d7457894a13429c0b5a4bee7a6a506b1ea670d53
☑ SHA256 71f9fa977b14ab83b7bd20c5081210c111b9e4ff0c5e8cd510578ebccd05ef77

☑ MD5 d730c991cbe9c42b9a9b64875352ce28
☐ MD4
☑ SHA1 a89f414c00e837fdd04f7c7a702ad8a346ed07db
☑ SHA256 bb7ff6821d336a298e31e1c7b802b48044066f0160b04121b29480cdd499d8ce

Figure 4 Hash value of image before alteration and after alteration

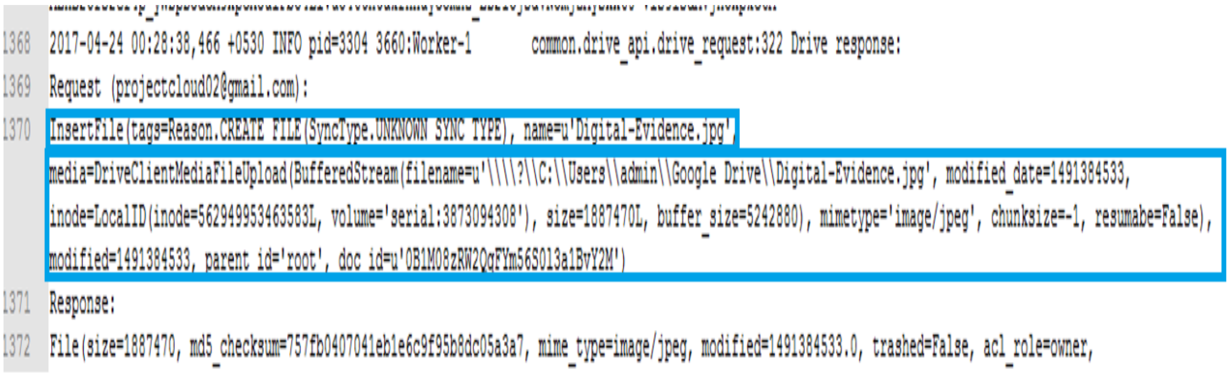
When the file was deleted from Google Drive and changes in the file systems was observed. It was found that 7 NOEXT files, 5 LOG1 files, 4 DAT files, 2 DB-WAL files and 1 JPG files were changed.

3.3 Log analysis: Sync_log.log is log file containing information about the client sync session and this file contains information about sync sessions, file created, file saved and file deleted. For a digital forensic examiner , sync_log.log file is a very important and I found artifacts related to email-id and last login date and time (Figure 5), upload file detail (Figure 6.) , deleted file detail (Figure 7) and last access time (Figure 8).

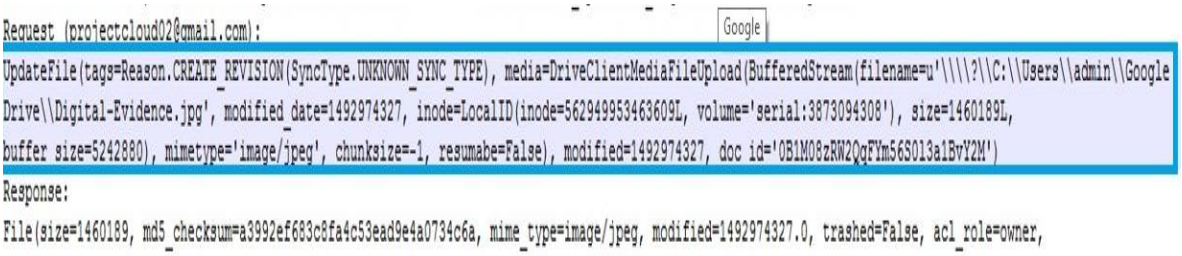


```
encoding:gzip)
017-04-24 00:24:48,789 +0530 INFO pid=3304 3916:RunAsync-_OnLogin-11 common.drive_api.drive_request:322 Drive response:
equest (None):
bout(tags=Reason.SYNC_OTHER(SyncType.UNKNOWN_SYNC_TYPE))
esponse:
bout(root_id=0AFM08zRW2QqFUk9PVA, email address=projectcloud02@gmail.com quota_bytes_total=16106127360, quota_bytes_used_aggregate=1963940,
uota_bytes_used_in_trash=0, quota_type=LIMITED)
```

