


ARTIFACTS OF GOOGLE DRIVE USAGE IN WINDOWS

 digitalinvestigator.blogspot.com/2021/03/artifacts-of-google-drive-usage-on.html

Joseph Moronwi

Google drive is an online file storage and sharing service from Google that supports sharing of different types of files such as pictures, videos, documents, spreadsheets, presentations, etc. The service supports various devices including desktops, mobiles, etc. through different modes such as desktop client, web portal, mobile applications etc.

The users can also invite others to view, download, and collaborate on the files. The storage works in collaboration with Google docs, sheets, and slides, an office suite that allows users to edit the documents, spreadsheets, presentations, and so on, online.

Google Drive Forensic Artifacets

Google Drive's native app name is **Backup and Sync from Google**. After installing the application, the following entries will be created on the root drive.

Directories created when Google Drive is installed	
<SYSTEMROOT>\Program Files\Google\Drive	In this folder you will find the executable file of the application
<SYSTEMROOT>\Program Files (x86)\Google\Drive	Here you will find information about the updates of the application
<SYSTEMROOT>\Users\ <username>\GoogleDrive	This is the default folder used for synchronizing the user's files with Google Drive cloud service
<SYSTEMROOT>\Users\ <username>\AppData\Local\Google\Drive	Here you will find all the native app's files that store information about the app and the user's data

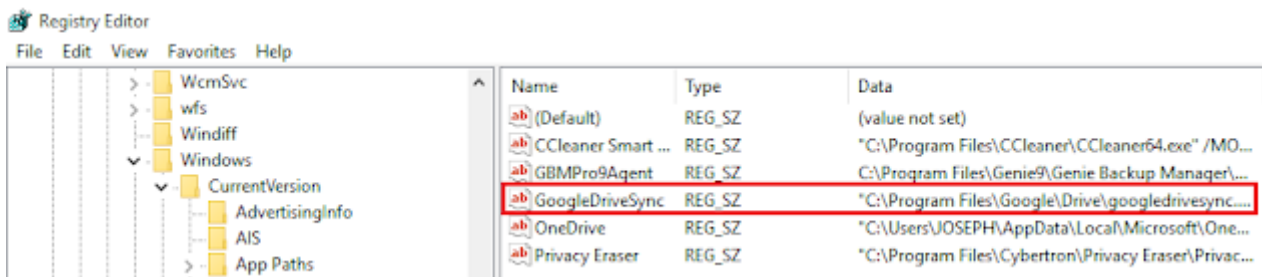
Registry

The installation of Google drive creates various keys and values inside the Registry. View the registry hives listed below in the forensic image of the suspect's hard disk.

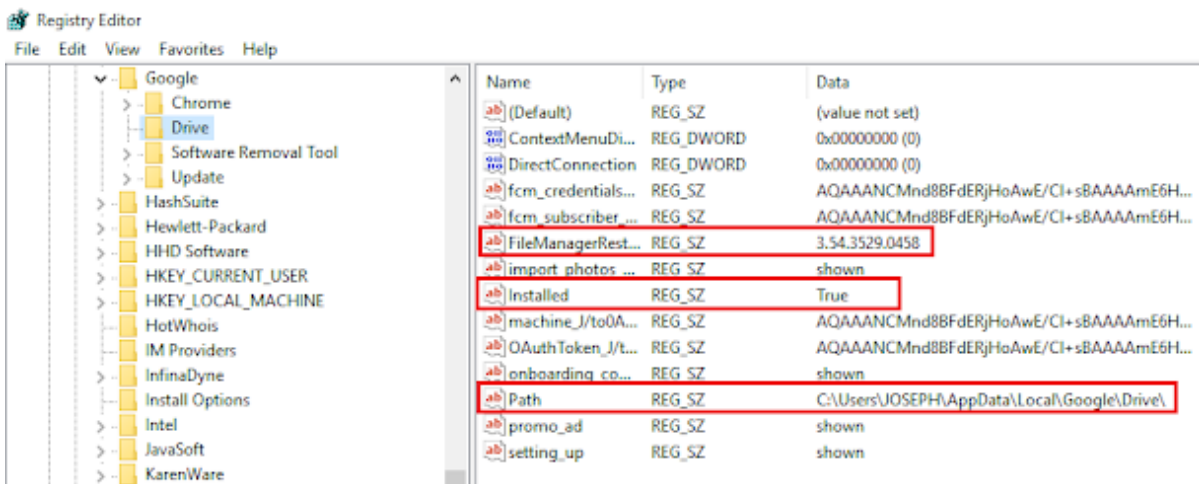
- SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders
- SOFTWARE\Google\Drive
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run\GoogleDriveSync
- NTUSER.DAT\Software\Classes

From the Registry we can obtain the **installed version** and the **user folder**.

Let's check the Registry to see if the sync process starts automatically with the user's login. The right key to view here is
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run



The version and installation of Google Drive in Window's Registry can be found at
NTUSER.DAT\Software\Google\Drive.



Event Log

We can also determine the installation of Google drive on the hard disk of the suspect by viewing the details of the following event log.

