doi:10.20944/preprints201812.0345.v1

Cloud Drives Forensic Artifacts

A Google Drive Case

Tariq Z. Khairallah
Information Systems Security and Digital Criminology
King Hussein School of Computing Sciences
Princess Sumaya University for Technology (PSUT)
tar20168014@std.psut.edu.jo
Amman, Jordan

***Abstract*— This research proposed in this paper focuses on gathering evidence from devices with Windows 10 operating systems in order to discover and collect artifacts left by cloud storage applications that suggest their use even after the deletion of the Google client application. We show where and what type of data remnants can be found using our analysis which can be used as evidence in a digital forensic investigations.**

***Keywords*— Cloud Storage Forensics, Cloud Application Artifacts, Data Remnants, Data Carving, Digital Forensic Investigations**

I. Introduction

Cloud computing is a quite recent term to describe computer resources available as a service accessible over a network, The National Institute of Standards and Technology (NIST) define cloud computing in its publication (SP 800-145)[1]:" *Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models*."

The mandate for Storage as a Service (StaaS) grounded by Cisco Global Cloud Index: Forecast and Methodology, 2015–2020 [2] is increasing because of the popularity and availability of digital devices and the wide use of the Internet over these devices, which leads to the increased utilization of cloud storage apps that allows users to access their data anywhere, anytime.

There is a range of cloud storage hosting providers, and many offer free cloud storage services; such as Dropbox, Microsoft SkyDrive, and Google Drive Accessing the various cloud storage services can be undertaken in a variety of ways; a user can install client software on a personal computer (PC), mobile device, or use a web browser to access the cloud storage service.

Cloud storage services are an important source of evidence in investigations for both cybercrime and traditional crimes. It is possible nowadays to abuse cloud storage services for malicious activities. Cloud storage services are being used to distribute Malware [3][4][5], or as command and control to distribute infections. Cloud storage has also been used to launch DDoS attack on US banks [6], in child pornography, and data exfiltration.

The objective of this paper is contribute to digital forensic investigation of cloud storage services through the identification of data forensic artifacts of user activities by conducting an experiment on Google Drive on Windows 10.

II. Literature Review

This section aims to explore the techniques and approaches used by other researchers in this particular field.

Available studies used for the purpose of this paper suggest that types of artifacts collected can be:

1. Artifacts related to files that have been accessed, modified or deleted by the cloud storage applications on the client machine,
2. Artifacts related to web-based activities which are accessed through a web browser.

Two main approaches were used to identify the artifacts:

1. Assumption approach: of where artifacts should be located on a device, and then perform a search in those specifics locations, based on the examiner's knowledge.
2. Dynamic approach: this approach uses tools and programs such as Process Monitor by Sysinternals Suite [7] to determine the location and changes made by the application.

The paper, Digital Forensic Investigation of Cloud Storage Services [8] proposes a procedure to examine devices (PCs and smartphones) that depends on the type of the device being investigated to collect and analyze data; If the device is a PC then it is very important to collect volatile data from physical memory (if live forensic analysis is possible) and nonvolatile data such as files, directories, internet history, and log files. The physical memory contains useful information about users and their activities. For example, physical memory can contain login attempts and login credentials used to access cloud storage accounts through a web browser, and different approach for mobile devices.

The rest of the paper provides examples where artifacts are found on PC or a smartphone. The cloud services that were investigated in this work, are Amazon S3, Dropbox, Google Docs, and Evernote.

The research Cloud Storage Forensics [9] provides a structured methodology and a very comprehensive analysis of artifacts left by cloud storage applications. This research is done on a Windows 7 Machine and the cloud storage services analyzed are SkyDrive Dropbox and Google Drive.

The research explains about the artifacts either accessed or modified, and remnants left behind by the applications are found inside:

- Prefetch files
- Registry files
- link files
- thumbnails pictures within the thumb cache,
- event logs
- Directory lists file ($MFT files).
- Memory
- $Recycle.Bin
- analysis of installation path
- sample files
- synchronized files and folders
- account accessed through a web browser

Researchers of the Cloud Storage Forensics [10] on SkyDrive Google Drive, Dropbox, and iCloud use a methodology of the following process :Reg-Shot execution and state saving, Disk-Pulse start, Client installation, Disk-Pulse stop, Reg-Shot execution and state saving, Reg-Shot differences, Registry keys analysis, and File created analysis.

