



Discover / Develop / Deliver

Enumerating Cloud File Storage Gems

Michael Wylie, MBA, CISSP



1



About Me:



Michael Wylie, TPN, MBA, CISSP

Director, Cybersecurity Services

RICHEY MAY TECHNOLOGY SOLUTIONS

Additional <ul style="list-style-type: none"> • GPEN • GMON • PenTest+ • Project+ • Security+ • CEH & CEI 	Certifications <ul style="list-style-type: none"> • CCNA R&S • CCNA CyberOps • Pentest+ • CHPA • Splunk User • GCFE
--	--

[!\[\]\(8ab712341e26f54b8926c905e7b4ba61_img.jpg\) linkedin.com/in/mwylie](https://linkedin.com/in/mwylie)

[!\[\]\(cea3b58553dd7a2f700cb9448371cd81_img.jpg\) twitter.com/TheMikeWylie](https://twitter.com/TheMikeWylie)

2



About Richey May Technology Solutions

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



3



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



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



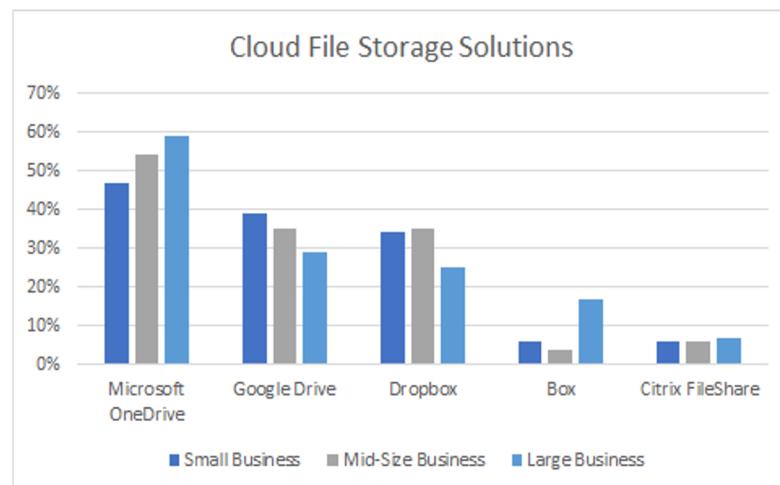
Cloud File Storage Overview

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



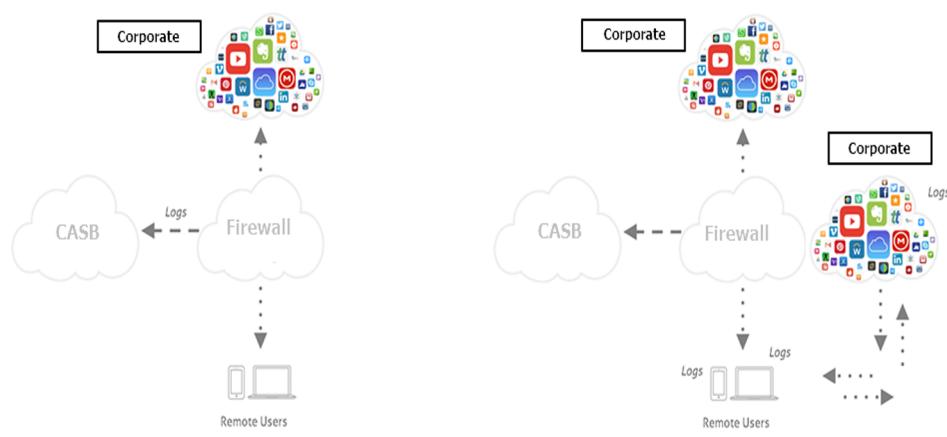
6

Cloud File Storage Solutions Usage



7

Cloud File Storage Scenarios

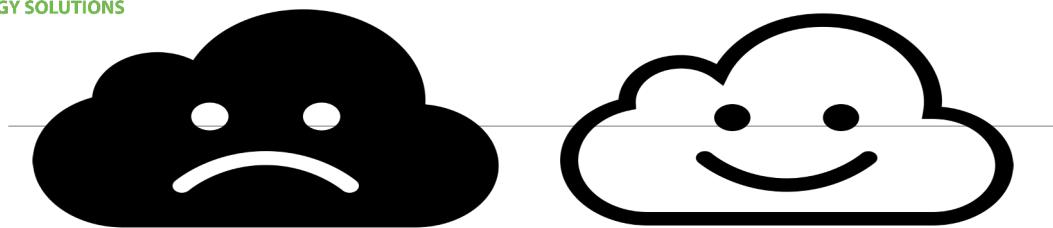


8

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

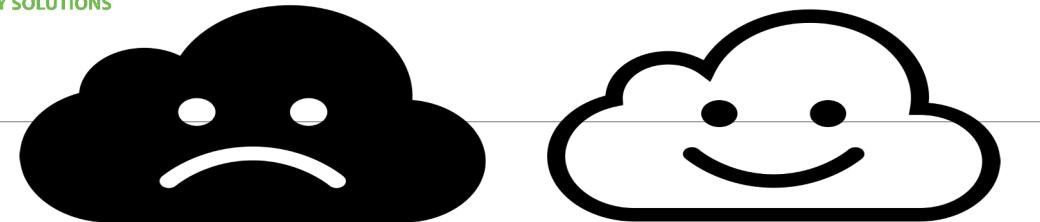
9



Business/Enterprise Account: Personal/Free Account:

- | | |
|--|--|
| <ul style="list-style-type: none"> • Company issued • Access to admin portal • CASB (possibly) • Access to cloud-side data • Cloud based logs | <ul style="list-style-type: none"> • Not company issued • No access to account • No central visibility • Access to endpoint data • Local logs |
|--|--|

10

**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



Microsoft OneDrive

12



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\\Business1\\
- O365 Unified Audit Logs provides businesses with detailed logs up to 90 by default
- Personal OneDrive doesn't have the Audit log feature

