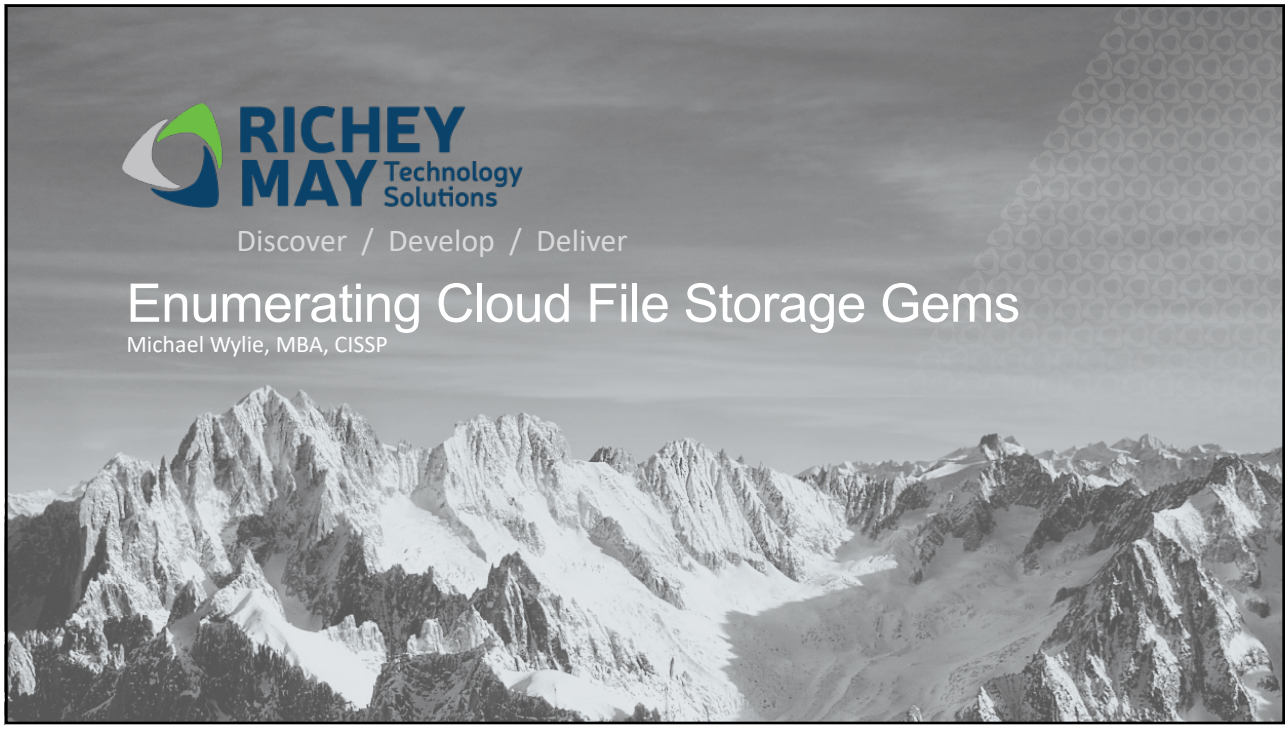


1

RICHEY MAY
TECHNOLOGY SOLUTIONS

About Me:

linkedin.com/in/mwylie

twitter.com/TheMikeWylie

Michael Wylie, TPN, MBA, CISSP

Director, Cybersecurity Services

RICHEY MAY TECHNOLOGY SOLUTIONS

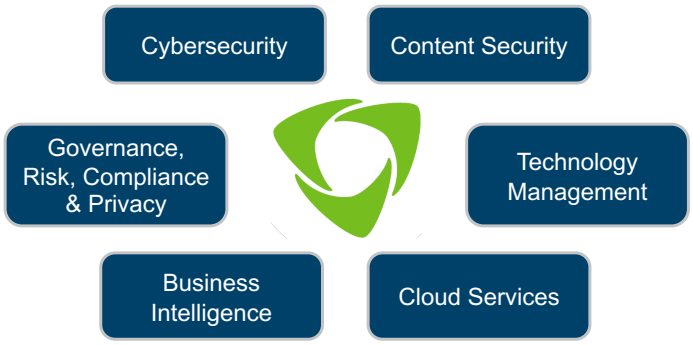
Additional	Certifications
• GPEN • GMON • PenTest+ • Project+ • Security+ • CEH & CEI	• CCNA R&S • CCNA CyberOps • Pentest+ • CHPA • Splunk User • GCFE

2

RICHEY MAY
TECHNOLOGY SOLUTIONS

About Richey May Technology Solutions

- Cloud Workflow Integration
- TPN Assessments & Readiness
- Vulnerability Scanning & Penetration Testing
- Forensics & Incident Response



3

RICHEY MAY
TECHNOLOGY SOLUTIONS

Learning Objectives

- Learn what file artifacts are available (e.g. local, cloud, deleted, and cached)
- See what kind of cloud file storage user activity can be enumerated
- Be introduced to application log capabilities
- Examine the differences between providers

4

RICHEY MAY
TECHNOLOGY SOLUTIONS

Credits

- Rob Lee
- Carlos Cajigas
- SANS Institute
- Mattia Eppifani
- Francesco Picasso
- Nicolas Ruff
- Florian Ledoux
- Eric Zimmerman
- Bit Forensics
- Spiceworks
- Insider Threat Report
- Chad Tilbury's
- Mark Hallman
- Peter Morin

5

RICHEY MAY
TECHNOLOGY SOLUTIONS

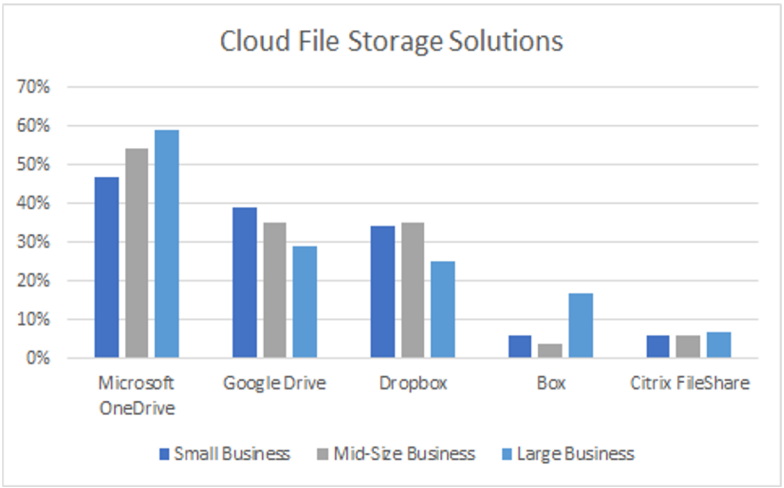
Cloud File Storage Overview

- Perceived Cloud File Storage Organization Benefits
  - Protection against disasters
  - Decrease in maintenance
  - High availability
  - Scalability
  - Ease of management
- Usage
  - Business
  - Personal

6

RICHEY MAY
TECHNOLOGY SOLUTIONS

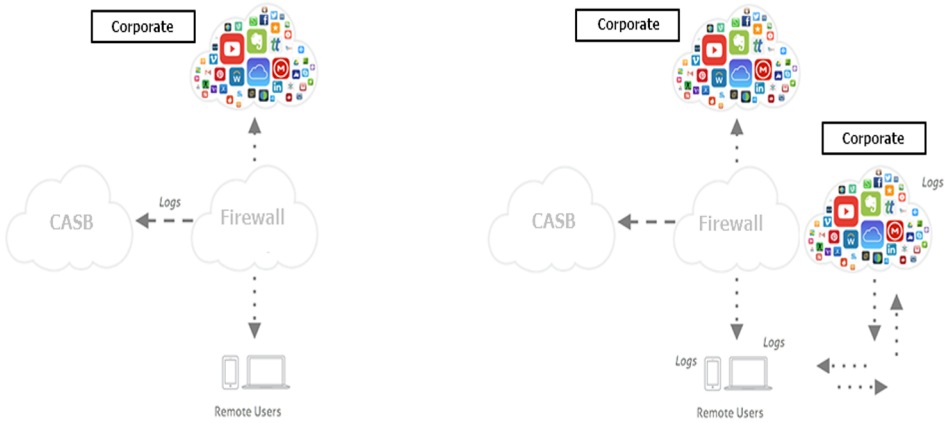
Cloud File Storage Solutions Usage



7

RICHEY MAY
TECHNOLOGY SOLUTIONS

Cloud File Storage Scenarios



8

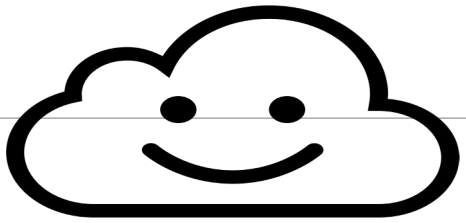
RICHEY MAY
TECHNOLOGY SOLUTIONS

Gems

- Many organizations are using cloud file storage as a file server replacement
  - Customer data, Financials, Employee data, etc.
- Cloud file storage apps leave behind:
  - Cached files
  - Local files
  - Database of local/cloud files
  - File usage
  - Traces of deleted files

9

RICHEY MAY
TECHNOLOGY SOLUTIONS



Business/Enterprise Account:

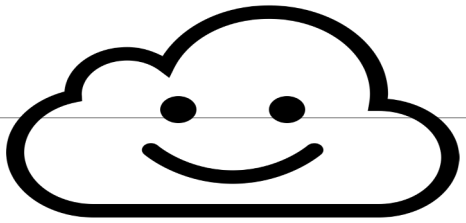
- Company issued
- Access to admin portal
- CASB (possibly)
- Access to cloud-side data
- Cloud based logs

Personal/Free Account:

- Not company issued
- No access to account
- No central visibility
- Access to endpoint data
- Local logs

10

RICHEY MAY TECHNOLOGY SOLUTIONS



Business/Enterprise Account

- G-Suite
- O365
- Box bus/enterprise
- Dropbox Pro

Personal/Free Account

- Google Drive (15GB)
- OneDrive Basic (5GB)
- Dropbox Basic (2GB)
- Box Starter (100GB)

11

RICHEY MAY TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Microsoft OneDrive