Researchers have collected evidence from the same locations as the previous researches.

The methods and techniques applied in these aforementioned studies came to the conclusion that the locations analyzed and the data remnants found were similar.

III. Problem

The digital forensic analysis is the process of examining the electronic evidence for legal purposes. for an examiner, it is also important to have a current understanding of the location and type of data remnants left behind by cloud storage incidents, so a proper studies for such services should asses the investigator in collecting evidences an artifacts in systematic manner.

IV. PREPARATION FOR EXPERIMENTATION & Testing Environment

In preparation for the experiment, a virtual machine (VM) using Oracle VM VirtualBox was download from Microsoft developer website [12] to be ready to host Google Drive; the machine was loaded with following tools prior installation of Google Drive:

- **Sysinternals Process Monitor** to record any and all changes/additions that the cloud services made during their use, from the installation to when the services were uninstalled[7],
- **Windows System State Analyze**: The basic functionality of the System State Analyzer tool is to allow you to compare two snapshots taken at different points in time. This allows you to compare the state of a machine both before and after an application install for instance[13].
- **Windows System State Monitor:** the application is capable of keeping an eye on certain areas of your computer, such as the file system, registries, services, and drivers. Once monitoring is started, changes are detected
- **SysTracer**: System utility tool that can scan and analyze your computer to find changed (added, modified or deleted) data into registry and files[14].
- **WinHex**: WinHex is at its core a universal hexadecimal editor, particularly helpful in the realm of computer forensics, data recovery, low-level data processing, and IT security[15].
- **AccessData FTK Imager**: Data preview and imaging tool used to acquire data (evidence) in a forensically sound manner.
- **DB Browser for SQLite**[16]: DB Browser for SQLite Database.
- **Active Disk editor**[17]: Advanced tool for viewing & editing raw sectors on Physical Disks, Partitions & Files content in hexadecimal form
- **Registry Explorer**[18]: Registry. Full-featured, offline Registry parser in C#.
- Windows 10 64 bit Operating System [12]
- Google Drive client

V. RESEARCH METHODOLOGY

In this research, the dynamic process method was used to determine the artifacts and remnants found on windows 10 system as following

- System Snapshot acquisition (File and registry) state saving (*SysTracer* [14], *Windows System State Analyze* [13])
- Prepare system to collect changes during installation (*Windows System State Monitor*[13])
- Google Drive Client installation on targeted system,
- Stop Windows System State Monitor and generate reports.
- System Snapshot acquisition (File and registry) state saving(After installation),
- Generate system Snapshot differences,
- Study and analyses of the snapshot difference report,

- Registry keys analysis
- File created analysis
- Add /update/delete files (drive functionality
- Monitor actions using process monitor
- Revalidate changes made by the system,

VI. Results and Analysis

A. *Summary of changes*

Using Window System State Monitor the below results summarized by files, folders, Executables, Services, registry entries and location, describes changes done by installing Google drive on our windows 10 system.

Files/Folders		
Added	Modified	Deleted
6384	161	161

Table 1- Summary of Files/Folders

Services		
Added	Modified	Deleted
0	3	0

Table 2-Summary of Services

Registry		
Added	Modified	Deleted

HKCR (61)
HKLM(468)
HKU(372)
	HKLM (121)
	HKU (212)
		HKCR (1)
		HKLM(51)
		HKU(70)

Table 3-Summary of Registry

Executables		
Added	Modified	Deleted
DLL (104) ***EXE (11)*** ***MSI (6)***	***DLL (42)*** ***MSI (1)***	***DLL (61)*** ***EXE (9)*** ***MSI (5)***

Table 4 -Binary summary

Location		
Files/Folder changes outside %program files%	Added	6172
	Modified	151
	Deleted	88
Files/Folder changes Inside InetPub, Temp	Added	Temp (5927)
	Modified	Temp (72)
	Deleted	Temp (3)

Table 5- Location summary

B. *Analysis*

Google client uses the googledrivesync.exe executable file located in C:\Program Files (x86)\Google\Drive

During installation google drive downloaded and used other executable files form temp folders shown in below list. After installation all these executable files were deleted, temp folder in our experiment was C:\Program Files (x86)\GUM5678.tmp :