13



Microsoft OneDrive: Log Files

Personal	Business																																								
<p>: > AppData > Local > Microsoft > OneDrive > settings</p> <p>Name</p> <ul style="list-style-type: none"> ab6591... led8bc.dat ab6591... led8bc.ini ClientPolicy.ini <p>> AppData > Local > Microsoft > OneDrive > logs</p> <p>Name</p> <ul style="list-style-type: none"> DeviceFailureDatagram DeviceHealth.json DeviceHealthSummaryConfiguration.ini ObfuscationStringMap.txt SyncDiagnostics.log SyncEngine-2020-03-16.1513.16080.289.odsent 	<p>Results 547 results found</p> <p>Date ▲ User Activity Item Detail</p> <table border="1"> <thead> <tr> <th>Date</th> <th>User</th> <th>Activity</th> <th>Item</th> <th>Detail</th> </tr> </thead> <tbody> <tr> <td>2015-09-21 16:48:33</td> <td>admin@...</td> <td>User signed in to mailbox</td> <td></td> <td></td> </tr> <tr> <td>2015-09-21 16:49:16</td> <td>admin@...</td> <td>Viewed file</td> <td>admin@...com_5Thumb.jpg</td> <td>Viewed in User Photos/Profile Pic...</td> </tr> <tr> <td>2015-09-21 16:49:28</td> <td>admin@...</td> <td>Viewed file</td> <td>Run the Office 365 activity repor...</td> <td>Viewed in Documents</td> </tr> <tr> <td>2015-09-21 16:49:28</td> <td>admin@...</td> <td>Downloaded file</td> <td>Run the Office 365 activity repor...</td> <td>Downloaded from Documents</td> </tr> <tr> <td>2015-09-21 16:49:44</td> <td>v-temp@...</td> <td>Viewed file</td> <td>IT Dept Salaries.docx</td> <td>Viewed in IT_Elangs_Only</td> </tr> <tr> <td>2015-09-21 16:50:27</td> <td>ping@...</td> <td>Modified file</td> <td>Olympics (Sample).xlsx</td> <td>Modified in Documents</td> </tr> <tr> <td>2015-09-21 16:50:28</td> <td>admin@...</td> <td>Renamed file</td> <td>Scale Auditing - Exchange2.pptx</td> <td>Renamed to Scale Auditing_Final</td> </tr> </tbody> </table>	Date	User	Activity	Item	Detail	2015-09-21 16:48:33	admin@...	User signed in to mailbox			2015-09-21 16:49:16	admin@...	Viewed file	admin@...com_5Thumb.jpg	Viewed in User Photos/Profile Pic...	2015-09-21 16:49:28	admin@...	Viewed file	Run the Office 365 activity repor...	Viewed in Documents	2015-09-21 16:49:28	admin@...	Downloaded file	Run the Office 365 activity repor...	Downloaded from Documents	2015-09-21 16:49:44	v-temp@...	Viewed file	IT Dept Salaries.docx	Viewed in IT_Elangs_Only	2015-09-21 16:50:27	ping@...	Modified file	Olympics (Sample).xlsx	Modified in Documents	2015-09-21 16:50:28	admin@...	Renamed file	Scale Auditing - Exchange2.pptx	Renamed to Scale Auditing_Final
Date	User	Activity	Item	Detail																																					
2015-09-21 16:48:33	admin@...	User signed in to mailbox																																							
2015-09-21 16:49:16	admin@...	Viewed file	admin@...com_5Thumb.jpg	Viewed in User Photos/Profile Pic...																																					
2015-09-21 16:49:28	admin@...	Viewed file	Run the Office 365 activity repor...	Viewed in Documents																																					
2015-09-21 16:49:28	admin@...	Downloaded file	Run the Office 365 activity repor...	Downloaded from Documents																																					
2015-09-21 16:49:44	v-temp@...	Viewed file	IT Dept Salaries.docx	Viewed in IT_Elangs_Only																																					
2015-09-21 16:50:27	ping@...	Modified file	Olympics (Sample).xlsx	Modified in Documents																																					
2015-09-21 16:50:28	admin@...	Renamed file	Scale Auditing - Exchange2.pptx	Renamed to Scale Auditing_Final																																					

14



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\Business1\	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



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



Microsoft OneDrive: SyncDiagnostics.log

Detailed SyncDiagnostics File

```

SyncDiagnostics - Notepad
File Edit Format View Help
Sync Diagnostics - Sync Verification
Footprint Integration
Footprint Integration invocation failed. Telemetry was not collected.
Local Metadata:
=====
DAT: 0 folders, 0 full files, 0 dehydrated files, 0 stub files, 0 unmapped files, 0
=====
Scope verification for E9423588BA271DC81101
=====
Scanning 'SMountPoint[E9423588BA271DC81101]'.
- file 'SMountPoint[E9423588BA271DC81101]\VarJumpSeq' is ignored (low-visibi
- folder 'SMountPoint[E9423588BA271DC81101]\Seabatteee'
- file 'SMountPoint[E9423588BA271DC81101]\ImpCatSea.int' is ignored (low-vis
- folder 'SMountPoint[E9423588BA271DC81101]\CarRagTax'
- folder 'SMountPoint[E9423588BA271DC81101]\VatfRadius'

```

Summary SyncDiagnostics File

```

SyncDiagnostics - Notepad
File Edit Format View Help
Sync Diagnostics - Sync Progress
SyncProgressState: 16777216
=====
Diagnostic Report
UtcNow: 2020-04-15T02:16:20.000000Z
=====
BytesDownloaded = 0
BytesToDownload = 0
BytesToUpload = 0
BytesUploaded = 0
ChangesToProcess = 0
ChangesToSend = 0
DownloadSpeedBytesPerSec = 0
EstTimeRemainingInSec = 0

```

17



Microsoft OneDrive: SyncDiagnostics.log

Summary Version

```

SyncDiagnostics.log - Notepad
File Edit Format View Help
Sync Diagnostics - Sync Progress
SyncProgressState: 16777216
=====
=====
Diagnostic Report
UtcNow: 2020-04-13T16:34:10.000000Z
=====
BytesDownloaded = 0
BytesToDownload = 0
BytesToUpload = 0
BytesUploaded = 0
ChangesToProcess = 0
ChangesToSend = 0
DownloadSpeedBytesPerSec = 132258
=====
numHashMismatchErrorsReported = 0
numLcChangeFile = 853
numLcChangeFolder = 16
numLcCreateFile = 1416
numLcCreateFolder = 313
numLcDeleteFile = 545
numLcDeleteFolder = 150
numLcMoveFile = 22
numLcMoveFolder = 4
numLocalChanges = 0
numProcessors = 8
numRealizerErrorsReported = 0

```

18

RICHEY MAY TECHNOLOGY SOLUTIONS

Microsoft OneDrive: SyncDiagnostics.log

Detailed Version Decoded

Key	Value
JokeYakLog	C
FigEmuHam	3bSI
MawUrnicy	1586921694
RagZlgRag	45f4f864-0cc5-4c17-ba4c-1372c0848d98
RodOafGad	Users
VatHugFoo	Tcpview
SeaBatEgg	Desktop
PewForthGad	2fqQUgklo3ifx5yz
FigWeeZig	\$metadata
YakDogeLog	Update

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

Key	Value
YakLogKid	f3633624
JokeYakLog	C
KoiYewQuill	mwylie

20



Microsoft OneDrive: [cid].dat

HxD - C:\Users\[REDACTED]\AppData\Local\Microsoft\OneDrive\settings\Business1\ab6[REDACTED] 82bc0cded8bc.dat

File Edit Search View Analysis Tools Window Help

16 Windows (ANSI) hex

ab6[REDACTED]-82bc0cded8bc.dat

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text

```

004571F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  

00457200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  

00457210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  

00457220 00 AB .....  

00457230 00 00 00 00 01 01 01 01 AB AB AB AB AB AB AB AB .....  

00457240 38 72 45 00 00 00 00 01 00 00 00 00 00 00 00 00 8xE.....  

00457250 31 62 35 35 63 63 36 62 36 35 63 64 34 31 37 30 1b55cc6b65cd4170  

00457260 62 34 30 35 33 34 33 36 36 61 62 30 65 33 39 65 .....  

00457270 00 00 00 00 00 00 00 00 36 65 35 66 32 37 34 33 .....  

00457280 30 35 31 34 33 64 39 61 34 61 30 61 30 32 62 38 .....  

00457290 31 32 63 32 30 31 61 00 00 00 00 00 00 22 7B 1B55CC6B65CD4170.....  

004572A0 31 42 35 35 43 43 36 42 2D 36 35 43 44 2D 34 31 1B55CC6B65CD4170.....  

004572B0 37 30 2D 42 34 30 35 2D 33 34 33 36 36 41 42 30 1B55CC6B65CD4170.....  

004572C0 45 33 39 45 7D 2C 31 22 00 00 00 00 00 00 00 00 E39E},1",.....  

004572D0 00 00 00 00 00 00 AB AB OE D6 78 A6 00 00 00 00 .....<<0x>};...  

004572E0 F9 BE 05 00 00 00 11 00 00 AB AB AB AB 00 00 00 00 .....  

004572F0 7D FB 0A 3B 78 13 38 D7 69 AE 04 27 3A B5 3B )Ù..tx.8*i®.';;;  

00457300 AF 50 DF 5D AB AB AB AB F9 C2 03 SD 00 00 00 00 "B}æœedÃ,)...  

00457310 A4 4A 01 00 00 00 00 00 54 00 72 00 61 00 76 00 #Û.....T.r.a.v.  

00457320 66 00 6C 00 20 00 49 00 74 00 69 00 6E 00 65 00 e.l...I.t.i.n.e.  

00457330 72 00 61 00 72 00 79 00 2E 00 70 00 64 00 66 00 r.a.r.y...p.d.f.  

00457340 00 00 AB ..  

00457350 AB ..  

00457360 1D 1D

```

21



Microsoft OneDrive: [cid].dat (personal)

C:\Windows\System32\cmd.exe

Strings v2.53 - Search for ANSI and Unicode strings in binary images.