12

RICHEY MAY
TECHNOLOGY SOLUTIONS

Microsoft OneDrive

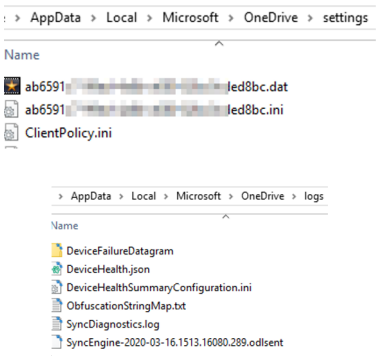
- Baked into Windows 8+
- Must be enabled via authentication
- Upon enabling OneDrive, ...\AppData\Local\Microsoft\OneDrive is created
- Personal OneDrive: %USERPROFILE%\AppData\Local\Microsoft\OneDrive\logs\Personal\
- Business/O365 OneDrive: %USERPROFILE%\AppData\Local\Microsoft\OneDrive\logs\Busines1\
- O365 Unified Audit Logs provides businesses with detailed logs up to 90 by default
- Personal OneDrive doesn't have the Audit log feature

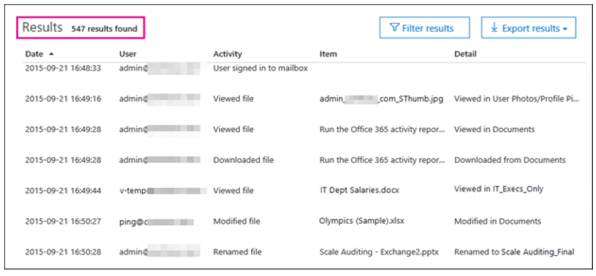
13

RICHEY MAY
TECHNOLOGY SOLUTIONS

Microsoft OneDrive: Log Files

Personal	Business





14

RICHEY MAY
TECHNOLOGY SOLUTIONS

Microsoft OneDrive: Files & Folders

Path	Details
%USERPROFILE%\OneDrive\	Default personal file store
%USERPROFILE%\OneDrive - [Company Name]	Default O365 file store
%USERPROFILE%\AppData\Local\Microsoft\OneDrive\logs\Personal\	Personal root log directory
%USERPROFILE%\AppData\Local\Microsoft\OneDrive\logs\Busines1\	O365 root log directory
%USERPROFILE%\AppData\Local\Microsoft\OneDrive\logs\[Personal | Business1]\SyncDiagnostics.log	Metadata for local & cloud file
%USERPROFILE%\AppData\Local\Microsoft\OneDrive\settings\[Personal | Business1]\[Cid].dat	List of local & cloud file names
%USERPROFILE%\AppData\Local\Microsoft\OneDrive\settings\[Personal | Business1]\[Cid].ini	File store location, sync time, usage details
%USERPROFILE%\AppData\Local\Microsoft\OneDrive\settings\Personal\[Cid]-ProfileServiceResponse.txt	Name, email, cid, email, phone, title, etc.
%USERPROFILE%\AppData\Local\Microsoft\OneDrive\logs\Business1\ObfuscationStringMap.txt	Key to obfuscated file/folder names

15

RICHEY MAY
TECHNOLOGY SOLUTIONS

Microsoft OneDrive: SyncDiagnostics.log

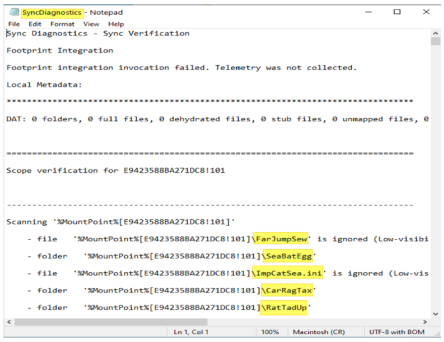
- Two types of SyncDiagnostics.log files
- During Testing:
  - O365 OneDrive = Summary SyncDiagnostics file
  - Lab VM 1 = Detailed SyncDiagnostics file
  - Lab VM 2 = Summary SyncDiagnostics file
- One theory is that the first system to sync with OneDrive gets the detailed file (assuming two or more devices), additional endpoints that sync with the same account get the summary file
- Location: %USERPROFILE%\AppData\Local\Microsoft\OneDrive\logs\[Personal | Business1]\SyncDiagnostics.log

16

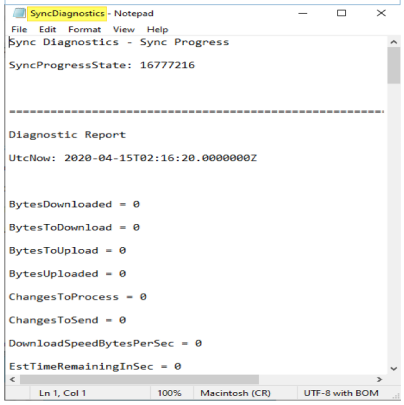
RICHEY MAY
TECHNOLOGY SOLUTIONS

Microsoft OneDrive: SyncDiagnostics.log

Detailed SyncDiagnostics File



Summary SyncDiagnostics File

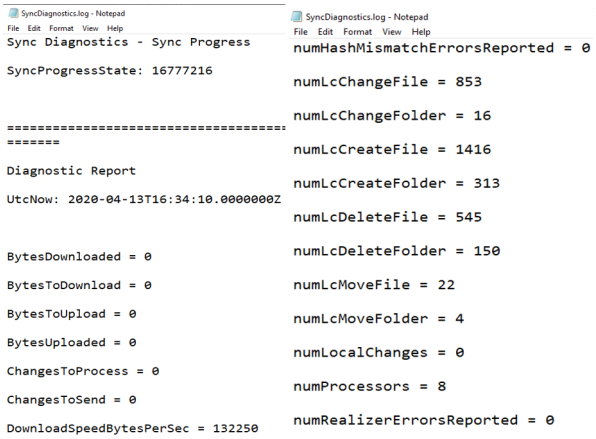


17

RICHEY MAY
TECHNOLOGY SOLUTIONS

Microsoft OneDrive: SyncDiagnostics.log

Summary Version

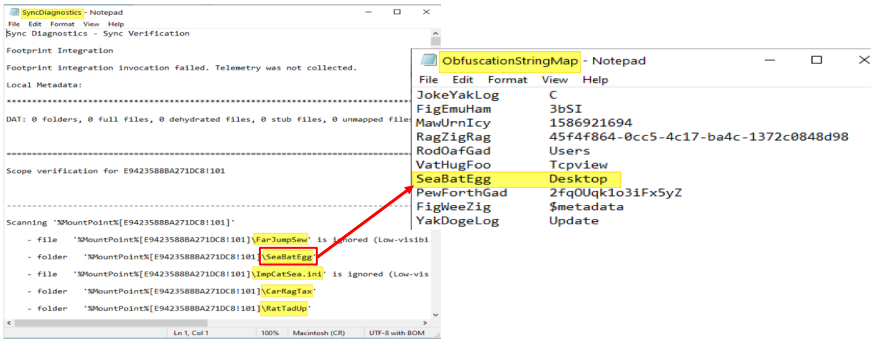


18

RICHEY MAY
TECHNOLOGY SOLUTIONS

Microsoft OneDrive: SyncDiagnostics.log

Detailed Version Decoded

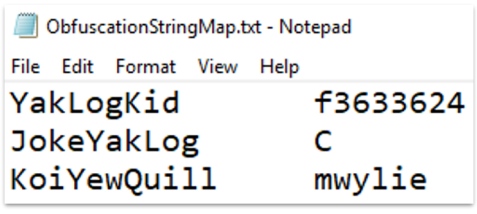


19

RICHEY MAY
TECHNOLOGY SOLUTIONS

Microsoft OneDrive: ObfuscationStringMap.txt

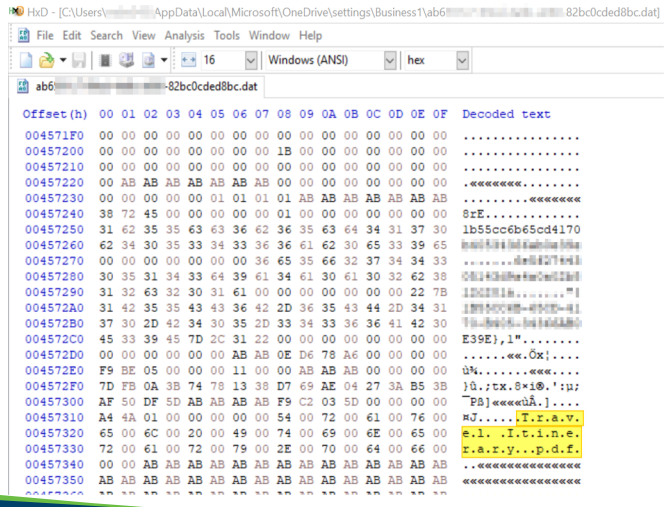
- De-obfuscation key to identify files and folders
- Left-side contains three-word key
- Right-side contains actual file or folder



20

RICHEY MAY
TECHNOLOGY SOLUTIONS

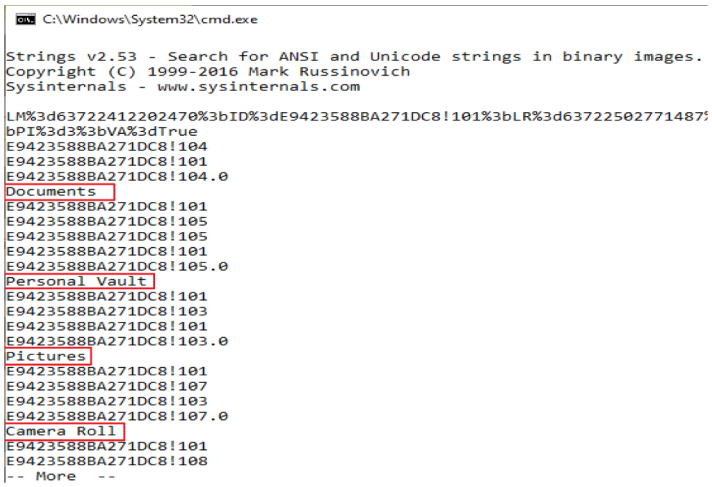
Microsoft OneDrive: [cid].dat



21

RICHEY MAY
TECHNOLOGY SOLUTIONS

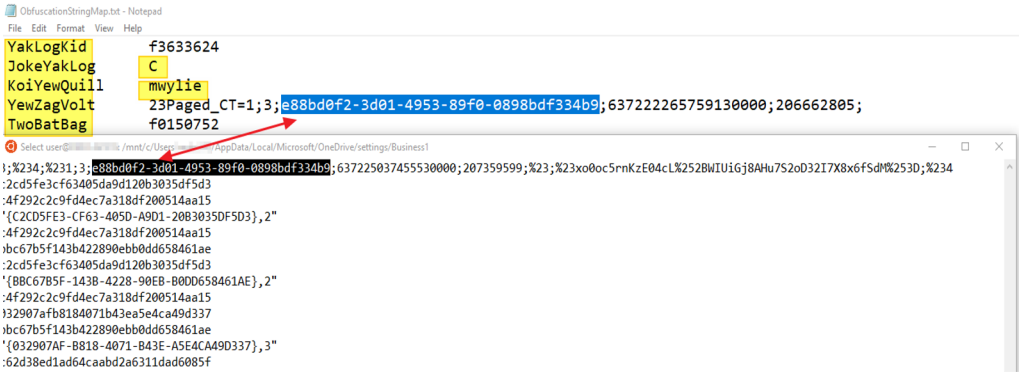
Microsoft OneDrive: [cid].dat (personal)