- GoogleCrashHandler.exe
- GoogleCrashHandler64.exe
- GoogleUpdate.exe
- GoogleUpdateBroker.exe
- GoogleUpdateComRegisterShell64.exe
- GoogleUpdateCore.exe
- GoogleUpdateOnDemand.exe
- GoogleUpdateSetup.exe
- GoogleUpdateWebPlugin.exe

1) *SQLite databases*

An important artifact location is the virtual user folder files, which is located on the following location C:\Users\IEUser\AppData\Local\Google\Drive

The most important files are the following files 2 SQLite format 4 database files:

1. sync_config.db : Small SQLite database that contains one table named *data* and have the following fields
   - entry_key,
   - data_key,
   - data_value

   The table contains google drive configuration shown in Appendix 1, the most important value is the username value. In our case the entry value was equal to "user_email" and the data_key was equal to "value", and the data_value equal to "psut.dfi@gmail.com", the latter is the user account used in this experiment. Another important entry_key is the root_config 0 and its data_key varies between "rowkey" and the full path to the mapped folders to monitor and use for google drive sync.

2. snapshot.db :Another Small SQLite database that contains 7 tables:
   - cloud_entry
   - cloud_relations
   - local_entry
   - local_relations
   - mapping
   - pre_mapping
   - volume_infos

These tables contain file(s) details stored in the Google Drive account and other relations to the cloud presence of these files, one important notice was the volume_info table that contains volume information of the system were the clines was installed. Another important table was the local_entry table which contains the local files locations, ids, type, checksum and size below sample record extracted from local_entry table:

inode	562949953421366
volume	serial:3661233214
filename	psut.bmp
modified	1516118514
checksum	d41d8cd98f00b204e9800998ecf8427e
size	0
is_folder	0

3. cloud_graph.db: another SQLight database contains 3 tables and contains files synced files information same as snapshop.db.
4. Global.db: this data base file located in the following path C:\Users\IEUser\AppData\Local\Google\Drive And contains user name for the uses using goggle drive.

2) *Account folders*

Each added account have another account folder in the same path for the user but in a different folder. Another file in interest is a json file named com.google.drive.nativeproxy.json in the same directory of the SQLite Databases, contains the location, description of an another exe file called nativeproxy.exe

3) *Prefetch*

As any windows exe fil a , Prefetch file was also created in the Windows Prefetch folder with the named ‘GOOGLEDRIVESYNC.EXE-XXXXXXXX.pf’.

4) *Other locations*

Software references were also placed in a variety of places, such as; $LogFile, $MFT, $UsnJrnl, and pagefile.sys. Link files were created on the Windows Desktop and in the Windows Start Menu.

5) *Registry*

Analyzing the registry we found that there is different references for after installing Google Drive client most of the values was related to installation path for googledrivesync.exe and temp installation files, MRU values, and Google Docs.

At the registry ShellIconOverlayIdentifiers keys were added for google drive contains GoogleDriveBlacklisted, GoogleDriveSynced and GoogleDriveSyncing entryes keys are used by google drive client for Icons and Icon Overlays [19].

Another important registry are shown in below table’s

Key	Description
HKEY_CLASSES_ROOT\installer\features\865bd809af5e7c042aaaba43100958b8	Contains the value of GoogleDriveSync and ProductName that indicates the installation of the files
HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\installer\folders	Contains the location for the installer folder that is used when installing the client the drive
HKEY_LOCAL_MACHINE\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation	Contains reference for googledrivesync.exe
HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\installer\folders	Contains the installation folder for google client
HKEY_USERS\msedgewin10\ieuser\software\google\drive	Contains the installation folder for google client and some settings information , and an OAuthToken
HKEY_USERS\msedgewin10\ieuser\software\google\chrome\extensions\apdfllckaahabafndbhieahigkjlhalf	Chrome Extension path and version

6) *Log Files*

Event Log & Log files are sources of information and artifacts, Gogol Drive maintain a verbose log client folder, the log contains data about actions and along with time and dates, with notable python script references

7) *Network Trafic analsys*

Traffic capture was done during installation and during adding, deleting files using Wireshark , the network communication showing its encrypted using TLS V1.2 and APPENDIX 2 showing resolved addresses during installation, all data exchange was done using TCP with no reference for http connections, though the folder contains some reference for cached responses in cash folder resident in uses folder.