Copyright (C) 1999-2016 Mark Russinovich

Sysinternals - www.sysinternals.com

LM&3d63722412202470%3bID%3dE9423588BA271DC8!101%3bLR%3d63722502771487;
bP%3d3%3bVA%3dTrue
E9423588BA271DC8!104
E9423588BA271DC8!101
E9423588BA271DC8!104.0
Documents
E9423588BA271DC8!101
E9423588BA271DC8!105
E9423588BA271DC8!105
E9423588BA271DC8!101
E9423588BA271DC8!105.0
Personal Vault
E9423588BA271DC8!101
E9423588BA271DC8!103
E9423588BA271DC8!101
E9423588BA271DC8!103.0
Pictures
E9423588BA271DC8!101
E9423588BA271DC8!107
E9423588BA271DC8!103
E9423588BA271DC8!107.0
Camera Roll
E9423588BA271DC8!101
E9423588BA271DC8!108
-- More --

22



Microsoft OneDrive: [cid].dat (business)

ObfuscationStringMap.txt - Notepad

```

YakLogKid f3633624
JokeYakLog C
KoiYewQuill mwylie
YewZagVolt 23Paged_Ct=1;3;e88bd0f2-3d01-4953-89f0-0898bdf334b9;637222265759130000;206662805;
TwoBatBag f0150752

```

1;234;%231;3;e88bd0f2-3d01-4953-89f0-0898bdf334b9;637225037455530000;207359599;%23;%23xo0oc5rnKzE04cL%252BWlUj8AHu7S2oD32I7X8x6fsdM%253d;%234
:2cd5fe3cf63405da9d120b3035df5d3
:4f292c2c9fd4ec7a318df200514aa15
'{C2CD5FE3-CF63-405D-A9D1-20030305DF5D3},2"
:4f292c2c9fd4ec7a318df200514aa15
:bc67b5f143b422890ebbdd658461ae
:2cd5fe3cf63405da9d120b3035df5d3
'{B8C67B5F-143B-4228-90EB-B0DD658461AE},2"
:4f292c2c9fd4ec7a318df200514aa15
329907af8184071b43ea5e4ca49d337
:bc67b5f143b422890ebbdd658461ae
'{032907AF-8818-4071-B43E-A5E4CA49D337},3"
:62d38ed1ad64caabd2a6311dad6085f

23



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

ab659.ini - Read & Write - Untitled - Obfuscatedbcini - Notepad

```

libraryScope = 0 d7a6... 8960ad2e 5 "MySite" "ODB" 2 "https://
libraryScope = 1 b736... a9b392f4+1 5 "RMTS Cyber" "Documents"
libraryScope = 2 c4f2... 0514aa15+2 5 "RMTS - Cyber Practic"
libraryScope = 3 d8f1... aa816268+3 5 "Project Mater" "Docume
installID = 1
originatorID = 74f93c5... 22aa086261
lastRefreshTime = 1586898667
requestSent = 133
bytesTransferred = 1615349

```

24



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

```
e9423...1dc8-ProfileServiceResponse - Notepad
File Edit Format View Help
{"@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users/$entity", "displayName": "mike wylie", "surname": "wylie", "givenName": "mike", "id": "e9423...1dc8", "userPrincipalName": "mike.wylie@workshop@gmail.com", "businessPhones": [], "jobTitle": null, "mail": null, "mobilePhone": null, "officeLocation": null, "preferredLanguage": null}
```

25



Microsoft OneDrive: Registry Keys

Business1	Personal	Common
IsGoov WebServiceUrl ECSConfigurationETag ECSConfigurationExpires ECSConfigurationMaxAge ECSConfigurationLastSuccess ConfiguredTenantId cid UserEmail SPOnlineUpdate TeamSiteSPResourceId DisplayName SPOResourceId ServiceEndpointUri PUD UserName FirstRunSignInOrigin Business NamespaceRootId LastSignInTime GrooveTakeoverAttemptedOperations GrooveTakeoverSuccessfulOperations ClientFirstSignInTimestamp ProviderOptInEnabled UserFolder EdmManaged LastKnownCloudFilesEnabled FirstRun LastMigrationScanResult NextCheckInUpdateTime HasMadeFirstUpload ShareTimeStamp NextMigrationScan CrashDetectionKey AuthenticationURLs {ScopeIdToMountPointPathCache \Tenants \WindowsSecurityCenterIntegration	ECSConfigurationETag ECSConfigurationExpires ECSConfigurationMaxAge ECSConfigurationLastSuccess IsGoov FirstRunSignInOrigin UserEmail NamespaceRootId LastSignInTime ClientFirstSignInTimestamp cid ProviderOptInEnabled UserFolder LastKnownCloudFilesEnabled FirstRun UpgradeAvailable VaultShortcutsPath Business NamespaceRootId HasMadeFirstUpload LastMigrationScanResult NextCheckInUpdateTime CrashDetectionKey AuthenticationURLs {ScopeIdToMountPointPathCache \Tenants \WindowsSecurityCenterIntegration	ECSConfigurationETag ECSConfigurationExpires ECSConfigurationMaxAge ECSConfigurationLastSuccess IsGoov FirstRunSignInOrigin UserEmail NamespaceRootId LastSignInTime ClientFirstSignInTimestamp cid ProviderOptInEnabled UserFolder LastKnownCloudFilesEnabled FirstRun HasMadeFirstUpload NextMigrationScan LastMigrationScanResult NextCheckInUpdateTime CrashDetectionKey AuthenticationURLs {ScopeIdToMountPointPathCache \Tenants \WindowsSecurityCenterIntegration

26



Microsoft OneDrive: O365 Shared Folders

Administrator: Command Prompt

```
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>reg query HKCU\Software\SyncEngines\Providers\OneDrive
```

HKEY_CURRENT_USER\Software\SyncEngines\Providers\OneDrive

```
HKEY_CURRENT_USER\Software\SyncEngines\Providers\OneDrive\b726eebe ace2d707a9b392f4+1
HKEY_CURRENT_USER\Software\SyncEngines\Providers\OneDrive\c4f292c2 a318df208514aa15+2
HKEY_CURRENT_USER\Software\SyncEngines\Providers\OneDrive\d7a68847 8c9e482f8966ad2e
HKEY_CURRENT_USER\Software\SyncEngines\Providers\OneDrive\d8f166f9 la86a6508aa816268+3
```

```
C:\Windows\system32>reg query HKCU\Software\SyncEngines\Providers\OneDrive\d8f166f9 la86a6508aa816268+3
```