22

RICHEY MAY
TECHNOLOGY SOLUTIONS

Microsoft OneDrive: [cid].dat (business)

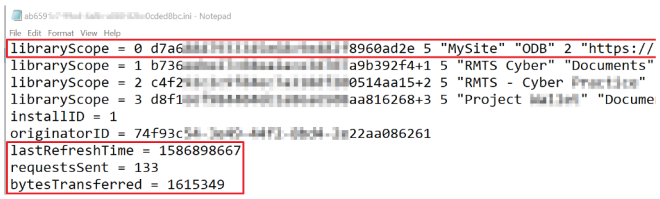


23

RICHEY MAY
TECHNOLOGY SOLUTIONS

Microsoft OneDrive: [cid].ini

- library (Personal) = cid, local OneDrive path
- libraryScope (Business) = cid, local OneDrive path
- lastRefreshTime = last sync with cloud (epoch time)
- requestSent = sync activity during last sync
- BytesTransferred = amount of data transferred at last sync

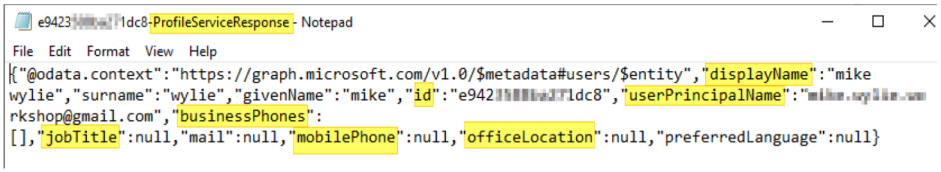


24

RICHEY MAY
TECHNOLOGY SOLUTIONS

Microsoft OneDrive: [cid]-ProfileServiceResponse

- Does not exist in business/O365 accounts, only personal accounts
- Contains:
  - Display Name
  - First / Last Name
  - Cid
  - Email Address
  - Phone
  - Title
  - Address
  - More



25

RICHEY MAY
TECHNOLOGY SOLUTIONS

Microsoft OneDrive: Registry Keys

Business1	Personal	Common
IsGoSov WebServiceUrl ECSConfigurationETag ECSConfigurationExpires ECSConfigurationMaxAge ECSConfigurationLastSuccess ConfiguredTenantId cid UserEmail SPOLastUpdate TeamSiteSPOResourceId DisplayName SPOResourceId ServiceEndpointUri PUID UserName FirstRunSignInOrigin Business NamespaceRootId LastSignInTime GrooveTakeoverAttemptedOperations GrooveTakeoverSuccessfulOperations ClientFirstSignInTimestamp ProviderOptInEnabled UserFolder EdpManaged LastKnownCloudFilesEnabled FirstRun LastMigrationScanResult NextOneRmUpdateTime HasMadeFirstUpload ShareTimeStamp NextMigrationScan CrashDetectionKey \AuthenticationURLs \ScopeIdToMountPointPathCache \Tenants \WindowsSecurityCenterIntegration	ECSConfigurationETag ECSConfigurationExpires ECSConfigurationMaxAge ECSConfigurationLastSuccess IsGoSov FirstRunSignInOrigin UserEmail NamespaceRootId LastSignInTime ClientFirstSignInTimestamp cid ProviderOptInEnabled UserFolder LastKnownCloudFilesEnabled FirstRun IsUpgradeAvailable VaultShortcutPath HasMadeFirstUpload NextMigrationScan LastMigrationScanResult NextOneRmUpdateTime CrashDetectionKey \AuthenticationURLs \ScopeIdToMountPointPathCache \Tenants \WindowsSecurityCenterIntegration	ECSConfigurationETag ECSConfigurationExpires ECSConfigurationMaxAge ECSConfigurationLastSuccess IsGoSov FirstRunSignInOrigin UserEmail NamespaceRootId LastSignInTime ClientFirstSignInTimestamp cid ProviderOptInEnabled UserFolder LastKnownCloudFilesEnabled FirstRun HasMadeFirstUpload NextMigrationScan LastMigrationScanResult NextOneRmUpdateTime CrashDetectionKey \AuthenticationURLs \ScopeIdToMountPointPathCache \Tenants \WindowsSecurityCenterIntegration

26

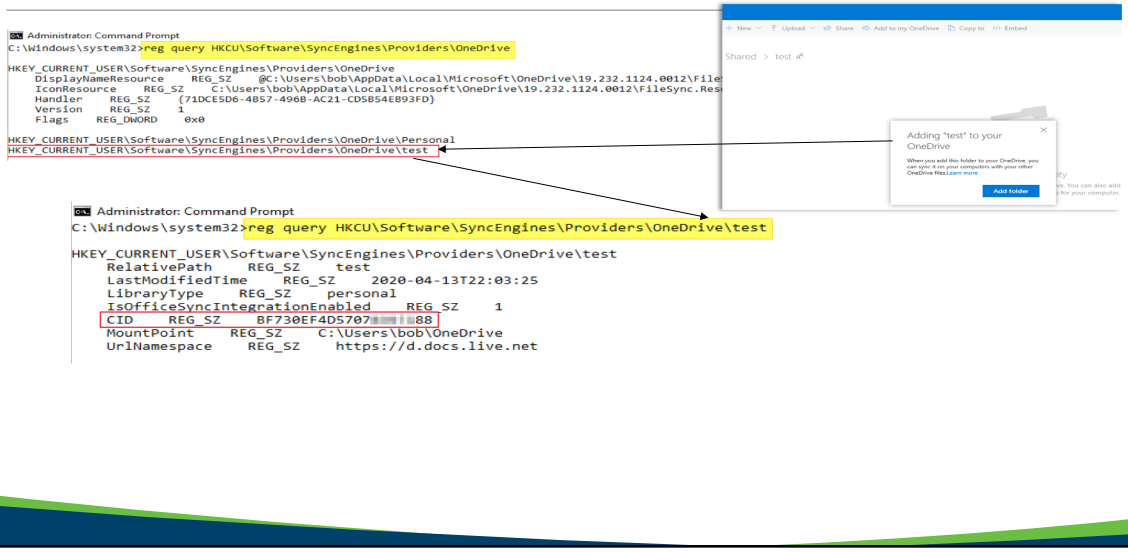
RICHEY MAY
TECHNOLOGY SOLUTIONS

Microsoft OneDrive: O365 Shared Folders

27

RICHEY MAY
TECHNOLOGY SOLUTIONS

Microsoft OneDrive: Personal Shared Folders

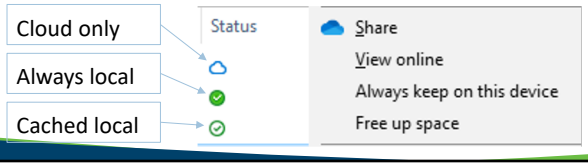


28

RICHEY MAY TECHNOLOGY SOLUTIONS

Microsoft OneDrive: Space Saver

- Early days of cloud file storage mass local storage and bandwidth
- Early storage solutions allowed for folder inclusion/exclusion
- Newer solutions allow users to view cloud stored file names
  - E.g. OneDrive - “Always keep on this device” and “Free up space”
  - E.g. Dropbox Smart Sync
- Depending on the client/solution, metadata may exist for local and cloud files
- Deleted files are often moved from all synced endpoints to independent recycle bins
- Deleted files are often moved in the cloud file storage solution to a recycle bin



29

RICHEY MAY TECHNOLOGY SOLUTIONS

RICHEY MAY TECHNOLOGY SOLUTIONS

Google Drive

30

RICHEY MAY
TECHNOLOGY SOLUTIONS

Google Drive

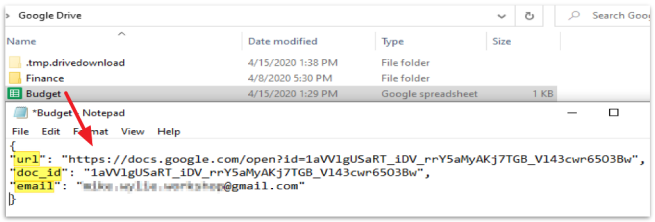
- Personal = Backup and Sync (formerly called Google Drive)
- Business = Drive File Stream (part of G-Suite)
- SQLite database rather than text files used by OneDrive

31

RICHEY MAY
TECHNOLOGY SOLUTIONS

Google Drive

- Drive File Stream creates a virtual volume (FAT32) and is mounted
- Synced Google formatted files create shells with the following attributes:
  - URL
  - Doc_id
  - Email



32

RICHEY MAY
TECHNOLOGY SOLUTIONS

Google Drive: Files

Path	Details
%USERPROFILE%\Google Drive\	Default personal file store
%USERPROFILE%\Google Drive\	Default business file store
%USERPROFILE%\Appdata\Local\Google\Drive\user_default\sync_config.db	User info, preferences, and initial application install info
%USERPROFILE%\Appdata\Local\Google\Drive\user_default\cloud_graph\cloud_graph.db	Metadata for local, cloud, and shared files/folders
%USERPROFILE%\Appdata\Local\Google\Drive\user_default\sync_log.log	File add/delete/modify/rename
%USERPROFILE%\Appdata\Local\Google\Drive\user_default\snapshot.db	Local file metadata
%USERPROFILE%\Appdata\Local\Google\DriveFS\[GSuite Email in Base64]\content_cache	Local file cache (G-Suite)
%USERPROFILE%\Appdata\Local\Google\DriveFS\metadata_sqlite_db	Offline file, cloud, and deleted file metadata