VII. Conclusion

Remnants and artifacts of cloud drive activity can be found on local machines found on local folders. The username, the cache files, and log activity which helps in recovering the deleted files and data.

It was concluded during investigating that findings in the initial stages for cloud service files changes and user account details, this includes the places of these artifacts and details for pinpointing these evidences during an investigation on windows 10 operating system and extracting these to be mapped to the under investigated case, the artifacts are

doi:10.20944/preprints201812.0345.v1

matching for ones that can be found on windows 7 operating systems, except that earlier researchers missed out that there is another artifacts found, these are also important artifact for the investigation (cloud_graph.db , Global.db, log files and the rejestry i, OpenAuth IDs), one important artifact is the registry ShellIconOverlayIdentifiersthat google drive uses for file icons while process its state(synced, syncing, error) , one notable point; running a forensic image in vm can access the user cloud storage.

VIII. References

[1] P. Mell and T. Grance, “NIST Special Publication 800-145: The NIST Definition of Cloud Computing,” 2011.

[2] “What You Will Learn,” pp. 2015–2020.

[3] “Dropbox used by Chinese hackers to spread malware - NBC News.” [Online]. Available: https://www.nbcnews.com/tech/security/dropbox-used-chinese-hackers-spread-malware-f6C10642402. [Accessed: 16-Jan-2018].

[4] “Attackers turning to legit cloud services firms to plant malware | Computerworld.” [Online]. Available: https://www.computerworld.com/article/2484596/cybercrime-hacking/attackers-turning-to-legit-cloud-services-firms-to-plant-malware.html. [Accessed: 16-Jan-2018].

[5] “Cloud Services Being Used to Distribute Malware | CloudWedge.” [Online]. Available: http://www.cloudwedge.com/cloud-services-used-distribute-malware/. [Accessed: 16-Jan-2018].

[6] “How Iranian Hackers Used The Cloud To Attack Major Banks And Why It Matters – ThinkProgress,” 2013. [Online]. Available: https://thinkprogress.org/how-iranian-hackers-used-the-cloud-to-attack-major-banks-and-why-it-matters-1f8c722b7fcc/. [Accessed: 16-Jan-2018].

[7] “Process Monitor - Windows Sysinternals | Microsoft Docs,” 2017. [Online]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/procmon. [Accessed: 16-Jan-2018].

[8] 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, 2016.

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

[10] B. Martini and K. K. R. Choo, “Cloud storage forensics: OwnCloud as a case study,” *Digit. Investig.*, vol. 10, no. 4, pp. 287–299, 2013.

[11] H. Guo, B. Jin, and T. Shang, “Forensic investigations in Cloud environments,” in *Proceedings - 2012 International Conference on Computer Science and Information Processing, CSIP 2012*, 2012, pp. 248–251.

[12] “Free Virtual Machines from IE8 to MS Edge - Microsoft Edge Development.” [Online]. Available: https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/. [Accessed: 16-Jan-2018].

[13] Tim Newton, “An Introduction to the Windows System State Analyzer | Ask the Performance Team Blog,” 2010. [Online]. Available: https://blogs.technet.microsoft.com/askperf/2010/01/11/an-introduction-to-the-windows-system-state-analyzer/. [Accessed: 16-Jan-2018].

[14] “SysTracer - Track file and registry changes in your computer,” 2018. [Online]. Available: http://www.blueproject.ro/systracer. [Accessed: 16-Jan-2018].

[15] “WinHex: Hex Editor &amp; Disk Editor, Computer Forensics &amp; Data Recovery Software,” 2018. [Online]. Available: https://www.x-ways.net/winhex/. [Accessed: 16-Jan-2018].

[16] “DB Browser for SQLite.” [Online]. Available: http://sqlitebrowser.org/. [Accessed: 16-Jan-2018].

[17] “Active@ Disk Editor Freeware - Hex Data Viewer &amp; Hex Editor,” 2018. [Online]. Available: http://www.disk-editor.org/. [Accessed: 16-Jan-2018].

[18] “Eric Zimmerman’s Tools,” 2018. [Online]. Available: https://ericzimmerman.github.io/. [Accessed: 16-Jan-2018].