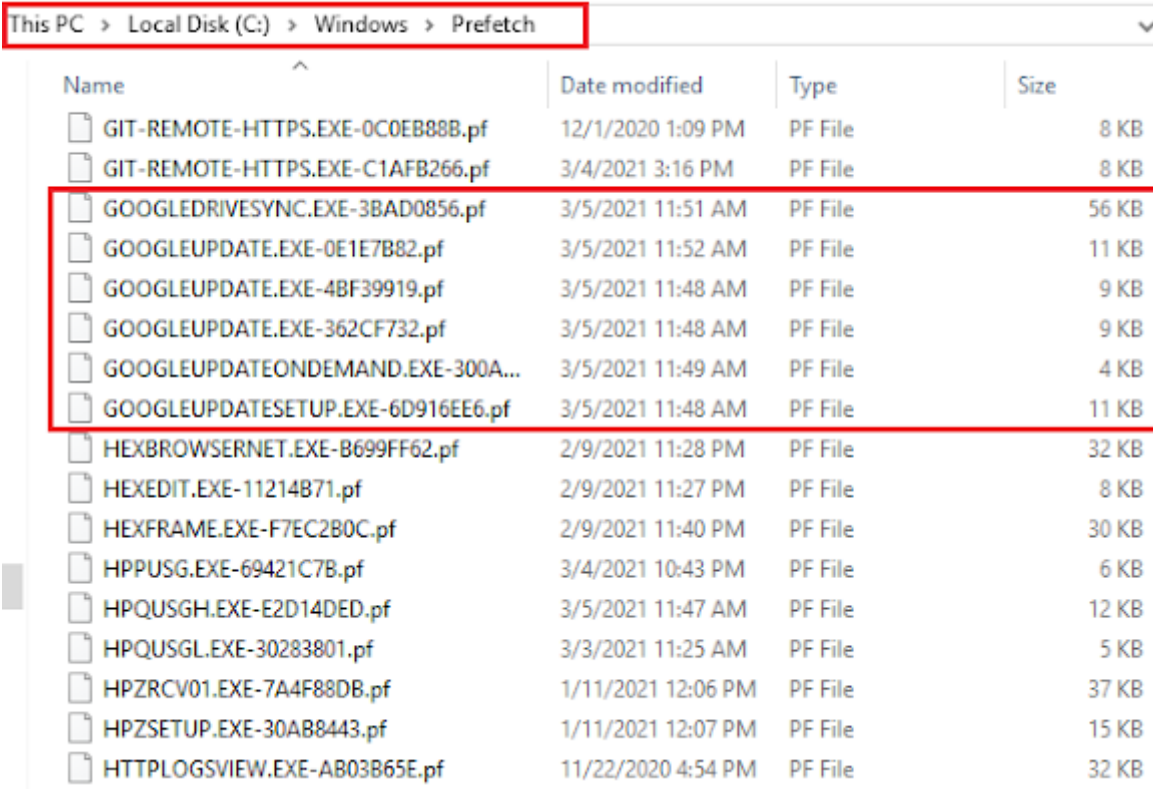
Path	<SYSTEMROOT>\Windows\System32\winevt\Logs\Application.evtx
Event ID	1033
Event Description Summary	Windows installer installed the product

Provider Name	MsiInstaller
Event Data	Among others "<EventData> <Data> Backup and Sync From Google3.43.2448.907110330Google,Inc.(NULL)</Data>"

To determine the execution of the Google drive application by the suspect, there are plethora of artifacts to look out for.

Prefetch

Windows stores Prefetch files at <SYSTEMROOT>\Windows\Prefetch. Prefetch files are all named using common naming criteria. The name of the running application comes first, then comes an eight-character hash of the location where the application was run, and finally it ends with the .PF extension.



Name	Date modified	Type	Size
GIT-REMOTE-HTTPS.EXE-0C0EB88B.pf	12/1/2020 1:09 PM	PF File	8 KB
GIT-REMOTE-HTTPS.EXE-C1AFB266.pf	3/4/2021 3:16 PM	PF File	8 KB
GOOGLEDRIVESYNC.EXE-3BAD0856.pf	3/5/2021 11:51 AM	PF File	56 KB
GOOGLEUPDATE.EXE-0E1E7B82.pf	3/5/2021 11:52 AM	PF File	11 KB
GOOGLEUPDATE.EXE-4BF39919.pf	3/5/2021 11:48 AM	PF File	9 KB
GOOGLEUPDATE.EXE-362CF732.pf	3/5/2021 11:48 AM	PF File	9 KB
GOOGLEUPDATEONDEMAND.EXE-300A...	3/5/2021 11:49 AM	PF File	4 KB
GOOGLEUPDATESETUP.EXE-6D916EE6.pf	3/5/2021 11:48 AM	PF File	11 KB
HEXBROWSERNET.EXE-B699FF62.pf	2/9/2021 11:28 PM	PF File	32 KB
HEXEDIT.EXE-11214B71.pf	2/9/2021 11:27 PM	PF File	8 KB
HEXFRAME.EXE-F7EC2B0C.pf	2/9/2021 11:40 PM	PF File	30 KB
HPPUSG.EXE-69421C7B.pf	3/4/2021 10:43 PM	PF File	6 KB
HPQUSGH.EXE-E2D14DED.pf	3/5/2021 11:47 AM	PF File	12 KB
HPQUSGL.EXE-30283801.pf	3/3/2021 11:25 AM	PF File	5 KB
HPZRCV01.EXE-7A4F88DB.pf	1/11/2021 12:06 PM	PF File	37 KB
HPZSETUP.EXE-30A88443.pf	1/11/2021 12:07 PM	PF File	15 KB
HTTPLOGSVIEW.EXE-AB03B65E.pf	11/22/2020 4:54 PM	PF File	32 KB

You can parse the prefetch file with Eric Zimmerman's PECmd to obtained a more detailed information. A truncated output is shown below.

```
04. Administrator: Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>PECmd.exe -f "C:\Windows\Prefetch\GOOGLEDRIVESYNC.EXE-3BAD0856.pf"
PECmd version 1.4.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -f C:\Windows\Prefetch\GOOGLEDRIVESYNC.EXE-3BAD0856.pf

Keywords: temp, tmp

Processing 'C:\Windows\Prefetch\GOOGLEDRIVESYNC.EXE-3BAD0856.pf'

Created on: 2021-03-05 10:50:24
Modified on: 2021-03-05 10:51:27
Last accessed on: 2021-03-05 10:50:24

Executable name: GOOGLEDRIVESYNC.EXE
Hash: 3BAD0856
File size (bytes): 313,890
Version: Windows 10

Run count: 2
Last run: 2021-03-05 10:51:10
Other run times: 2021-03-05 10:49:55

Volume information:
```

LNK (Shortcut) Files

LNK files hold a wealth of useful information about the computer at which the file was first created time in addition to the computer where it resides currently. For Google drive, the files to look out for are:

- <SYSTEMROOT>\Users\<username>\Desktop\Google Drive.lnk
- <SYSTEMROOT>\Users\<username>\Links\Google Drive.lnk
- <SYSTEMROOT>\ProgramData\Microsoft\Windows\Start Menu\Programs\Google Drive\Google Drive.lnk

You can parse each of these lnk files with Eric Zimmerman's LECmd for detailed information. A truncated output is shown below.

```
Administrator Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>LECmd.exe -f "C:\Users\JOSEPH\Desktop\Google Drive.lnk"
LECmd version 1.4.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd

Command line: -f C:\Users\JOSEPH\Desktop\Google Drive.lnk

Processing 'C:\Users\JOSEPH\Desktop\Google Drive.lnk'

Source file: C:\Users\JOSEPH\Desktop\Google Drive.lnk
Source created: 2021-03-05 10:54:05
Source modified: 2021-03-05 10:54:05
Source accessed: 2021-03-05 10:54:05

--- Header ---
Target created: 2021-03-05 10:54:04
Target modified: 2021-03-05 10:54:04
Target accessed: 2021-03-05 10:54:04

File size: 0
Flags: HasTargetIdList, HasLinkInfo, HasName, HasRelativePath, HasIconLocation, IsUnicode, HasExpIcon
File attributes: FileAttributeReadOnly, FileAttributeDirectory
Icon index: 15
Show window: SWNormal (Activates and displays the window. The window is restored to its original size and position if
the window is minimized or maximized.)
```

Database Artifacts

To find evidence of usage of the application, the examiner will have to examine valuable information that can be stored in the following databases of the application.

- <SYSTEMROOT>\Users\<username>\AppData\Local\Google\Drive\user_default\snapshot.db
- <SYSTEMROOT>\Users\<username>\AppData\Local\Google\Drive\user_default\sync_config.db
- <SYSTEMROOT>\Users\<username>\AppData\Local\Google\Drive\cloud_graph\cloud_graph.db
- <SYSTEMROOT>\Users\<username>\AppData\Local\Google\Drive\global.db

You should definitely check the above databases as they are full of valuable information.

Sync_config.db

The sync_config.db is a SQLite3 dB which contain profile configuration like:

- Client version installed
- Local sync root path
- User email

DB Browser for SQLite - C:\Users\JOSEPH\AppData\Local\Google\Drive\user_default\sync_config.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Pro

Database Structure Browse Data Edit Pragma Execute SQL

Table: data

	entry_key	data_key	data_value
	Filter	Filter	Filter
1	upgrade_number	value	48
2	highest_app_version	value	3.54.3529.0458
3	cloud_docs_feed_mode	value	0
4	rlz_brand_code	value	GGLS
5	feature_switch	value	gAJy29tbW9uLmZlYXR1cmVfc3dpd...
6	shown_setup_overlays	setup_overlay...	choose_folders_setup_overlay
7	shown_setup_overlays	setup_overlay...	google_drive_setup_overlay
8	selective_sync	value	0
9	usb_sync_enabled	value	1
10	show_unparent_warni...	value	1
11	delete_mode	value	1
12	storage_policy_mode	value	original
13	always_show_in_photos	value	0
14	share_notification	value	1
15	local_sync_root_path	value	\\?\C:\Users\JOSEPH\Google Drive
16	copy_duplicate_photos	value	1
17	user_email	value	moronwiayodelej@gmail.com
18	user_id	value	105428331405681916311

Snapshot.db

The snapshot.db is a SQLite3 dB that contains information about local and cloud entries

- Cloud_entry table
 - File name
 - Created (UNIX timestamp)
 - Modified (UNIX timestamp)
 - URL
 - Checksum (MD5 hash)
 - Size
 - Shared
- Local_entry
 - File name
 - Modified (UNIX timestamp)

- Checksum (Md5 hash)
- Size

DB Browser for SQLite - C:\Users\JOSEPH\AppData\Local\Google\Drive\user_default\snapshot.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragma Execute SQL

Table: cloud_entry

	doc_id	filename	modified	created	acl_role	doc_type	removed	size	checksum
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	root	root	NULL	NULL	NULL	0	NULL	NULL	NULL
2	1c18YjID21MF...	Pictures	NULL	NULL	NULL	0	NULL	NULL	NULL
3	1Aztg4Hh9ku...	Desktop	NULL	NULL	NULL	0	NULL	NULL	NULL
4	1rv0t1Lc_odN...	Documents	NULL	NULL	NULL	0	NULL	NULL	NULL
5	113asznIMNY...	Blogger docu...	1609691164	NULL	0	0	0	NULL	NULL
6	1-VYhipxRwA...	Baby Clara	1590645590	NULL	0	0	0	NULL	NULL
7	1e4fQsV8w9q...	Opt-Out Doc.x...	1612540117	NULL	0	1	0	24071	3cfced4f7
8	1GR7YVRfx7iq...	Bellingcat's O...	1612539022	NULL	0	1	0	3249504	452218e1
9	119VS2eQnW...	certificate.pdf	1610046958	NULL	0	1	0	94527	a950e02c
10	1zkfOijtqCp8y...	file	1607895595	NULL	0	4	0	NULL	NULL
11	1UWekS7W2s...	file	1607895532	NULL	0	1	0	19951	258975bb
12	1ZNFWFyOYc...	file	1607895479	NULL	0	4	0	NULL	NULL
13	111wNO6-mU...	ECC-Evaluatio...	1606222928	NULL	0	1	0	1078268	f6545a7f
14	1527vQ-ViQik...	file	1607895478	NULL	0	4	0	NULL	NULL
15	1I3-wN86Jkw...	file	1607895475	NULL	0	1	0	19951	258975bb
16	1x1yR3HZmo...	IMG-2020090...	1599153502	NULL	0	1	0	77579	c69553b4
17	10wDXVNxekw...	IMG_2020052...	1590646127	NULL	0	1	0	3885318	10644494

From the above, you can find important information about the synced files' metadata, such as hash value and last modified timestamp.