HKEY_CURRENT_USER\Software\SyncEngines\Providers\OneDrive\d8f166f9 la86a6508aa816268+3

MountPoint	REG_SZ	C:\Users\bob\OneDrive\Project - Documents
LastModifiedTime	REG_SZ	2020-04-10T18:46:38
UrlNamespace	REG_SZ	https://[REDACTED].sharepoint.com/sites/Project-[REDACTED]/Shared Documents/
IsOfficeSyncIntegrationEnabled	REG_SZ	1
LibraryType	REG_SZ	teamsite

27



Microsoft OneDrive: Personal Shared Folders

Administrator: Command Prompt

```
C:\Windows\system32>
C:\Windows\system32>reg query HKCU\Software\SyncEngines\Providers\OneDrive
```

HKEY_CURRENT_USER\Software\SyncEngines\Providers\OneDrive

DisplayNameResource	REG_SZ	@%s\OneDrive\Local\Microsoft\OneDrive\19.232.1124.0012\FileSync.Resource
IconResource	REG_SZ	C:\Users\bob\AppData\Local\Microsoft\OneDrive\19.232.1124.0012\FileSync.Res
Header	REG_SZ	{71DCE5D6-4B57-496B-AC21-C09854E893FD}
Version	REG_SZ	1
Flags	REG_DWORD	0x0

```
HKEY_CURRENT_USER\Software\SyncEngines\Providers\OneDrive\Personal
```

```
HKEY_CURRENT_USER\Software\SyncEngines\Providers\OneDrive\test
```

Administrator: Command Prompt

```
C:\Windows\system32>reg query HKCU\Software\SyncEngines\Providers\OneDrive\test
```

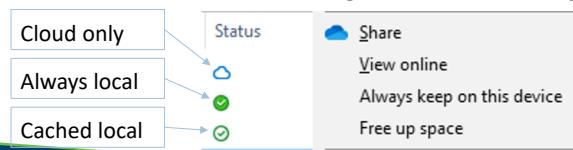
HKEY_CURRENT_USER\Software\SyncEngines\Providers\OneDrive\test

RelativePath	REG_SZ	test
LastModifiedTime	REG_SZ	2020-04-13T22:03:25
LibraryType	REG_SZ	personal
IsOfficeSyncIntegrationEnabled	REG_SZ	1
CID	REG_SZ	BF730EF4D5707[REDACTED]88
MountPoint	REG_SZ	C:\Users\bob\OneDrive
UrlNamespace	REG_SZ	https://d.docs.live.net

28

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

Google Drive

30

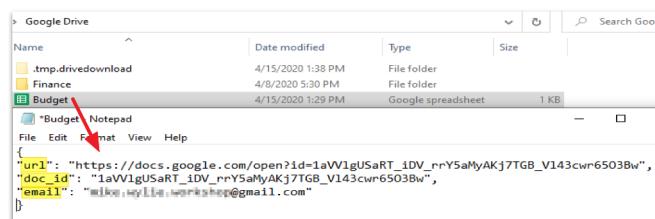
Google Drive

- 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

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



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



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



Google Drive: sync_config.db

Database Structure | Browse Data | Edit Pragmas | Execute SQL | Table: data

entry_key	data_key	data_value
1	upgrade_number	47
2	highest_app_version	3.49.9800.0000
3	cloud_docs_feed_mode	0
4	rlz_brand_code	GGLS
5	feature_switch	gAJYJ29tbW9uLmZlYXR1cmVfc3dpdGNoX21hbmlFnZxI...
6	shown_setup_overlays	choose_folders_setup_overlay
7	machine_folder_doc_id	1mXRL52c4DnDWqt1T533vgFCmATuHJcd0
8	machine_folder_name	My PC (1)
9	shown_setup_overlays	google_drive_setup_overlay
10	selective_sync	0
11	usb_sync_enabled	1
12	show_unparent_warning	1
13	delete_mode	1
14	storage_policy_mode	original
15	always_show_in_photos	0
16	share_notification	1
17	local_sync_root_path	\\\?\C:\Users\matt\Google Drive
18	copy_duplicate_photos	1
19	user_email	matt.wilson.merchandise@gmail.com
20	domain_policy	default_sync_all
21	domain_policy	domain_policy_description_url

35



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 formatted 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



Google Drive: cloud_graph.db

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

Table: cloud_graph_entry									
doc_id	filename	modified	created	ad_role	doc_type	removed	size	checksum	
1	root	NULL	NULL	NULL	0	NULL	NULL	NULL	
2	1ngR1Nv-7wq...	Finance	1586216467	NULL	0	0	NULL	NULL	
3	11vr3KjUD86...	TheMikeWylie - 2021 Finance Plan.xls	1585867993	NULL	0	1	0	218	9a943ef6136e...
4	1eqrkqbT7hv...	TheMikeWylie - 2021 Finance Plan.xls	1585867803	NULL	0	1	0	1399734	c0885b2c375c...
5	1eC4B_pJgJK...	TheMikeWylie - 2021 Finance Plan.xls	1585867506	NULL	0	1	0	235	d36f4399bfaf...
6	1RkbUgBLxY...	TheMikeWylie - 2021 Finance Plan.xls	1585867214	NULL	0	1	0	58	8a5168890d7...
7	0832k-oYr2...	Getting started	1585862322	NULL	0	1	0	1560010	dff1432d0c63...
8	1Bauy7N4UG...	TheMikeWylie - 2021 Finance Plan.xls	1586216490	NULL	0	1	0	402646	4d089c7e20cc...
9	1ON8o9XPO2...	TheMikeWylie - 2021 Finance Plan.xls	1586216490	NULL	0	1	0	141250	d47de375a28...
10	12_CEEggpx...	TheMikeWylie - Finance parameter file.xls	1586216489	NULL	0	1	0	11222	a5a4228de30...
11	1IAV4eQXV...	TheMikeWylie - 2021 General Finance.xlsx	1586216489	NULL	0	1	0	9041	e2d610d2635...
12	1jdAzKhoOBv...	Business Plan-Financial Risk	1586559655	NULL	0	1	0	22709	f2e3813a20f4...
13	1-gtMvwddSU...	Documents	1586392179	NULL	0	0	0	NULL	NULL

