A Little Bit of This, A Little Bit of dat

ONEDRIVE FORENSICS

A Little Bit of This, A Little Bit of ~~dat~~ SQLite

ONEDRIVE FORENSICS

BIO

Brian Maloney

DFIR Analyst

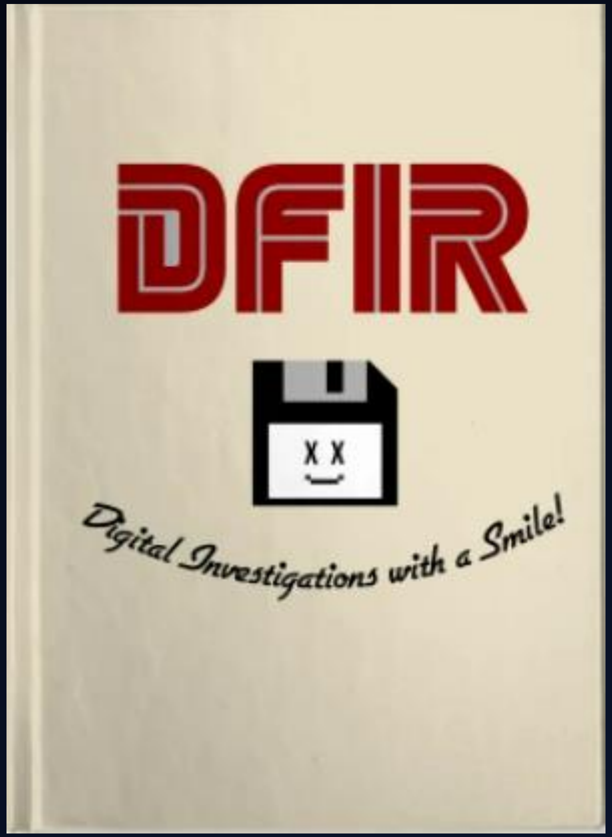
- OneDriveExplorer
- SEPparser
- DeXRAY (McAfee/Symantec)
- PCAP_tools plugin (ProcDOT)
- Targets/Modules for KAPE

https://keybase.io/beercow

https://github.com/Beercow/OneDriveExplorer

Agenda

- Collection
- OneDrive Artifacts
- OneDriveExplorer
- Demo
- Automation With KAPE
- Lessons Learned
- Roadmap

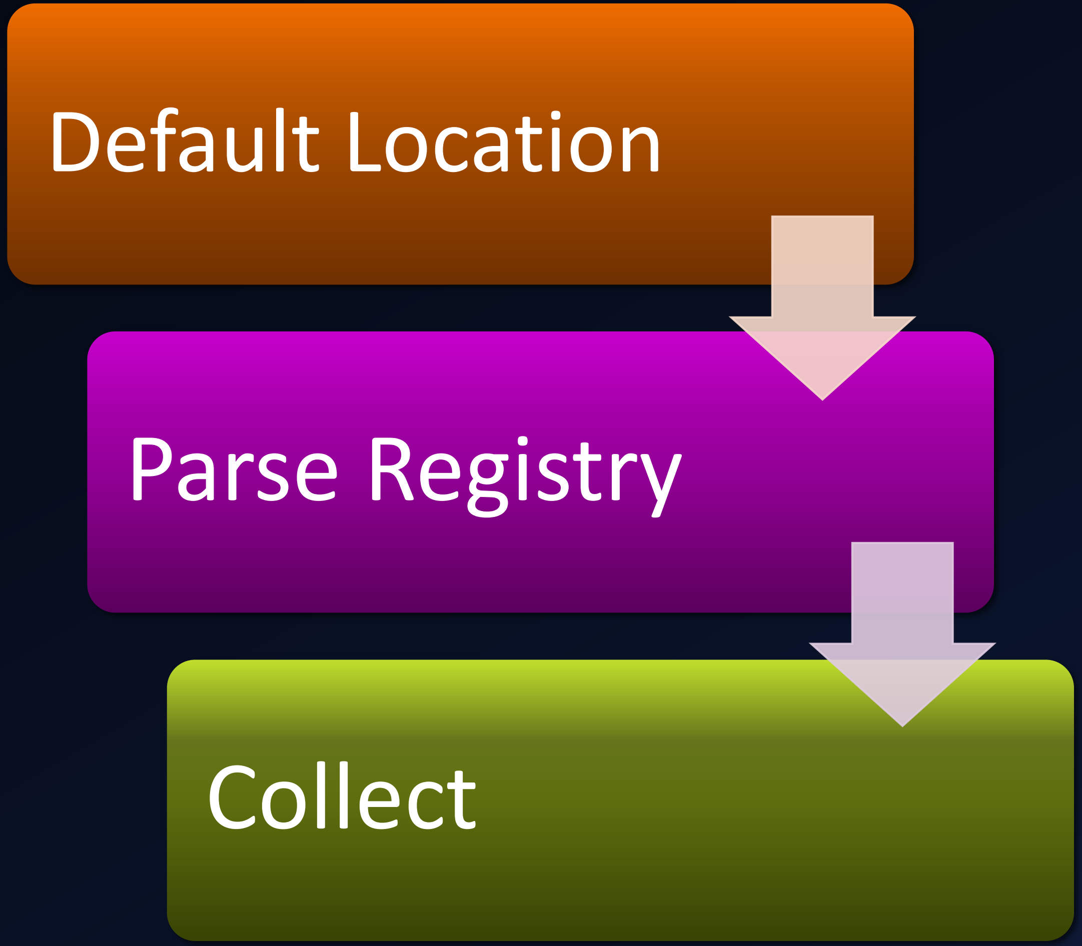


Why Collect From The Endpoint?

- Grab OneDrive files from the cloud
  - Collect all user's files and folders
  - UAL for activity
- Collecting from endpoint
  - OneDrive point of view from user
  - What files are on the endpoint
  - What Files/Folders/Libraries have been synced/linked
  - ODL for user activity

Collecting Data From OneDrive

- Know the default location
  - This can be changed
- Check registry for synced/linked folders
- Collect OneDrive files
  - Storage space and scope of authority issues
- Gets complicated on multi-user systems



Default Location

Parse Registry

Collect

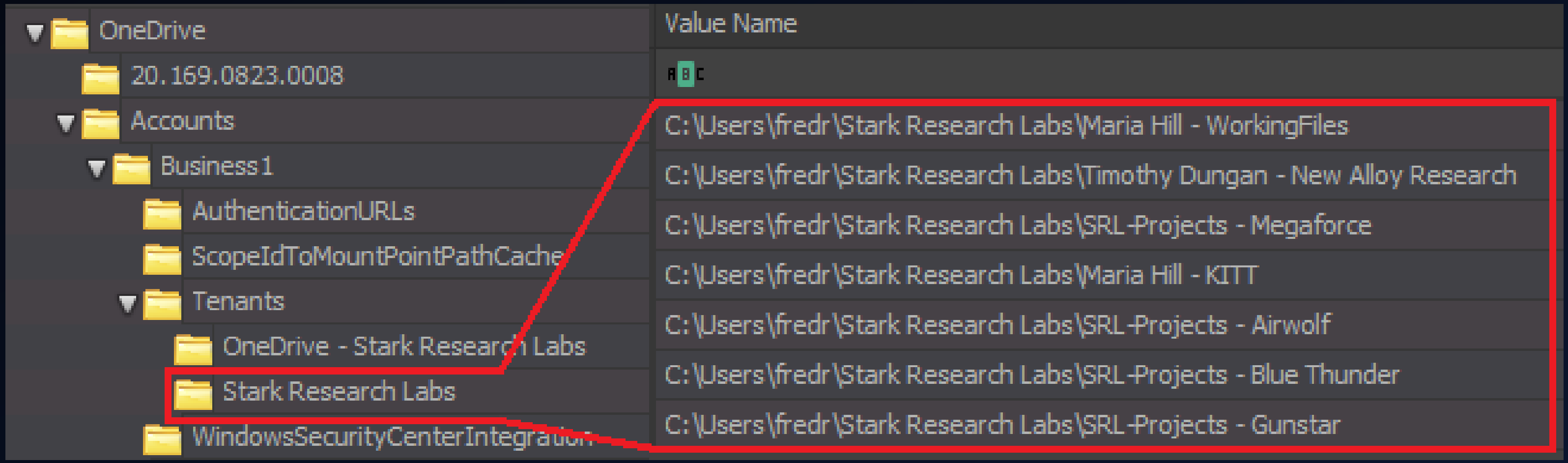
The Artifacts

- Local Files
  - %USERPROFILE%\OneDrive
  - NTUSER\Software\Microsoft\Microsoft\OneDrive\Accounts\<*Personal**Business1-9*>
  - NTUSER\Software\SyncEngines\Providers\OneDrive
- Metadata
  - %AppData%\Local\Microsoft\OneDrive\logs\<*Personal**Business1-9*>
  - %AppData%\Local\Microsoft\OneDrive\settings\<*Personal**Business1-9*>

Tenants Key

NTUSER\SOFTWARE\MICROSOFT\ONEDRIVE\ACCOUNTS\PERSONAL\TENANTS
NTUSER\SOFTWARE\MICROSOFT\ONEDRIVE\ACCOUNTS\BUSINESS<1-9>\TENANTS

- Tracks folders synchronized from other sources
- Important to find all synced/linked folders



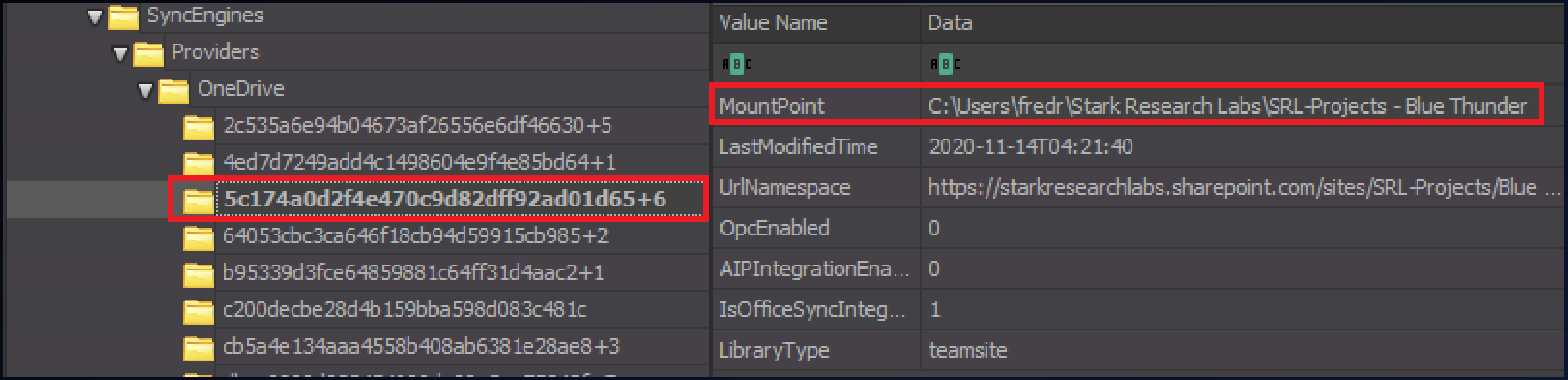
```
▼ OneDrive
    20.169.0823.0008
  ▼ Accounts
    ▼ Business1
        AuthenticationURLs
        ScopeIdToMountPointPathCache
      ▼ Tenants
          OneDrive - Stark Research Labs
          Stark Research Labs
        WindowsSecurityCenterIntegration
```

Value Name
C:\Users\fredr\Stark Research Labs\Maria Hill - WorkingFiles
C:\Users\fredr\Stark Research Labs\Timothy Dungan - New Alloy Research
C:\Users\fredr\Stark Research Labs\SRL-Projects - Megaforce
C:\Users\fredr\Stark Research Labs\Maria Hill - KITT
C:\Users\fredr\Stark Research Labs\SRL-Projects - Airwolf
C:\Users\fredr\Stark Research Labs\SRL-Projects - Blue Thunder
C:\Users\fredr\Stark Research Labs\SRL-Projects - Gunstar

SyncEngines

NTUSER\SOFTWARE\SYNCENGINES\PROVIDERS\ONEDRIVE

- Identify default local file storage
- Locally synced/linked folders from different owners



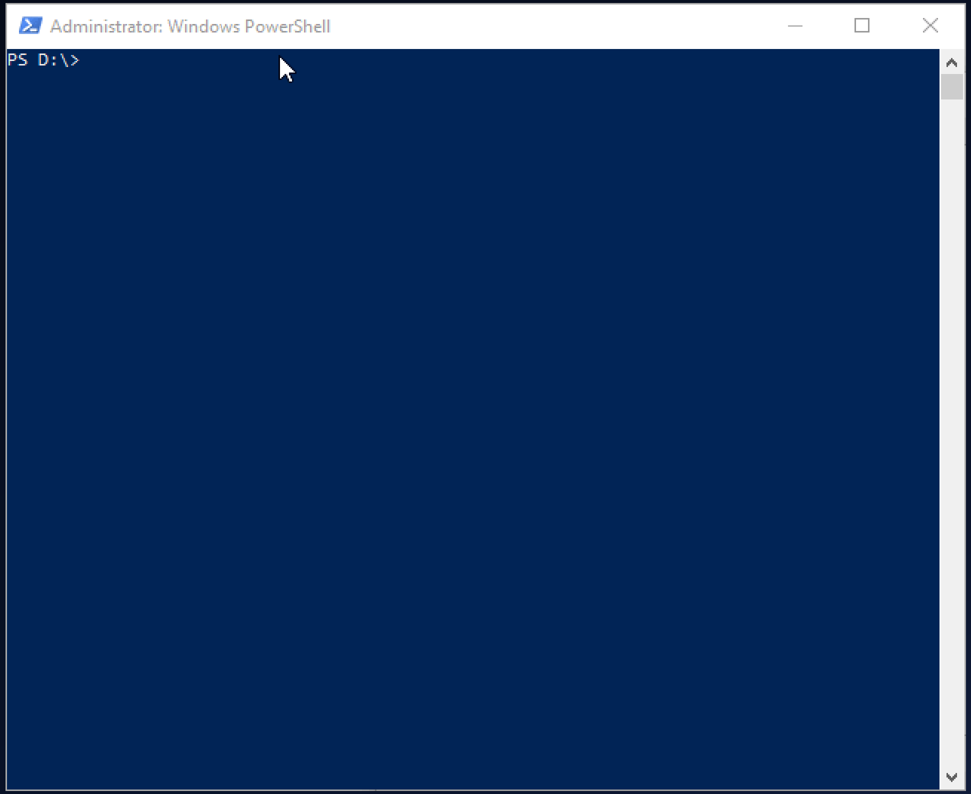
- SyncEngines
  - Providers
    - OneDrive
      - 2c535a6e94b04673af26556e6df46630+5
      - 4ed7d7249add4c1498604e9f4e85bd64+1
      - 5c174a0d2f4e470c9d82dff92ad01d65+6
      - 64053cbc3ca646f18cb94d59915cb985+2
      - b95339d3fce64859881c64ff31d4aac2+1
      - c200decbe28d4b159bba598d083c481c
      - cb5a4e134aaa4558b408ab6381e28ae8+3

Value Name	Data
ABC	ABC
MountPoint	C:\Users\fredr\Stark Research Labs\SRL-Projects - Blue Thunder
LastModifiedTime	2020-11-14T04:21:40
UrlNamespace	https://starkresearchlabs.sharepoint.com/sites/SRL-Projects/Blue ...
OpcEnabled	0
AIPIntegrationEna...	0
IsOfficeSyncInteg...	1
LibraryType	teamsite

<UserCid>.dat

%APPDATA%\LOCAL\MICROSOFT\ONEDRIVE\SETTINGS\<*PERSONAL\BUSINESS1-9*>

- Strings shows every file in synced folders
  - Local Files
  - Cloud Files
  - Files/Folders shared with user



```
PS D:\>
```