[19] “How to Register Icon Overlay Handlers (Windows).” [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/hh127455(v=vs.85).aspx. [Accessed: 20-Jan-2018].

IX. APPENDIXIES

A. Appendix 1

entry_key	data_key	data_value
upgrade_number	value	40
highest_app	value	3.38.7642.3857

_version		
cloud_docs_feed_mode	value	0
rlz_brand_code	value	GGLS
feature_switch	value	gAJjY29tbW9uLmZlYXR1cmVfc3dpdGNoX21hbmFnZXIKRmVhdHVyZVN3aXRjaFNldHRpbmdzCnEBKYFxAn1xAyhVGGVuYWJsZV9oaWdoX3F1YWxpdHlfbW9kZXEEiFUIb3Blbl91cmxxBVUpaHR0cHM6Ly9kcml2ZS5nb29nbGUuY29tL29wZW4/aWQ9e2RvY19pZH1xBlUHdmVyc2lvbnEHVQ4zLjM4Ljc2NDIuMzg1N3EIVSJtYXhfcGFnZV9zaXplX2Nsb3VkX2dyYXBoX2ZhbGxiYWNrcQlN6ANVHWVuYWJsZV9jb3B5X2R1cGxpY2F0ZV9zZXR0aW5ncQqJVRRTdG9yYWdlUG9saWN5RW5hYmxlZHELiFUUY3Jhc2hfbG9nX3NpemVfbGltaXRxDEqAlpgAVRZtYXhfYmF0Y2hfdXBsb2FkX2ZpbGVzcQ1LHlUcYmFja3VwX3BvbGluZmaW50ZXJ2YWxfc2Vjc3EOTSAcVRljcmFzaF90aHJvdHRsZV9wZXJjZW50YWdlcQ9HAAAAAAAAAABVE25ld19zcHJlYWRzaGVldF91cmxxEFUzaHR0cHM6Ly9kb2NzLmdvb2dsZS5jb20vc3ByZWFkc2hlZXRzP3VzcD1kcml2ZV9zeW5jRFVD2VuYWJsZV9mZWVkYmFja3ESiFUWbWF4X251bV9uZXR3b3JrX2Vycm9yc3ETSwZVF2VuYWJsZV9waG90b3NfZGVkdXBlX3YycRSJVRRwdm9fdmlkZW9fZXh0ZW5zaW9uc3EVXXEWKFUELm1wNHEXVQQubW92cRhVBC53bXZxGVUELm1wZ3EaVQUubXBlZ3EbVQQuYXZpcRxVBC5hc2ZxHVUELm10c3EeVQUubTJ0c3EfVQQuM2dwcSBVBC5tb2RxIVUELm1tdnEiVQQudG9kcSNVBS5kaXZ4cSRVBC5tNHZxJVUELjNnMnEmVQQubTJ0cSdVBC5ta3ZxKGVVE2VuYWJsZV9iYXRjaF91cGxvYWRxKYhVHG1heF9wYWdlX3NpemVfc2VsZWN0aXZlX3N5bmNxKk2gD1UQZW5hYmxlX21pZ3JhdGlvbnEriFUVdG9rZW5fYnVja2V0X3JlYWRfcXBzcSxLClUiYWNjZXB0X2Jsb2JfZG93bmxvYWRfZ3ppcF9lbmNvZGluZ3EtiFUgaW1wcmVzc2lvbnNfdXBsb2FkX2l