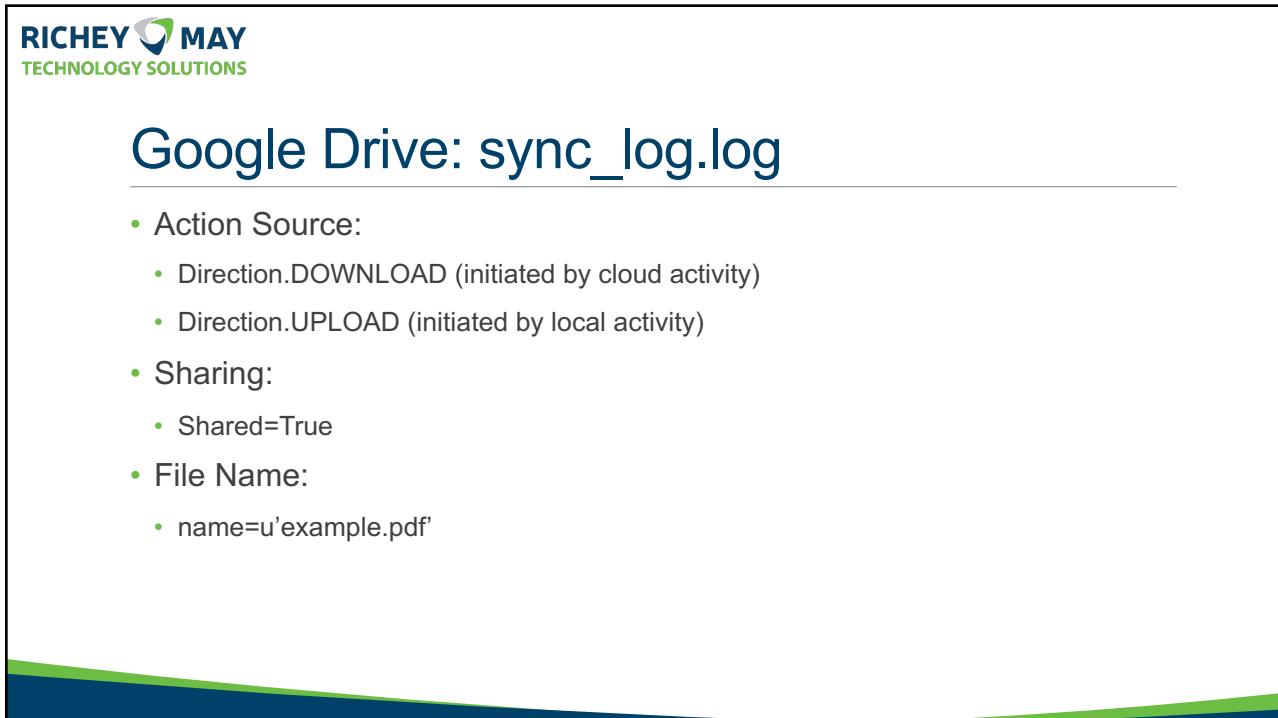
37



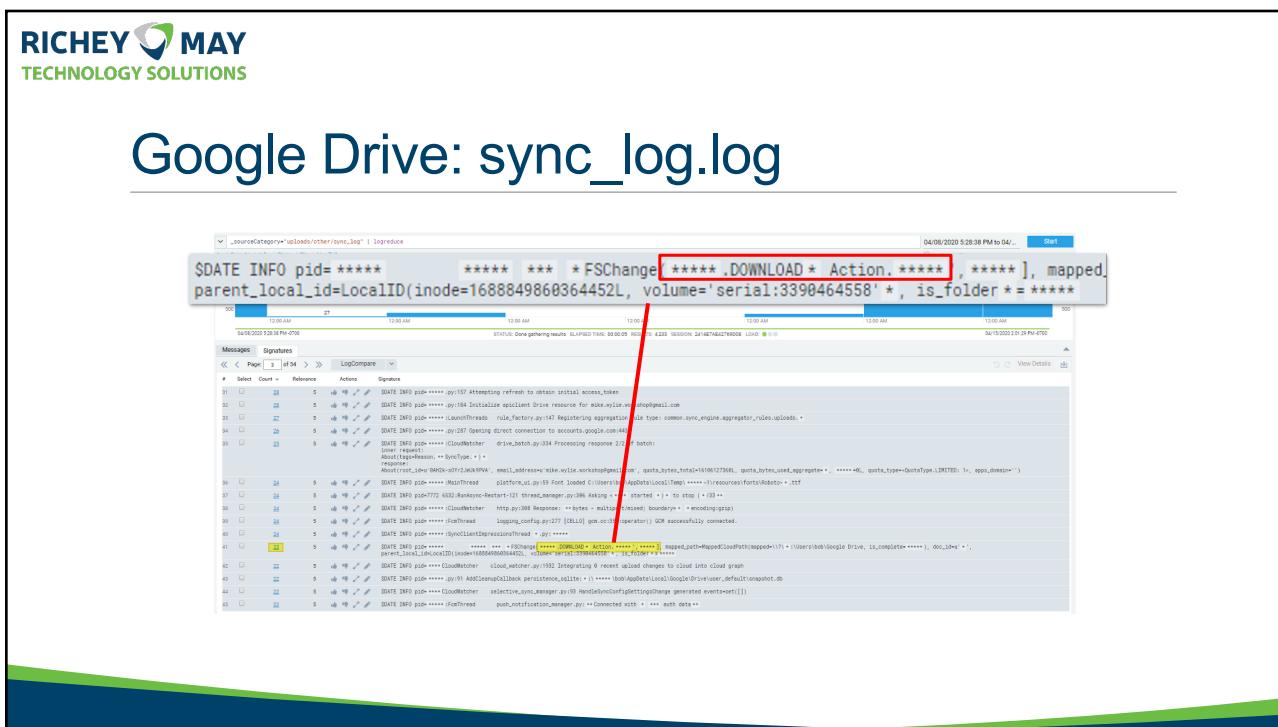
Google Drive: sync_log.log

- 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



39



40



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



Google Drive: snapshot.db

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

doc_id	filename	modified	created	acl_role	doc_type	removed	size	checksum	shared
1	root	NULL	NULL	0	NULL	NULL	NULL	0	
2	1-gtMwcdSUy...	Documents	NULL	0	NULL	NULL	NULL	0	
3	1ngR1Nv-7wq...	Finance	1586216467	0	0	0	NULL	NULL	0
4	12_CEEgg6px...	TheMikeWylie...	1586216489	0	1	0	11222	a5a4228de30...	0
5	1oNBor9XPOz...	TheMikeWylie...	1586216490	0	1	0	141250	d47de375a28...	0
6	1Bausy17NUG...	TheMikeWylie...	1586216490	0	1	0	402646	4d089c7a20cc...	0
7	1IAV94eQXV...	TheMikeWylie...	1586216489	0	1	0	9041	e2d610d2635...	0
8	1lvrJXYUIn86...	TheMikeWylie...	1585867993	0	1	0	218	9a943ef6136e...	0
9	1cqqrkbt7h-z...	TheMikeWylie...	1585867803	0	1	0	1399734	c0885b2c375c...	0
10	1eC48_p1gkj...	TheMikeWylie...	1585867506	0	1	0	235	d36f4399bfaf...	0
11	1KkbUg8LlxvB...	TheMikeWylie...	1585867214	0	1	0	58	8a5168890df7...	0
12	0832k-s0Yr23...	Getting started	1585862322	0	1	0	1560010	d1f1432d0c63...	0
13	1jdLAzkhoobv...	Business-Plan...	1586559655	0	1	0	22709	f2e3813a20f4...	0

42



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)

cloud_relations	
child_doc_id	parent_doc_id
1 NgR1Nv-7wqrqMkwbeUmf3WgTxgdiQE	root
2 12_CEEggpdp7x1av3AanPjtz9YCKVCD	NgR1Nv-7wqrqMkwbeUmf3WgT...
3 1ONBo9XPoZd92D19kmnH04blsEP9jku7	NgR1Nv-7wqrqMkwbeUmf3WgT...
4 1Bauyi7HUUG2tYgOLvp3pVBlExkBNi5	NgR1Nv-7wqrqMkwbeUmf3WgT...
5 11AvAe4eQX7gQrEVN2ekTnGd57nsB8i	NgR1Nv-7wqrqMkwbeUmf3WgT...
6 11vrDXJU86ukm-Y1XXW6VTD5hmuJa5o	root
7 1cqrlqbT7h-zkLXPDbfVGz2EKNk3m_	root
8 1eC48_p1gJk3g7ZARPNdA4oc0v0K3WNat	root
9 1RKbuG8LjXy8ewquS28b-DvAFAnx9-	root
10 1jdLAzkhooBv0Vo-DQzVZj5Qxb0Fph6W	root
11 1cpvtFzghzOOhGqPXLgxG0jx4t31VMWWS	root
12 1AW2-PSb8FSxaCSoQ3pN6kvBB8DjAbUK3p	root
13 1Y1mdTHccBMZ0OaAe4ilmOHyo3DTWhRL	root