DB Browser for SQLite - C:\Users\JOSEPH\AppData\Local\Google\Drive\user_default\snapshot.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragma Execute SQL

Table: cloud_entry

	novod	size	checksum	shared	resource_type	original_size	original_checksum	wn_sample_stat	resource_key
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	NULL	NULL	0	NULL	NULL	NULL	NULL	NULL	NULL
2	NULL	NULL	0	NULL	NULL	NULL	NULL	NULL	NULL
3	NULL	NULL	0	NULL	NULL	NULL	NULL	NULL	NULL
4	NULL	NULL	0	NULL	NULL	NULL	NULL	NULL	NULL
5	NULL	NULL	0	NULL	NULL	NULL	NULL	NULL	NULL
6	NULL	NULL	0	NULL	NULL	NULL	NULL	NULL	NULL
7	24071	3cfcd4f7c81...	0	NULL	NULL	NULL	NULL	NULL	NULL
8	3249504	452218e14ca...	0	NULL	NULL	NULL	NULL	NULL	NULL
9	94527	a950e02c279...	0	NULL	NULL	NULL	NULL	NULL	NULL
10	NULL	NULL	0	NULL	NULL	NULL	NULL	NULL	NULL
11	19951	258975bb60e...	0	NULL	NULL	NULL	NULL	NULL	NULL
12	NULL	NULL	0	NULL	NULL	NULL	NULL	NULL	NULL
13	1078268	f6545a7f7b60...	0	NULL	NULL	NULL	NULL	NULL	NULL
14	NULL	NULL	0	NULL	NULL	NULL	NULL	NULL	NULL
15	19951	258975bb60e...	0	NULL	NULL	NULL	NULL	NULL	NULL
16	77579	c69553b49f72...	0	NULL	NULL	NULL	NULL	NULL	NULL
17	3885318	106444949e0...	0	NULL	NULL	NULL	NULL	NULL	NULL

You can tell if a synced file is shared with others and determine possible distribution of this file. (As always 1=True and 0=False for shared attribute)

By selecting cloud_entry from the table, we obtained information such as file name, date of files created, removed, and modified size, checksum, shared, resource_type, etc. We can also select local_entry for more information.

DB Browser for SQLite - C:\Users\JOSEPH\AppData\Local\Google\Drive\user_default\snapshot.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach

Database Structure Browse Data Edit Pragma Execute SQL

Table: local_entry

	inode	volume	filename	modified	checksum	size	is_folder
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	10414574138...	serial:209532...	\\?\C:\Users\J...	NULL	NULL	NULL	1
2	56294995346...	serial:209532...	\\?\C:\Users\J...	NULL	NULL	NULL	1
3	56294995346...	serial:209532...	\\?\C:\Users\J...	NULL	NULL	NULL	1
4	56294995346...	serial:209532...	\\?\C:\Users\J...	NULL	NULL	NULL	1
5	84442493052...	serial:209532...	Blogger docu...	1614941743	NULL	NULL	1
6	53761720551...	serial:209532...	Baby Clara	1614941761	NULL	NULL	1
7	20547673300...	serial:209532...	Opt-Out Doc.x...	1612540117	3cfced4f7c81...	24071	0
8	33776997209...	serial:209532...	Bellingcat's O...	1612539022	452218e14ca...	3249504	0
9	30399297484...	serial:209532...	certificate.pdf	1610046958	a950e02c279...	94527	0
10	56294995381...	serial:209532...	file.gsheel	1607895595	7b8a2906504...	183	0
11	16888498606...	serial:209532...	file	1607895532	258975bb60e...	19951	0
12	30962247442...	serial:209532...	file (1).gsheet	1607895479	f29baa17b50f...	183	0
13	45035996277...	serial:209532...	ECC-Evaluatio...	1606222928	f6545a7f7b60...	1078268	0
14	56294995346...	serial:209532...	file (2).gsheet	1607895478	a8db15acf078...	183	0
15	42221246510...	serial:209532...	file (1)	1607895475	258975bb60e...	19951	0
16	47287796087...	serial:209532...	IMG-2020090...	1599153502	c69553b49f72...	77579	0
17	56294995381...	serial:209532...	IMG_2020052...	1590646127	106444949e0...	3885318	0
18	56294995381...	serial:209532...	IMG_2020050...	1590645954	20d55c51d3fb...	4253949	0

From the local_entry, investigators can pull out values like inode number, file name, modified, checksum, size, and is_folder, where 1 = true (it's folder) and 0 = false (it's file).

The Log File

You can obtain information about the client sync session from the **sync_log.log** file located at <SYSTEMROOT>\Users\
<username>\AppData\Local\Google\Drive\user_default. The logfile logs EVERYTHING that a user does with the application and it is what I consider the gold mine in Google drive forensic investigation. Information available includes: sync sessions, file created, file modified, and file deleted.

Note: Because log files are easy to modify (even by novice computer users) and are usually subject to integrity debate at the court of law as a result, the investigator is advised to take a hash of the log file in order to prove its integrity in the court.

Let us open it in notepad to see what it looks like.

```
sync_log - Notepad
File Edit Format View Help
2021-03-05 11:54:08,624 +0100 INFO pid=4544 5284:LaunchThreads root_wrangler.py:1161 LoadExtraRoots adding extra roots []
2021-03-05 11:54:08,654 +0100 INFO pid=4544 5284:LaunchThreads user.py:90 [Initializing User instance with new credentials. morowaiyodele@gmail.com]
2021-03-05 11:54:08,654 +0100 INFO pid=4544 5284:LaunchThreads sync_app.py:1323 Configuring sync app from feature switches.
2021-03-05 11:54:08,654 +0100 INFO pid=4544 5284:LaunchThreads sync_app.py:1341 Feature Switches:
FeatureSwitchSettings{
StoragePolicyEnabled=True,
accept_blob_download_gzip_encoding=True,
add_delete_mode_property_to_machine_root=True,
additional_mime_types=['audio/flac'],
allow_hq_download_modify=False,
backup_and_sync_is_changing_url='https://www.google.com/drive/download/?hl=%(locale)s',
backup_polling_interval_secs=7200,
change_buffer_journal_disabled_platforms=['win'],
change_filters=['DRIVE_SYNC'],
cloud_graph_disk_generation=8,
cloud_watcher_backoff_wait_time_sec=300,
consumer_drive_promo_url='https://www.google.com/drive/download/?hl=%(locale)s',
crash_log_size_limit=10000000,
crash_throttle_percentage=0.0,
download_change_throttle_sec=0.05,
download_url='https://www.googleapis.com/drive/v2internal/files/{doc_id}?alt=media',
drive_fs_process_name='Google Drive',
drive_fs_process_name_win='GoogleDriveFS.exe',
enable_always_show_in_photos=True,
```