		udGVydmFsX3NlY3NxLk0IB1UVZW5hYmxlX3JlY3Vyc2l2ZV9zaXplcS+IVRJzaGFyZV90ZW1wbGF0ZV91cmxxMFWOaHR0cHM6Ly9kcml2ZS5nb29nbGUuY29tL3NoYXJpbmcvc2hhcmU/c3ViYXBwPTEwJnNoYXJlUHJvdG9jb2xWZXJzaW9uPTImdGhlbWU9MiZjb21tYW5kPXNldHRpbmdzJnNoYXJlVWlUeXBlPWRlZmF1bHQmYXV0aHVzZXI9MCZjbGllbnQ9ZGVza3RvcHExVQtlbmFibGVfcHVzaHEyiFUTcHVzaF9jbGllbnRfdmVyc2lvbnEzSwFVGWVuYWJsZV9zdXJmYWNlX2hxX2ZhaWx1cmVxNIlVFGVuYWJsZV9waG90b3NfZGVkdXBlcTWIVR5lbmFibGVfcGVyc2lzdGVkX2NoYW5nZV9idWZmZXJxNolVDGRvd25sb2FkX3VybHE3WEQAAABodHRwczovL3d3dy5nb29nbGVhcGlzLmNvbS9kcml2ZS92MmludGVybmFsL2ZpbGVzL3tkb2NfaWR9P2FsdD1tZWRpYXE4VRRlbmFibGVfbmF0aXZlX29wZW5lcnE5iFUYcHZvX21heF9zaXplX3Bob3RvX2J5dGVzcTpKAACwBFUdcHZvX3N0YW5kYXJkX3Bob3RvX2V4dGVuc2lvbnNxO11xPChVBC5qcGdxPVUFLmpwZWdxPlUELmpwZXE/VQQuZ2lmcUBVBC5wbmdxQVUFLnRpZmZxQlUFLndlYnBxQ2VVF2VuYWJsZV9maWxlX3N5bmNfc3RhdHVzcUSIVQ10ZWxlbWV0cnlfdXJscUVVL2h0dHBzOi8vZHJpdmUuZ29vZ2xlLmNvbS9zeW5jY2xpZW50X2ltcHJlc3Npb25zcUZVEGxvZ19iYWNrdXBfY291bnRxR0sAVR50ZWxlbWV0cnlfdXBsb2FkX2ludGVydmFsX3NlY3NxSE0IB1UOY2hhbmdlX2ZpbHRlcnNxSV1xSlUKRFJJVkVfU1lOQ3FLYVUUbmV3X3ByZXNlbnRhdGlvbl91cmxxTFUzaHR0cHM6Ly9kb2NzLmdvb2dsZS5jb20vcHJlc2VudGF0aW9uP3VzcD1kcml2ZV9zeW5jcU1VDWxvZ2dpbmdfbGV2ZWxxTlUEaW5mb3FPVRZ0b2tlbl9idWNrZXRfd3JpdGVfcXBzcVBLA1UPZW5hYmxlX3VwbG9hZGVycVGIVRtlbmFibGVfZGVsZXRlX25vdGlmaWNhdGlvbnNxUohVIG92ZXJsYXlzX2VuYWJsZWRfZmluZGVyX3ZlcnNpb25zcVNdcVQoWAQAAAAxMC43cVVYBgAAADEwLjcuMXFWWAYAAAAxMC43LjJxV1gGAAAAMTAuNy4zcVhYBgAAADEwLjcuNXFZWAQAAAAxMC44cVpYBgAAADEwLjguMXFbWAYAAAAxMC44LjJxXFg