33

RICHEY MAY
TECHNOLOGY SOLUTIONS

Google Drive: sync_config.db

entry_key	Description
highest_app_version	Installed application version
local_sync_root_path	Path to local file store
user_email	Gmail account/email

34

RICHEY MAY
TECHNOLOGY SOLUTIONS

Google Drive: sync_config.db

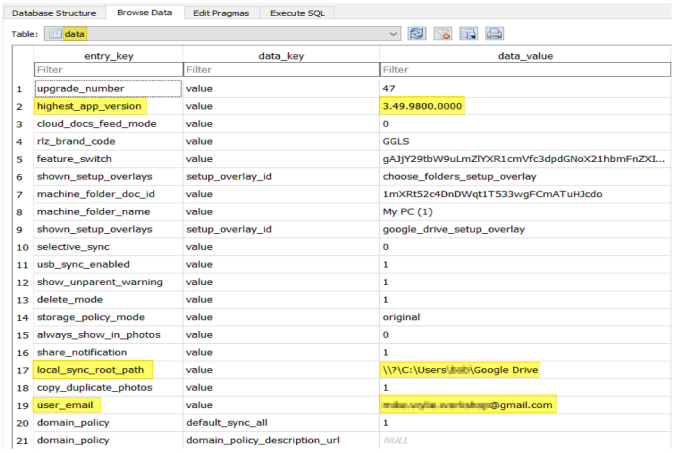

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: data

	entry_key	data_key	data_value
	Filter	Filter	Filter
1	upgrade_number	value	47
2	highest_app_version	value	3.49.9800.0000
3	cloud_docs_feed_mode	value	0
4	rlz_brand_code	value	GGLS
5	feature_switch	value	gAJjY29tbW9uLmZlYXR1cmVfc3dpdGNoX21hbmFnZXI...
6	shown_setup_overlays	setup_overlay_id	choose_folders_setup_overlay
7	machine_folder_doc_id	value	1mXRt52c4DnDWqt1T533wgFCmATuHJcdo
8	machine_folder_name	value	My PC (1)
9	shown_setup_overlays	setup_overlay_id	google_drive_setup_overlay
10	selective_sync	value	0
11	usb_sync_enabled	value	1
12	show_unparent_warning	value	1
13	delete_mode	value	1
14	storage_policy_mode	value	original
15	always_show_in_photos	value	0
16	share_notification	value	1
17	local_sync_root_path	value	\\?\C:\Users\bob\Google Drive
18	copy_duplicate_photos	value	1
19	user_email	value	[redacted]@gmail.com
20	domain_policy	default_sync_all	1
21	domain_policy	domain_policy_description_url	NULL

35

RICHEY MAY
TECHNOLOGY SOLUTIONS

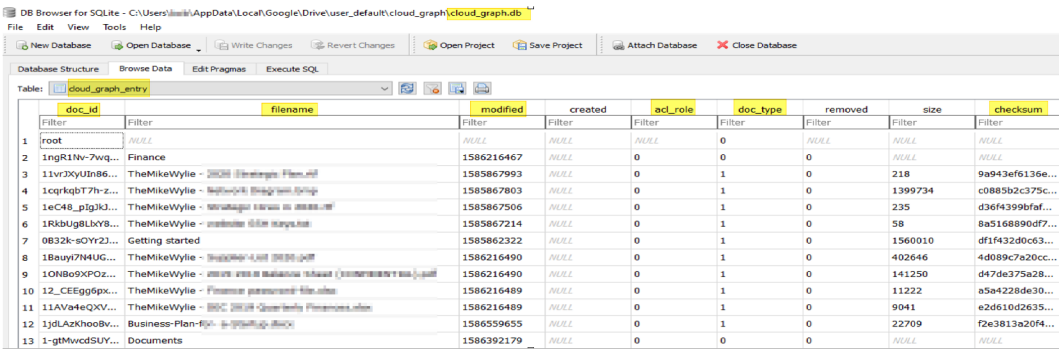
Google Drive: cloud_graph.db

Column	Description
doc_id	Unique ID for each file/folder
filename	File/folder name
modified	Time when file was added go Google Drive (Unix epoch)
acl_role	0 = this user is the owner / 1 = other owner
doc_type	Google formated file or traditional file (e.g. 0 = folder / 1 = traditional file / 2-13 = Google Files / 2 = Presentation / 4 = Spreadsheet / 6 = Google Doc)
removed	Deleting a file doesn't appear to modify this field
checksum	MD5 hash

36

RICHEY MAY
TECHNOLOGY SOLUTIONS

Google Drive: cloud_graph.db



	doc_id	filename	modified	created	acl_role	doc_type	removed	size	checksum
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	root	NULL	NULL	NULL	NULL	0	NULL	NULL	NULL
2	1ngR1Nv-7wq...	Finance	1586216467	NULL	0	0	0	NULL	NULL
3	11vrJXyUIn86...	TheMikeWylie - [redacted]	1585867993	NULL	0	1	0	218	9a943ef6136e...
4	1cqrkqbT7h-z...	TheMikeWylie - [redacted]	1585867803	NULL	0	1	0	1399734	c0885b2c375c...
5	1eC48_pIg3kJ...	TheMikeWylie - [redacted]	1585867506	NULL	0	1	0	235	d36f4399bfaf...
6	1RkbUg8LbY8...	TheMikeWylie - [redacted]	1585867214	NULL	0	1	0	58	8a5168890df7...
7	0B32k-sOYr2J...	Getting started	1585862322	NULL	0	1	0	1560010	df1f432d0c63...
8	1Bauyi7N4UG...	TheMikeWylie - [redacted]	1586216490	NULL	0	1	0	402646	4d089c7a20cc...
9	1ON8o9XPOz...	TheMikeWylie - [redacted]	1586216490	NULL	0	1	0	141250	d47de375a28...
10	12_CEEgg6px...	TheMikeWylie - [redacted]	1586216489	NULL	0	1	0	11222	a5a4228de30...
11	11AVa4eQXV...	TheMikeWylie - [redacted]	1586216489	NULL	0	1	0	9041	e2d610d2635...
12	1jdLAzKhooBv...	Business-Plan-[redacted]	1586559655	NULL	0	1	0	22709	f2e3813a20f4...
13	1-gtMwcdSUY...	Documents	1586392179	NULL	0	0	0	NULL	NULL

37

RICHEY MAY
TECHNOLOGY SOLUTIONS

Google Drive: sync_log.log

- Insights into a user's activity on a personal account
- Bash, SIEM, ElasticStack, SumoLogic, etc. can parse the events
- Interesting Actions:
  - Action.CREATE
  - Action.DELETE
  - Action.MODIFY
  - Action.RENAME
  - Action.CHANGE
  - Action.MOVE
  - Action.CHANGE_ACL

38

RICHEY MAY
TECHNOLOGY SOLUTIONS

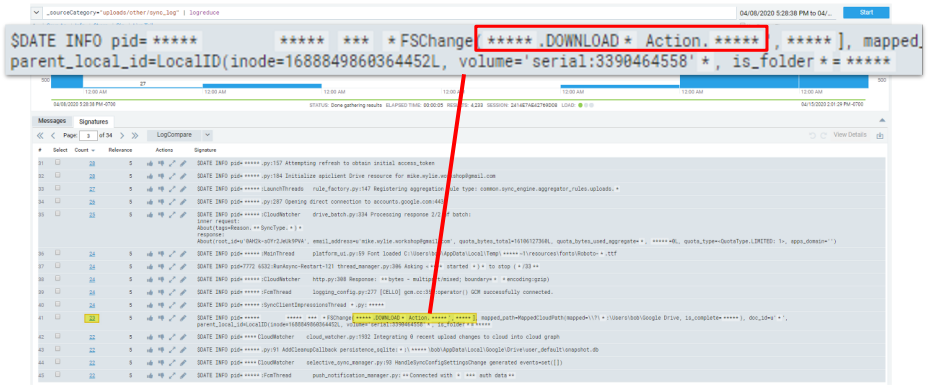
Google Drive: sync_log.log

- Action Source:
  - Direction.DOWNLOAD (initiated by cloud activity)
  - Direction.UPLOAD (initiated by local activity)
- Sharing:
  - Shared=True
- File Name:
  - name=u'example.pdf'

39

RICHEY MAY
TECHNOLOGY SOLUTIONS

Google Drive: sync_log.log



40

RICHEY MAY
TECHNOLOGY SOLUTIONS

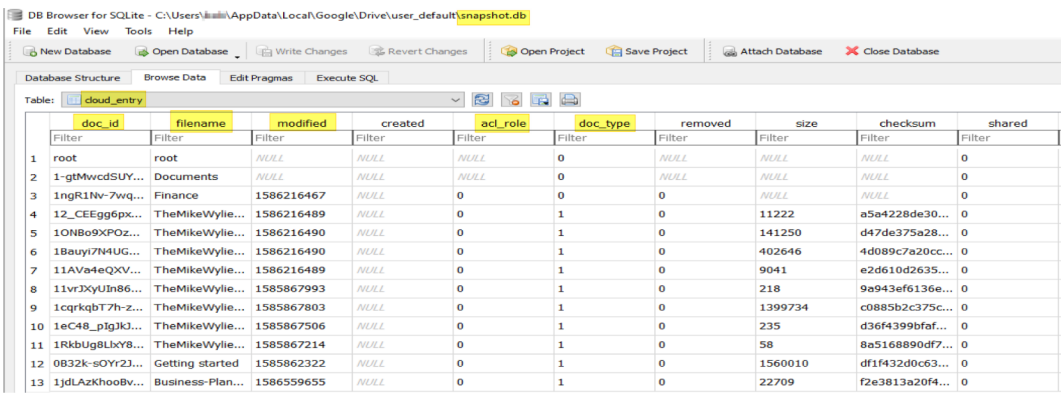
Google Drive: snapshot.db

Column	Description
doc_id	Unique ID for each file/folder
filename	File/folder name
modified	Time when file was added go Google Drive (Unix epoch)
acl_role	0 = this user is the owner / 1 = other owner
doc_type	Google formated file or traditional file (e.g. 0 = folder / 1 = traditional file / 2-13 = Google Files / 2 = Presentation / 4 = Spreadsheet / 6 = Google Doc)
removed	Deleting a file doesn't appear to modify this field
checksum	MD5 hash
shared	Shared with other users (0 = not shared / 1 = shared)