Above is the entries that were created when the user logged in the native application. Search using the strings below:

- Action.CREATE
- Action.DELETE
- Action.MODIFY

```
sync_log - Notepad
File Edit Format View Help
ed between when the modify was detected and when the upload was done. Observed checksum: e21cd7fedd4d5644ff597543f3f33a3c mod_time: 1614958584 Observed size
type=DocType.BLOB,removed=False,parent_doc_ids=frozenset([u'1c1BYjID21MFc8hw741kA1ASnZXQrFDf8']),child_doc_ids=set([]),size=35435,checksum=e21cd7fedd4d5644ff5
o-ta-cXEG5kTAF, filename=None
96049115300700L, volume='serial:2095323097'), modified=1614958584, checksum=e21cd7fedd4d5644ff597543f3f33a3c, size=35435
D, Action.CREATE, local_id=LocalID(inode=10696049115300700L, volume='serial:2095323097'), path=u'\\\\?\\C:\\Users\\JOSEPH\\Pictures', name=u'prefetch.PNG', p
connection.googleapis.com:443.
n entries, waiting before upgrading the remainder.
CREATE, local_id=LocalID(inode=168884986449715L, volume='serial:2095323097'), path=u'\\\\?\\C:\\Users\\JOSEPH\\Documents\\Partition 6', name=u'SANTHOSH PROB
gybIM'. 2767 IDs left in store.
849860449715L, volume='serial:2095323097'), doc_id=1bb13HYX41fEAWkxp2HJNcE5JgybIM
upAsyncReference'
e/Drive-Z-j1SYAMZFT7RSOG1MuamA: 81927
ncReference'
E(SyncType.UNKNOWN_SYNC_TYPE), name=u'SANTHOSH PROBE.db', media=DriveClientMediaFileUpload(BufferedStream(filename=u'\\\\?\\C:\\Users\\JOSEPH\\Documents\\Par
/upload/drive/v2internal/files/enforceSingleParent=true&convert=false&fields=title%2Cparents%2Fid%2Cmime%2CmodifiedDate%2Clabels%2Frestricted%2CuserPerm
t) google-api-python-client/1.7.12 (gzip) (Windows/10.0 [64-bit])
n entries, waiting before upgrading the remainder.
one)
eond5krhLTxpm3c2888E6TC5-MtmIs0ERL121WmVbqFeNwTeFatz3EcJDF3Dm4xIA
t) google-api-python-client/1.7.12 (gzip) (Windows/10.0 [64-bit])
freenEntry(state=IN_PROGRESS, fschange=FSChange(DIRECTION_UPLOAD, Action.CREATE, local_id=LocalID(inode=10696049115300700L, volume='serial:2095323097'), path=
Action.CREATE, local_id=LocalID(inode=10696049115300700L, volume='serial:2095323097'), path=u'\\\\?\\C:\\Users\\JOSEPH\\Pictures', name=u'prefetch.PNG', par
```

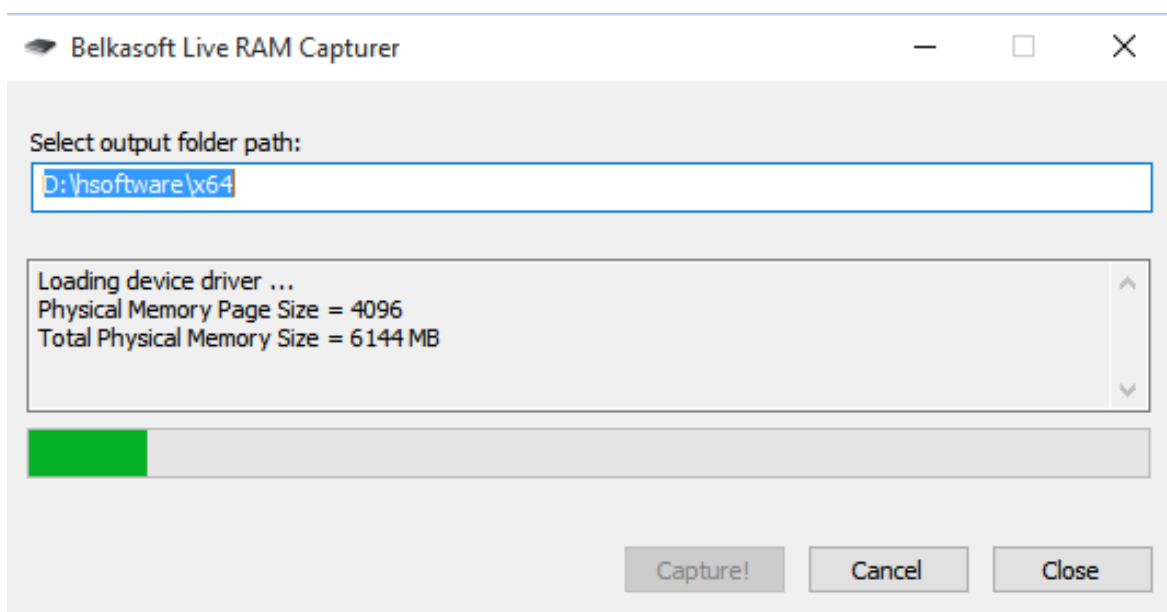
Modifying a synced file with the app, created the above entry. This helps to document actions taken on the synced files. The entries stored in this log matches most of the data that are inside the databases. However, this log also stores user actions, which are not stored in the databases.