		GAAAAMTAuOC4zcV1YBAAAADEwLjlxXlgGAAAAMTAuOS4xcV9YBgAAADEwLjkuMnFgWAYAAAAxMC45LjNxYWVVGWRyaXZlX2ZzX3Byb2Nlc3NfbmFtZV93aW5xYlURR29vZ2xlRHJpdmVGUy5leGVxY1UZbWF4X3BhZ2Vfc2l6ZV9jbG91ZF9ncmFwaHFkTaAPVQtudW1fd29ya2Vyc3FlSwNVGXB2b19tYXhfc2l6ZV9waG90b19waXhlbHNxZkoA4fUFVShjaGFuZ2VfYnVmZmVyX2pvdXJuYWxfZGlzYWJsZWRfcGxhdGZvcm1zcWddcWhVA3dpbnFpYVUecHZvX21pbl9kaW1lbnNpb25fcGhvdG9fcGl4ZWxzcWpNAAFVFW1heF9wYWdlX3NpemVfY2hhbmdlc3FrTaAPVRVlbmFibGVfY2hhbmdlX2ZpbHRlcnNxbIlVC2xvZ19zaXplX21icW1NAAFVEG5ld19kb2N1bWVudF91cmxxblUvaHR0cHM6Ly9kb2NzLmdvb2dsZS5jb20vZG9jdW1lbnQ/dXNwPWRyaXZlX3N5bmNxb1UTZW5hYmxlX2RhcHBlcl90cmFjZXFwiVUXZW5hYmxlX2NvbnRleHRfbWVudV9hZGRxcYhVCGhlbHBfdXJscXJVNmh0dHBzOi8vc3VwcG9ydC5nb29nbGUuY29tL2RyaXZlLz9obD0lcyZwPWRlc2t0b3BfaG9tZXFzVRtjbG91ZF9ncmFwaF9kaXNrX2dlbmVyYXRpb25xdEsHVRhvdm9fbWF4X3NpemVfdmlkZW9fYnl0ZXNxdYoFAAAAgAJVEmZpbHRlcl9saXZlX3Bob3Rvc3F2iFUjaGluaF9xdWFsaXR5X3N1cHBvcnRlZF9vbl9jb3B5X2l0ZW1xd4lVDnF1ZXJ5X3N0cmF0ZWd5cXhYBAAAAHJvb3RxeVUlcHZvX21pbl9kaW1lbnNpb25faWdub3JlX2N1dG9mZl9ieXRlc3F6SgAAMABVDWZlZWRiYWNrX3R5cGVxe1UEcHJvZHF8VRVkcml2ZV9mc19wcm9jZXNzX25hbWVxfVUYR29vZ2xlIERyaXZlIEZpbGUgU3RyZWFtcX5VGWVuYWJsZV9zaGFyZV9ub3RpZmljYXRpb25xf4lVEm11bHRpX2FjY291bnRfbW9kZXGAWAcAAABlbmFibGVkcYFVEXRlbGVtZXRyeV9lbmFibGVkcYKIVRh1c2JfaWdub3JlZF9kZXZpY2VfbmFtZXNxg11xhChYCwAAAFJlY292ZXJ5IEhEcYVYAwAAAEVGSXGGWAIAAABWTXGHWAgAAABSZWNvdmVyeXGIWAcAAABQcmVib290cYlYCwAAAEdvb2dsZURyaXZlcYpYGAAAAEdvb2dsZSBEcml2ZSBGaWxlIFN0cmVhbXGLZVUecHZvX21heF9kaW1lbnNpb25fcGhvdG9fcGl4ZWxzcYxN/z9V

		HGVuYWJsZV9hbHdheXNfc2hvd19pbl9waG90b3NxjYhVGHBlcmZfdGhyb3R0bGVfcGVyY2VudGFnZXGOR0BYwAAAAAAAVRd1c2VyX2NvbmZpcm1hdGlvbl9kZWxheXGPR0AAAAAAAAAAVR1yZWd1bGFyX3BvbGxpbmdfaW50ZXJ2YWxfc2Vjc3GQSx5VGHB2b19yYXdfcGhvdG9fZXh0ZW5zaW9uc3GRXXGSKFgEAAAALmFyd3GTWAQAAAAuZG5ncZRYBAAAAC5uZWZxlVgEAAAALm5yd3GWWAQAAAAub3JmcZdYBAAAAC5wZWZxmFgEAAAALnJhZnGZWAQAAAAucncycZpYBAAAAC5zcndxm1gEAAAALmNyMnGcZVUcZG93bmxvYWRfY2hhbmdlX3Rocm90dGxlX3NlY3GdRz+pmZmZmZmaVSVtYXhfcGFnZV9zaXplX3NlbGVjdGl2ZV9zeW5jX2ZhbGxiYWNrcZ5N6ANVGW1heF9zaGExX21hdGNoX2JhdGNoX3NpemVxn0syVSNpbXByZXNzaW9uc19oZWFydGJlYXRfaW50ZXJ2YWxfc2Vjc3GgTTAqVRNlbmFibGVfY29udGV4dF9tZW51caGIVRZlbmFibGVfbmV0d29ya19zdG9yYWdlcaKJVRtlbmFibGVfaWdub3JhYmxlX2V4dGVuc2lvbnNxo4h1Yi4=
shown_setup_overlays	setup_overlay_id	choose_folders_setup_overlay
machine_folder_doc_id	value	1VyoeICinNi6u-MHRAosw-gcs84Za5azF
machine_folder_name	value	My PC (3)
shown_setup_overlays	setup_overlay_id	google_drive_setup_overlay
selective_sync	value	0
usb_sync_enabled	value	1
show_unparent_warning	value	1
delete_mode	value	1