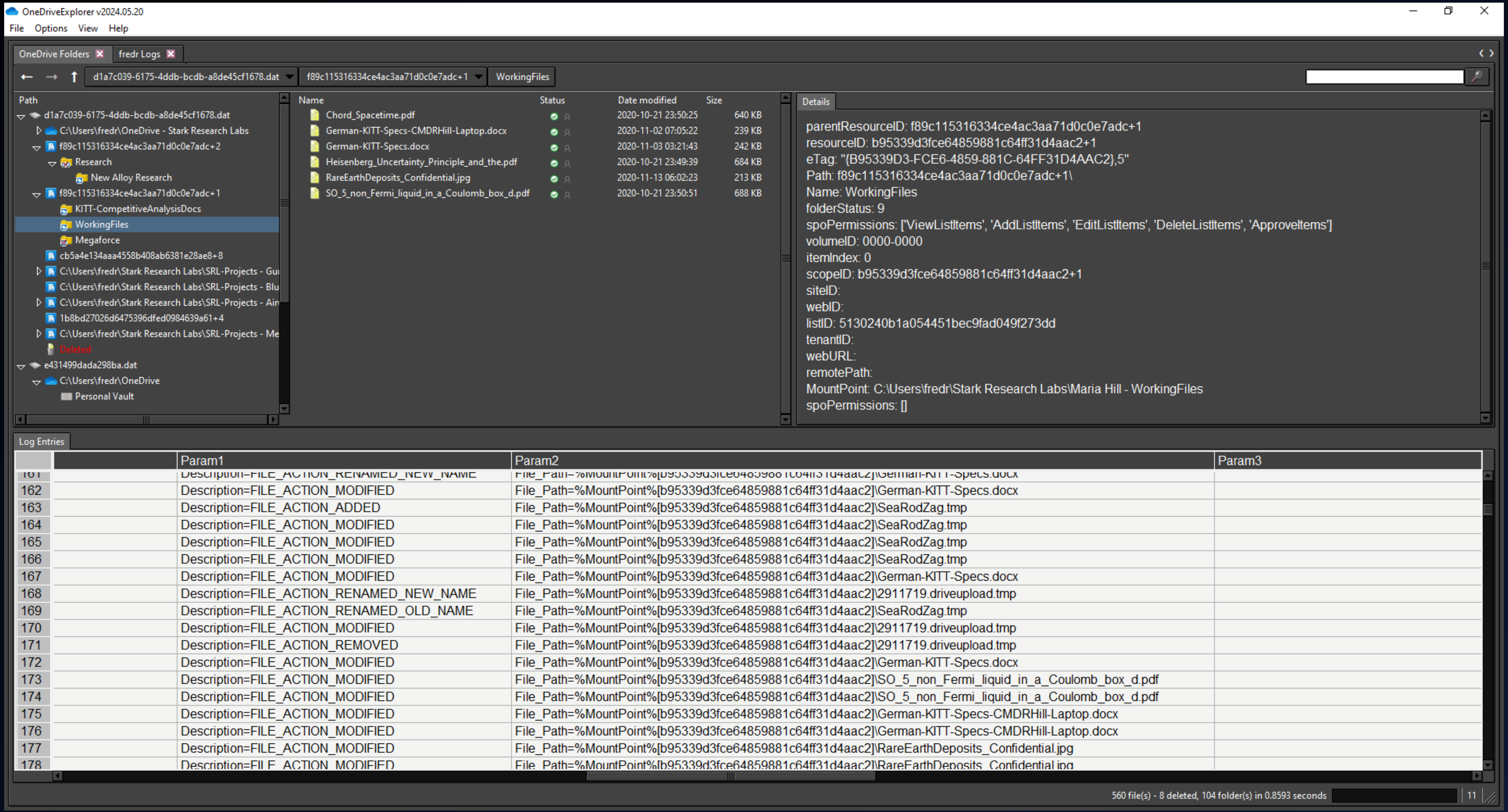
Let’s Rethink How We’re Doing Things

ONEDRIVEEXPLORER

OneDriveExplorer (ODE)

- Built on 400 + version of OneDrive
- Parser for <UserCid>.dat and SQLite
- Names of local, shared, synced/linked, and cloud only files
- GUI rebuilds folder structure and provides searching
- Decrypts log files
  - Cstruct files for individual records

OneDriveExplorer (ODE)


OneDriveExplorer v2024.05.20
File Options View Help
OneDrive Folders
fredr Logs
d1a7c039-6175-4ddb-bcdb-a8de45cf1678.dat
f89c115316334ce4ac3aa71d0c0e7adc+1
WorkingFiles
Details
Log Entries

```
Path
▽ d1a7c039-6175-4ddb-bcdb-a8de45cf1678.dat
    ▷ C:\Users\fredr\OneDrive - Stark Research Labs
    ▽ f89c115316334ce4ac3aa71d0c0e7adc+2
        ▽ Research
              New Alloy Research
    ▽ f89c115316334ce4ac3aa71d0c0e7adc+1
          KITT-CompetitiveAnalysisDocs
          WorkingFiles
          Megaforce
      cb5a4e134aaa4558b408ab6381e28ae8+8
    ▷ C:\Users\fredr\Stark Research Labs\SRL-Projects - Gu
      C:\Users\fredr\Stark Research Labs\SRL-Projects - Blu
    ▷ C:\Users\fredr\Stark Research Labs\SRL-Projects - Air
      1b8bd27026d6475396dfed0984639a61+4
    ▷ C:\Users\fredr\Stark Research Labs\SRL-Projects - Me
      Deleted
▽ e431499dada298ba.dat
    ▽ C:\Users\fredr\OneDrive
          Personal Vault
```

Name	Status	Date modified	Size
Chord_Spacetime.pdf	●	2020-10-21 23:50:25	640 KB
German-KITT-Specs-CMDRHill-Laptop.docx	●	2020-11-02 07:05:22	239 KB
German-KITT-Specs.docx	●	2020-11-03 03:21:43	242 KB
Heisenberg_Uncertainty_Principle_and_the.pdf	●	2020-10-21 23:49:39	684 KB
RareEarthDeposits_Confidential.jpg	●	2020-11-13 06:02:23	213 KB
SO_5_non_Fermi_liquid_in_a_Coulomb_box_d.pdf	●	2020-10-21 23:50:51	688 KB

```
parentResourceID: f89c115316334ce4ac3aa71d0c0e7adc+1
resourceID: b95339d3fce64859881c64ff31d4aac2+1
eTag: "{B95339D3-FCE6-4859-881C-64FF31D4AAC2},5"
Path: f89c115316334ce4ac3aa71d0c0e7adc+1\
Name: WorkingFiles
folderStatus: 9
spoPermissions: ['ViewListItems', 'AddListItems', 'EditListItems', 'DeleteListItems', 'ApproveItems']
volumeID: 0000-0000
itemIndex: 0
scopeID: b95339d3fce64859881c64ff31d4aac2+1
siteID:
webID:
listID: 5130240b1a054451bec9fad049f273dd
tenantID:
webURL:
remotePath:
MountPoint: C:\Users\fredr\Stark Research Labs\Maria Hill - WorkingFiles
spoPermissions: []
```

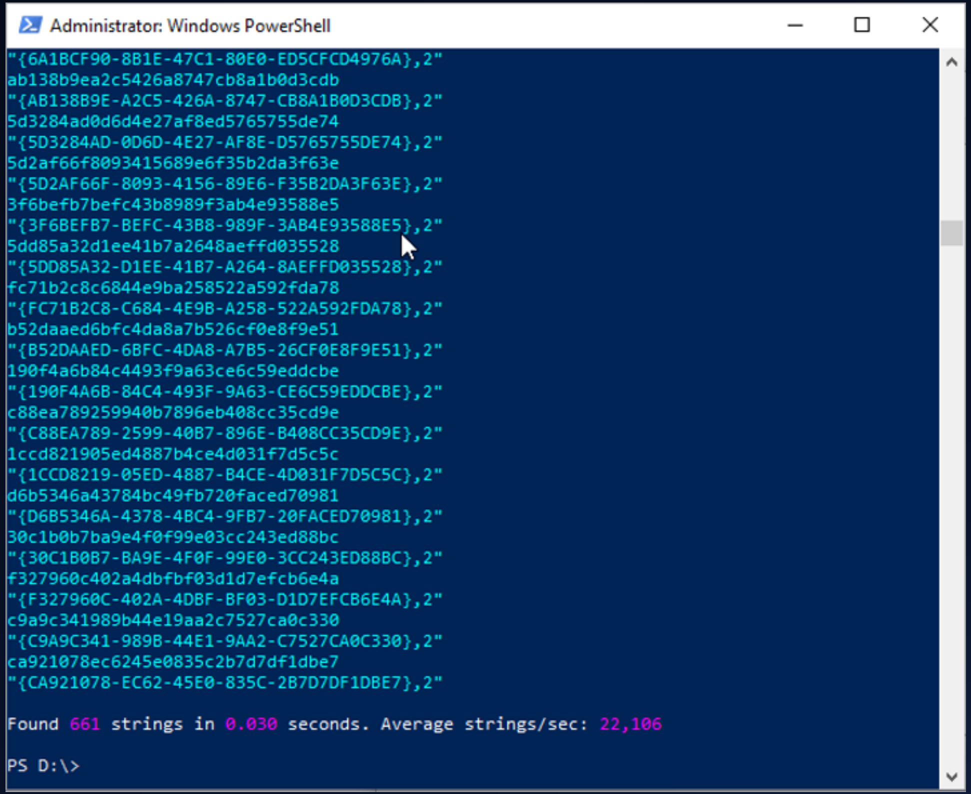
		Param1	Param2	Param3
161		Description=FILE_ACTION_RENAMED_NEW_NAME	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\German-KITT-Specs.docx	
162		Description=FILE_ACTION_MODIFIED	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\German-KITT-Specs.docx	
163		Description=FILE_ACTION_ADDED	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\SeaRodZag.tmp	
164		Description=FILE_ACTION_MODIFIED	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\SeaRodZag.tmp	
165		Description=FILE_ACTION_MODIFIED	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\SeaRodZag.tmp	
166		Description=FILE_ACTION_MODIFIED	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\SeaRodZag.tmp	
167		Description=FILE_ACTION_MODIFIED	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\German-KITT-Specs.docx	
168		Description=FILE_ACTION_RENAMED_NEW_NAME	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\2911719.driveupload.tmp	
169		Description=FILE_ACTION_RENAMED_OLD_NAME	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\SeaRodZag.tmp	
170		Description=FILE_ACTION_MODIFIED	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\2911719.driveupload.tmp	
171		Description=FILE_ACTION_REMOVED	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\2911719.driveupload.tmp	
172		Description=FILE_ACTION_MODIFIED	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\German-KITT-Specs.docx	
173		Description=FILE_ACTION_MODIFIED	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\SO_5_non_Fermi_liquid_in_a_Coulomb_box_d.pdf	
174		Description=FILE_ACTION_MODIFIED	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\SO_5_non_Fermi_liquid_in_a_Coulomb_box_d.pdf	
175		Description=FILE_ACTION_MODIFIED	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\German-KITT-Specs-CMDRHill-Laptop.docx	
176		Description=FILE_ACTION_MODIFIED	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\German-KITT-Specs-CMDRHill-Laptop.docx	
177		Description=FILE_ACTION_MODIFIED	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\RareEarthDeposits_Confidential.jpg	
178		Description=FILE_ACTION_MODIFIED	File_Path=%MountPoint%[b95339d3fce64859881c64ff31d4aac2]\RareEarthDeposits_Confidential.jpg	

560 file(s) - 8 deleted, 104 folder(s) in 0.8593 seconds | 11

<UserCid>.dat

%APPDATA%\LOCAL\MICROSOFT\ONEDRIVE\SETTINGS\<*PERSONAL\BUSINESS1-9*>

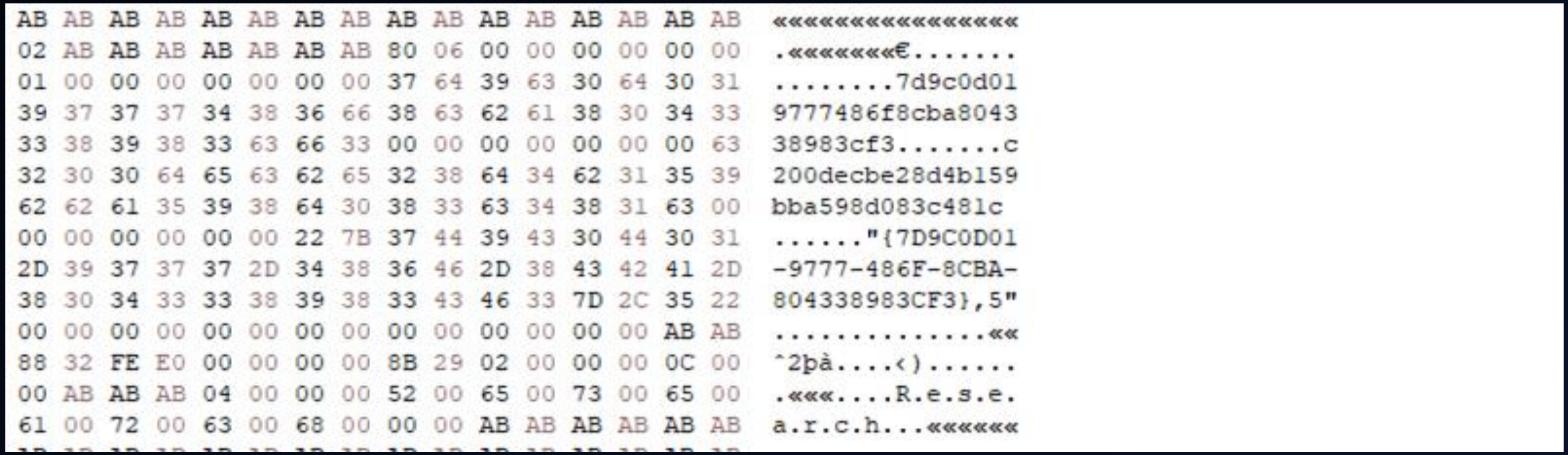
- Strings shows every file in synced folders
  - Local Files
  - Cloud Files
  - Files/Folders shared with user



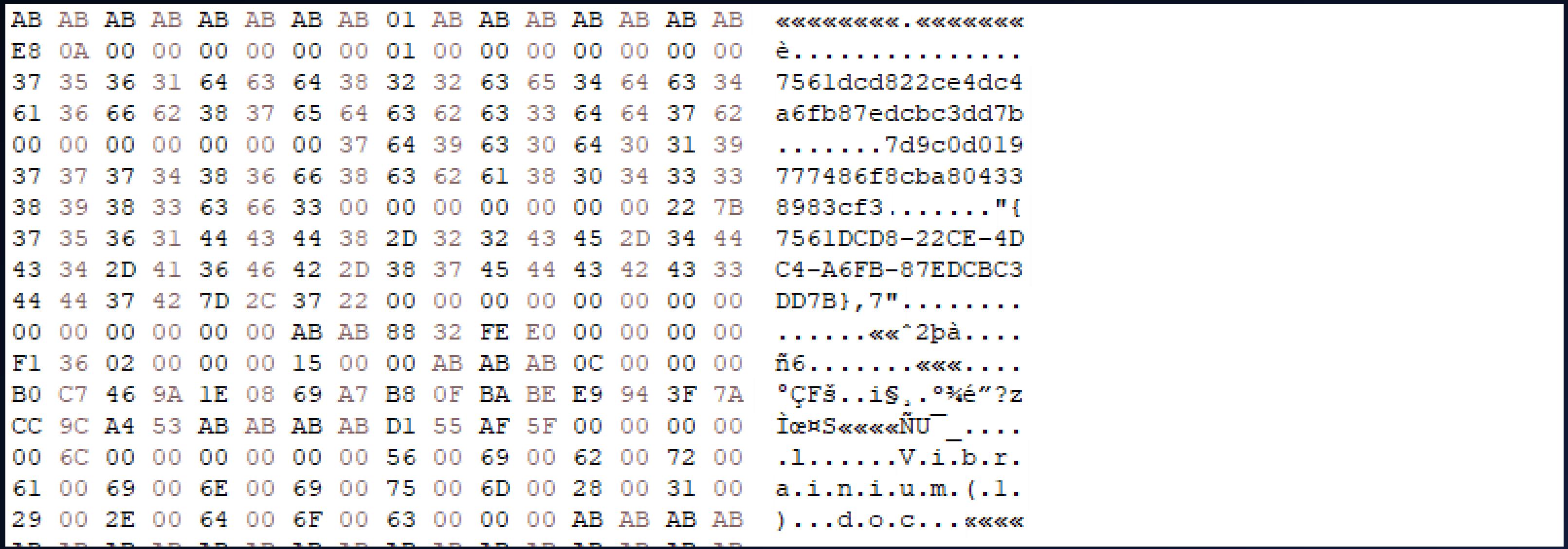
```
"{6A1BCF90-8B1E-47C1-80E0-ED5CFCD4976A},2"
ab138b9ea2c5426a8747cb8a1b0d3cdb
"{AB138B9E-A2C5-426A-8747-CB8A1B0D3CDB},2"
5d3284ad0d6d4e27af8ed5765755de74
"{5D3284AD-0D6D-4E27-AF8E-D5765755DE74},2"
5d2af66f8093415689e6f35b2da3f63e
"{5D2AF66F-8093-4156-89E6-F35B2DA3F63E},2"
3f6befb7befc43b8989f3ab4e93588e5
"{3F6BEFB7-BEFC-43B8-989F-3AB4E93588E5},2"
5dd85a32d1ee41b7a2648aeffd035528
"{5DD85A32-D1EE-41B7-A264-8AEFFD035528},2"
fc71b2c8c6844e9ba258522a592fda78
"{FC71B2C8-C684-4E9B-A258-522A592FDA78},2"
b52daaed6bfc4da8a7b526cf0e8f9e51
"{B52DAAED-6BFC-4DA8-A7B5-26CF0E8F9E51},2"
190f4a6b84c4493f9a63ce6c59eddcbe
"{190F4A6B-84C4-493F-9A63-CE6C59EDDCBE},2"
c88ea789259940b7896eb408cc35cd9e
"{C88EA789-2599-40B7-896E-B408CC35CD9E},2"
1ccd821905ed4887b4ce4d031f7d5c5c
"{1CCD8219-05ED-4887-B4CE-4D031F7D5C5C},2"
d6b5346a43784bc49fb720faced70981
"{D6B5346A-4378-4BC4-9FB7-20FACED70981},2"
30c1b0b7ba9e4f0f99e03cc243ed88bc
"{30C1B0B7-BA9E-4F0F-99E0-3CC243ED88BC},2"
f327960c402a4dbfbf03d1d7efcb6e4a
"{F327960C-402A-4DBF-BF03-D1D7EFCB6E4A},2"
c9a9c341989b44e19aa2c7527ca0c330
"{C9A9C341-989B-44E1-9AA2-C7527CA0C330},2"
ca921078ec6245e0835c2b7d7df1dbe7
"{CA921078-EC62-45E0-835C-2B7D7DF1DBE7},2"

Found 661 strings in 0.030 seconds. Average strings/sec: 22,106

PS D:\>
```