Memory Artifacts

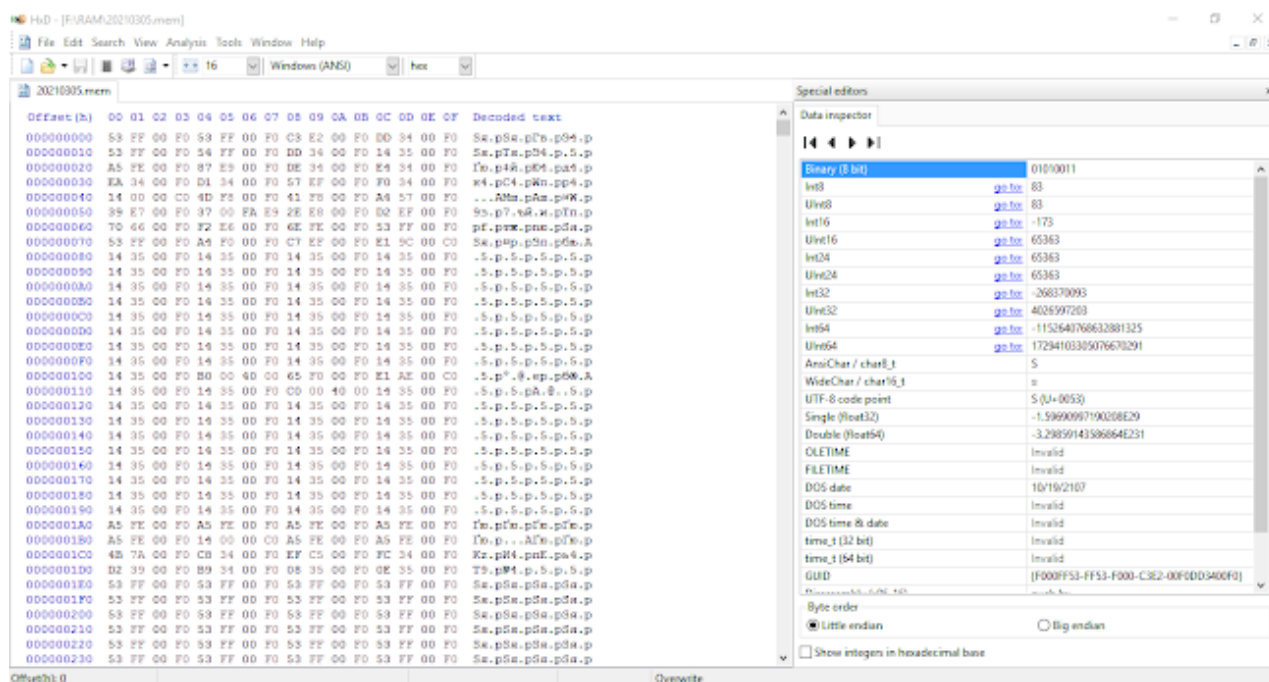
Investigators can find out information about the sessions of a Google Drive client from RAM analysis. This, of course, can only be achieved if, on arriving at the crime scene, the incident responder finds the system powered on. For this, the investigator can run a RAM

capture tool to dump the RAM contents, and then use a hex editor tool to analyze the captured RAM contents. The tool of choice here will be **Belkasoft RAM capturer**. To use this tool, follow these steps:

- Download the tool from [here](#) (you will need to fill out a simple registration form first in order to proceed to the download section).
- Transfer the tool onto a USB drive—the USB should have more storage than target computer RAM memory. As an incident responder, you ought to have had a USB drive prepared with the RAM capturer tool in it already.\
- Execute the program on the PC where you want to capture its RAM and click the “Capture” button.



- Open your .mem file (here 20210305.mem) captured using the RAM Capturer tool from the previous step in your HxD hex editor for analysis.