Figure 5 Login Email ID & Login Date and Time – Google Drive

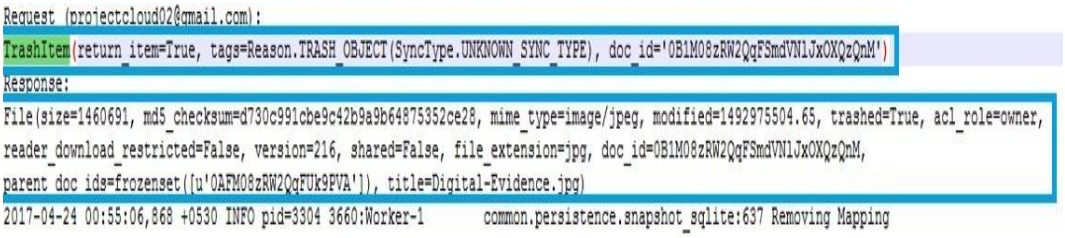


```
2017-04-24 00:28:38,466 +0530 INFO pid=3304 3660:Worker-1       common.drive_api.drive_request:322 Drive response:
Request (projectcloud02@gmail.com):
InsertFile(tags=Reason.CREATE FILE(SyncType.UNKNOWN SYNC TYPE), name=u'Digital-Evidence.jpg',
media=DriveClientMediaFileUpload(BufferedStream(filename=u'\\\\?\\C:\\Users\\admin\\Google Drive\\Digital-Evidence.jpg', modified_date=1491384533,
inode=LocalID(inode=562949953463583L, volume='serial:3873094308'), size=1887470L, buffer_size=5242880), mimetype='image/jpeg', chunksize=-1, resumabe=False),
modified=1491384533, parent id='root', doc id=u'0B1M08zRW2QqFYm56S013a1BvY2M')
Response:
File(size=1887470, md5_checksum=757fb0407041eb1e6c9f95b8dc05a3a7, mime_type=image/jpeg, modified=1491384533.0, trashed=False, acl_role=owner,
```



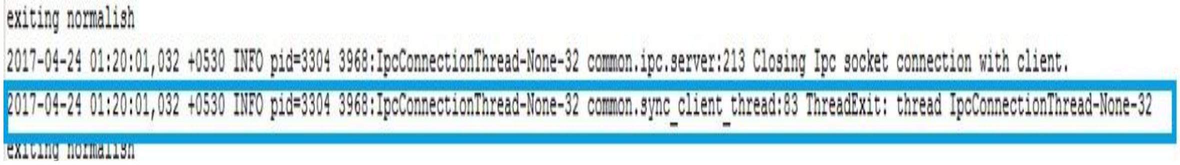
```
Request (projectcloud02@gmail.com):                                   Google
UpdateFile(tags=Reason.CREATE_REVISION(SyncType.UNKNOWN_SYNC_TYPE), media=DriveClientMediaFileUpload(BufferedStream(filename=u'\\\\?\\C:\\Users\\admin\\Google
Drive\\Digital-Evidence.jpg', modified_date=1492974327, inode=LocalID(inode=562949953463609L, volume='serial:3873094308'), size=1460189L,
buffer size=5242880), mimetype='image/jpeg', chunksize=-1, resumabe=False), modified=1492974327, doc id='0B1M08zRW2QgFYm56S013a1BvY2M')
Response:
File(size=1460189, md5_checksum=a3992ef683c8fa4c53ead9e4a0734c6a, mime_type=image/jpeg, modified=1492974327.0, trashed=False, acl_role=owner,
```