43



Google Drive: snapshot.db & cloud_graph.db

cloud_relations	
child_doc_id	parent_doc_id
1 NgR1Nv-7wqrqMkwbeUmf3WgTxgdiQE	root
2 12_CEEggpdp7x1av3AanPjtz9YCKVCD	NgR1Nv-7wqrqMkwbeUmf3WgT...
3 1ONBo9XPoZd92D19kmnH04blsEP9jku7	NgR1Nv-7wqrqMkwbeUmf3WgT...
4 1Bauyi7HUUG2tYgOLvp3pVBlExkBNi5	NgR1Nv-7wqrqMkwbeUmf3WgT...
5 11AvAe4eQX7gQrEVN2ekTnGd57nsB8i	NgR1Nv-7wqrqMkwbeUmf3WgT...
6 11vrDXJU86ukm-Y1XXW6VTD5hmuJa5o	root
7 1cqrlqbT7h-zkLXPDbfVGz2EKNk3m_	root
8 1eC48_p1gJk3g7ZARPNdA4oc0v0K3WNat	root
9 1RKbuG8LjXy8ewquS28b-DvAFAnx9-	root
10 1jdLAzkhooBv0Vo-DQzVZj5Qxb0Fph6W	root
11 1cpvtFzghzOOhGqPXLgxG0jx4t31VMWWS	root
12 1AW2-PSb8FSxaCSoQ3pN6kvBB8DjAbUK3p	root
13 1Y1mdTHccBMZ0OaAe4ilmOHyo3DTWhRL	root

cloud_entry					
doc_id	filename	modified	created	acl_role	
1 root	root	NULL	NULL	NULL	
2 1-gtMwdcdSU...	Documents	NULL	NULL	0	
3 NgR1Nv-7wq...	Finance	1586216467	NULL	0	
4 12_CEEggpdp...	TheMikeWylie...	1586216489	NULL	0	
5 1ONBo9XPoZ...	TheMikeWylie...	1586216490	NULL	0	
6 1Bauyi7HUUG...	TheMikeWylie...	1586216490	NULL	0	

44



Dropbox

45



Dropbox

- Dropbox uses encrypted SQLite 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



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



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



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



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



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



Box: Box_Streem_[#][date].log

- Parse Box_Streem log(s) for key actions:

- addFile
- addFolder
- onDeleteFile
- onDeleteFolder
- onOpenFile
- onClosefile
- onReadFile
- onCreateFile
- onWriteFile
- onGetFileInfo

```
Box_Streem_0_2020-04-08.log - Notepad
File Edit Format View Help
[info][2020-04-08 17:45:05.121910][0x000011a8][baseipcreceiver:1077][addFile] "\TheMikeWylie - 2020 Strategic Plan.rtf", NodeMetadata(name="TheMikeWylie - 2020 Strategic Plan.rtf", vpath="", type=FILE, inodeId=0, parentId=2, size=218, createdAtTimestamp=1585868633, modifiedAtTimestamp=1585867993, isLocked=0, packageRoot=<null>, checksum=<null>, sendsFLE=<null>, version=<null>)
[info][2020-04-08 17:45:05.121910][0x000011a8][baseipcreceiver:1060][addFolder] "\Finance", NodeMetadata(name="Finance", vpath="", type=FOLDER, inodeId=0, parentId=2, size=0, createdAtTimestamp=1586216637, modifiedAtTimestamp=1586216655, isLocked=0, packageRoot=<null>, checksum=<null>. sendsFLE=<null>. version=<null>)
```

53



Box: Box_Streem_[#][date].log

Name	Date modified	Type	Size
Shell_Ext_explorer_000.log	4/16/2020 11:30 AM	Text Document	14 KB
Box_Streem_1_2020-04-14.log	4/16/2020 12:04 PM	Text Document	299 KB
Box-2.13.518.log	4/16/2020 11:58 AM	Text Document	310 KB
BoxUI_0_2020-04-14.log	4/16/2020 11:29 AM	Text Document	42 KB

Box_Streem_1_2020-04-14.log - Notepad

```
File Edit Format View Help
[info][2020-04-14 19:16:50.663][0x0000111c][logger:103][addFileLog] Starting Streem version: 2.13.518.0
10.0.18363
[info][2020-04-14 19:16:50.728][0x0000111c][logger:108][addFileLog] info logging enabled
[warning][2020-04-14 19:16:50.728][0x0000111c][logger:109][addFileLog] warning logging enabled
[error][2020-04-14 19:16:50.728][0x0000111c][logger:110][addFileLog] error logging enabled
[fatal][2020-04-14 19:16:50.728][0x0000111c][logger:111][addFileLog] fatal logging enabled
[info][2020-04-14 19:16:50.729][0x00001814][dumpgenerator:100][dumpCreationThread] Dump Creation Thread
[debug][2020-04-14 19:16:50.729][0x0000111c][main:112][main] Options:
Cache Path: "C:\Users\bob\AppData\Local\Box\Box\Cache"
Dirty Data Cache Path: "C:\Users\bob\AppData\Local\Box\Box\unsyncedFiles"
Database Path: "C:\Users\bob\AppData\Local\Box\Box\data"
Logs Path: "C:\Users\bob\AppData\Local\Box\Box\logs"
Mount Path: "C:\Users\bob\Box"
Standalone: false
Log Level: info
```

54

RICHEY MAY
TECHNOLOGY SOLUTIONS

Box: ...\\Box\\Box\\cache

> AppData > Local > Box > Box > cache

Name	Date modified	Type
6d8f9a82-6492-4fb2-bf45-94610a42f22f	4/16/2020 11:26 AM	File
6866c8c5-d035-48a4-9349-24947f0eeb21	4/14/2020 7:16 PM	File
17625571-dbe6-47c3-95d9-52ce6cffeb3	4/16/2020 11:26 AM	File

6d8f9a82-6492-4fb2-bf45-94610a42f22f - Notepad

```

File Edit Format View Help
[{\rtf1\ansi\deff0\nouicompat{\fonttbl{\f0\fnil\fcharset0 Calibri;}}
{\*\generator Riced20 10.0.18362}\viewkind4\uc1
\pard\sa200\s1276\slmult1\f0\fs22\lang9 Make a ton of money. \par
Rule zee world.\par
\par
}

```

55

RICHEY MAY
TECHNOLOGY SOLUTIONS

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

> AppData > Local > Box > Box > logs

Name	Date modified	Type	Size
Shell_Ext_explorer_000.log	4/16/2020 11:30 AM	Text Document	14 KB
Box_Stream_1_2020-04-14.log	4/16/2020 11:39 AM	Text Document	298 KB
Box-2.13.518.log	4/16/2020 11:58 AM	Text Document	310 KB
BoxUI_0_2020-04-14.log	4/16/2020 11:29 AM	Text Document	42 KB