<UserCid>.dat

%APPDATA%\LOCAL\MICROSOFT\ONEDRIVE\SETTINGS\<*PERSONAL**BUSINESS1-9*>



```
AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB   ««««««««««««««««
02 AB AB AB AB AB AB AB 80 06 00 00 00 00 00 00   .«««««««€.......
01 00 00 00 00 00 00 00 37 64 39 63 30 64 30 31   ........7d9c0d01
39 37 37 37 34 38 36 66 38 63 62 61 38 30 34 33   9777486f8cba8043
33 38 39 38 33 63 66 33 00 00 00 00 00 00 00 63   38983cf3.......c
32 30 30 64 65 63 62 65 32 38 64 34 62 31 35 39   200decbe28d4b159
62 62 61 35 39 38 64 30 38 33 63 34 38 31 63 00   bba598d083c481c
00 00 00 00 00 00 22 7B 37 44 39 43 30 44 30 31   ......"{7D9C0D01
2D 39 37 37 37 2D 34 38 36 46 2D 38 43 42 41 2D   -9777-486F-8CBA-
38 30 34 33 33 38 39 38 33 43 46 33 7D 2C 35 22   804338983CF3},5"
00 00 00 00 00 00 00 00 00 00 00 00 00 00 AB AB   ..............««
88 32 FE E0 00 00 00 00 8B 29 02 00 00 00 0C 00   ˆ2þà....‹)......
00 AB AB AB 04 00 00 00 52 00 65 00 73 00 65 00   .«««....R.e.s.e.
61 00 72 00 63 00 68 00 00 00 AB AB AB AB AB AB   a.r.c.h...««««««
```

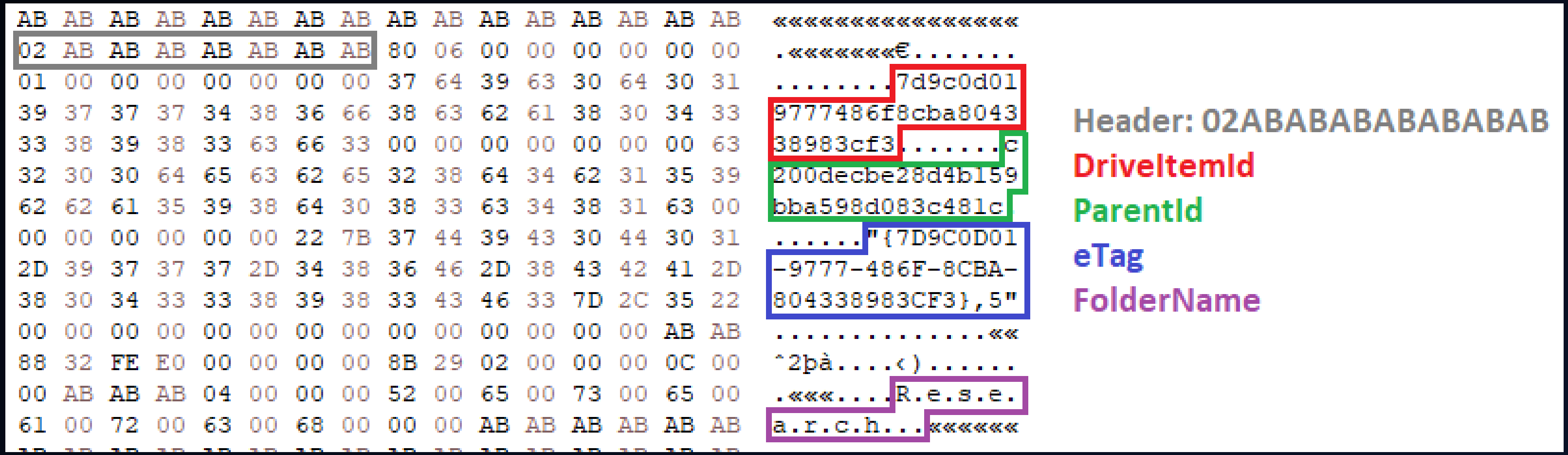


```
AB AB AB AB AB AB AB AB 01 AB AB AB AB AB AB AB   ««««««««.«««««««
E8 0A 00 00 00 00 00 00 01 00 00 00 00 00 00 00   è...............
37 35 36 31 64 63 64 38 32 32 63 65 34 64 63 34   7561dcd822ce4dc4
61 36 66 62 38 37 65 64 63 62 63 33 64 64 37 62   a6fb87edcbc3dd7b
00 00 00 00 00 00 00 37 64 39 63 30 64 30 31 39   .......7d9c0d019
37 37 37 34 38 36 66 38 63 62 61 38 30 34 33 33   777486f8cba80433
38 39 38 33 63 66 33 00 00 00 00 00 00 00 22 7B   8983cf3......."{
37 35 36 31 44 43 44 38 2D 32 32 43 45 2D 34 44   7561DCD8-22CE-4D
43 34 2D 41 36 46 42 2D 38 37 45 44 43 42 43 33   C4-A6FB-87EDCBC3
44 44 37 42 7D 2C 37 22 00 00 00 00 00 00 00 00   DD7B},7"........
00 00 00 00 00 00 AB AB 88 32 FE E0 00 00 00 00   ......««ˆ2þà....
F1 36 02 00 00 00 15 00 00 AB AB AB 0C 00 00 00   ñ6.......«««....
B0 C7 46 9A 1E 08 69 A7 B8 0F BA BE E9 94 3F 7A   °ÇFš..i§¸.º¾é”?z
CC 9C A4 53 AB AB AB AB D1 55 AF 5F 00 00 00 00   Ìœ¤S««««ÑU¯_....
00 6C 00 00 00 00 00 00 56 00 69 00 62 00 72 00   .l......V.i.b.r.
61 00 69 00 6E 00 69 00 75 00 6D 00 28 00 31 00   a.i.n.i.u.m.(.1.
29 00 2E 00 64 00 6F 00 63 00 00 00 AB AB AB AB   )...d.o.c...««««
```

<UserCid>.dat

%APPDATA%\LOCAL\MICROSOFT\ONEDRIVE\SETTINGS\<*PERSONAL\BUSINESS1-9*>

- Folders



```
AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB   ««««««««««««««««
02 AB AB AB AB AB AB AB 80 06 00 00 00 00 00 00   .«««««««€.......
01 00 00 00 00 00 00 00 37 64 39 63 30 64 30 31   ........7d9c0d01
39 37 37 37 34 38 36 66 38 63 62 61 38 30 34 33   9777486f8cba8043
33 38 39 38 33 63 66 33 00 00 00 00 00 00 00 63   38983cf3.......c
32 30 30 64 65 63 62 65 32 38 64 34 62 31 35 39   200decbe28d4b159
62 62 61 35 39 38 64 30 38 33 63 34 38 31 63 00   bba598d083c481c.
00 00 00 00 00 00 22 7B 37 44 39 43 30 44 30 31   ......"{7D9C0D01
2D 39 37 37 37 2D 34 38 36 46 2D 38 43 42 41 2D   -9777-486F-8CBA-
38 30 34 33 33 38 39 38 33 43 46 33 7D 2C 35 22   804338983CF3},5"
00 00 00 00 00 00 00 00 00 00 00 00 00 00 AB AB   ..............««
88 32 FE E0 00 00 00 00 8B 29 02 00 00 00 0C 00   ˆ2þà....‹)......
00 AB AB AB 04 00 00 00 52 00 65 00 73 00 65 00   .«««....R.e.s.e.
61 00 72 00 63 00 68 00 00 00 AB AB AB AB AB AB   a.r.c.h...««««««
```

Header: 02ABABABABABABAB

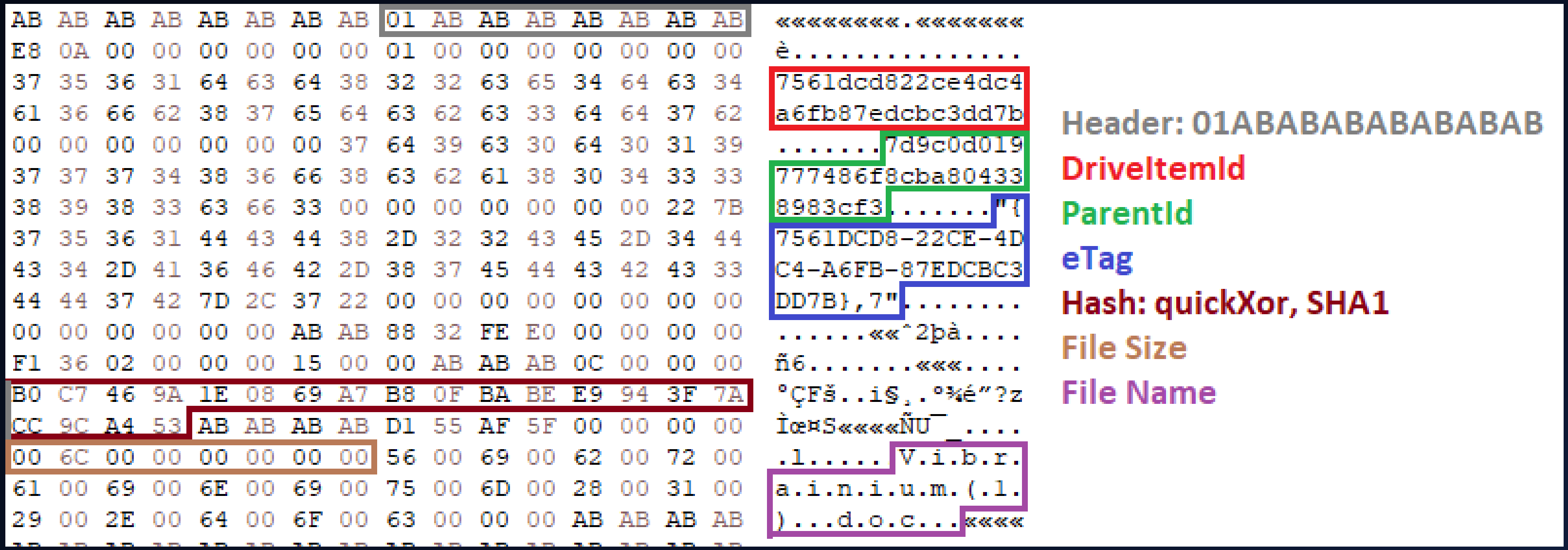
DriveItemId

ParentId

eTag

FolderName

- Files



```
AB AB AB AB AB AB AB AB 01 AB AB AB AB AB AB AB   ««««««««.«««««««
E8 0A 00 00 00 00 00 00 01 00 00 00 00 00 00 00   è...............
37 35 36 31 64 63 64 38 32 32 63 65 34 64 63 34   7561dcd822ce4dc4
61 36 66 62 38 37 65 64 63 62 63 33 64 64 37 62   a6fb87edcbc3dd7b
00 00 00 00 00 00 00 37 64 39 63 30 64 30 31 39   .......7d9c0d019
37 37 37 34 38 36 66 38 63 62 61 38 30 34 33 33   777486f8cba80433
38 39 38 33 63 66 33 00 00 00 00 00 00 00 22 7B   8983cf3......."{
37 35 36 31 44 43 44 38 2D 32 32 43 45 2D 34 44   7561DCD8-22CE-4D
43 34 2D 41 36 46 42 2D 38 37 45 44 43 42 43 33   C4-A6FB-87EDCBC3
44 44 37 42 7D 2C 37 22 00 00 00 00 00 00 00 00   DD7B},7"........
00 00 00 00 00 00 AB AB 88 32 FE E0 00 00 00 00   ......««ˆ2þà....
F1 36 02 00 00 00 15 00 00 AB AB AB 0C 00 00 00   ñ6.......«««....
B0 C7 46 9A 1E 08 69 A7 B8 0F BA BE E9 94 3F 7A   °ÇFš..i§¸.º¾é”?z
CC 9C A4 53 AB AB AB AB D1 55 AF 5F 00 00 00 00   Ìœ¤S««««ÑU¯_....
00 6C 00 00 00 00 00 00 56 00 69 00 62 00 72 00   .l......V.i.b.r.
61 00 69 00 6E 00 69 00 75 00 6D 00 28 00 31 00   a.i.n.i.u.m.(.1.
29 00 2E 00 64 00 6F 00 63 00 00 00 AB AB AB AB   )...d.o.c...««««
```

Header: 01ABABABABABABAB

DriveItemId

ParentId

eTag

Hash: quickXor, SHA1

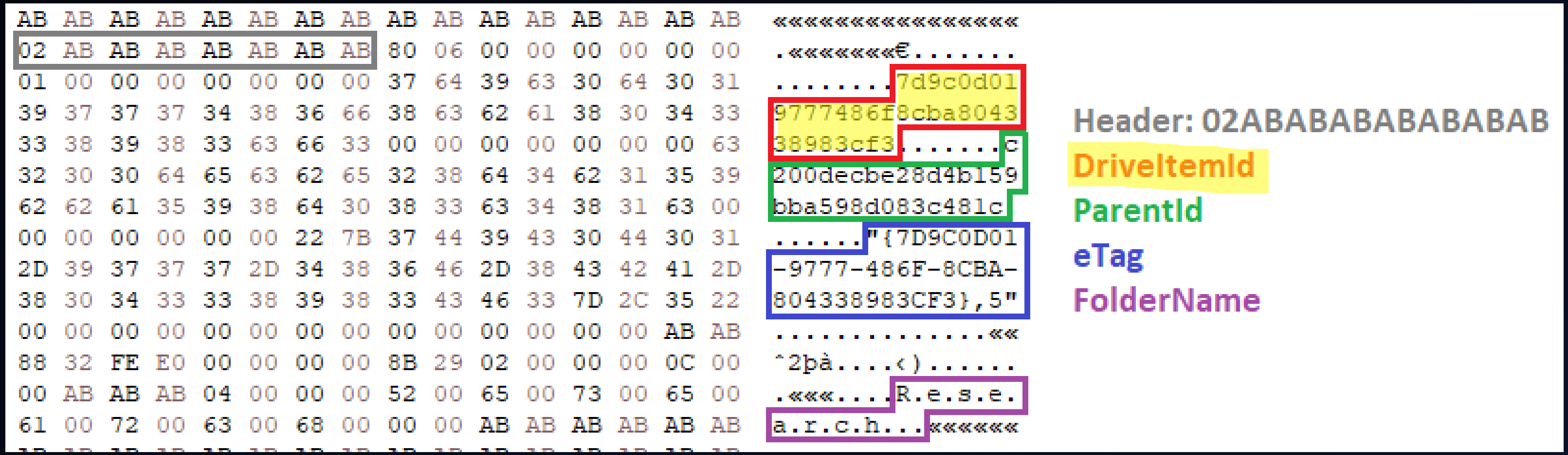
File Size

File Name

<UserCid>.dat

%APPDATA%\LOCAL\MICROSOFT\ONEDRIVE\SETTINGS\*<PERSONAL\BUSINESS1-9>*

- Folders



```
AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB   ««««««««««««««««
02 AB AB AB AB AB AB AB 80 06 00 00 00 00 00 00   .«««««««€.......
01 00 00 00 00 00 00 00 37 64 39 63 30 64 30 31   ........7d9c0d01
39 37 37 37 34 38 36 66 38 63 62 61 38 30 34 33   9777486f8cba8043
33 38 39 38 33 63 66 33 00 00 00 00 00 00 00 63   38983cf3.......c
32 30 30 64 65 63 62 65 32 38 64 34 62 31 35 39   200decbe28d4b159
62 62 61 35 39 38 64 30 38 33 63 34 38 31 63 00   bba598d083c481c.
00 00 00 00 00 00 22 7B 37 44 39 43 30 44 30 31   ......"{7D9C0D01
2D 39 37 37 37 2D 34 38 36 46 2D 38 43 42 41 2D   -9777-486F-8CBA-
38 30 34 33 33 38 39 38 33 43 46 33 7D 2C 35 22   804338983CF3},5"
00 00 00 00 00 00 00 00 00 00 00 00 00 00 AB AB   ..............««
88 32 FE E0 00 00 00 00 8B 29 02 00 00 00 0C 00   ˆ2þà....‹)......
00 AB AB AB 04 00 00 00 52 00 65 00 73 00 65 00   .«««....R.e.s.e.
61 00 72 00 63 00 68 00 00 00 AB AB AB AB AB AB   a.r.c.h...««««««
```