storage_policy_mode	value	original
always_show_in_photos	value	1
share_notification	value	1
local_sync_root_path	value	\\?\C:\Users\IEUser\Google Drive
copy_duplicate_photos	value	1
user_email	value	psut.dfi@gmail.com
domain_policy	default_sync_all	1
domain_policy	domain_policy_description_url	
win10_icons_upgraded	value	1
cloud_graph_generation	value	7
tango_storage	value	gAJ9cQFVC0NsaWVudFRva2VucQJVVENpY0tKUW9HQ2dRSUF4QUJFaElKWmZteTBScjVhb0VSTUVVL1JqcHVwaVlhQndpQ01oQURHQUVTRkMvb3BENnhRNzFqdTZIU0pjNWZqaHlqbkpxSnMu
snapshot_reconstruct	value	0
root_config__0	rowkey	\\?\X:\PSUT
root_config__1	\\?\X:\PSUT	2
root_config__2	\\?\X:\PSUT	1

root_config__0	rowkey	\\?\C:\Users\IEUser\Google Drive
root_config__1	\\?\C:\Users\IEUser\Google Drive	2
root_config__2	\\?\C:\Users\IEUser\Google Drive	1
root_config__0	rowkey	\\?\X:\images
root_config__1	\\?\X:\images	2
root_config__2	\\?\X:\images	1
root_config__0	rowkey	\\?\X:\DFI
root_config__1	\\?\X:\DFI	2
root_config__2	\\?\X:\DFI	1
user_paused	value	0

B. APPENDIX 2

172.217.16.202 googleapis.l.google.com
216.239.36.10 ns3.google.com
204.79.197.1 ns1.a-msedge.net
172.217.22.42 googleapis.l.google.com
23.50.155.27 e8218.dscb1.akamaiedge.net
88.221.81.192 n0dscb1.akamaiedge.net
213.57.23.181 n5dscb1.akamaiedge.net
8.254.37.27 es-2.ns.nsatc.net
216.58.205.234 googleapis.l.google.com
172.217.21.234 googleapis.l.google.com
216.58.214.42 googleapis.l.google.com
199.93.59.27 b.ns.nsatc.net
172.217.23.138 googleapis.l.google.com
216.239.34.10 ns2.google.com
13.79.239.82 smartscreensvc.microsoft.com.nsatc.net
204.79.197.200 a-0001.a-msedge.net

172.217.18.10 googleapis.l.google.com
172.217.22.74 googleapis.l.google.com
213.57.23.183 n2dscb1.akamaiedge.net
216.58.210.10 googleapis.l.google.com
192.229.254.5 ns3.edgecastcdn.net
4.26.227.27 e.ns.nsatc.net
68.232.35.139 cs479.wac.edgecastcdn.net
216.239.32.10 ns1.google.com
216.58.207.42 googleapis.l.google.com
192.229.254.6 ns4.edgecastcdn.net
172.217.18.170 googleapis.l.google.com
82.212.80.76 r1.sn-q5h5h5m-5hhl.gvt1.com
82.102.180.204 n7dscb1.akamaiedge.net
172.217.23.161 googlehosted.l.googleusercontent.com
4.23.39.155 nl-1.ns.nsatc.net
172.217.22.106 googleapis.l.google.com
213.57.23.176 n4dscb1.akamaiedge.net
216.58.214.106 googleapis.l.google.com
8.254.92.155 b.ns.nsatc.net
216.58.207.74 googleapis.l.google.com
82.102.180.206 n3dscb1.akamaiedge.net
172.217.23.163 accounts-cctld.l.google.com
172.217.23.173 accounts.google.com
216.239.38.10 ns4.google.com
64.233.167.125 talk.l.google.com
198.78.208.155 b.ns.nsatc.net
82.102.180.207 n6dscb1.akamaiedge.net
216.58.206.10 googleapis.l.google.com
72.21.80.5 ns1.edgecastcdn.net
172.217.22.10 googleapis.l.google.com
172.217.23.174 drive.google.com
8.253.92.27 b.ns.nsatc.net
13.107.21.200 a-0001.a-msedge.net
72.21.80.6 ns2.edgecastcdn.net
2606:2800:e::5 ns3.edgecastcdn.net
2606:2800:e::6 ns4.edgecastcdn.net
2606:2800:1::5 ns1.edgecastcdn.net
2606:2800:1::6 ns2.edgecastcdn.net
2600:1480:e800::c0 a0dscb1.akamaiedge.net