To find the email ID of the user, enter the string ***user_emailvalue*** in the hex editor (use Ctrl F).

```

HxD - [F:\RAM\20210305.mem]
File Edit Search View Analysis Tools Window Help
16 Windows (ANSI) hex
20210305.mem

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
01266CC50 6E 5F 70 6F 6C 69 63 79 5F 64 65 73 63 72 69 70 n_policy_descrip
01266CC60 74 69 6F 6E 5F 75 72 6C 22 2D 04 27 2D 0F 64 6F tion_url"-.'-.do
01266CC70 6D 61 69 6E 5F 70 6F 6C 69 63 79 64 65 66 61 75 main_policydefau
01266CC80 6C 74 5F 73 79 6E 63 5F 61 6C 6C 31 6F 2C 05 2D lt_sync_alllo,-
01266CC90 17 81 37 75 73 65 72 5F 70 69 63 74 75 72 65 5F .f7user_picture
01266CCA0 75 72 6C 76 61 6C 75 65 68 74 74 70 73 3A 2F 2F urlvaluehttps://
01266CCB0 6C 68 33 2E 67 6F 6F 67 6C 65 75 73 65 72 63 6F lh3.googleuserco
01266CCC0 6E 74 65 6E 74 2E 63 6F 6D 2F 61 2D 2F 41 4F 68 ntent.com/a-/AOh
01266CCD0 31 34 47 6A 44 32 67 50 69 55 48 73 6F 61 4C 68 14GjD2gPiUHsoaLh
01266CCE0 2D 57 56 45 4E 77 77 63 7A 6E 78 4B 75 62 7A 39 -WVENwzcznxKubz9
01266CCF0 66 54 71 42 36 62 4E 4D 4B 3D 73 36 34 29 2B 04 fTqB6bNMK=s64)+.
01266CD00 2F 17 2B 75 73 65 72 5F 64 69 73 70 6C 61 79 5F /.+user_display_
01266CD10 6E 61 6D 65 76 61 6C 75 65 41 79 6F 64 65 6C 65 namevalueAyodele
01266CD20 20 4D 6F 72 6F 6E 77 69 25 2A 04 1B 17 37 75 73 Moronwi&*...7us
01266CD30 65 72 5F 69 64 76 61 6C 75 65 31 30 35 34 32 38 er_idvalue105428
01266CD40 33 33 31 34 30 35 36 38 31 39 31 36 33 31 31 2C 331405681916311
01266CD50 29 04 21 17 3F 75 73 65 72 5F 65 6D 61 69 6C 76 ).!.?user_emailv
01266CD60 61 6C 75 65 6D 6F 72 6F 6E 77 69 61 79 6F 64 65 aluemoronwiayode
01266CD70 6C 65 6A 40 67 6D 61 69 6C 2E 63 6F 6D 00 00 00 lej@gmail.com...
01266CD80 80 00 0F 72 6F 6F 74 5F 63 6F 6E 66 69 67 5F 5F b..root_config_
01266CD90 33 5C 5C 3F 5C 43 3A 5C 00 00 00 00 73 5C 2F 3A 3\\?\\C:\\....s\\/:
01266CDA0 90 FB DD 0B 00 00 00 00 5F 63 6F 6E 66 69 67 5F h9....._config_
01266CDB0 0E 00 00 00 00 00 00 80 00 73 65 72 73 5C 4A .....b.sers\\J
01266CDC0 4F 53 45 50 48 5C 50 69 63 74 75 72 65 73 32 34 OSEPH\\Pictures24
01266CDD0 00 00 00 00 45 72 6F 6F 90 FB DD 0B 00 00 00 00 ....Erooh9.....
01266CDE0 5F 5F 30 72 6F 77 6B 65 79 5C 5C 3F 5C 43 3A 5C __orowkey\\?\\C:\\
01266CDF0 80 00 01 72 0C 00 00 00 30 23 E5 1F 00 00 00 00 b..r....0#e.....
01266CE00 74 75 72 65 73 33 38 04 00 00 00 00 6F 6F 74 5F tures38.....oot_
01266CE10 90 FB DD 0B 00 00 00 00 33 5C 5C 3F 5C 43 3A 5C h9.....3\\?\\C:\\
01266CE20 55 73 65 72 73 5C 4A 4F 80 00 01 48 04 00 00 00 Users\\JOB..H....
01266CE30 B0 22 E5 1F 00 00 00 00 65 30 33 37 04 29 4D 0F *"e.....e037.)M.
01266CE40 00 00 00 00 5F 63 6F 6E 90 FB DD 0B 00 00 00 00 ...._confh9.....
01266CE50 3F 5C 43 3A 5C 55 73 65 00 00 00 00 00 00 00 00 ?\\C:\\Use.....
01266CE60 80 00 47 6F 6F 67 6C 65 20 44 72 69 76 65 31 33 b.Google Drive13
01266CE70 36 04 29 4D 0F 72 6F 6F 00 00 00 00 6E 66 69 67 6.)M.roo....nfig
01266CE80 90 FB DD 0B 00 00 00 00 3A 5C 55 73 65 72 73 5C h9.....:\\Users\\

```

To check the version of Google Drive client, enter the string ***highest_app_versionvalue*** in the hex editor.

HxD - [F:\RAM\20210305.mem]

File Edit Search View Analysis Tools Window Help

16 Windows (ANSI) hex

20210305.mem

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00A4C7EC0	5A	56	39	78	63	48	4E	78	57	45	73	44	56	52	31	6C	ZV9xcHNxWEsDVR1l
00A4C7ED0	62	6D	46	69	62	47	56	66	59	32	39	77	65	56	39	6B	bmFibGVfY29weV9k
00A4C7EE0	64	58	42	73	61	57	4E	68	64	47	56	66	63	32	56	30	dXBsaWNhdGVfc2V0
00A4C7EF0	64	47	6C	75	5A	33	46	5A	69	56	55	5A	62	57	46	34	dGluZ3F2iVUZbWf4
00A4C7F00	58	33	42	68	5A	32	56	66	63	32	6C	36	5A	56	39	6A	X3BhZ2Vfc2l6ZV9j
00A4C7F10	62	47	39	31	5A	46	39	6E	63	6D	46	77	61	48	46	61	bG91ZF9ncmFwaHFa
00A4C7F20	53	32	52	56	47	58	42	32	62	31	39	74	59	58	68	66	S2RVGXB2b19tYXhf
00A4C7F30	63	32	6C	36	5A	56	39	77	61	47	39	30	62	31	39	77	c2l6ZV9waG90b19w
00A4C7F40	61	58	68	6C	62	48	4E	78	57	30	6F	41	34	66	55	46	aXh1bHNxW0oA4fUF
00A4C7F50	56	52	42	7A	63	47	39	79	61	31	39	73	59	58	56	75	VRBzcG9ya19sYXVu
00A4C7F60	59	32	68	66	64	58	4A	73	63	56	78	56	50	6D	68	30	Y2hfdXJscVxVPmh0
00A4C7F70	64	48	42	7A	4F	69	38	76	00	00	00	06	1B	04	04	29	dHBzO18v.....)
00A4C7F80	17	15	72	6C	7A	5F	62	72	61	6E	64	5F	63	6F	64	65	..rlz_brand_code
00A4C7F90	76	61	6C	75	65	47	47	4C	53	1E	03	04	35	17	0F	63	valueGGLS...5..c
00A4C7FA0	6C	6F	75	64	5F	64	6F	63	73	5F	66	65	65	64	5F	6D	loud_docs_feed_m
00A4C7FB0	6F	64	65	76	61	6C	75	65	30	2A	02	04	33	17	29	68	odevalue0*...3.)
00A4C7FC0	69	67	68	65	73	74	5F	61	70	70	5F	76	65	72	73	69	ighest_app versi
00A4C7FD0	6F	6E	76	61	6C	75	65	33	2E	35	34	2E	33	35	32	39	onvalue3.54.3529
00A4C7FE0	2E	30	34	35	38	19	01	04	29	17	11	75	70	67	72	61	.0458...).upgra
00A4C7FF0	64	65	5F	6E	75	6D	62	65	72	76	61	00	00	00	07	05	de_numberva.....
00A4C8000	E5	C5	F4	59	CA	C5	FC	59	C3	C5	F4	5C	C0	C5	DC	58	eEфYKEьYTEф\AEьX
00A4C8010	8C	35	7C	FE	FF	FF	C5	FC	58	44	35	80	C5	FC	11	8C	ь5 юяяьXD5ььь.ь
00A4C8020	35	7C	FE	FF	FF	C5	FC	11	44	35	80	C5	FC	10	82	80	5 юяяь.D5ьььь.,ь
00A4C8030	00	00	00	C5	FC	10	8A	84	01	00	00	C4	C1	7C	10	94	...ьь.ь.....ДБ ."
00A4C8040	32	9C	FE	FF	FF	C4	C1	7C	10	5C	32	A0	C5	FC	59	E2	2юяяДБ .2 ььYв
00A4C8050	C5	F4	59	EB	C5	DC	58	E5	C5	F4	59	CA	C5	FC	59	C3	ЕфYлEьXeEфYKEьYT
00A4C8060	C5	F4	5C	C0	C5	DC	58	8C	35	9C	FE	FF	FF	C5	FC	58	Еф\AEьXь5юяяььX
00A4C8070	44	35	A0	C5	FC	11	8C	35	9C	FE	FF	FF	C5	FC	11	44	D5 ььь.ь5юяяьь.D
00A4C8080	35	30	C5	FC	10	82	80	00	00	00	C5	FC	10	82	80	01	ь ьььььььььььььь