Header: 02ABABABABABABAB

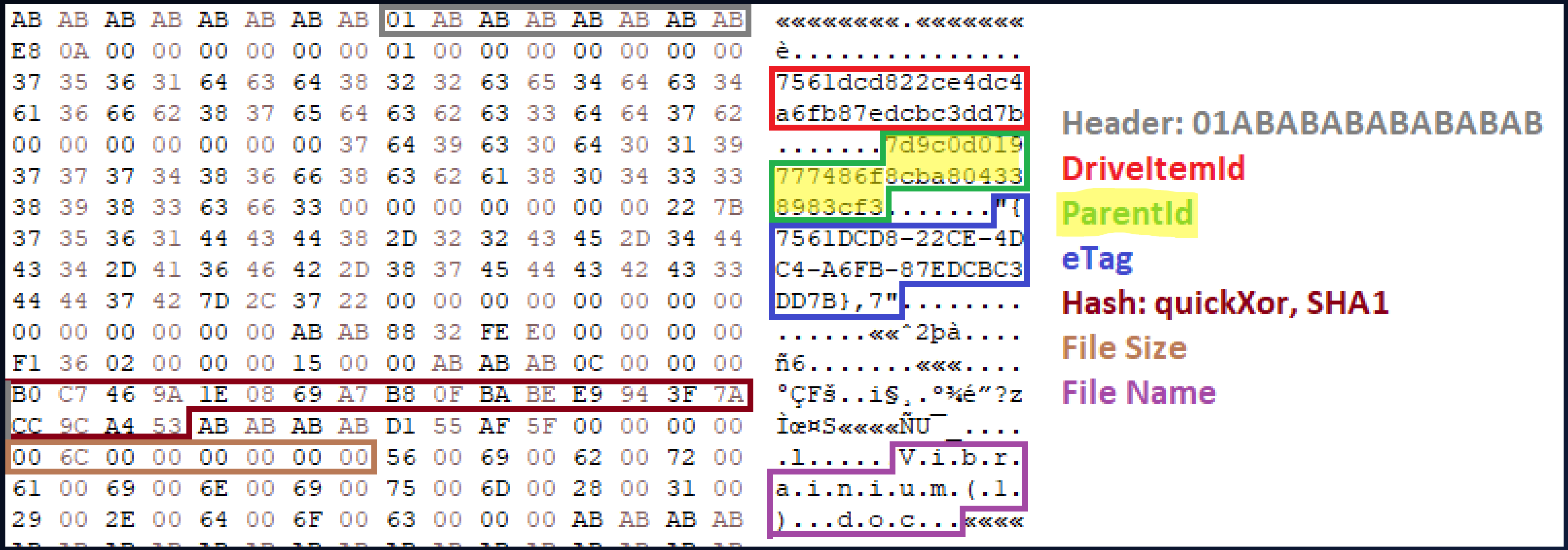
DriveItemId

ParentId

eTag

FolderName

- Files



```
AB AB AB AB AB AB AB AB 01 AB AB AB AB AB AB AB   ««««««««.«««««««
E8 0A 00 00 00 00 00 00 01 00 00 00 00 00 00 00   è...............
37 35 36 31 64 63 64 38 32 32 63 65 34 64 63 34   7561dcd822ce4dc4
61 36 66 62 38 37 65 64 63 62 63 33 64 64 37 62   a6fb87edcbc3dd7b
00 00 00 00 00 00 00 37 64 39 63 30 64 30 31 39   .......7d9c0d019
37 37 37 34 38 36 66 38 63 62 61 38 30 34 33 33   777486f8cba80433
38 39 38 33 63 66 33 00 00 00 00 00 00 00 22 7B   8983cf3......."{
37 35 36 31 44 43 44 38 2D 32 32 43 45 2D 34 44   7561DCD8-22CE-4D
43 34 2D 41 36 46 42 2D 38 37 45 44 43 42 43 33   C4-A6FB-87EDCBC3
44 44 37 42 7D 2C 37 22 00 00 00 00 00 00 00 00   DD7B},7"........
00 00 00 00 00 00 AB AB 88 32 FE E0 00 00 00 00   ......««ˆ2þà....
F1 36 02 00 00 00 15 00 00 AB AB AB 0C 00 00 00   ñ6.......«««....
B0 C7 46 9A 1E 08 69 A7 B8 0F BA BE E9 94 3F 7A   °ÇFš..i§¸.º¾é”?z
CC 9C A4 53 AB AB AB AB D1 55 AF 5F 00 00 00 00   Ìœ¤S««««ÑU¯_....
00 6C 00 00 00 00 00 00 56 00 69 00 62 00 72 00   .l......V.i.b.r.
61 00 69 00 6E 00 69 00 75 00 6D 00 28 00 31 00   a.i.n.i.u.m.(.1.
29 00 2E 00 64 00 6F 00 63 00 00 00 AB AB AB AB   )...d.o.c...««««
```

Header: 01ABABABABABABAB

DriveItemId

ParentId

eTag

Hash: quickXor, SHA1

File Size

File Name

Folder Reconstruction

ONEDRIVEEXPLORER

DriveItem

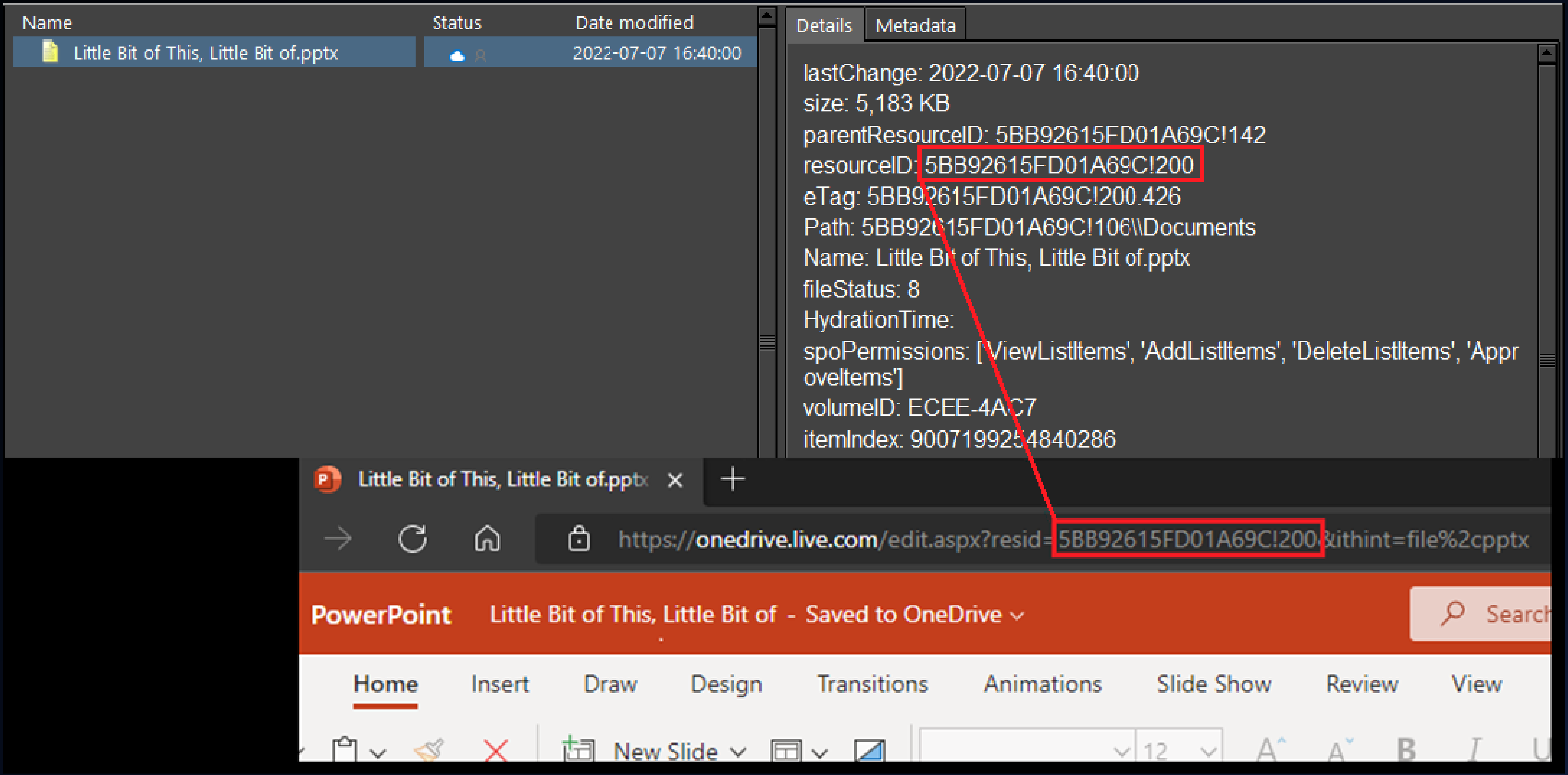
The **driveItem** resource represents a file, folder, or other item stored in a drive. All file system objects in OneDrive and SharePoint are returned as **driveItem** resources.

There are two primary ways of addressing a **driveItem** resource:

- By the driveitem unique identifier using Drive/items/{item-id}
- By file system path using /drive/root:/path/to/file

Source: DriveItem - OneDrive API - OneDrive dev center | Microsoft Docs

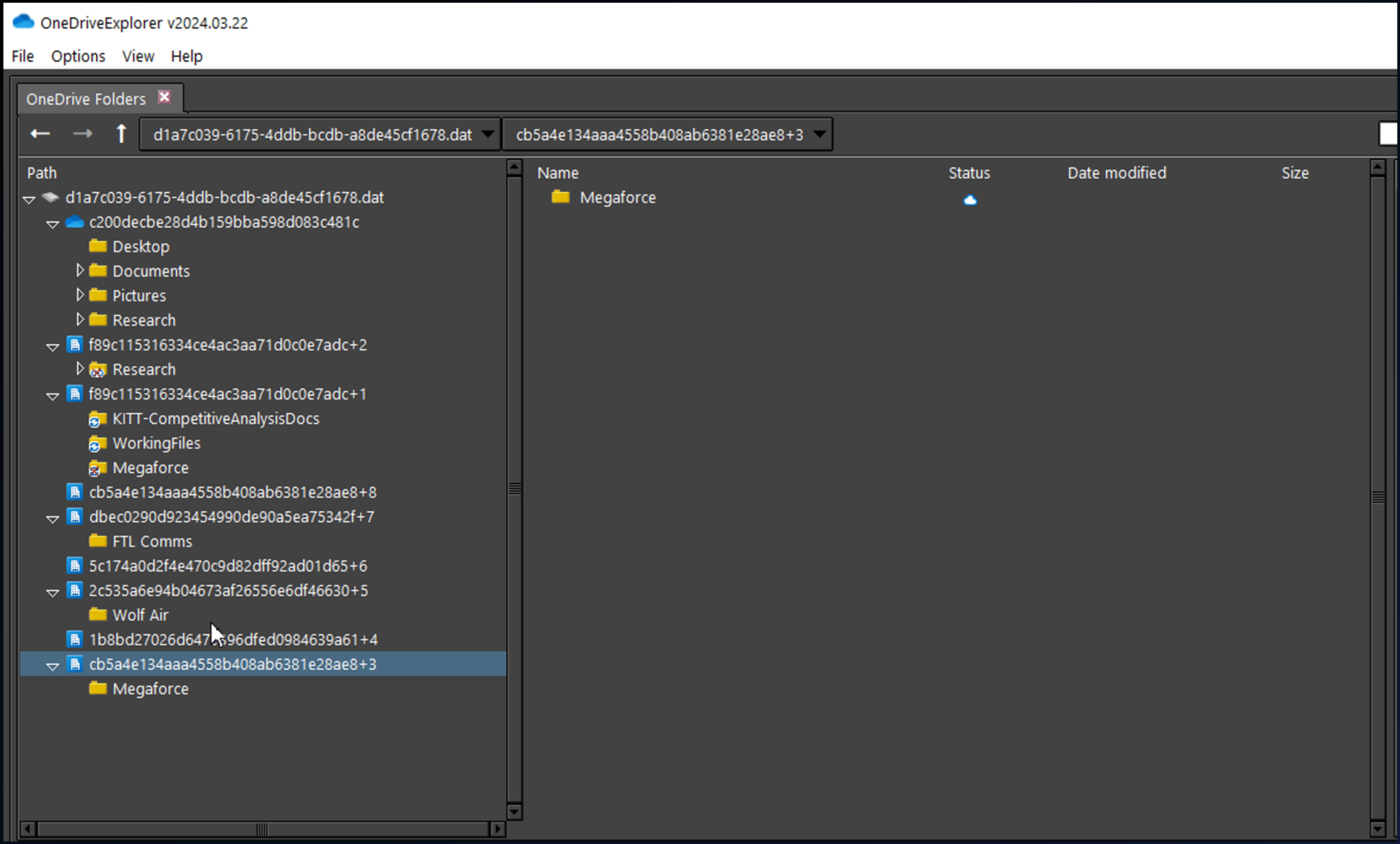
DriveItem



Name	Status	Date modified
Little Bit of This, Little Bit of.pptx	☁	2022-07-07 16:40:00

lastChange: 2022-07-07 16:40:00
size: 5,183 KB
parentResourceID: 5BB92615FD01A69C!142
resourceID: 5BB92615FD01A69C!200
eTag: 5BB92615FD01A69C!200.426
Path: 5BB92615FD01A69C!106\\Documents
Name: Little Bit of This, Little Bit of.pptx
fileStatus: 8
HydrationTime:
spoPermissions: ['ViewListItems', 'AddListItems', 'DeleteListItems', 'ApproveItems']
volumeID: ECEE-4AC7
itemIndex: 9007199254840286

https://onedrive.live.com/edit.aspx?resid=5BB92615FD01A69C!200&ithint=file%2cpptx

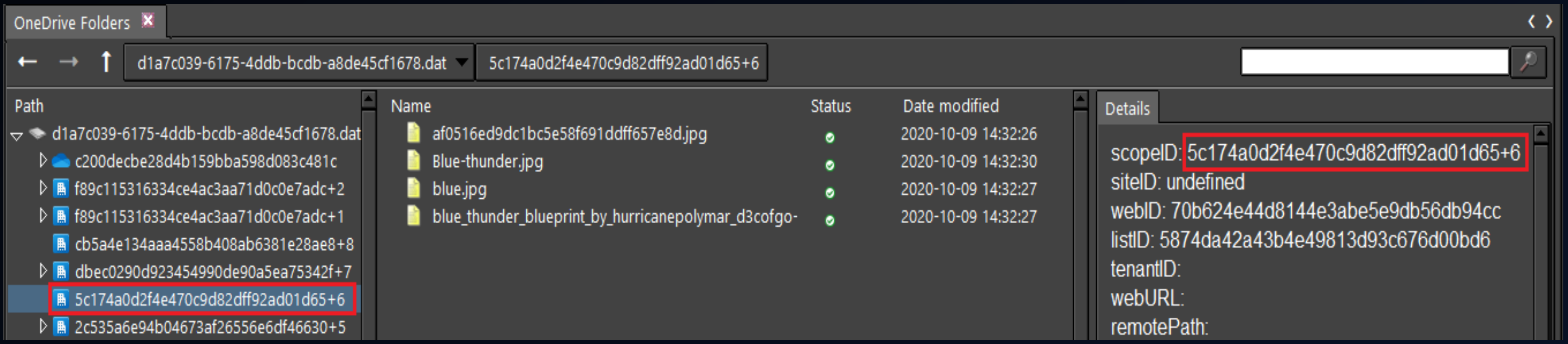

OneDriveExplorer v2024.03.22
File
Options
View
Help
OneDrive Folders
d1a7c039-6175-4ddb-bcdb-a8de45cf1678.dat
cb5a4e134aaa4558b408ab6381e28ae8+3

```
Path
d1a7c039-6175-4ddb-bcdb-a8de45cf1678.dat
  c200decbe28d4b159bba598d083c481c
    Desktop
    Documents
    Pictures
    Research
  f89c115316334ce4ac3aa71d0c0e7adc+2
    Research
  f89c115316334ce4ac3aa71d0c0e7adc+1
    KITT-CompetitiveAnalysisDocs
    WorkingFiles
    Megaforce
  cb5a4e134aaa4558b408ab6381e28ae8+8
  dbec0290d923454990de90a5ea75342f+7
    FTL Comms
  5c174a0d2f4e470c9d82dff92ad01d65+6
  2c535a6e94b04673af26556e6df46630+5
    Wolf Air
  1b8bd27026d647[illegible]596dfed0984639a61+4
  cb5a4e134aaa4558b408ab6381e28ae8+3
    Megaforce
```

Name	Status	Date modified	Size
Megaforce	☁		

Finding MountPoints

ONEDRIVEEXPLORER



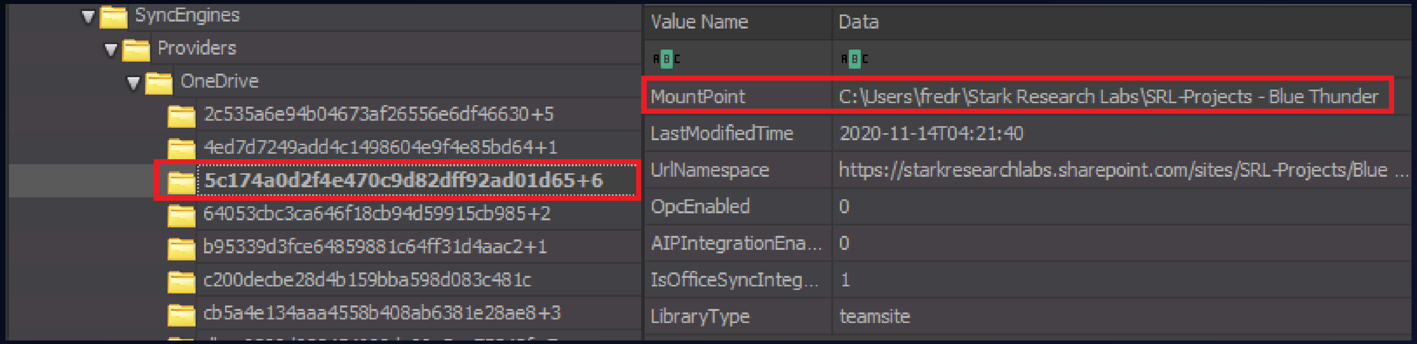
d1a7c039-6175-4ddb-bcdb-a8de45cf1678.dat ▼ | 5c174a0d2f4e470c9d82dff92ad01d65+6

```
Path
▽ d1a7c039-6175-4ddb-bcdb-a8de45cf1678.dat
    ▷ c200decbe28d4b159bba598d083c481c
    ▷ f89c115316334ce4ac3aa71d0c0e7adc+2
    ▷ f89c115316334ce4ac3aa71d0c0e7adc+1
      cb5a4e134aaa4558b408ab6381e28ae8+8
    ▷ dbec0290d923454990de90a5ea75342f+7
      5c174a0d2f4e470c9d82dff92ad01d65+6
    ▷ 2c535a6e94b04673af26556e6df46630+5
```