BoxUI_0_2020-04-14.log - Notepad

```

File Edit Format View Help
status: LoggedOut, online status: Offline, application status: Idle, update available: None, problem item count: BoxUI.Model.ProblemItemCount
[info][2020-04-14 19:16:50.154][0x00001c34][TrayIcon:46][Icon] value: (Icon)
[info][2020-04-14 19:16:50.154][0x00001c34][WPNotifyIcon:355][UpdateIcon] created: True, hwnd: 66552, id: 0, msg: 49624
[info][2020-04-14 19:16:50.154][0x00001c34][TrayIcon:55][Tooltip] value: Box Drive is not logged in
[info][2020-04-14 19:16:50.154][0x00001c34][WPNotifyIcon:355][UpdateIcon] created: True, hwnd: 66552, id: 0, msg: 49624
[info][2020-04-14 19:16:50.154][0x00001c34][TimerUtils:18][OneShotTimer] timeout: 00:00:10
[info][2020-04-14 19:16:50.154][0x00001c34][SafeUIDispatcher:75][Listen] name: BoxDriveUpdateAvailableEvent
[info][2020-04-14 19:16:50.154][0x00001c34][MainWindowViewModel:1010][ListenForInstaller]
[info][2020-04-14 19:16:50.154][0x00001c34][SafeUIDispatcher:75][Listen] name: BoxDriveInstallEvent
[info][2020-04-14 19:16:50.154][0x00001c34][SafeUIDispatcher:75][Listen] name: BoxDriveForceQuitInstallEvent
[info][2020-04-14 19:16:50.154][0x00001c34][SafeUIDispatcher:75][Listen] name: BoxDriveUninstallEvent

```

56



Box: Box-[version].log

> AppData > Local > Box > Box > logs

Name	Date modified	Type	Size
Shell_Ext_explorer_000.log	4/16/2020 11:30 AM	Text Document	
Box_Streem_1_2020-04-14.log	4/16/2020 11:39 AM	Text Document	
Box-2.13.518.log	4/16/2020 11:43 AM	Text Document	

Box-2.13.518.log - Notepad

```
[[36;49m2020-04-16 11:30:05.148 7608 INFO    LocalFSMonitor
fs_monitor          Processing item change TN: _00000010_;
new_native_state: (<LocalNativeState native_id: LocalNativeID
(inode=15, native_item_type=0); parent_native_id: 2; name: test.txt;
item_type: 0; size: 0; is_deleted: False; syncability: SYNCABLE;
checksum: None; content_created_at: 1587061803; content_updated_at:
```

57



Box: Databases

> Box > Box > data >

Name
shell
item_status.db
local_state_store.db
metrics.db
monitor_state.db
streemfs.db
sync.db

58



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



Box: sync.db

DB Browser for SQLite - C:\Users\bob\AppData\Local\Box\Box\data\sync.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 Pragmas Execute SQL

Table: local_item

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

60



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



Box: streemfs.db

DB Browser for SQLite - C:\Users\bob\AppData\Local\Box\Box\data\streemfs.db

touchSequence	cacheDataId	dirtyData	size	sizeAtLastConsistentState	intervals	inodeId	age
1	6d8f9a82-6492-4fb2-bf45-94610a42f22f	0	218	218	BLOB	4	1587061603
2	17625571-dbe6-47c3-95d9-52ce6cfef9b3	0	1399734	1399734	BLOB	6	1587061592
3	cba5cad-bc97-4456-a302-18231db1ec3a	0	235	235	BLOB	7	0
4	ec350e64-a403-4324-ba1d-097ec1c98c36	0	58	58	BLOB	8	0
5	b527d119-9f3b-4f86-9f6b-acd1a05658eb	0	141250	141250	BLOB	9	0
6	fd61e927-8c10-478d-b1ee-c14ff35db5a7	0	402646	402646	BLOB	10	0
7	8d760ef6-f55e-4539-bcad-b1c7cf779c4e	0	9041	9041	BLOB	11	0
8	3f628ff3-94cd-4ad4-b5ee-accafe10d08c	0	11222	11222	BLOB	12	0
9	a1b45d9b-d175-4aa0-a9fa-ba7ed4b5044d	0	22709	22709	BLOB	13	1586559670
10	a0cad09b-14f1-43bb-941f-69a2dd27236	0	0	0	BLOB	15	0
11	4398a1bf-792c-4ba5-946e-7ee2a8f9b3fb	1	62	0	BLOB	17	1587066195

62

RICHEY MAY TECHNOLOGY SOLUTIONS

Box: streemfs.db

DB Browser for SQLite - C:\Users\bob\AppData\Local\Box\Box\data\streemfs.db

Table: local_item

local_id	native_item_type	parent_item_id	name	content_created_at	content_updated_at	size	inode	checksum	date	intervals	inodeId	age
1	0	NULL				0	2		NULL			
2	0	0	TheMikeWyle - 2...	1585866003	15858667993	218	4		NULL			
3	2	1	Finance	1596216057	0	6	5		NULL			
4	3	0	TheMikeWyle - N...	1585866002	15858667803	1399734	6		NULL			
5	4	0	TheMikeWyle - St...	1585866003	15858667506	235	7		NULL			
6	5	0	TheMikeWyle - 0...	1585866003	15858667214	58	8		NULL			
7	6	0	TheMikeWyle - 2...	1586215063	1586215063	141250	9		NULL			
8	7	0	TheMikeWyle - Su...	1586215405	1586215405	402646	10		NULL			
9	8	0	TheMikeWyle - Du...	1586214863	1586214863	9041	11		NULL			
10	9	0	TheMikeWyle - El...	1586215685	1586215685	11222	12		NULL			
11	10	0	Business-Plan-for...	158601807	158601807	13	13		NULL			
12	11	0	test.txt	1587061803	1587061803	0	15		NULL			
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	

63

RICHEY MAY TECHNOLOGY SOLUTIONS

Box: streemfs.db

DB Browser for SQLite - C:\Users\bob\AppData\Local\Box\Box\data\streemfs.db

Table: cachefiles

touchSequence	cacheDataId	dirtyData	size	sizeAtLastConsistentState	intervals	inodeId	age
1	6d8f9a82-6492-4fb2-bf45-94610a42f22f	0	218	218		BLOB	4 1587061603
2	17625571-dbe6-47c3-95d9-52ce6cffeb3	0	1300774	1300774			1587061603
3	cba53cad-bc97-4456-a302-18231db1ec3a	0	23	AppData > Local > Box > Box > cache			
4	ec350e64-a403-4324-ba1d-007ec1c98c36	0	58				
5	b527d119-9f3b-f1f8-9f6b-acd1a05658eb	0	14	Name			
6	fd61e927-8c10-47bd-b1ee-c14f35db5a7	0	40				
7	8d760eef-5f5e-4539-bcad-b1c7cf79c4	0	90				
8	3f628f3-94cd-44d1-b5ee-ac5afe1e0d08c	0	11				
9	a1b45d9b-d175-4aa0-a9fa-ba7ed4b5044d	0	22				
10	a0cad09b-14f1-43bb-941f-69a2ddd27236	0	62				
11	4398a1bf-792c-4ba5-946e-7ee2a8f9b3fb	1					

Magic Number for .docx:
50 48 03 04 [PK]

File Edit Format View Help
PK [] €SP [] _rels/ []
çæÈà, () Ñ9M.+È=+0]™-ASápwAjrò

64



Box: streemfs.db

65



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



Citrix ShareFile

67



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



Citrix ShareFile

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

69



Citrix ShareFile: Databases

db > ef7357c4-b21e-4e76-92f3-9f19;	
older	
	Name
▲	capabilities.db
▲	conflictedFiles.db
▲	deltaToken.db
▲	directoryEntry.db
▲	localItem.db
▲	nonDisposableContent.db
▲	pendingActions.db
▲	pendinguploadstate.db
▲	raygun.db
▲	remote.db