41

RICHEY MAY
TECHNOLOGY SOLUTIONS

Google Drive: snapshot.db



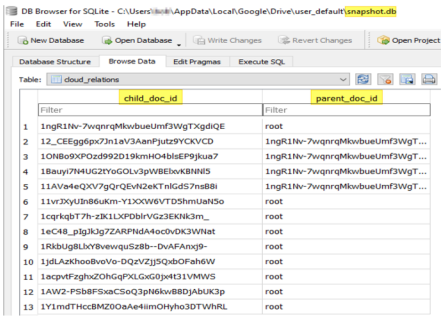
	doc_id	filename	modified	created	acl_role	doc_type	removed	size	checksum	shared
1	root	root	NULL	NULL	NULL	0	NULL	NULL	NULL	0
2	1-gtMwcdSUY...	Documents	NULL	NULL	NULL	0	NULL	NULL	NULL	0
3	1ngR1Nv-7wq...	Finance	1586216467	NULL	0	0	0	NULL	NULL	0
4	12_CEEgg6px...	TheMikeWylie...	1586216489	NULL	0	1	0	11222	a5a4228de30...	0
5	1ONBo9XPOz...	TheMikeWylie...	1586216490	NULL	0	1	0	141250	d47de375a28...	0
6	1Bauyi7N4UG...	TheMikeWylie...	1586216490	NULL	0	1	0	402646	4d089c7a20cc...	0
7	11AVa4eQXV...	TheMikeWylie...	1586216489	NULL	0	1	0	9041	e2d610d2635...	0
8	11vrJXyUIn86...	TheMikeWylie...	1585867993	NULL	0	1	0	218	9a943ef6136e...	0
9	1cqrkqbT7h-z...	TheMikeWylie...	1585867803	NULL	0	1	0	1399734	c0885b2c375c...	0
10	1eC48_pIgJkJ...	TheMikeWylie...	1585867506	NULL	0	1	0	235	d36f4399bfaf...	0
11	1RkbUg8LlxY8...	TheMikeWylie...	1585867214	NULL	0	1	0	58	8a5168890df7...	0
12	0B32k-sOYr2J...	Getting started	1585862322	NULL	0	1	0	1560010	df1f432d0c63...	0
13	1jdLAzKhooBv...	Business-Plan...	1586559655	NULL	0	1	0	22709	f2e3813a20f4...	0

42

RICHEY MAY
TECHNOLOGY SOLUTIONS

Google Drive: snapshot.db & cloud_graph.db

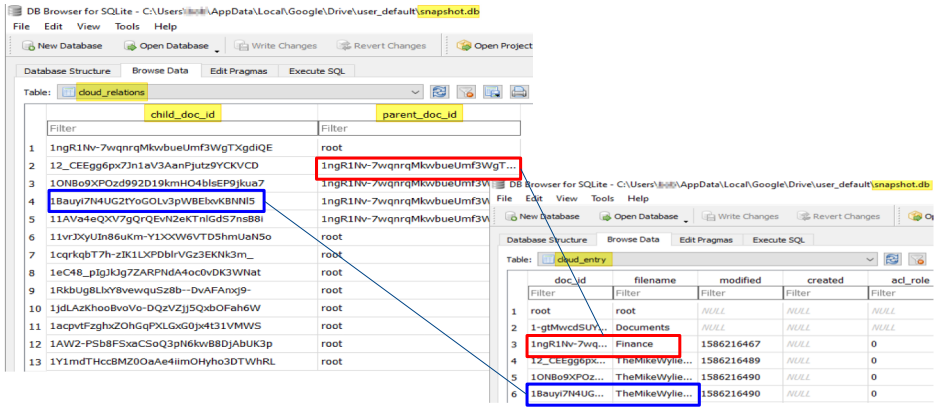
Column	Description
child_doc_id	Sub-subject (e.g. a file within a folder)
parent_doc_id	Parent object (e.g. folder which a file is located in)



43

RICHEY MAY
TECHNOLOGY SOLUTIONS

Google Drive: snapshot.db & cloud_graph.db



44

RICHEY MAY TECHNOLOGY SOLUTIONS

Dropbox

45

RICHEY MAY TECHNOLOGY SOLUTIONS

Dropbox

- Dropbox uses encrypted SQLlite databases (SQLite Encryption Extension (SEE)) since 2011
  - Key stored in registry and encrypted with Windows Data Protection API (DPAPI)
  - Options to access the database content:
    - Brute force password
    - Extract DPAPI from memory
  - Francesco Picasso's decwindbx toolkit can be used to extract keys

46

RICHEY MAY
TECHNOLOGY SOLUTIONS

Dropbox

- .dropbox.cache contains misc. temporary/cached files (e.g. files deleted by others)
- Deleted items go into local recycle bin and online “Deleted files” folder
  - Deleted files do not get purged from the local recycle bin
  - Deleted files get purged online between 30-120 days depending on subscription
- Cloud logging:
  - Detailed online in paid/business accounts
  - Limited event logging in free versions

47

RICHEY MAY
TECHNOLOGY SOLUTIONS

Dropbox: db Encryption

- Key is stored in the registry
  - HKCU\SOFTWARE\Dropbox\ks\Client
    - %USERPROFILE%\AppData\Local\Dropbox\instance_db
  - HKCU\SOFTWARE\Dropbox\ks1\Client
    - %USERPROFILE%\AppData\Local\Dropbox\instance1

48

RICHEY MAY
TECHNOLOGY SOLUTIONS

Dropbox: db Encryption

- Registry key is protected by DPAPI blobs
- .DBX decryption toolkit: https://github.com/dfirfpi/decwindbx
  - dbx-key-win-live.ps1 (unable to find keys in my lab)
  - dbx-key-win-live.ps1 (requires pbkdf2 & pypiwin32 - unable to find keys)
  - > sqlite-dbx-win64.exe -key <dbx_key> config.dbx ".backup config.db"

49

RICHEY MAY
TECHNOLOGY SOLUTIONS

Dropbox: Files

Path	Details
%USERPROFILE%\Dropbox\	Default file store
%USERPROFILE%\Dropbox\.dropbox.cache & .dropbox	Temporary file store
%USERPROFILE%\AppData\Local\Dropbox\filecache.dbx	Sometimes missing. Metadata for cloud, local, and deleted files
%USERPROFILE%\AppData\Local\Dropbox\info.json	File store path, host ID, team setting, and subscription type
%USERPROFILE%\AppData\Local\Dropbox\host.db	File store path in Base64
%USERPROFILE%\AppData\Local\Dropbox\host.dbx	
%USERPROFILE%\AppData\Local\Dropbox\instance1\	Location for numerous databases
%USERPROFILE%\AppData\Local\Dropbox\instance1\config.dbx	Email, local file store, email, hostname
%USERPROFILE%\AppData\Local\Dropbox\instance1\home.db	SQLite3 db - failed to open in DB browser tools. File names seen in file.
%USERPROFILE%\AppData\Local\Dropbox\instance1\aggregation.dbx	SQLite3 db - failed to open in DB browser tools. File names seen in file.

50

RICHEY MAY
TECHNOLOGY SOLUTIONS

Box

51

RICHEY MAY
TECHNOLOGY SOLUTIONS

Box: Files

Path	Details
%USERPROFILE%\Box\	Default file store
%USERPROFILE%\AppData\Local\Box\Box\cache\	Complete files which were opened locally and cached
%USERPROFILE%\AppData\Local\Box\Box\logs\	Path to log files
%USERPROFILE%\AppData\Local\Box\Box\logs\box-[version].log	Detailed activity log
%USERPROFILE%\AppData\Local\Box\Box\logs\BoxUI_[#]_[date].log	Box application log (e.g. login/off & network connectivity)
%USERPROFILE%\AppData\Local\Box\Box\logs\Box_Streem_[#]_[date].log	File activity - metadata, paths, log location, log level, free space, etc.
%USERPROFILE%\AppData\Local\Box\Box\data\	Path to databases
%USERPROFILE%\AppData\Local\Box\Box\data\shell\sync_root_folder.txt	Default file store path
%USERPROFILE%\AppData\Local\Box\Box\data\sync.db & streemfs.db	Local files, cloud files, cached files
%USERPROFILE%\AppData\Local\Box\Box\data\metrics.db	Username & email

52

RICHEY MAY
TECHNOLOGY SOLUTIONS

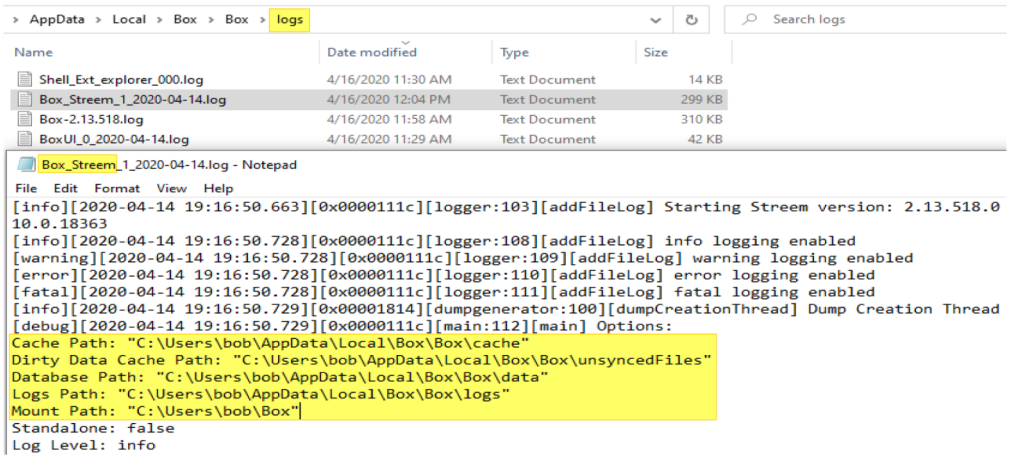
Box: Box_Streem_[#]_[date].log

- Parse Box_Streem log(s) for key actions:
  - addFile
  - addFolder
  - onDeleteFile
  - onDeleteFolder
  - onOpenFile
  - onClosefile
  - onReadFile
  - onCreateFile
  - onWriteFile
  - onGetFileInfo