Name	Status	Date modified
af0516ed9dc1bc5e58f691ddff657e8d.jpg	✓	2020-10-09 14:32:26
Blue-thunder.jpg	✓	2020-10-09 14:32:30
blue.jpg	✓	2020-10-09 14:32:27
blue_thunder_blueprint_by_hurricanepolymar_d3cofgo-	✓	2020-10-09 14:32:27

scopeID: 5c174a0d2f4e470c9d82dff92ad01d65+6
siteID: undefined
webID: 70b624e44d8144e3abe5e9db56db94cc
listID: 5874da42a43b4e49813d93c676d00bd6
tenantID:
webURL:
remotePath:

SYNCENGINES

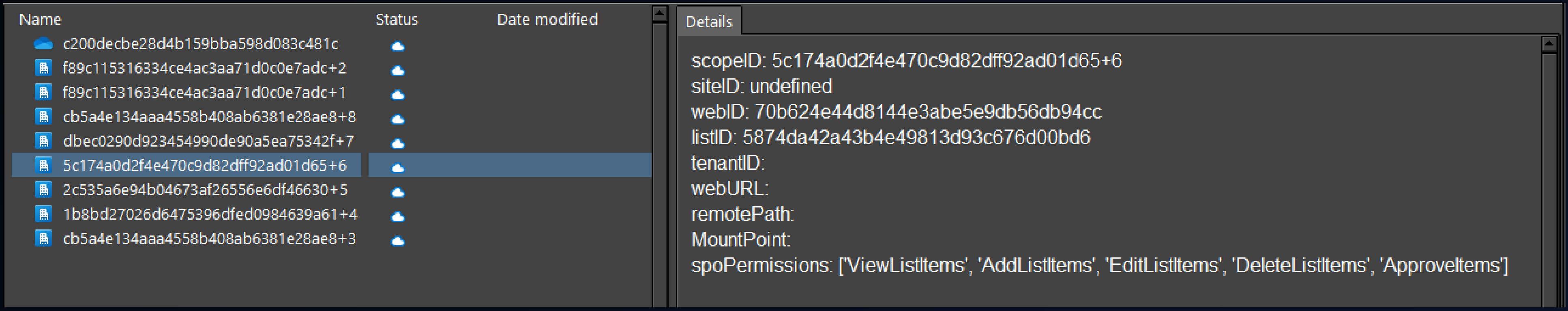


```
▼ SyncEngines
    ▼ Providers
        ▼ OneDrive
              2c535a6e94b04673af26556e6df46630+5
              4ed7d7249add4c1498604e9f4e85bd64+1
              5c174a0d2f4e470c9d82dff92ad01d65+6
              64053cbc3ca646f18cb94d59915cb985+2
              b95339d3fce64859881c64ff31d4aac2+1
              c200decbe28d4b159bba598d083c481c
              cb5a4e134aaa4558b408ab6381e28ae8+3
```

Value Name	Data
MountPoint	C:\Users\fredr\Stark Research Labs\SRL-Projects - Blue Thunder
LastModifiedTime	2020-11-14T04:21:40
UrlNamespace	https://starkresearchlabs.sharepoint.com/sites/SRL-Projects/Blue ...
OpcEnabled	0
AIPIntegrationEna...	0
IsOfficeSyncInteg...	1
LibraryType	teamsite

Finding MountPoints

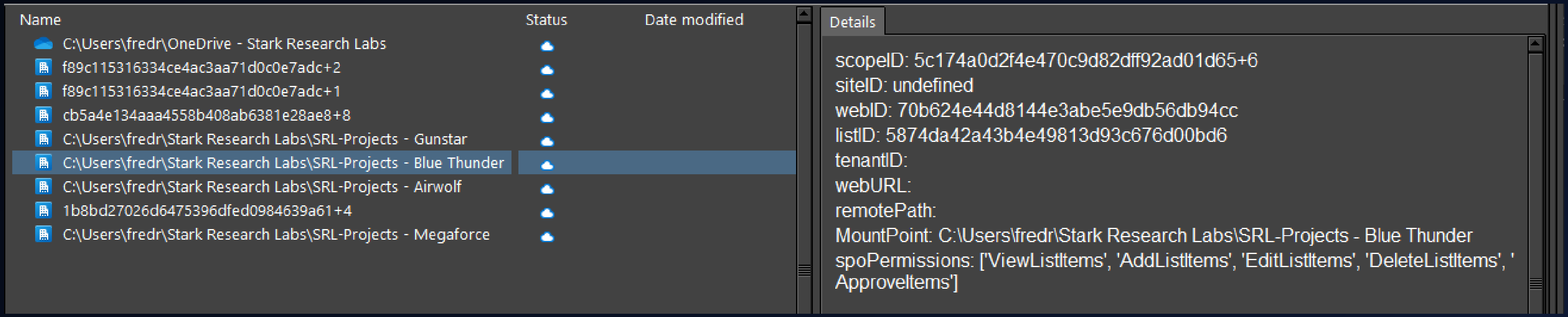
BEFORE



Name	Status	Date modified
c200decbe28d4b159bba598d083c481c	☁	
f89c115316334ce4ac3aa71d0c0e7adc+2	☁	
f89c115316334ce4ac3aa71d0c0e7adc+1	☁	
cb5a4e134aaa4558b408ab6381e28ae8+8	☁	
dbec0290d923454990de90a5ea75342f+7	☁	
5c174a0d2f4e470c9d82dff92ad01d65+6	☁	
2c535a6e94b04673af26556e6df46630+5	☁	
1b8bd27026d6475396dfed0984639a61+4	☁	
cb5a4e134aaa4558b408ab6381e28ae8+3	☁	

```
scopeID: 5c174a0d2f4e470c9d82dff92ad01d65+6
siteID: undefined
webID: 70b624e44d8144e3abe5e9db56db94cc
listID: 5874da42a43b4e49813d93c676d00bd6
tenantID:
webURL:
remotePath:
MountPoint:
spoPermissions: ['ViewListItems', 'AddListItems', 'EditListItems', 'DeleteListItems', 'ApproveItems']
```

AFTER



Name	Status	Date modified
C:\Users\fredr\OneDrive - Stark Research Labs	☁	
f89c115316334ce4ac3aa71d0c0e7adc+2	☁	
f89c115316334ce4ac3aa71d0c0e7adc+1	☁	
cb5a4e134aaa4558b408ab6381e28ae8+8	☁	
C:\Users\fredr\Stark Research Labs\SRL-Projects - Gunstar	☁	
C:\Users\fredr\Stark Research Labs\SRL-Projects - Blue Thunder	☁	
C:\Users\fredr\Stark Research Labs\SRL-Projects - Airwolf	☁	
1b8bd27026d6475396dfed0984639a61+4	☁	
C:\Users\fredr\Stark Research Labs\SRL-Projects - Megaforce	☁	

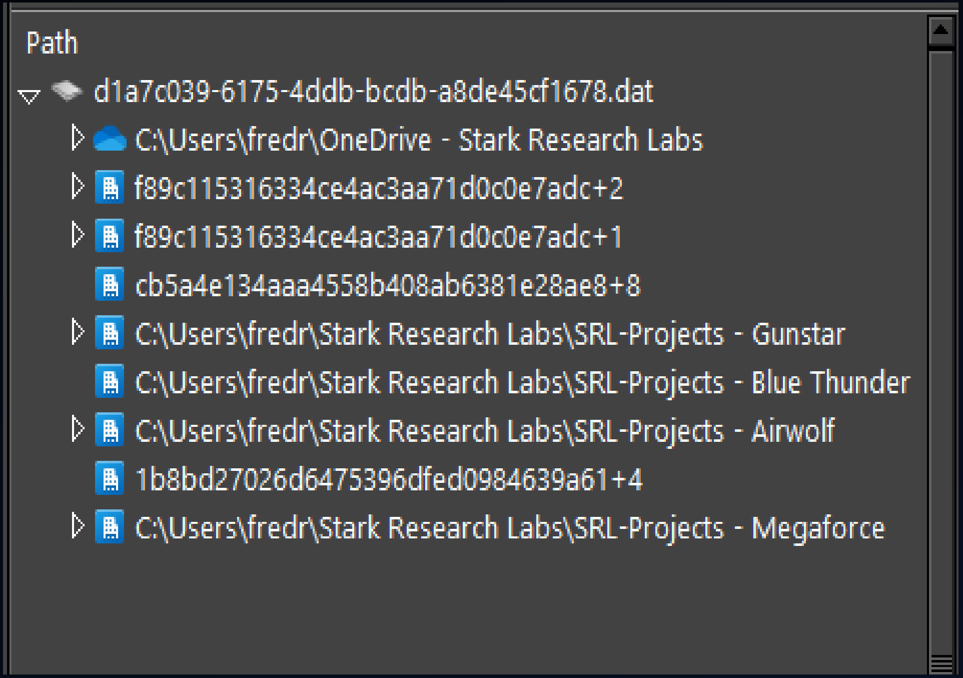
```
scopeID: 5c174a0d2f4e470c9d82dff92ad01d65+6
siteID: undefined
webID: 70b624e44d8144e3abe5e9db56db94cc
listID: 5874da42a43b4e49813d93c676d00bd6
tenantID:
webURL:
remotePath:
MountPoint: C:\Users\fredr\Stark Research Labs\SRL-Projects - Blue Thunder
spoPermissions: ['ViewListItems', 'AddListItems', 'EditListItems', 'DeleteListItems', '
ApproveItems']
```

$Recycle.Bin

- Deleted items are kept in an online recycle bin
- Kept 30 days for Personal
- Kept 93 days for Business
- Will appear in filesystem recycle bin if downloaded to filesystem

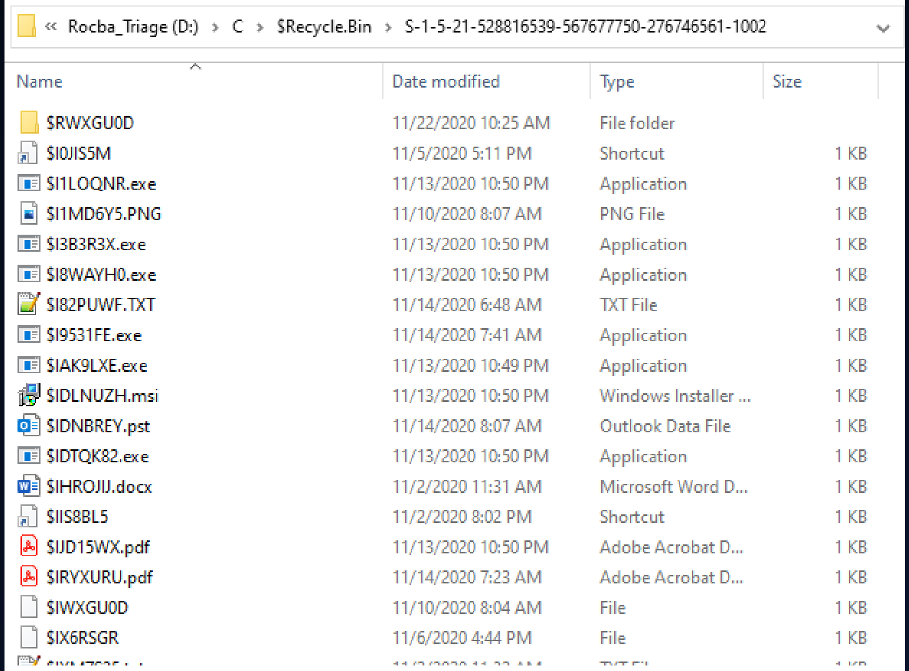
$Recycle.Bin

ONEDRIVEEXPLORER



```
Path
▽ d1a7c039-6175-4ddb-bcdb-a8de45cf1678.dat
    ▷ C:\Users\fredr\OneDrive - Stark Research Labs
    ▷ f89c115316334ce4ac3aa71d0c0e7adc+2
    ▷ f89c115316334ce4ac3aa71d0c0e7adc+1
      cb5a4e134aaa4558b408ab6381e28ae8+8
    ▷ C:\Users\fredr\Stark Research Labs\SRL-Projects - Gunstar
      C:\Users\fredr\Stark Research Labs\SRL-Projects - Blue Thunder
    ▷ C:\Users\fredr\Stark Research Labs\SRL-Projects - Airwolf
      1b8bd27026d6475396dfed0984639a61+4
    ▷ C:\Users\fredr\Stark Research Labs\SRL-Projects - Megaforce
```

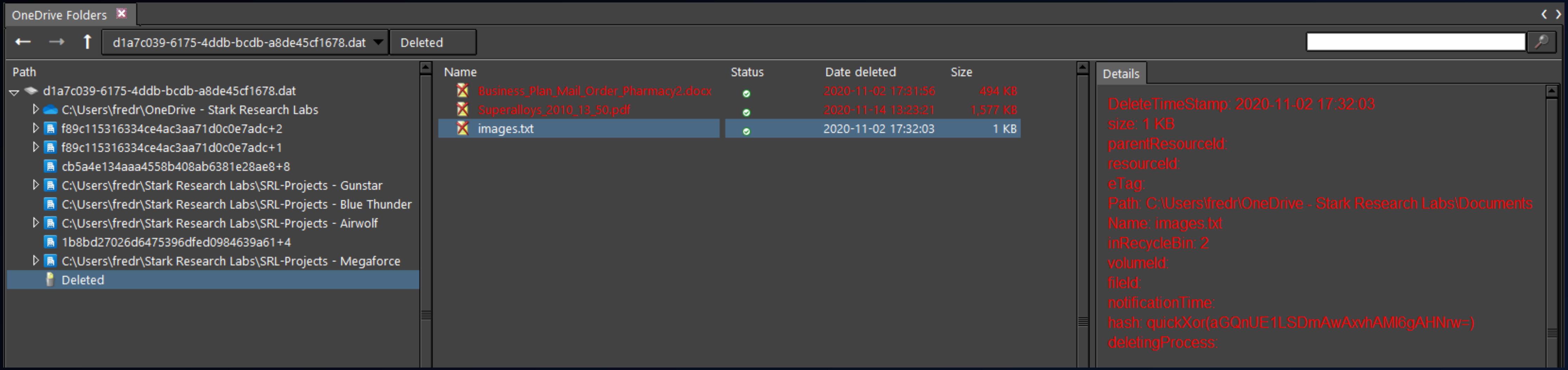
$RECYCLE.BIN FOLDER



« Rocba_Triage (D:) › C › $Recycle.Bin › S-1-5-21-528816539-567677750-276746561-1002

Name	Date modified	Type	Size
$RWXGU0D	11/22/2020 10:25 AM	File folder	
$I0JIS5M	11/5/2020 5:11 PM	Shortcut	1 KB
$I1LOQNR.exe	11/13/2020 10:50 PM	Application	1 KB
$I1MD6Y5.PNG	11/10/2020 8:07 AM	PNG File	1 KB
$I3B3R3X.exe	11/13/2020 10:50 PM	Application	1 KB
$I8WAYH0.exe	11/13/2020 10:50 PM	Application	1 KB
$I82PUWF.TXT	11/14/2020 6:48 AM	TXT File	1 KB
$I9531FE.exe	11/14/2020 7:41 AM	Application	1 KB
$IAK9LXE.exe	11/13/2020 10:49 PM	Application	1 KB
$IDLNUZH.msi	11/13/2020 10:50 PM	Windows Installer ...	1 KB
$IDNBREY.pst	11/14/2020 8:07 AM	Outlook Data File	1 KB
$IDTQK82.exe	11/13/2020 10:50 PM	Application	1 KB
$IHROJIJ.docx	11/2/2020 11:31 AM	Microsoft Word D...	1 KB
$IIS8BL5	11/2/2020 8:02 PM	Shortcut	1 KB
$IJD15WX.pdf	11/13/2020 10:50 PM	Adobe Acrobat D...	1 KB
$IRYXURU.pdf	11/14/2020 7:23 AM	Adobe Acrobat D...	1 KB
$IWXGU0D	11/10/2020 8:04 AM	File	1 KB
$IX6RSGR	11/6/2020 4:44 PM	File	1 KB

$Recycle.Bin



Path

- d1a7c039-6175-4ddb-bcdb-a8de45cf1678.dat
  - C:\Users\fredr\OneDrive - Stark Research Labs
  - f89c115316334ce4ac3aa71d0c0e7adc+2
  - f89c115316334ce4ac3aa71d0c0e7adc+1
  - cb5a4e134aaa4558b408ab6381e28ae8+8
  - C:\Users\fredr\Stark Research Labs\SRL-Projects - Gunstar
  - C:\Users\fredr\Stark Research Labs\SRL-Projects - Blue Thunder
  - C:\Users\fredr\Stark Research Labs\SRL-Projects - Airwolf
  - 1b8bd27026d6475396dfed0984639a61+4
  - C:\Users\fredr\Stark Research Labs\SRL-Projects - Megaforce
  - Deleted