70



Citrix: remote.db

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

71



Citrix: remote.db

DB Browser for SQLite - C:\Users\bob\AppData\Local\Citrix\Citrix Files\db\ef7357c4-b21e-4e76-92f3-9f192c29ae4b\remote.db

File Edit View Tools Help

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

Database Structure Browse Data Edit Pragmas Execute SQL

Table: RemoteDirectoryEntry

DirectoryEntryId	ParentDirectoryEntryId	Name	DB_ShareFileId
1	0	Personal Folders	f0h37c12-7da...
2	0	Shared Folders	allshared
3	0	Favorites	favorites
4	1	TheMikeWylie - Net...	f150d23-626...
5	1	TheMikeWylie - Stra...	f12db802-7b6...
6	1	TheMikeWylie - web...	f1cb43e9-5b2a...
7	1	TheMikeWylie - 202...	f1fd9872-77bd...
8	1	Finance	f0309fc2-2b6f...
9	8	TheMikeWylie - 201...	f10a3856-353...
10	8	TheMikeWylie - DEC ...	f1e2d2fb-2d63...
11	8	TheMikeWylie - Fina...	f19f1031-d974...
12	8	TheMikeWylie - Sup...	f1ea6c49-2ab1...
13	1	Business-Plan-for- a...	f1b9a12-21e...

72



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



Citrix: remote.db

DB Browser for SQLite - C:\Users\bob\AppData\Local\Citrix\Files\db\ef7357c4-b21e-4e76-9f3-9f19c29aa4b\remote.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 Pragmas Execute SQL

Table: RemoteItem2

	DB_ItemId	DB_ParentId	ItemType	localFileSystem	Description	FavoriteUrl	CreationDate	Permissions	DB_ZoneId	DB_StreamId	Size	Hash	sMultipleVersion	DB_LockOwnerIc	ProgenyEditDate	
1	f150d23-626...	foh37c12-7da...	1	4	NULL	NULL	63721464891...	204	zp16ffd530-c...	st85984b-30...	1399734	c0885b2c375c...	0	NULL	NULL	3
2	f2dbdb02-706...	foh37c12-7da...	1	5	NULL	NULL	63721464891...	204	zp16ffd530-c...	stba0fc2-34ea...	235	d364a3999fa...	0	NULL	NULL	3
3	f1cb4e9-5b2a...	foh37c12-7da...	1	6	NULL	NULL	63721464890...	204	zp16ffd530-c...	stf6f09d-4306...	58	8a516a8890df7...	0	NULL	NULL	3
4	f1f998f2-77bd...	foh37c12-7da...	1	7	NULL	NULL	63721464892...	204	zp16ffd530-c...	ste91e1c-5cd...	218	9a943ae6f136e...	0	NULL	NULL	3
5	f0309fc2-2bf...	foh37c12-7da...	2	8	NULL	NULL	63721813773...	100	zp16ffd530-c...	st1d039d-809...	564159	NEA	0	NULL	63721813805...	3
6	f0a3b56-353...	fo309fc2-2bf...	1	9	NULL	NULL	63721813796...	204	zp16ffd530-c...	stbe9d11-960...	141250	d47de375a28...	0	NULL	NULL	3
7	fied2fb-2d6...	fo309fc2-2bf...	1	10	NULL	NULL	63721813799...	204	zp16ffd530-c...	st392497-264...	9041	e2d611d2d635...	0	NULL	NULL	3
8	f9f1031-4974...	fo309fc2-2bf...	1	11	NULL	NULL	63721813802...	204	zp16ffd530-c...	st7c7del1-17...	11222	5e54228de30...	0	NULL	NULL	3
9	fiedac49-2ab1...	fo309fc2-2bf...	1	12	NULL	NULL	63721813805...	204	zp16ffd530-c...	st531099-013...	402646	4d08947e20c...	0	NULL	NULL	3
10	f1b9e412-21e...	foh37c12-7da...	1	13	NULL	NULL	63722156503...	204	zp16ffd530-c...	st36e488-fa7...	22709	f2e3813a20f4...	0	NULL	NULL	3
11	foh37c12-7da...	top	2	1	NULL	NULL	63721459329...	877	stb4b6ed-edfc...	1987113	NEU	0	NULL	63722156503...	3	
12	allshared	top	2	2	NULL	NULL	63721459272...	365	stb4b6ed-edfc...	1987113	NEU	0	NULL	63722156503...	3	
13	favorites	top	2	3	NULL	NULL	0	0	favorites	0	NULL	0	NULL	0	0	

74



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



Citrix: directoryEntry.db

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

76



Citrix: CitrixFiles_date[date].log

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

77



Citrix: ...\\PartCache\\

'357c4-b21e-4e76-92f3-9f192c29ae4b > readwrite > f1373bad-9c91-4acd-ab15-5b24eb281811

Name	Date modified	Type
0.part	4/10/2020 4:01 PM	PART File
0.docx	4/10/2020 4:01 PM	Office Open XML ... 23 KB

0.docx - WordPad

Home View

Cut Copy Paste Font Paragraph Insert Editing

Business Plan for a Startup Business

78



Closing

79



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



KAPE: !CloudStorage-MetaData.tkape

```

!CloudStorage-MetaData.tkape
1 Description: Box Cloud Storage Metadata Only
2 Author: Michael Wylie
3 Version: 1
4 RecreateDirectories: true
5 Id: 34f118e0-687e-49c1-acdd-85cc68a98888
6 Targets:
7 # Box Metadata
8
9     Name: Box Drive Application Metadata
10    Category: App
11    Path: C:\Users\user\AppData\Local\Box\Box\*
12    IsDirectory: True
13    Recursive: True
14    Comment: ""
15
16    Name: Box Sync Application Metadata
17    Category: App
18    Path: C:\Users\user\AppData\Local\Box Sync\*
19    IsDirectory: True
20    Recursive: True
21    Comment: ""
22 # Dropbox Metadata
23
24    Name: Dropbox Metadata
25    Category: App
26    Path: C:\Users\user\AppData\Local\Dropbox\info.json
27    IsDirectory: False
28    Recursive: False
29    Comment: "Getting individual files because folder may contain very large extraneous files"
30
31    Name: Dropbox Metadata
32    Category: App
33    Path: C:\Users\user\AppData\Local\Dropbox\filecache.dbx
34    IsDirectory: False
35    Recursive: False
36    Comment: "Getting individual files because folder may contain very large extraneous files"
37
38    Name: Dropbox Metadata
39    Category: App
40    Path: C:\Users\user\AppData\Local\Dropbox\config.dbx
41    IsDirectory: False
42    Recursive: False
43    Comment: "Getting individual files because folder may contain very large extraneous files"
44 # Microsoft OneDrive Metadata

```

81



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\evide
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
\evidence5\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
\evidence5\C\users\Bob\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2'. Hashing source file...

Copied 117 (Duplicated: 12) out of 129 files in 11.9257 seconds. See '*_CopyLog.csv' in 'C:\Users\Bob\Downloads\evide
nce5' for copy details

Total execution time: 11.9745 seconds

Press any key to exit

```

82



Thank You!

MICHAEL WYLIE

TWITTER: @THEMIKEWYLIE

LINKEDIN: LINKEDIN.COM/IN/MWYLIE

WWW.RICHEYMAYTECH.COM