53

RICHEY MAY
TECHNOLOGY SOLUTIONS

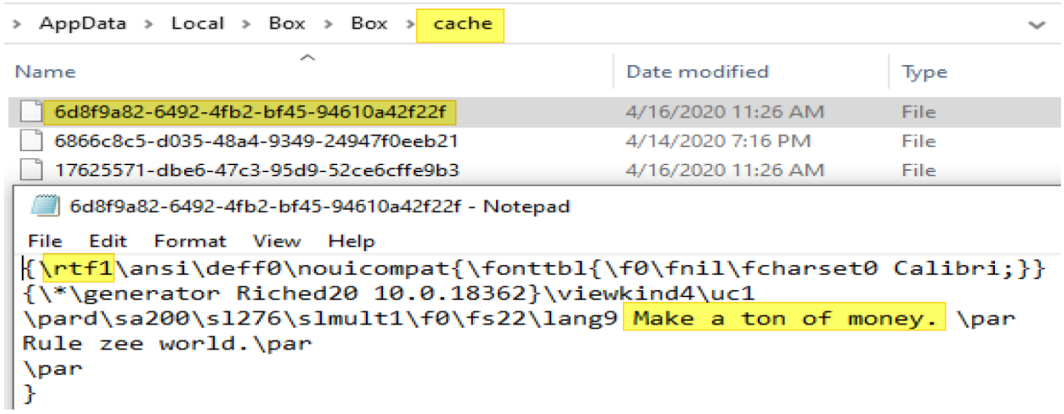
Box: Box_Streem_[#]_[date].log



54

RICHEY MAY
TECHNOLOGY SOLUTIONS

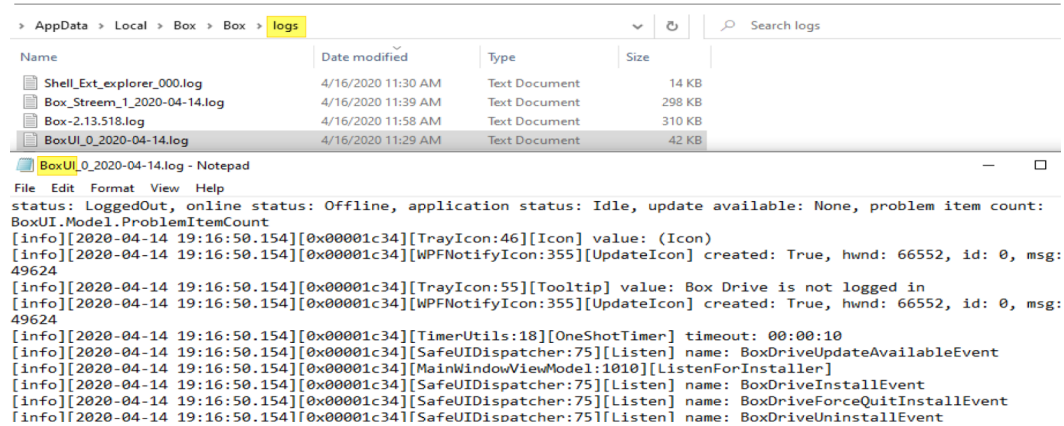
Box: …\Box\Box\cache



55

RICHEY MAY
TECHNOLOGY SOLUTIONS

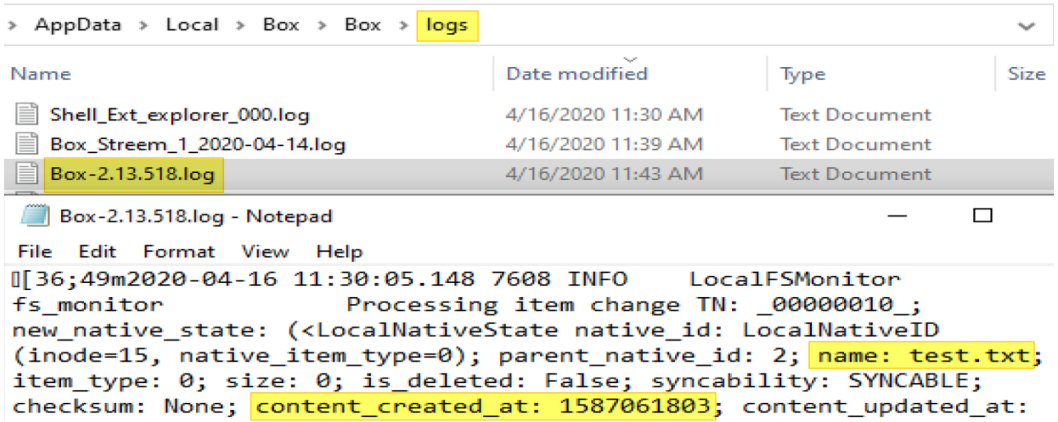
Box: BoxUI_[#]_[date].log



56

RICHEY MAY
TECHNOLOGY SOLUTIONS

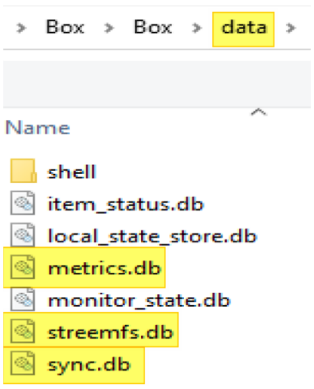
Box: Box-[version].log



57

RICHEY MAY
TECHNOLOGY SOLUTIONS

Box: Databases



58

RICHEY MAY
TECHNOLOGY SOLUTIONS

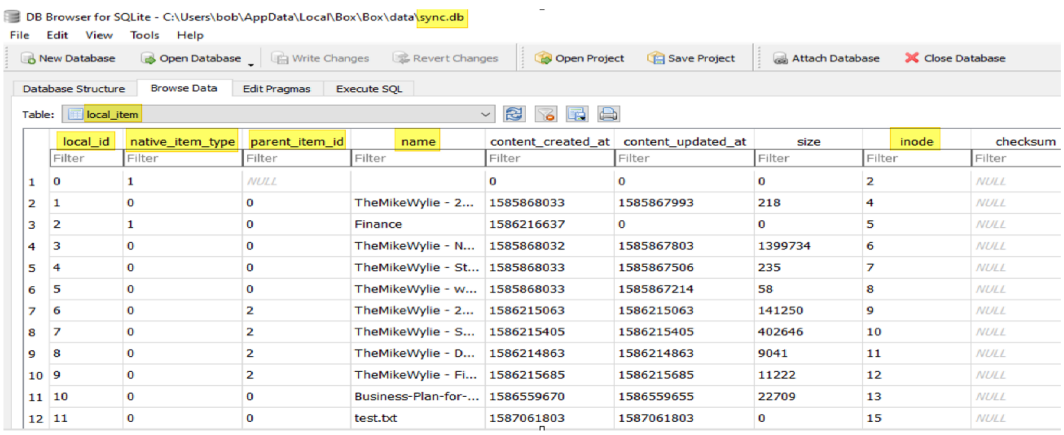
Box: sync.db

Column	Description
box_id	Unique object ID
item_type	0 = file / 1 = folder
parent_item_id	Parent folder's box_id
name	File name
owner_id	Box account owner's ID
checksum	SHA1 file hash
content_created_at	Object created time (Unix epoch)
content_updated_at	Object modified time (Unix epoch)

59

RICHEY MAY
TECHNOLOGY SOLUTIONS

Box: sync.db



	local_id	native_item_type	parent_item_id	name	content_created_at	content_updated_at	size	inode	checksum
1	0	1	NULL		0	0	0	2	NULL
2	1	0	0	TheMikeWylie - 2...	1585868033	1585867993	218	4	NULL
3	2	1	0	Finance	1586216637	0	0	5	NULL
4	3	0	0	TheMikeWylie - N...	1585868032	1585867803	1399734	6	NULL
5	4	0	0	TheMikeWylie - St...	1585868033	1585867506	235	7	NULL
6	5	0	0	TheMikeWylie - w...	1585868033	1585867214	58	8	NULL
7	6	0	2	TheMikeWylie - 2...	1586215063	1586215063	141250	9	NULL
8	7	0	2	TheMikeWylie - S...	1586215405	1586215405	402646	10	NULL
9	8	0	2	TheMikeWylie - D...	1586214863	1586214863	9041	11	NULL
10	9	0	2	TheMikeWylie - Fi...	1586215685	1586215685	11222	12	NULL
11	10	0	0	Business-Plan-for-...	1586559670	1586559655	22709	13	NULL
12	11	0	0	test.txt	1587061803	1587061803	0	15	NULL

60

RICHEY MAY
TECHNOLOGY SOLUTIONS

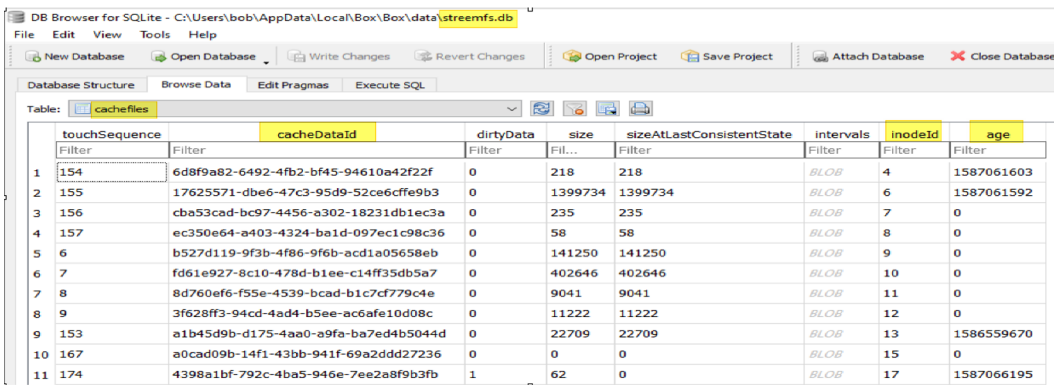
Box: Streemfs.db

Column	Description
touchSequence	
cacheDataId	File name of in %USERPROFILE%\AppData\Local\Box\Box\cache\
inodeId	Universal Box ID
age	When a file was cached (0 if not cached)