Name	Status	Date deleted	Size
Business_Plan_Mail_Order_Pharmacy2.docx	✓	2020-11-02 17:31:56	494 KB
Superalloys_2010_13_50.pdf	✓	2020-11-14 13:23:21	1,577 KB
images.txt	✓	2020-11-02 17:32:03	1 KB

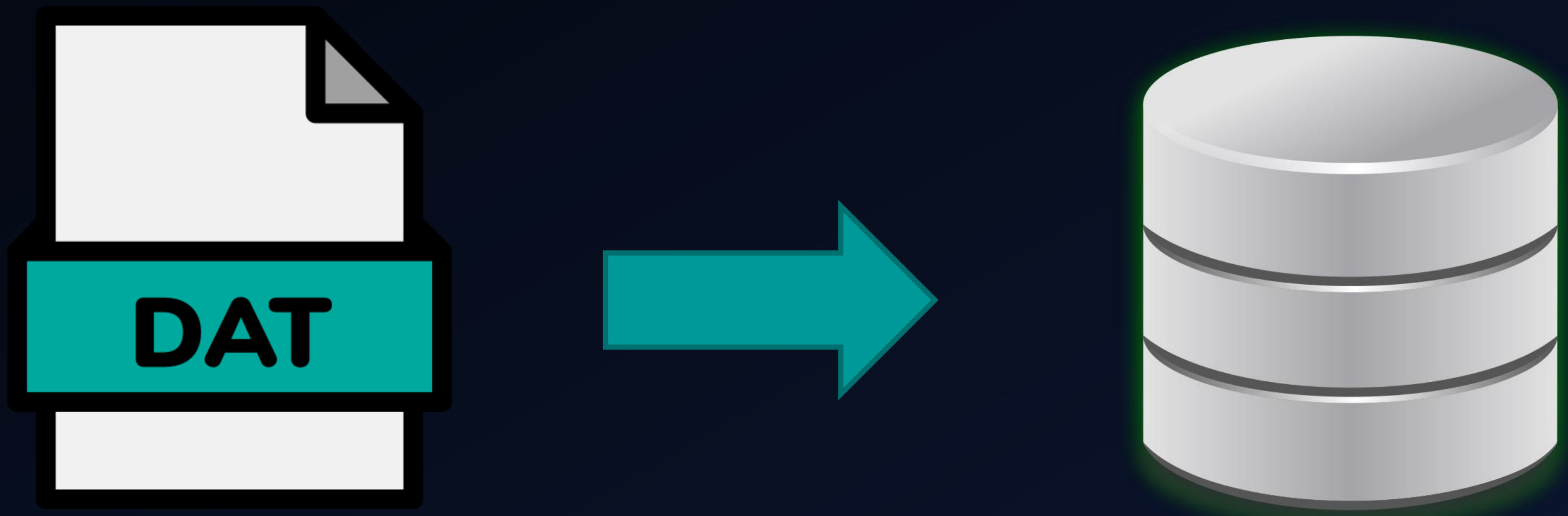
DeleteTimeStamp: 2020-11-02 17:32:03
size: 1 KB
parentResourceId:
resourceId:
eTag:
Path: C:\Users\fredr\OneDrive - Stark Research Labs\Documents
Name: images.txt
inRecycleBin: 2
volumeId:
fileId:
notificationTime:
hash: quickXor(aGQnUE1LSDmAwAxvhAMl6gAHNrw=)
deletingProcess:

SQLite Databases

ONEDRIVEEXPLORER

SQLite Databases

- Starting with v22.111.0522.0002, the SettingsDatabase.db appears
- v22.217.1016.0001 – KFM.db
- v23.002.0102.0001 – SafeDelete.db
- v23.038.0219.0001 – SyncEngineDatabase.db



SQLite Databases

%APPDATA%\LOCAL\MICROSOFT\ONEDRIVE\SETTINGS\<*PERSONAL\BUSINESS1-9*>

- SyncEngineDatabase.db
  - od_ClientFile_Records
  - od_ClietFolder_Records
  - od_GraphMetadata_Records
  - od_HydrationData
  - od_ScopeInfo_Records
- SafeDelete.db
  - filter_delete_info
  - Items_moved_to_recycle_bin

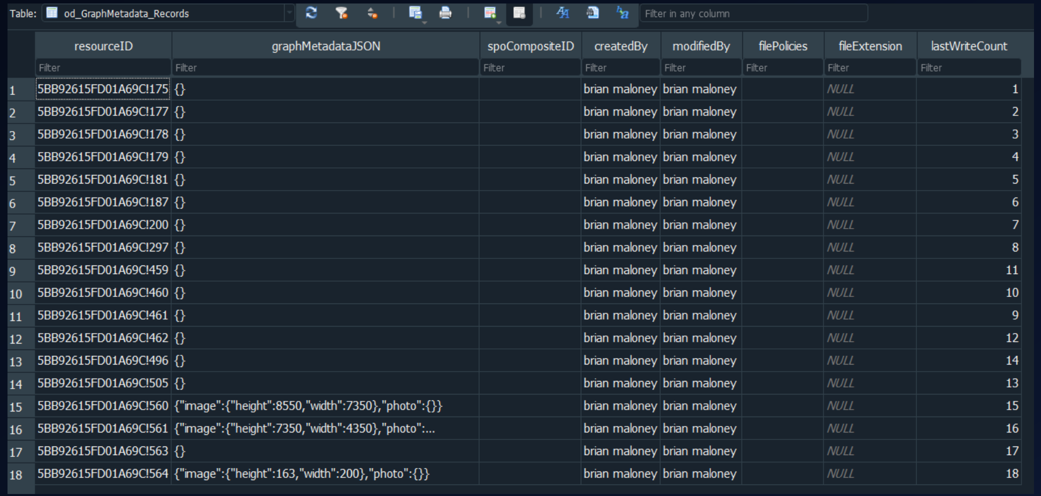
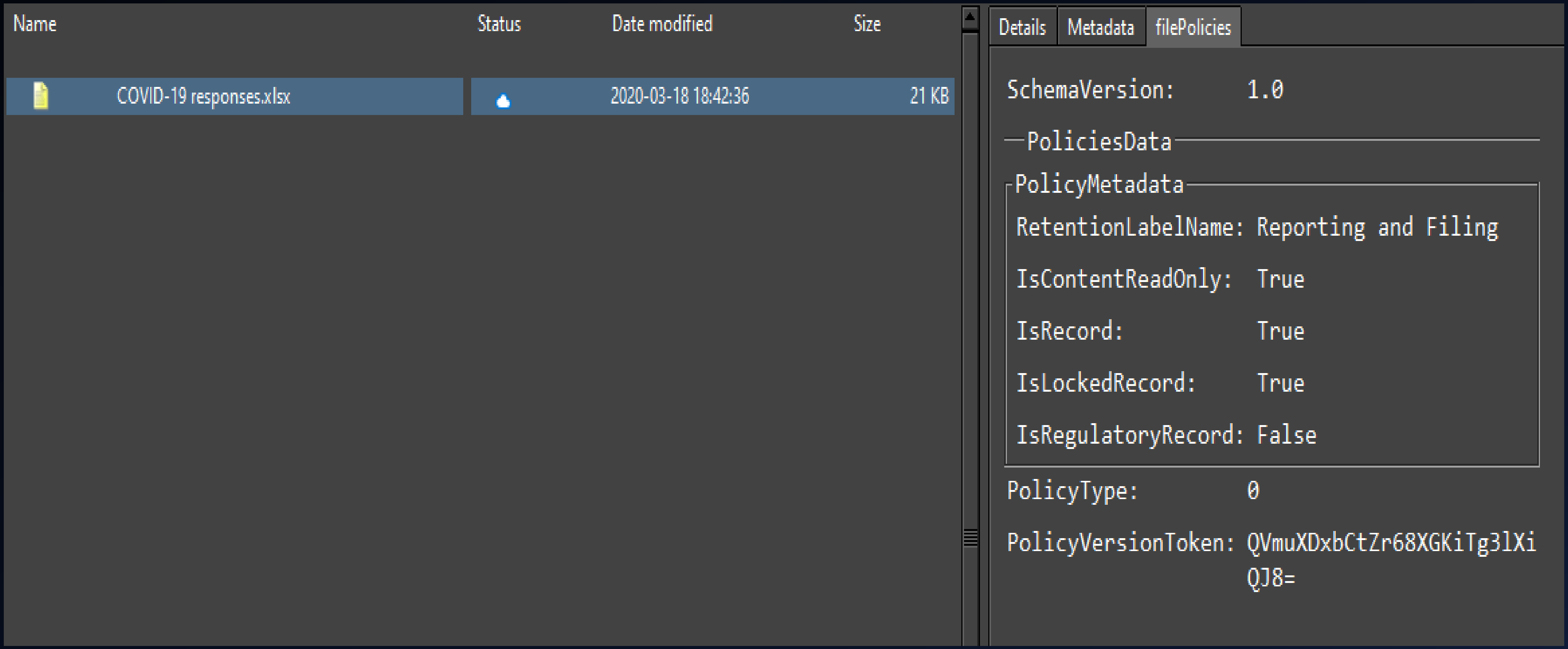


Table: od_GraphMetadata_Records

	resourceID	graphMetadataJSON	spoCompositeID	createdBy	modifiedBy	filePolicies	fileExtension	lastWriteCount
1	5BB92615FD01A69C!175	{}		brian maloney	brian maloney		NULL	1
2	5BB92615FD01A69C!177	{}		brian maloney	brian maloney		NULL	2
3	5BB92615FD01A69C!178	{}		brian maloney	brian maloney		NULL	3
4	5BB92615FD01A69C!179	{}		brian maloney	brian maloney		NULL	4
5	5BB92615FD01A69C!181	{}		brian maloney	brian maloney		NULL	5
6	5BB92615FD01A69C!187	{}		brian maloney	brian maloney		NULL	6
7	5BB92615FD01A69C!200	{}		brian maloney	brian maloney		NULL	7
8	5BB92615FD01A69C!297	{}		brian maloney	brian maloney		NULL	8
9	5BB92615FD01A69C!459	{}		brian maloney	brian maloney		NULL	11
10	5BB92615FD01A69C!460	{}		brian maloney	brian maloney		NULL	10
11	5BB92615FD01A69C!461	{}		brian maloney	brian maloney		NULL	9
12	5BB92615FD01A69C!462	{}		brian maloney	brian maloney		NULL	12
13	5BB92615FD01A69C!496	{}		brian maloney	brian maloney		NULL	14
14	5BB92615FD01A69C!505	{}		brian maloney	brian maloney		NULL	13
15	5BB92615FD01A69C!560	{"image":{"height":8550,"width":7350},"photo":{}}		brian maloney	brian maloney		NULL	15
16	5BB92615FD01A69C!561	{"image":{"height":7350,"width":4350},"photo":...		brian maloney	brian maloney		NULL	16
17	5BB92615FD01A69C!563	{}		brian maloney	brian maloney		NULL	17
18	5BB92615FD01A69C!564	{"image":{"height":163,"width":200},"photo":{}}		brian maloney	brian maloney		NULL	18

SQLite Databases

- SyncEngineDatabase.db
  - od_GraphMetadata_Records

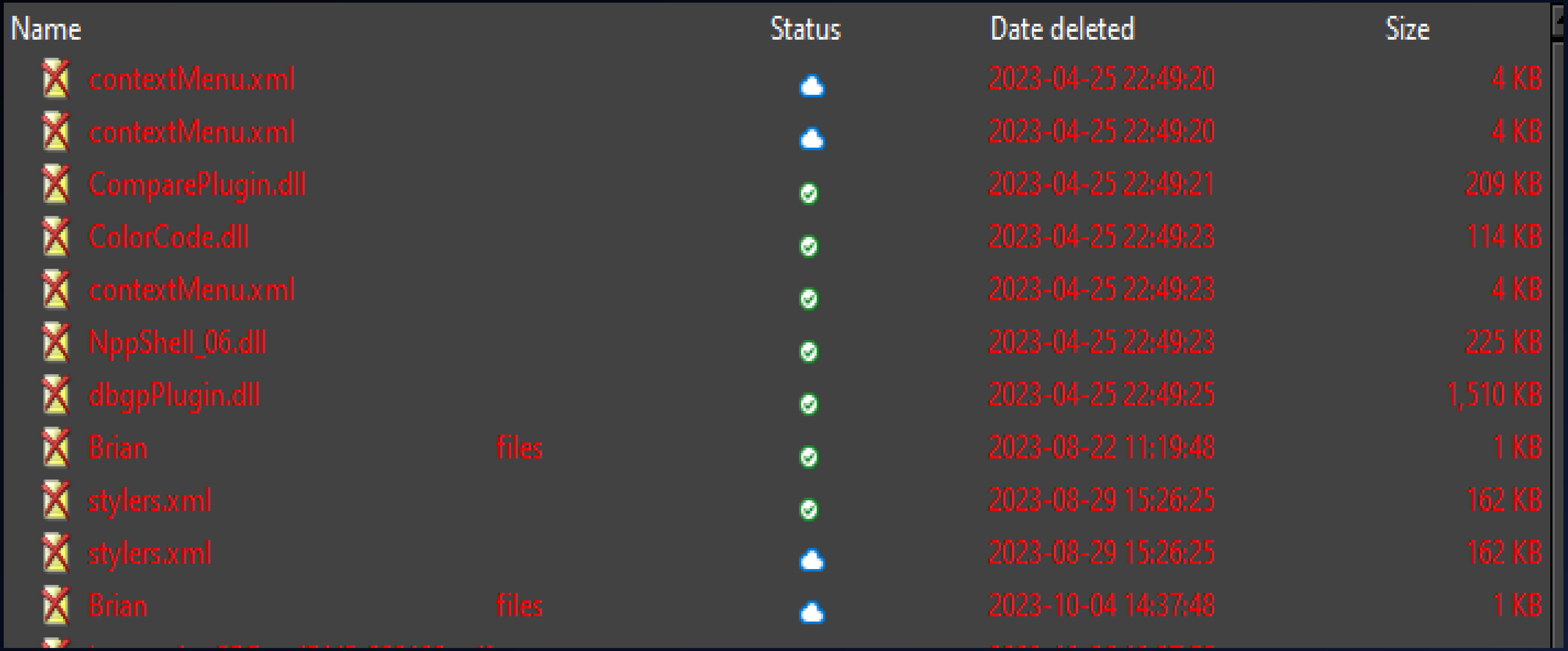


Name	Status	Date modified	Size
COVID-19 responses.xlsx	●	2020-03-18 18:42:36	21 KB

```
SchemaVersion:      1.0

─PoliciesData──────────────────────────────
┌PolicyMetadata─────────────────────────────┐
 RetentionLabelName: Reporting and Filing

 IsContentReadOnly:  True

 IsRecord:           True

 IsLockedRecord:     True

 IsRegulatoryRecord: False
└───────────────────────────────────────────┘
PolicyType:         0

PolicyVersionToken: QVmuXDxbCtZr68XGKiTg3lXi
                    QJ8=
```

SQLite Databases

- SafeDelete.db
    - filter_delete_info



Name		Status	Date deleted	Size
contextMenu.xml		☁	2023-04-25 22:49:20	4 KB
contextMenu.xml		☁	2023-04-25 22:49:20	4 KB
ComparePlugin.dll		✓	2023-04-25 22:49:21	209 KB
ColorCode.dll		✓	2023-04-25 22:49:23	114 KB
contextMenu.xml		✓	2023-04-25 22:49:23	4 KB
NppShell_06.dll		✓	2023-04-25 22:49:23	225 KB
dbgpPlugin.dll		✓	2023-04-25 22:49:25	1,510 KB
Brian	files	✓	2023-08-22 11:19:48	1 KB
stylers.xml		✓	2023-08-29 15:26:25	162 KB
stylers.xml		☁	2023-08-29 15:26:25	162 KB
Brian	files	☁	2023-10-04 14:37:48	1 KB

What About The Logs?