To find the display path for the default sync folder, enter the string **local_sync_root_pathvalue** in the hex editor.

HxD - [F:\RAM\20210305.mem]

File Edit Search View Analysis Tools Window Help

16 Windows (ANSI) hex

20210305.mem

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
01266C8E0	00	00	00	00	00	00	00	00	4F	FF	44	00	00	00	00	00OaD.....
01266C8F0	05	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
01266C900	4C	00	66	00	00	00	00	00	06	00	00	00	00	00	00	00	L.f.....
01266C910	00	00	00	00	00	00	00	00	57	00	48	00	01	00	00	00W.H.....
01266C920	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
01266C930	4B	00	6F	00	00	00	00	00	00	00	00	00	00	00	00	00	K.o.....
01266C940	00	00	00	00	00	00	00	00	02	F2	45	01	00	00	00	00tE.....
01266C950	00	00	00	00	33	00	00	00	00	00	00	00	00	00	00	003.....
01266C960	0D	00	5F	00	00	00	00	00	01	00	00	00	00	00	00	00	.._.....
01266C970	00	00	00	00	00	00	00	00	5C	55	73	65	72	73	5C	4A\Users\J
01266C980	4F	53	45	50	48	5C	44	6F	63	75	6D	65	6E	74	73	2F	OSEPH\Documents/
01266C990	3C	04	29	45	0F	72	6F	6F	74	5F	63	6F	6E	66	69	67	<.)E.root_config
01266C9A0	5F	5F	33	5C	5C	3F	5C	43	3A	5C	55	73	65	72	73	5C	_3\\?\C:\Users\
01266C9B0	4A	4F	53	45	50	48	5C	50	69	63	74	75	72	65	73	30	JOSEPH\Pictures0
01266C9C0	1F	18	04	37	17	0F	63	6F	70	79	5F	64	75	70	6C	69	...7..copy_dupli
01266C9D0	63	61	74	65	5F	70	68	6F	74	6F	73	76	61	6C	75	65	cate_photosvalue
01266C9E0	31	3D	13	04	35	17	4D	6C	6F	63	61	6C	5F	73	79	6E	1=..5.Mlocal_syn
01266C9F0	63	5F	72	6F	6F	74	5F	70	61	74	68	76	61	6C	75	65	c root pathvalue
01266CA00	5C	5C	3F	5C	43	3A	5C	55	73	65	72	73	5C	4A	4F	53	\\?\C:\Users\JOS
01266CA10	45	50	48	5C	47	6F	6F	67	6C	65	20	44	72	69	76	65	EPH\Google Drive
01266CA20	1C	0E	04	31	17	0F	73	68	61	72	65	5F	6E	6F	74	69	...1..share_noti
01266CA30	66	69	63	61	74	69	6F	6E	76	61	6C	75	65	31	1F	0D	ficationvalue1..
01266CA40	04	37	17	0F	61	6C	77	61	79	73	5F	73	68	6F	77	5F	.7..always_show_
01266CA50	69	6E	5F	70	68	6F	74	6F	73	76	61	6C	75	65	30	24	in_photosvalue0\$
01266CA60	0C	04	33	17	1D	73	74	6F	72	61	67	65	5F	70	6F	6C	..3..storage_pol
01266CA70	69	63	79	5F	6D	6F	64	65	76	61	6C	75	65	6F	72	69	icy_modevalueori
01266CA80	67	69	6E	61	6C	1F	0A	04	37	17	0F	73	68	6F	77	5F	ginal...7..show_
01266CA90	75	6E	70	61	72	65	6E	74	5F	77	61	72	6E	69	6E	67	unparent_warning
01266CAA0	76	61	6C	75	65	31	1A	09	04	2D	17	0F	75	73	62	5F	value1...-..usb_
01266CAB0	73	79	6E	63	5F	65	6E	61	62	6C	65	64	76	61	6C	75	sync_enabledvalu
01266CAC0	65	31	42	07	04	35	2D	41	73	68	6F	77	6E	5F	73	65	e1B..5-Ashown_se
01266CAD0	74	75	70	5F	6F	76	65	72	6C	61	79	73	73	65	74	75	tup_overlayssetu
01266CAE0	70	5F	6F	76	65	72	6C	61	79	5F	69	64	67	6F	6F	67	p_overlay_idgoog
01266CAF0	6C	65	5F	64	72	69	76	65	5F	73	65	74	75	70	5F	6F	le_drive_setup_o
01266CB00	76	65	72	6C	61	79	44	06	04	35	2D	45	73	68	6F	77	verlayD..5-Eshow
01266CB10	6E	5F	73	65	74	75	70	5F	6F	76	65	72	6C	61	79	73	n setup overlays

Well, that is all for now. I hope this article will help you in your investigations. Bye!