Figure 6 Uploaded File Details - Google Drive



```
Request (projectcloud02@gmail.com):
TrashItem(return_item=True, tags=Reason.TRASH_OBJECT(SyncType.UNKNOWN_SYNC_TYPE), doc_id='0B1M08zRW2QgFSmdVN1JxOXQzQnM')
Response:
File(size=1460691, md5_checksum=d730c991cbe9c42b9a9b64875352ce28, mime_type=image/jpeg, modified=1492975504.65, trashed=True, acl_role=owner,
reader_download_restricted=False, version=216, shared=False, file_extension=jpg, doc_id=0B1M08zRW2QgFSmdVN1JxOXQzQnM,
parent doc ids=frozenset([u'0AFM08zRW2QgFUk9PVA']), title=Digital-Evidence.jpg)
2017-04-24 00:55:06,868 +0530 INFO pid=3304 3660:Worker-1       common.persistence.snapshot_sqlite:637 Removing Mapping
```

Figure 7 Deleted File Details – Google Drive

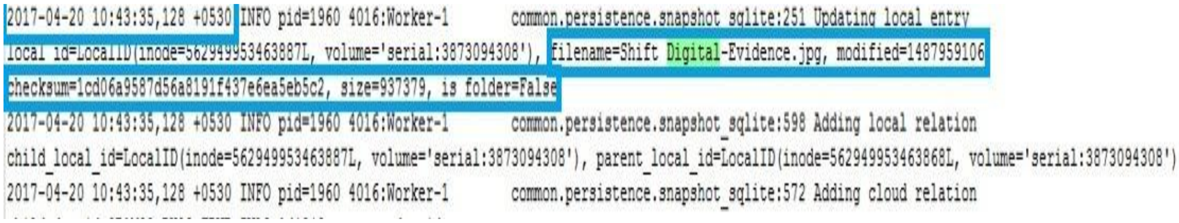


```
exiting normalish
2017-04-24 01:20:01,032 +0530 INFO pid=3304 3968:IpcConnectionThread-None-32 common.ipc.server:213 Closing Ipc socket connection with client.
2017-04-24 01:20:01,032 +0530 INFO pid=3304 3968:IpcConnectionThread-None-32 common.sync_client_thread:83 ThreadExit: thread IpcConnectionThread-None-32
exiting normalish
```

Figure 8 Last Access time – Google Drive

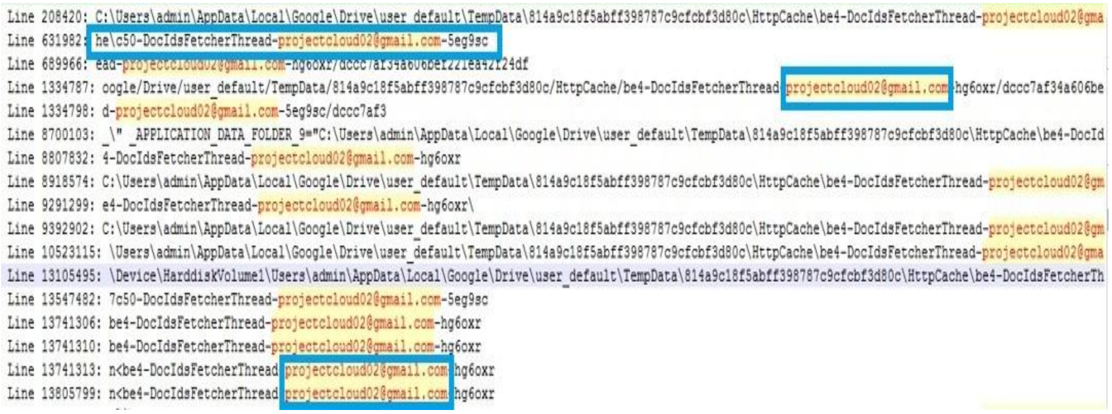
3.4 Memory Forensics:

Memory forensics is forensic analysis of a computer's memory dump. It's primary application is investigation of advanced computer attacks which are stealthy enough to avoid leaving artifacts on the computer's hard drive [14] and RAM forensics can capture the current state of a machine in a way that is not possible using disk analysis alone [15]. I used FTK imager to take the RAM dump and Sysinternal's tool string is used to convert RAM dump to string. I found artifacts related to email address and file path (Figure 10) and file details (Figure 9) from the analysis of RAM dump.



```
2017-04-20 10:43:35,128 +0530 INFO pid=1960 4016:Worker-1       common.persistence.snapshot sqlite:251 Updating local entry
local id=LocalID(inode=562949953463887L, volume='serial:3873094308'), filename=Shift Digital-Evidence.jpg, modified=1487959106
checksum=1cd06a9587d56a8191f437e6ea5eb5c2, size=937379, is folder=False
2017-04-20 10:43:35,128 +0530 INFO pid=1960 4016:Worker-1       common.persistence.snapshot_sqlite:598 Adding local relation
child_local_id=LocalID(inode=562949953463887L, volume='serial:3873094308'), parent_local_id=LocalID(inode=562949953463868L, volume='serial:3873094308')
2017-04-20 10:43:35,128 +0530 INFO pid=1960 4016:Worker-1       common.persistence.snapshot_sqlite:572 Adding cloud relation
```

Figure 9 Artifacts related to File Details on RAM



```
Line 208420: C:\Users\admin\AppData\Local\Google\Drive\user_default\TempData\814a9c18f5abff398787c9cfcbf3d80c\HttpCache\be4-DocIdsFetcherThread-projectcloud02@gma
Line 631982: he\c50-DocIdsFetcherThread-projectcloud02@gmail.com-5eg9sc
Line 689966: ead-projectcloud02@gmail.com-hg6oxr/dccc7af34a606bef221ea42f24df
Line 1334787: oogle/Drive/user_default/TempData/814a9c18f5abff398787c9cfcbf3d80c/HttpCache/be4-DocIdsFetcherThread projectcloud02@gmail.com hg6oxr/dccc7af34a606be
Line 1334798: d-projectcloud02@gmail.com-5eg9sc/dccc7af3
Line 8700103: _\" _APPLICATION_DATA_FOLDER_9="C:\Users\admin\AppData\Local\Google\Drive\user_default\TempData\814a9c18f5abff398787c9cfcbf3d80c\HttpCache\be4-DocId
Line 8807832: 4-DocIdsFetcherThread-projectcloud02@gmail.com-hg6oxr
Line 8918574: C:\Users\admin\AppData\Local\Google\Drive\user_default\TempData\814a9c18f5abff398787c9cfcbf3d80c\HttpCache\be4-DocIdsFetcherThread-projectcloud02@gm
Line 9291299: e4-DocIdsFetcherThread-projectcloud02@gmail.com-hg6oxr\
Line 9392902: C:\Users\admin\AppData\Local\Google\Drive\user_default\TempData\814a9c18f5abff398787c9cfcbf3d80c\HttpCache\be4-DocIdsFetcherThread-projectcloud02@gm
Line 10523115: \Users\admin\AppData\Local\Google\Drive\user_default\TempData\814a9c18f5abff398787c9cfcbf3d80c\HttpCache\be4-DocIdsFetcherThread-projectcloud02@gma
Line 13105495: \Device\HarddiskVolume1\Users\admin\AppData\Local\Google\Drive\user_default\TempData\814a9c18f5abff398787c9cfcbf3d80c\HttpCache\be4-DocIdsFetcherTh
Line 13547482: 7c50-DocIdsFetcherThread-projectcloud02@gmail.com-5eg9sc
Line 13741306: be4-DocIdsFetcherThread-projectcloud02@gmail.com-hg6oxr
Line 13741310: be4-DocIdsFetcherThread-projectcloud02@gmail.com-hg6oxr
Line 13741313: n<be4-DocIdsFetcherThread projectcloud02@gmail.com hg6oxr
Line 13805799: n<be4-DocIdsFetcherThread projectcloud02@gmail.com hg6oxr
```