LOGS FOLDER

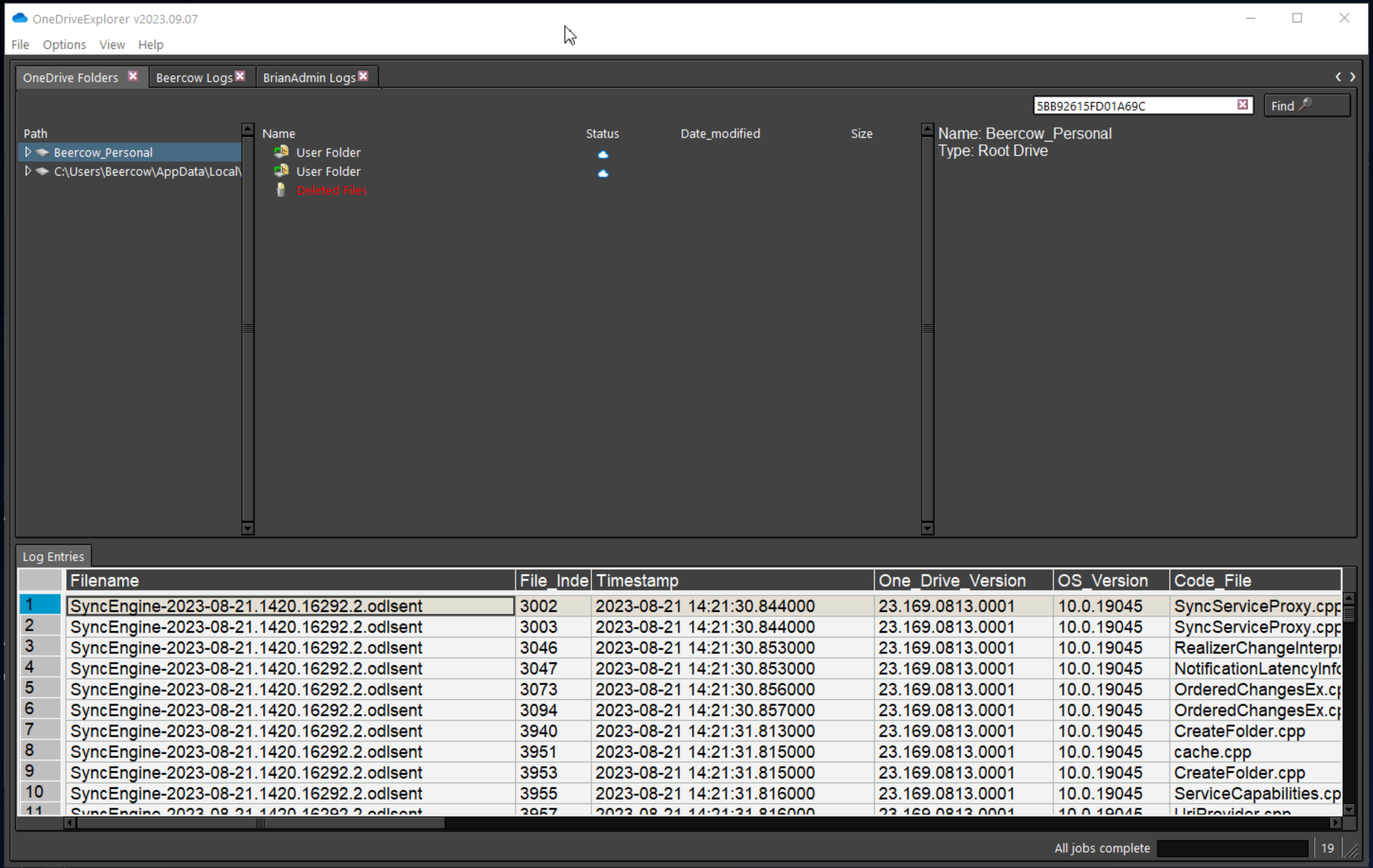
Log Files

%APPDATA%\LOCAL\MICROSOFT\ONEDRIVE\LOGS

- .odl, .odlgz, .odlsent and .aodl
  - Account linking/unlinking, uploads, downloads, file info, etc..
  - Files are obfuscated
- Yogesh Khatri's odl.py
  - Parses and un-obfuscate files
  - ObfuscationStringMap.txt (v22.027.0206.0002 -)
  - general.keystore (v22.033.0213.0002 +)
- OneDriveExplorer's log parsing based off of Yogesh's work
  - ODL version 3 (v23.180.0828.0001 +)

Log Files

%APPDATA%\LOCAL\MICROSOFT\ONEDRIVE\LOGS



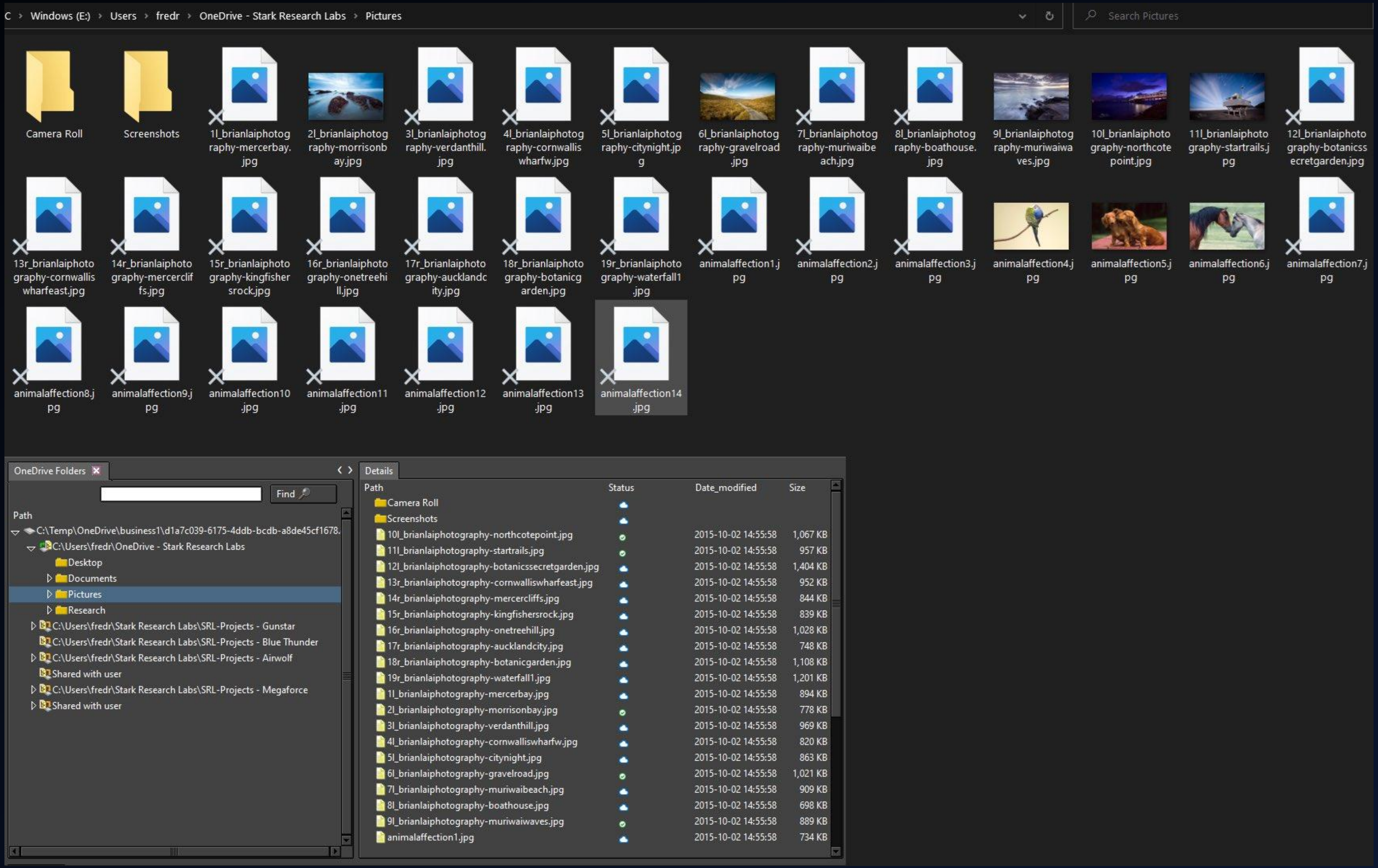
5BB92615FD01A69C

Name	Status	Date_modified	Size
User Folder	☁		
User Folder	☁		
Deleted Files			

Name: Beercow_Personal
Type: Root Drive

	Filename	File_Inde	Timestamp	One_Drive_Version	OS_Version	Code_File
1	SyncEngine-2023-08-21.1420.16292.2.odlsent	3002	2023-08-21 14:21:30.844000	23.169.0813.0001	10.0.19045	SyncServiceProxy.cpp
2	SyncEngine-2023-08-21.1420.16292.2.odlsent	3003	2023-08-21 14:21:30.844000	23.169.0813.0001	10.0.19045	SyncServiceProxy.cpp
3	SyncEngine-2023-08-21.1420.16292.2.odlsent	3046	2023-08-21 14:21:30.853000	23.169.0813.0001	10.0.19045	RealizerChangeInterpı
4	SyncEngine-2023-08-21.1420.16292.2.odlsent	3047	2023-08-21 14:21:30.853000	23.169.0813.0001	10.0.19045	NotificationLatencyInfo
5	SyncEngine-2023-08-21.1420.16292.2.odlsent	3073	2023-08-21 14:21:30.856000	23.169.0813.0001	10.0.19045	OrderedChangesEx.cp
6	SyncEngine-2023-08-21.1420.16292.2.odlsent	3094	2023-08-21 14:21:30.857000	23.169.0813.0001	10.0.19045	OrderedChangesEx.cp
7	SyncEngine-2023-08-21.1420.16292.2.odlsent	3940	2023-08-21 14:21:31.813000	23.169.0813.0001	10.0.19045	CreateFolder.cpp
8	SyncEngine-2023-08-21.1420.16292.2.odlsent	3951	2023-08-21 14:21:31.815000	23.169.0813.0001	10.0.19045	cache.cpp
9	SyncEngine-2023-08-21.1420.16292.2.odlsent	3953	2023-08-21 14:21:31.815000	23.169.0813.0001	10.0.19045	CreateFolder.cpp
10	SyncEngine-2023-08-21.1420.16292.2.odlsent	3955	2023-08-21 14:21:31.816000	23.169.0813.0001	10.0.19045	ServiceCapabilities.cp
11	SyncEngine-2023-08-21.1420.16292.2.odlsent	3957	2023-08-21 14:21:31.816000	23.169.0813.0001	10.0.19045	UriProvider.cpp

File/Folder Status

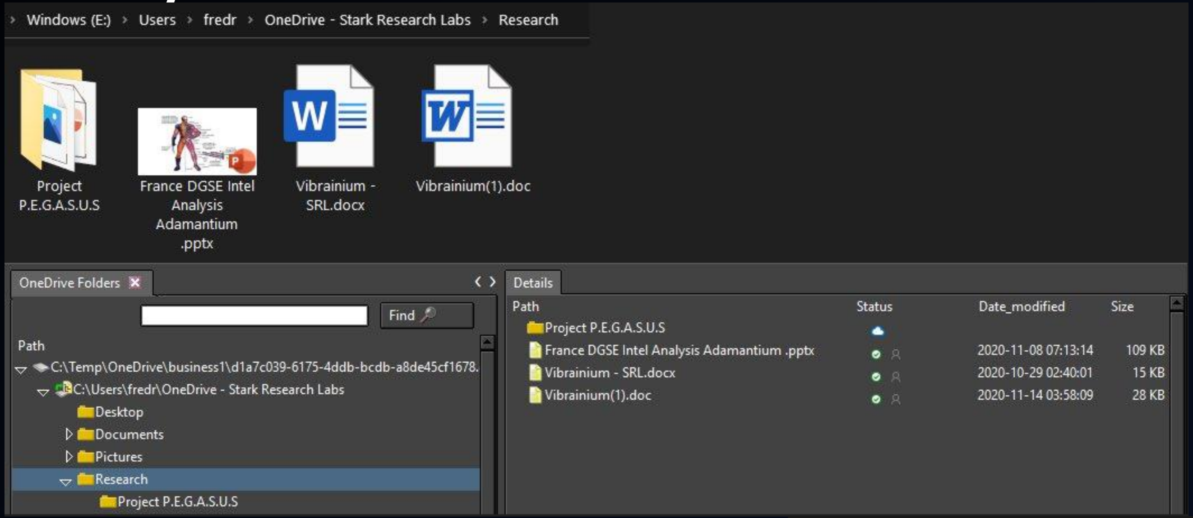

C › Windows (E:) › Users › fredr › OneDrive - Stark Research Labs › Pictures
Search Pictures
Camera Roll
Screenshots
1l_brianlaiphotography-mercerbay.jpg
2l_brianlaiphotography-morrisonbay.jpg
3l_brianlaiphotography-verdanthill.jpg
4l_brianlaiphotography-cornwalliswharfw.jpg
5l_brianlaiphotography-citynight.jpg
6l_brianlaiphotography-gravelroad.jpg
7l_brianlaiphotography-muriwaibeach.jpg
8l_brianlaiphotography-boathouse.jpg
9l_brianlaiphotography-muriwaiwaves.jpg
10l_brianlaiphotography-northcotepoint.jpg
11l_brianlaiphotography-startrails.jpg
12l_brianlaiphotography-botanicssecretgarden.jpg
13r_brianlaiphotography-cornwalliswharfeast.jpg
14r_brianlaiphotography-mercercliffs.jpg
15r_brianlaiphotography-kingfishersrock.jpg
16r_brianlaiphotography-onetreehill.jpg
17r_brianlaiphotography-aucklandcity.jpg
18r_brianlaiphotography-botanicgarden.jpg
19r_brianlaiphotography-waterfall1.jpg
animalaffection1.jpg
animalaffection2.jpg
animalaffection3.jpg
animalaffection4.jpg
animalaffection5.jpg
animalaffection6.jpg
animalaffection7.jpg
animalaffection8.jpg
animalaffection9.jpg
animalaffection10.jpg
animalaffection11.jpg
animalaffection12.jpg
animalaffection13.jpg
animalaffection14.jpg
OneDrive Folders
Find
Details

Path

```
▽ C:\Temp\OneDrive\business1\d1a7c039-6175-4ddb-bcdb-a8de45cf1678.
  ▽ C:\Users\fredr\OneDrive - Stark Research Labs
        Desktop
      ▷ Documents
      ▷ Pictures
      ▷ Research
  ▷ C:\Users\fredr\Stark Research Labs\SRL-Projects - Gunstar
    C:\Users\fredr\Stark Research Labs\SRL-Projects - Blue Thunder
  ▷ C:\Users\fredr\Stark Research Labs\SRL-Projects - Airwolf
    Shared with user
  ▷ C:\Users\fredr\Stark Research Labs\SRL-Projects - Megaforce
  ▷ Shared with user
```

Path	Status	Date_modified	Size
Camera Roll	☁		
Screenshots	☁		
10l_brianlaiphotography-northcotepoint.jpg	✓	2015-10-02 14:55:58	1,067 KB
11l_brianlaiphotography-startrails.jpg	✓	2015-10-02 14:55:58	957 KB
12l_brianlaiphotography-botanicssecretgarden.jpg	☁	2015-10-02 14:55:58	1,404 KB
13r_brianlaiphotography-cornwalliswharfeast.jpg	☁	2015-10-02 14:55:58	952 KB
14r_brianlaiphotography-mercercliffs.jpg	☁	2015-10-02 14:55:58	844 KB
15r_brianlaiphotography-kingfishersrock.jpg	☁	2015-10-02 14:55:58	839 KB
16r_brianlaiphotography-onetreehill.jpg	☁	2015-10-02 14:55:58	1,028 KB
17r_brianlaiphotography-aucklandcity.jpg	☁	2015-10-02 14:55:58	748 KB
18r_brianlaiphotography-botanicgarden.jpg	☁	2015-10-02 14:55:58	1,108 KB
19r_brianlaiphotography-waterfall1.jpg	☁	2015-10-02 14:55:58	1,201 KB
1l_brianlaiphotography-mercerbay.jpg	☁	2015-10-02 14:55:58	894 KB
2l_brianlaiphotography-morrisonbay.jpg	✓	2015-10-02 14:55:58	778 KB
3l_brianlaiphotography-verdanthill.jpg	☁	2015-10-02 14:55:58	969 KB
4l_brianlaiphotography-cornwalliswharfw.jpg	☁	2015-10-02 14:55:58	820 KB
5l_brianlaiphotography-citynight.jpg	☁	2015-10-02 14:55:58	863 KB
6l_brianlaiphotography-gravelroad.jpg	✓	2015-10-02 14:55:58	1,021 KB
7l_brianlaiphotography-muriwaibeach.jpg	☁	2015-10-02 14:55:58	909 KB
8l_brianlaiphotography-boathouse.jpg	☁	2015-10-02 14:55:58	698 KB
9l_brianlaiphotography-muriwaiwaves.jpg	✓	2015-10-02 14:55:58	889 KB
animalaffection1.jpg	☁	2015-10-02 14:55:58	734 KB

File/Folder Status



› Windows (E:) › Users › fredr › OneDrive - Stark Research Labs › Research

Project P.E.G.A.S.U.S

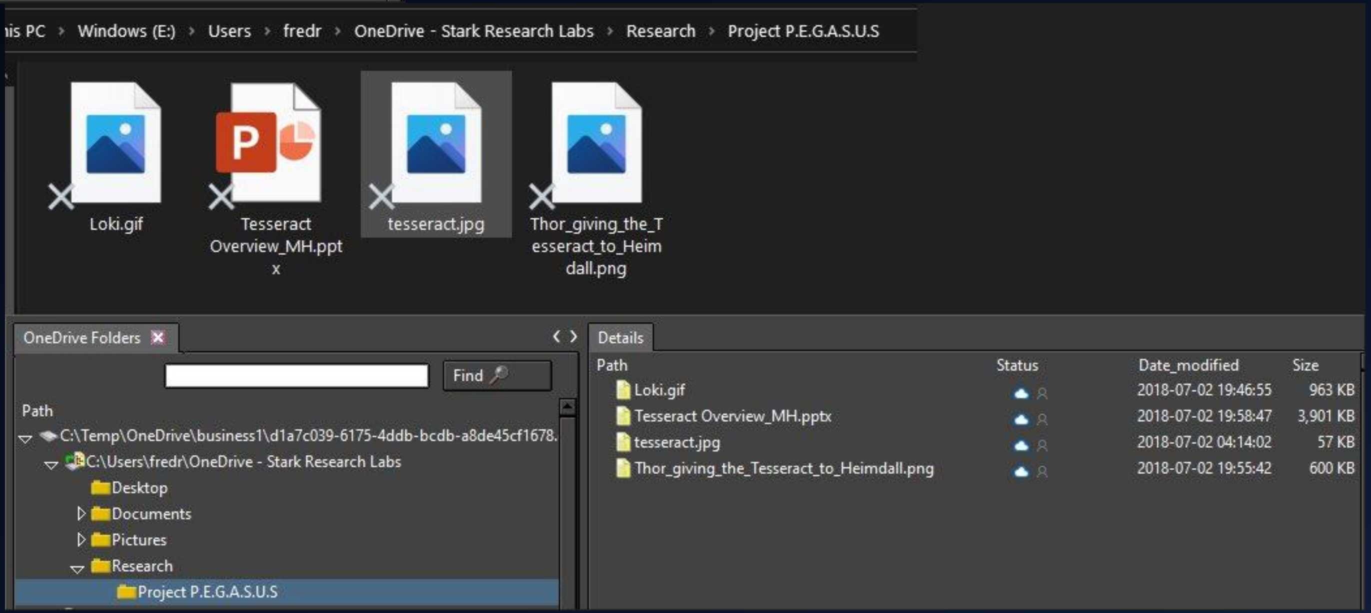
France DGSE Intel Analysis Adamantium .pptx