61

RICHEY MAY
TECHNOLOGY SOLUTIONS

Box: streemfs.db

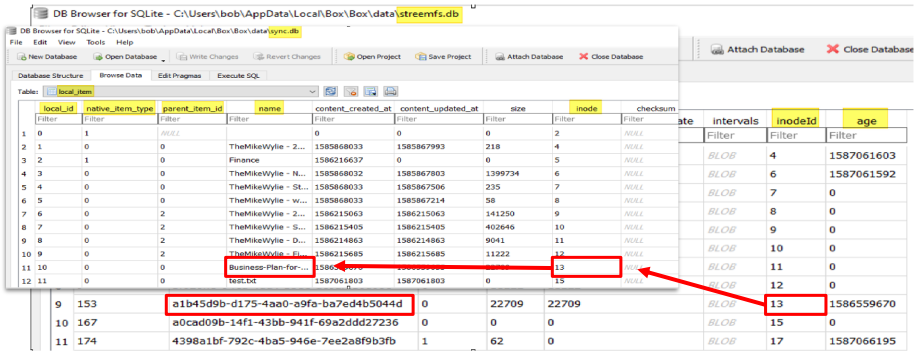


	touchSequence	cacheDataId	dirtyData	size	sizeAtLastConsistentState	intervals	inodeId	age
1	154	6d8f9a82-6492-4fb2-bf45-94610a42f22f	0	218	218	BLOB	4	1587061603
2	155	17625571-dbe6-47c3-95d9-52ce6cffe9b3	0	1399734	1399734	BLOB	6	1587061592
3	156	cba53cad-bc97-4456-a302-18231db1ec3a	0	235	235	BLOB	7	0
4	157	ec350e64-a403-4324-ba1d-097ec1c98c36	0	58	58	BLOB	8	0
5	6	b527d119-9f3b-4f86-9f6b-acd1a05658eb	0	141250	141250	BLOB	9	0
6	7	fd61e927-8c10-478d-b1ee-c14ff35db5a7	0	402646	402646	BLOB	10	0
7	8	8d760ef6-f55e-4539-bcad-b1c7cf779c4e	0	9041	9041	BLOB	11	0
8	9	3f628ff3-94cd-4ad4-b5ee-ac6afe10d08c	0	11222	11222	BLOB	12	0
9	153	a1b45d9b-d175-4aa0-a9fa-ba7ed4b5044d	0	22709	22709	BLOB	13	1586559670
10	167	a0cad09b-14f1-43bb-941f-69a2ddd27236	0	0	0	BLOB	15	0
11	174	4398a1bf-792c-4ba5-946e-7ee2a8f9b3fb	1	62	0	BLOB	17	1587066195

62

RICHEY MAY
TECHNOLOGY SOLUTIONS

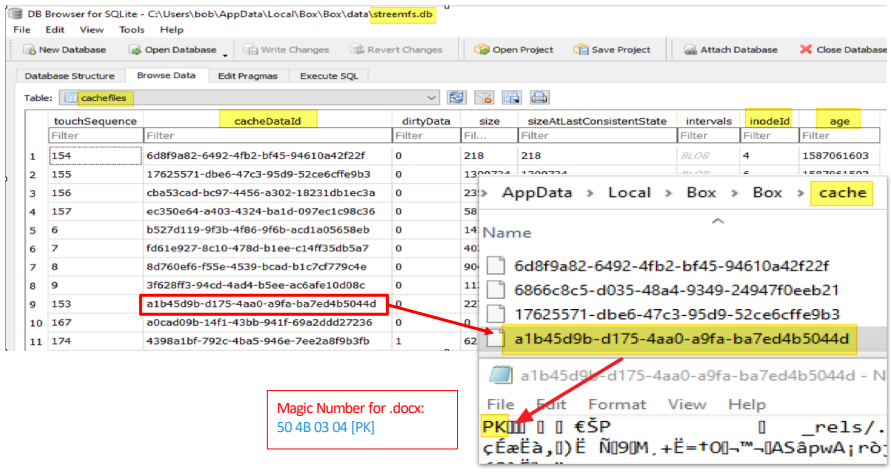
Box: streemfs.db



63

RICHEY MAY
TECHNOLOGY SOLUTIONS

Box: streemfs.db

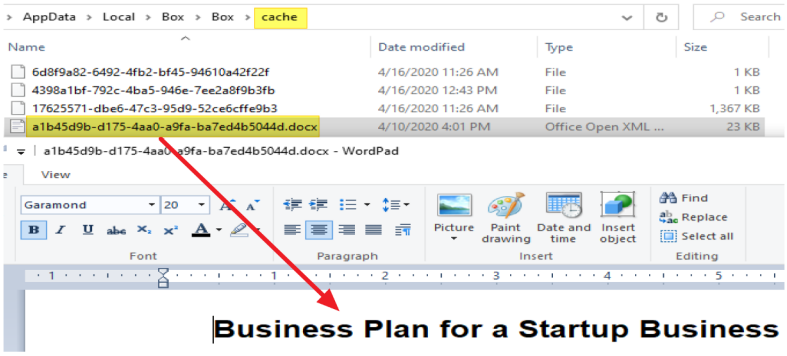


Magic Number for .docx:
50 4B 03 04 [PK]

64

RICHEY MAY
TECHNOLOGY SOLUTIONS

Box: streemfs.db



65

RICHEY MAY
TECHNOLOGY SOLUTIONS

Box: streemfs.db

Column	Description
isFile	0 = folder / 1 = file
parentInodeId	Parent folder inodeId
name	File name
createdAtTimestamp	Unix epoch time the object was created
ModifiedAtTimestamp	Unix epoch time the object was modified
accessedAtTimestamp	Unix epoch time the object was accessed
inodeId	Universal Box object ID
markForOffline	0 = folder to be kept as offline copy
folderFetchTimestamp	Unix epoch time of last folder sync

66

RICHEY MAY TECHNOLOGY SOLUTIONS

Citrix ShareFile

67

RICHEY MAY TECHNOLOGY SOLUTIONS

Citrix ShareFile

- Application download protected by trial registration
- Designed for business/enterprise
- No “free” version, however Gmail email addresses can instantly request a trial
- Upon installation, ShareFile creates a virtual volume (FAT32) and is mounted (S:\)
- Databases are SQLite and unencrypted

68

RICHEY MAY
TECHNOLOGY SOLUTIONS

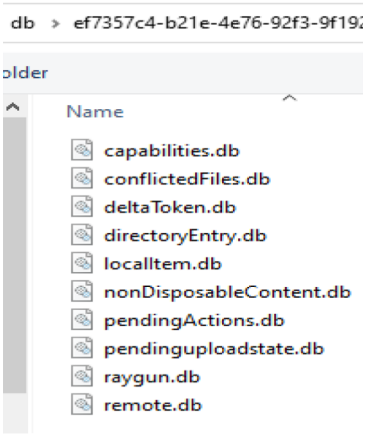
Citrix ShareFile

Path	Details
S:\	Default file store
%USERPROFILE%\AppaData\Local\Citrix\Citrix Files\db\[ID]\	Database location
%USERPROFILE%\AppaData\Local\Citrix\Citrix Files\db\[ID]\remote.db	List of remote files/folders
%USERPROFILE%\AppaData\Local\Citrix\Citrix Files\db\[ID]\localItem.db	List of local files/folders
%USERPROFILE%\AppaData\Local\Citrix\Citrix Files\Logs\	Log files
%USERPROFILE%\AppaData\Local\Citrix\Citrix Files\CitrixFiles_[date].log	Detailed activity log
%USERPROFILE%\AppaData\Local\Citrix\Citrix Files\PartCache\	Cached files

69

RICHEY MAY
TECHNOLOGY SOLUTIONS

Citrix ShareFile: Databases



70

RICHEY MAY
TECHNOLOGY SOLUTIONS

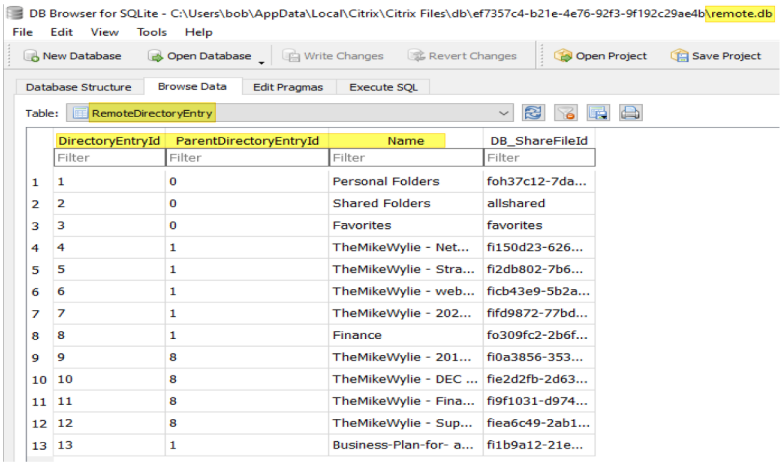
Citrix: remote.db

Column	Description
DirectoryEntryId	Folder ID
ParentDirectoryEntryId	Parent Folder ID
Name	File name
DB_SharedFileId	Global Sharefile ID

71

RICHEY MAY
TECHNOLOGY SOLUTIONS

Citrix: remote.db



	DirectoryEntryId	ParentDirectoryEntryId	Name	DB_ShareFileId
	Filter	Filter	Filter	Filter
1	1	0	Personal Folders	foh37c12-7da...
2	2	0	Shared Folders	allshared
3	3	0	Favorites	favorites
4	4	1	TheMikeWylie - Net...	fi150d23-626...
5	5	1	TheMikeWylie - Stra...	fi2db802-7b6...
6	6	1	TheMikeWylie - web...	ficb43e9-5b2a...
7	7	1	TheMikeWylie - 202...	fifd9872-77bd...
8	8	1	Finance	fo309fc2-2b6f...
9	9	8	TheMikeWylie - 201...	fi0a3856-353...
10	10	8	TheMikeWylie - DEC ...	fie2d2fb-2d63...
11	11	8	TheMikeWylie - Fina...	fi9f1031-d974...
12	12	8	TheMikeWylie - Sup...	fiea6c49-2ab1...
13	13	1	Business-Plan-for- a...	fi1b9a12-21e...