Figure 10 Artifacts related to Email and File path on RAM

4.0 Conclusion

File storage and synchronization cloud services such as Google Drive, DropBox and OneDrive etc. provide features through which person can store data, sync data with PC / mobile device or share with anyone in the internet. On one side cybercrime criminals used and/or targeted such cloud services to commit malicious activities and on another side forensics related cloud storage services have been identified as emerging challenges for digital forensic researchers and examiners. In this research paper, I discussed digital forensic techniques such as registry analysis, file system analysis, log analysis and memory forensics is used to collect artifacts left by the Google Drive. While applying these digital forensic techniques, I created verities of scenario which helps digital forensic examiner to help real time cases related to cloud storage services.

References

[1]. Hassan, Qusay (2011). "Demystifying Cloud Computing" (PDF). The Journal of Defense Software Engineering. CrossTalk. 2011 (Jan/Feb): 16–21. Retrieved 11 December 2008.

[2]. Haghighat, M., Zonouz, S., & Abdel-Mottaleb, M. CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification. Expert Systems with Applications, 2015;42(21):7905–7916.

[3]. "Google Drive, Dropbox, Box and iCloudReach the Top 5 Cloud Storage Security Breaches List". psg.hitachi-solutions.com. Retrieved 2015-11-22.

[4]. https://www.imperva.com/aspxerrorpath=/docs/imperva_Hacker_Intelligence_Initiative_No22_Jul2015_v1d.pdf

[5]. Spinbackup Team, https://spinbackup.com/blog/a-new-easy-way-to-hack-your-google-drive/, August 18, 2015

[6]. Dropbox, Google Drive and OneDrive users at risk from 'man-in-the-cloud' attacks, https://www.theinquirer.net/inquirer/news/2421076/dropbox-and-onedrive-at-risk-from-malware-injecting-man-in-the-cloud-attacks.

[7]. Biggs, S &Vidalis, S. Cloud Computing: The Impact on Digital Forensic Investigations. Proceedings of IEEE International Conference for Internet Technology and Secured Transactions. 2009;1–6.

[8]. McClain, F. Dropbox Forensics. 2011; https://articles.forensicfocus.com/2011/07/24/dropboxforensics/(Access on Jul 20, 2016).

[9]. D. Quick and K.-K. R. Choo, Dropbox analysis: Data remnants on user machines. Digital Investigation. 2013;10(1): 3-18.

[10]. Chung, H, Park, J, Lee, S & Kang, C (2012), Digital Forensic Investigation of Cloud Storage Services, Digital Investigation. 2012; 9(2): 81–95.

[11]. Darren Quick, Kim-Kwang Raymond Choo, "Digital droplets: Microsoft SkyDrive forensic data remnants," Future Generation Computer Systems. 2013;29(6):1378-1394.

[12]. S. Mehreen, B. Aslam. Windows 8 Cloud Storage Analysis: Dropbox Forensics. International Bhurban Conference on Applied Sciences & Technology. 2015;312-317

[13]. Ming Sang Chang, "Forensic Analysis of Google Drive on Windows ", IJISET - International Journal of Innovative Science, Engineering & Technology - Vol. 3 Issue 8, August 2016: ISSN (Online) 2348 – 7968,

[14]. Simson L. Garfinkel, "Digital forensics research: The next 10 years" , digital investigation 7 (2010) S64 eS73

[15]. Vrizlynn L. L. Thing , Kian-Yong Ng , Ee-Chien Chang , "Live memory forensics of mobile phones" digital investigation 7 (2010)