Vibrainium - SRL.docx

Vibrainium(1).doc

Path
- C:\Temp\OneDrive\business1\d1a7c039-6175-4ddb-bcdb-a8de45cf1678.
  - C:\Users\fredr\OneDrive - Stark Research Labs
    - Desktop
    - Documents
    - Pictures
    - Research
      - Project P.E.G.A.S.U.S

Path	Status	Date_modified	Size
Project P.E.G.A.S.U.S	☁		
France DGSE Intel Analysis Adamantium .pptx	✓ 👤	2020-11-08 07:13:14	109 KB
Vibrainium - SRL.docx	✓ 👤	2020-10-29 02:40:01	15 KB
Vibrainium(1).doc	✓ 👤	2020-11-14 03:58:09	28 KB



is PC › Windows (E:) › Users › fredr › OneDrive - Stark Research Labs › Research › Project P.E.G.A.S.U.S

Loki.gif

Tesseract Overview_MH.pptx

tesseract.jpg

Thor_giving_the_Tesseract_to_Heimdall.png

Path
- C:\Temp\OneDrive\business1\d1a7c039-6175-4ddb-bcdb-a8de45cf1678.
  - C:\Users\fredr\OneDrive - Stark Research Labs
    - Desktop
    - Documents
    - Pictures
    - Research
      - Project P.E.G.A.S.U.S

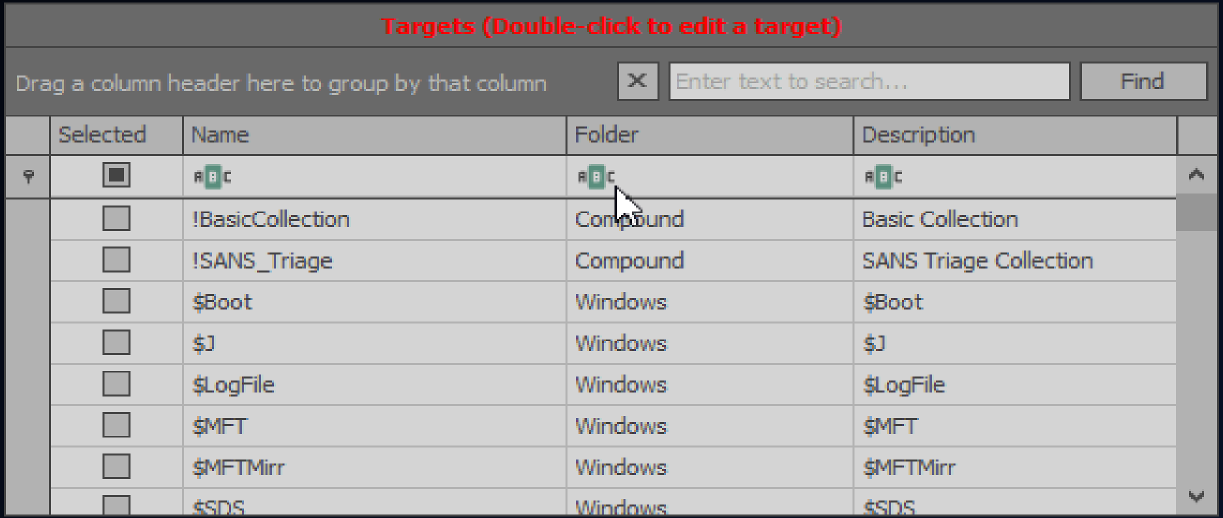
Path	Status	Date_modified	Size
Loki.gif	☁ 👤	2018-07-02 19:46:55	963 KB
Tesseract Overview_MH.pptx	☁ 👤	2018-07-02 19:58:47	3,901 KB
tesseract.jpg	☁ 👤	2018-07-02 04:14:02	57 KB
Thor_giving_the_Tesseract_to_Heimdall.png	☁ 👤	2018-07-02 19:55:42	600 KB

Automating Collection

KAPE

KAPE

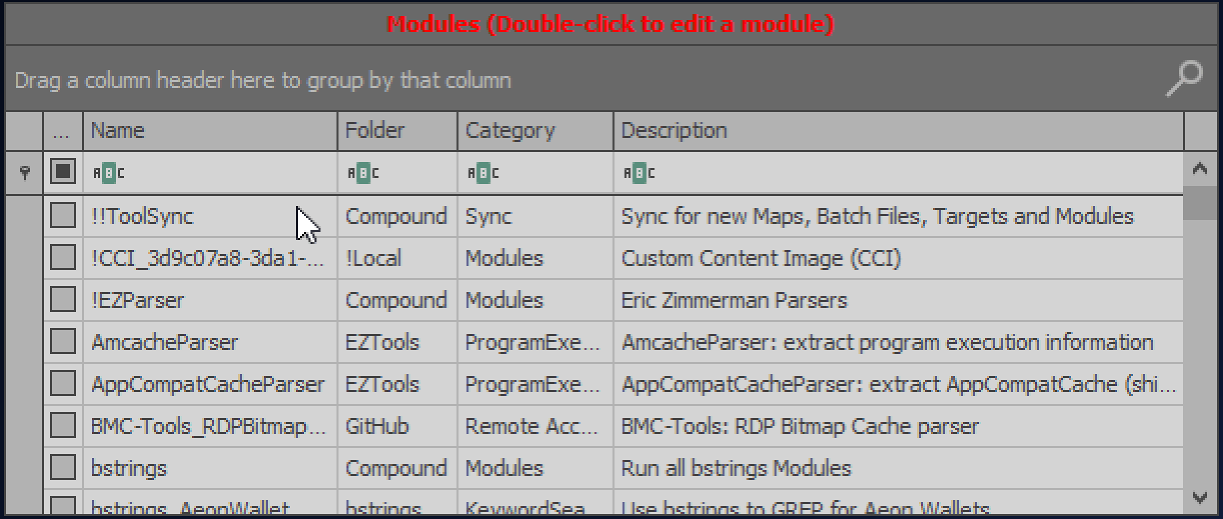
- Targets
  - CloudStorage_OneDriveExplorer
    - OneDrive_Metadata
    - RecycleBin
    - RegistryHives
- Modules
  - OneDriveExplorer
    - CSV
    - JSON
    - HTML



Targets (Double-click to edit a target)

Drag a column header here to group by that column

Selected	Name	Folder	Description
□	!BasicCollection	Compound	Basic Collection
□	!SANS_Triage	Compound	SANS Triage Collection
□	$Boot	Windows	$Boot
□	$J	Windows	$J
□	$LogFile	Windows	$LogFile
□	$MFT	Windows	$MFT
□	$MFTMirr	Windows	$MFTMirr
□	$SDS	Windows	$SDS

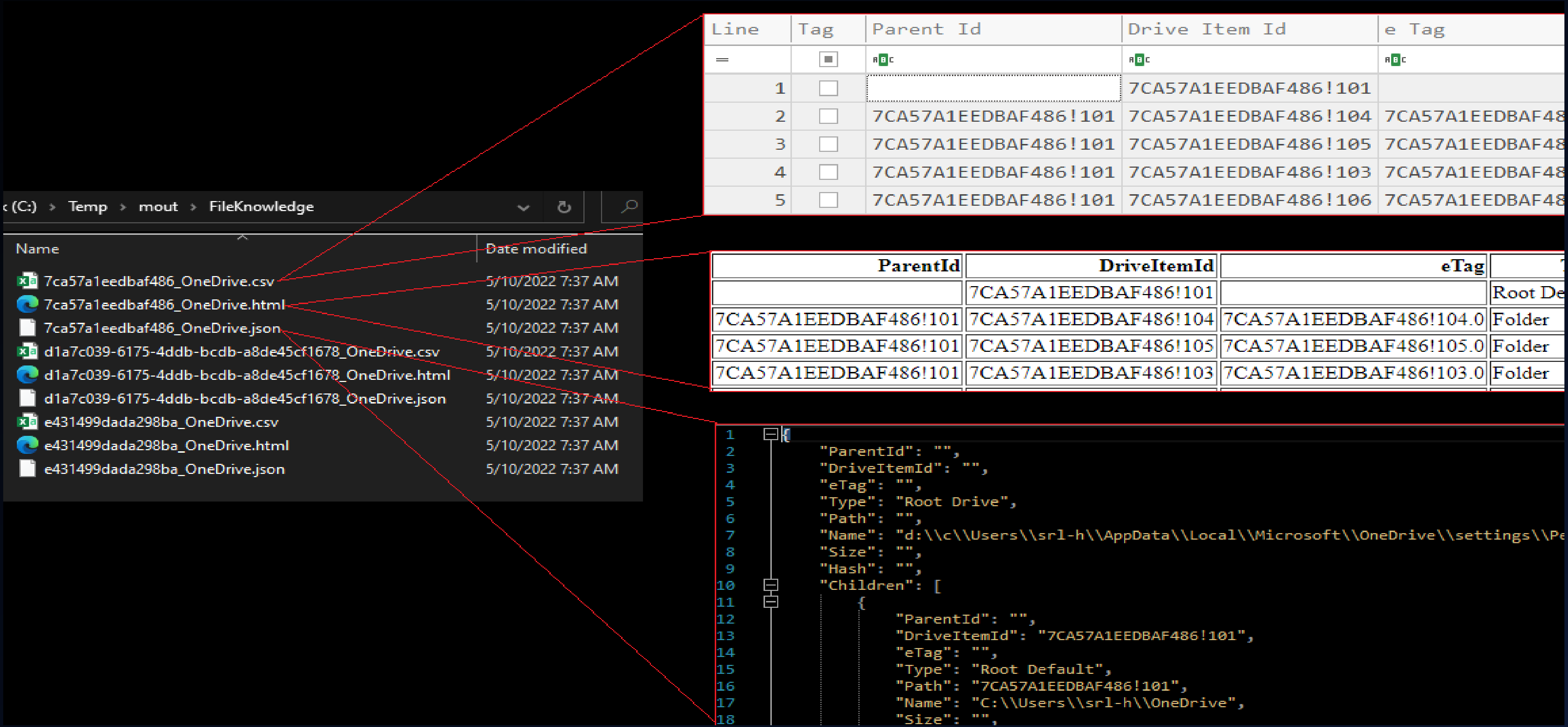


Modules (Double-click to edit a module)

Drag a column header here to group by that column

...	Name	Folder	Category	Description
□	!!ToolSync	Compound	Sync	Sync for new Maps, Batch Files, Targets and Modules
□	!CCI_3d9c07a8-3da1-...	!Local	Modules	Custom Content Image (CCI)
□	!EZParser	Compound	Modules	Eric Zimmerman Parsers
□	AmcacheParser	EZTools	ProgramExe...	AmcacheParser: extract program execution information
□	AppCompatCacheParser	EZTools	ProgramExe...	AppCompatCacheParser: extract AppCompatCache (shi...
□	BMC-Tools_RDPBitmap...	GitHub	Remote Acc...	BMC-Tools: RDP Bitmap Cache parser
□	bstrings	Compound	Modules	Run all bstrings Modules
□	bstrings_AeonWallet	bstrings	KeywordSea	Use bstrings to GREP for Aeon Wallets

KAPE Output



‹ (C:) › Temp › mout › FileKnowledge

Name	Date modified
7ca57a1eedbaf486_OneDrive.csv	5/10/2022 7:37 AM
7ca57a1eedbaf486_OneDrive.html	5/10/2022 7:37 AM
7ca57a1eedbaf486_OneDrive.json	5/10/2022 7:37 AM
d1a7c039-6175-4ddb-bcdb-a8de45cf1678_OneDrive.csv	5/10/2022 7:37 AM
d1a7c039-6175-4ddb-bcdb-a8de45cf1678_OneDrive.html	5/10/2022 7:37 AM
d1a7c039-6175-4ddb-bcdb-a8de45cf1678_OneDrive.json	5/10/2022 7:37 AM
e431499dada298ba_OneDrive.csv	5/10/2022 7:37 AM
e431499dada298ba_OneDrive.html	5/10/2022 7:37 AM
e431499dada298ba_OneDrive.json	5/10/2022 7:37 AM

Line	Tag	Parent Id	Drive Item Id	e Tag
1	□		7CA57A1EEDBAF486!101	
2	□	7CA57A1EEDBAF486!101	7CA57A1EEDBAF486!104	7CA57A1EEDBAF48
3	□	7CA57A1EEDBAF486!101	7CA57A1EEDBAF486!105	7CA57A1EEDBAF48
4	□	7CA57A1EEDBAF486!101	7CA57A1EEDBAF486!103	7CA57A1EEDBAF48
5	□	7CA57A1EEDBAF486!101	7CA57A1EEDBAF486!106	7CA57A1EEDBAF48

ParentId	DriveItemId	eTag	T
	7CA57A1EEDBAF486!101		Root De
7CA57A1EEDBAF486!101	7CA57A1EEDBAF486!104	7CA57A1EEDBAF486!104.0	Folder
7CA57A1EEDBAF486!101	7CA57A1EEDBAF486!105	7CA57A1EEDBAF486!105.0	Folder
7CA57A1EEDBAF486!101	7CA57A1EEDBAF486!103	7CA57A1EEDBAF486!103.0	Folder

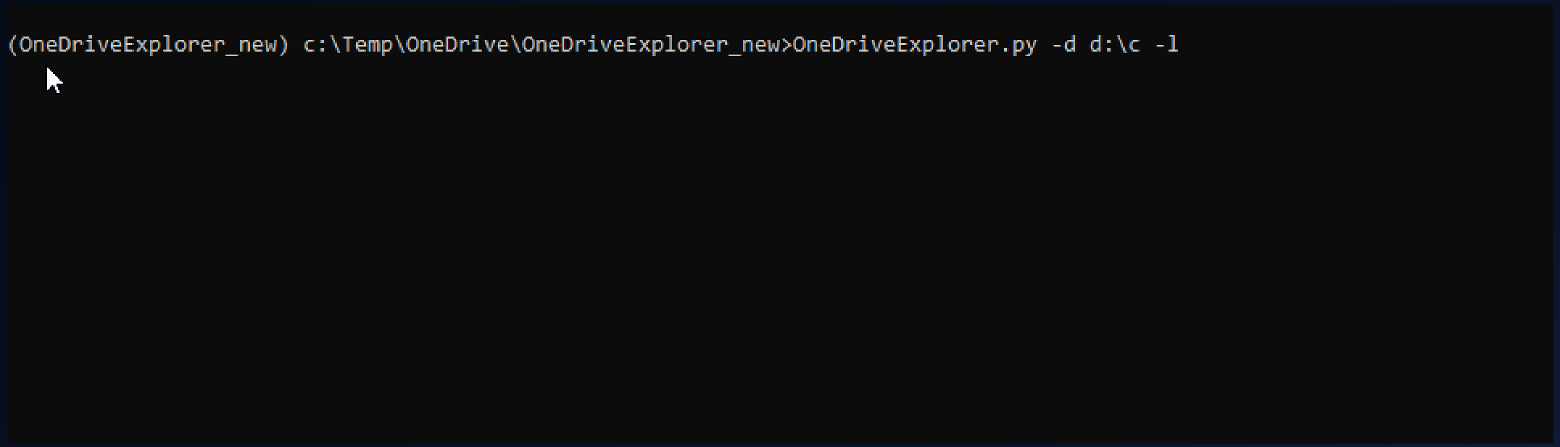
```
{
    "ParentId": "",
    "DriveItemId": "",
    "eTag": "",
    "Type": "Root Drive",
    "Path": "",
    "Name": "d:\\c\\Users\\srl-h\\AppData\\Local\\Microsoft\\OneDrive\\settings\\Pe
    "Size": "",
    "Hash": "",
    "Children": [
        {
            "ParentId": "",
            "DriveItemId": "7CA57A1EEDBAF486!101",
            "eTag": "",
            "Type": "Root Default",
            "Path": "7CA57A1EEDBAF486!101",
            "Name": "C:\\Users\\srl-h\\OneDrive",
            "Size": "",
```

Lessons Learned

RECAP

Take Away Items

- Find data from one or multiple sources
- Eliminates multiple collections
- Easy to use on multi-user systems
- Solves storage and scope of authority
- Easy to automate



```
(OneDriveExplorer_new) c:\Temp\OneDrive\OneDriveExplorer_new>OneDriveExplorer.py -d d:\c -l
```

OneDriveExplorer Roadmap

- Parse freelist and unallocated space (SQLite)
- Parse .dat files for broken records
- “Time travel” (kind of like Restore your OneDrive feature)
- Will take some time, I’m only one person

Special Thanks To

- Kevin Pagano @KevinPagano3
- Phill Moore @phillmoore
- Eric Zimmerman @EricZimmerman
- Andrew Rathbun @bunsofwrath12
- Chad Tilbury @chadtilbury
- Yogesh Khatri @SwiftForensics
- Ali Hadi @binaryzOne