72

RICHEY MAY
TECHNOLOGY SOLUTIONS

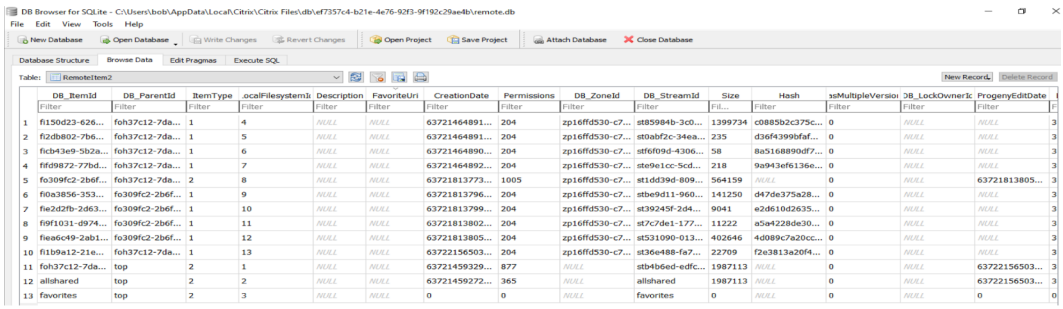
Citrix: remote.db

Column	Description
DB_ItemID	Object ID in the database
DB_ParentId	Parent object ID
ItemType	Identifies if the entry is a file or folder
CreateDate	Date created in Unix epoch
Hash	File hash
More	Many more columns in this table

73

RICHEY MAY
TECHNOLOGY SOLUTIONS

Citrix: remote.db



74

RICHEY MAY
TECHNOLOGY SOLUTIONS

Citrix: localitem.db

Column	Description
Key	
ChangeDate	Last change time (Unix epoch)
LastAccessDate	Last access time (Unix epoch)
LastWriteDate	Last write time (Unix epoch)
Id	
ContentId	
CreationDate	Time object was created (Unix epoch)
Url	Cloud URL [instance].sf-api.com/sf/v3/Items([ID])
Hash	File hash
Much more...	

75

RICHEY MAY
TECHNOLOGY SOLUTIONS

Citrix: directoryEntry.db

Column	Description
ParentId	Parent ID of the object
Name	File name
Id	ID of the object

76

RICHEY MAY
TECHNOLOGY SOLUTIONS

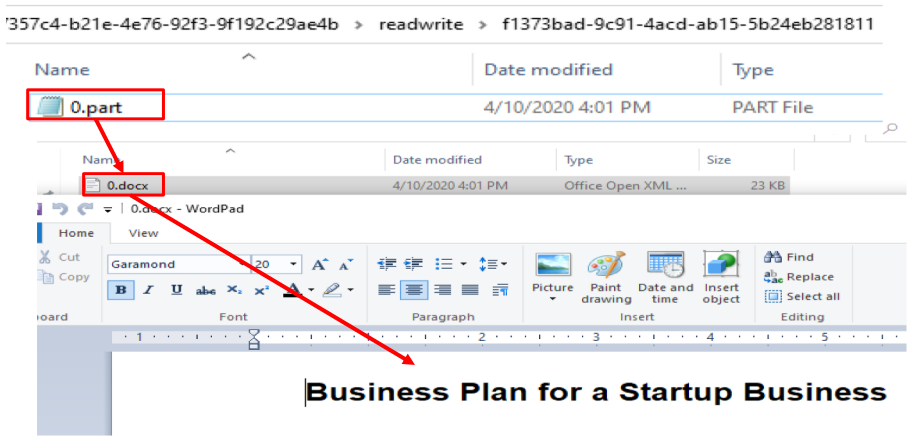
Citrix: CitrixFiles_date[date].log

- Parse for keywords:
  - [UploadFile]
  - [FileSystemNotifier]
  - [LOCAL]
  - [WINFSP]
  - [DeleteItem]
  - [Download]
  - [Upload]
  - [ReadCallback]

77

RICHEY MAY
TECHNOLOGY SOLUTIONS

Citrix: …\PartCache\



78

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Closing

79

RICHEY MAY
TECHNOLOGY SOLUTIONS

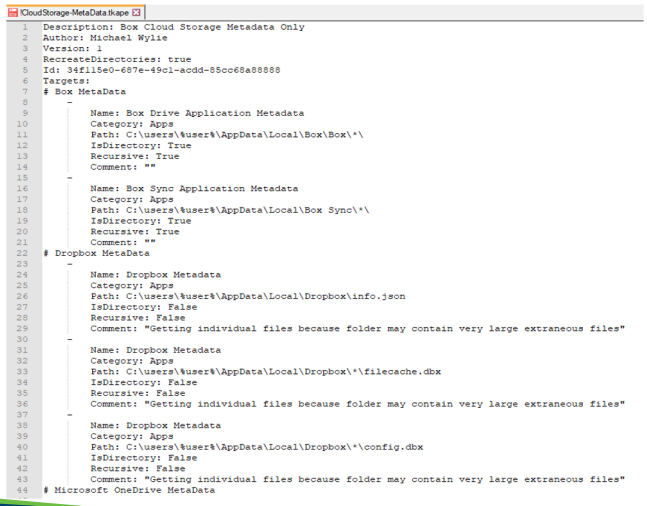
Non-App Cloud File Storage Use

URL	Description
docs.google.com/spreadsheets/	Viewing/editing a Google spreadsheet
docs.google.com/presentation/	Viewing/editing a Google presentation
docs.google.com/document/	Viewing/editing a Google document
drive.google.com/drive/my-drive	Root of a personal Google Drive
drive.google.com/drive/folders/	Browsing a sub-folder in Google Drive
drive.google.com/drive/trash	Viewing contents of Google Drive Trash
https://app.box.com/folder/0	Viewing the root of box.com
https://onedrive.live.com/?id=root&cid=[cid]	Viewing the root of OneDrive (personal)
https://www.dropbox.com/home	Viewing the root of Dropbox
https://www.dropbox.com/scl/	Viewing a document on Dropbox.com
https://www.dropbox.com/home/[folder]	Viewing contents of a folder

80

RICHEY MAY
TECHNOLOGY SOLUTIONS

KAPE: !CloudStorage-MetaData.tkape

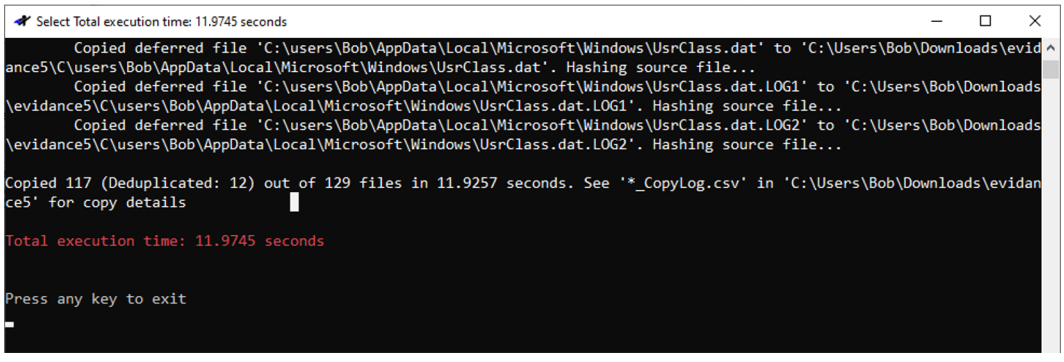


```
Description: Box Cloud Storage Metadata Only
Author: Michael Wylie
Version: 1
RecreateDirectories: true
Id: 34f115e0-687e-49c1-acdd-85cc68a88888
Targets:
# Box MetaData
    -
        Name: Box Drive Application Metadata
        Category: Apps
        Path: C:\users\%user%\AppData\Local\Box\Box\*\
        IsDirectory: True
        Recursive: True
        Comment: ""
    -
        Name: Box Sync Application Metadata
        Category: Apps
        Path: C:\users\%user%\AppData\Local\Box Sync\*\
        IsDirectory: True
        Recursive: True
        Comment: ""
# Dropbox MetaData
    -
        Name: Dropbox Metadata
        Category: Apps
        Path: C:\users\%user%\AppData\Local\Dropbox\info.json
        IsDirectory: False
        Recursive: False
        Comment: "Getting individual files because folder may contain very large extraneous files"
    -
        Name: Dropbox Metadata
        Category: Apps
        Path: C:\users\%user%\AppData\Local\Dropbox\*\filecache.dbx
        IsDirectory: False
        Recursive: False
        Comment: "Getting individual files because folder may contain very large extraneous files"
    -
        Name: Dropbox Metadata
        Category: Apps
        Path: C:\users\%user%\AppData\Local\Dropbox\*\config.dbx
        IsDirectory: False
        Recursive: False
        Comment: "Getting individual files because folder may contain very large extraneous files"
# Microsoft OneDrive MetaData
```

81

RICHEY MAY
TECHNOLOGY SOLUTIONS

KAPE: !CloudStorage-MetaData.tkape



```
Select Total execution time: 11.9745 seconds
        Copied deferred file 'C:\users\Bob\AppData\Local\Microsoft\Windows\UsrClass.dat' to 'C:\Users\Bob\Downloads\evid
ance5\C\users\Bob\AppData\Local\Microsoft\Windows\UsrClass.dat'. Hashing source file...
        Copied deferred file 'C:\users\Bob\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1' to 'C:\Users\Bob\Downloads
\evidance5\C\users\Bob\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1'. Hashing source file...
        Copied deferred file 'C:\users\Bob\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2' to 'C:\Users\Bob\Downloads
\evidance5\C\users\Bob\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2'. Hashing source file...

Copied 117 (Deduplicated: 12) out of 129 files in 11.9257 seconds. See '*_CopyLog.csv' in 'C:\Users\Bob\Downloads\evidan
ce5' for copy details

Total execution time: 11.9745 seconds


Press any key to exit
```

82

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Thank You!

MICHAEL WYLIE

TWITTER: @THEMIKEWYLIE
LINKEDIN: LINKEDIN.COM/IN/MWYLIE

WWW.RICHEYMAYTECH.COM

83