**Examining Cloud File Storage Incidents – LAB**

Microsoft OneDrive

**LAB INSTRUCTIONS**

**Step 1:**

Navigate to the evidence and open the [Cid]-ProfileServiceResponse.txt file with Notepad++:   
…evidence-DESKTOP-Q50SISB\C\Users\Bob\AppData\Local\Microsoft\OneDrive\settings\Personal\[Cid]-ProfileServiceResponse.txt

**Question**:

What’s Bob’s Microsoft OneDrive CID?

**Question**:

Examine the [Cid]-ProfileServiceResponse.txt file and get the “userPrincipalName” of the authenticated OneDrive account.

**Step 2:**

Navigate to …evidence-DESKTOP-Q50SISB\C\Users\Bob\AppData\Local\Microsoft\OneDrive\logs\Personal\ and open SyncDiagnostics.log with Notepad++.

**Question**:

What is the deviceID of the system you’re investigating?

**Question**:

How many files/folders are being synced?

**Step 3:**

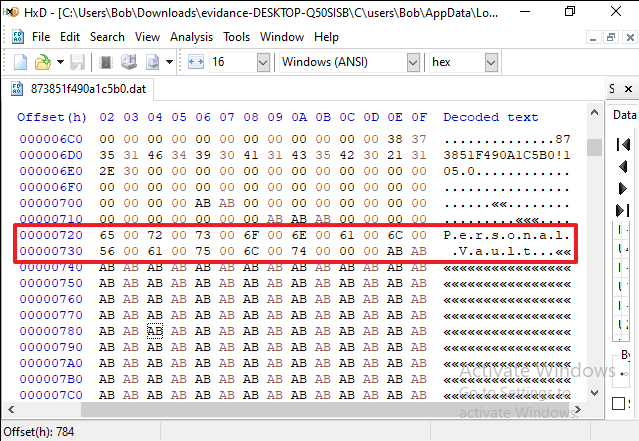
Navigate to …evidence-DESKTOP-Q50SISB\C\Users\Bob\AppData\Local\Microsoft\OneDrive\logs\Personal\ and open ObfuscationStringMap.txt with Notepad++.

**Question**:

Looking at the right column of the text file, identify which keys (left column) would equate to: C\Users\Bob. Example answer: OneTwoThree\MeYouThey\WhoWhatWhere

**Step 4**:

Navigate to …evidence-DESKTOP-Q50SISB\C\Users\Bob\AppData\Local\Microsoft\OneDrive\settings\Personal\ and open [cid].dat in HxD hex editor. At offset (h) 00000720 you’ll see “P.e.r.s.o.n.a.l..V.a.u.l.t…” in the Decoded text column.



**Question**:

Continue to scroll down in HxD looking for the next human readable folder name. What’s the next folder name you see?

**Step 5:**

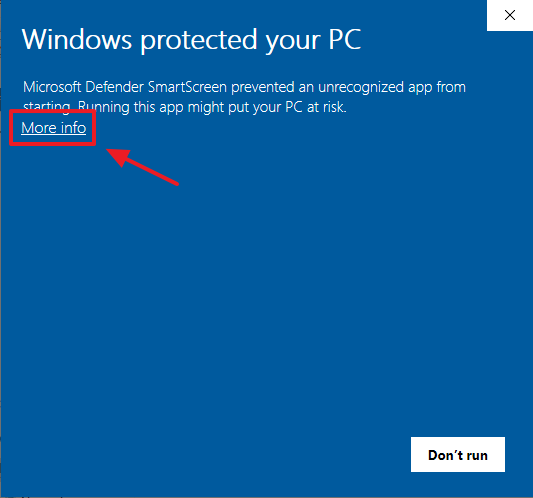
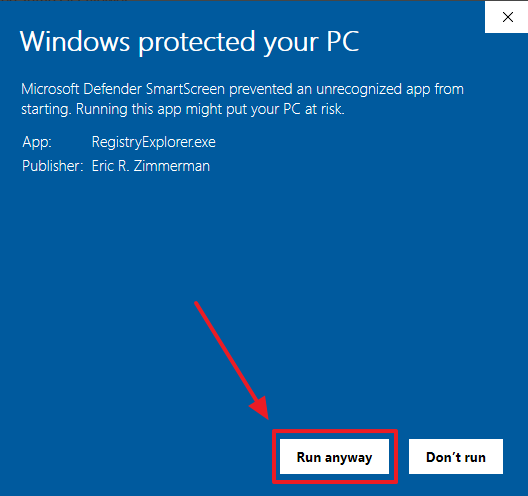
Navigate to …evidence-DESKTOP-Q50SISB\C\Users\Bob\AppData\Local\Microsoft\OneDrive\settings\Personal\ and open [cid].ini in Notepad++.

**Question**:

What’s the local path being used to store files by Microsoft OneDrive?

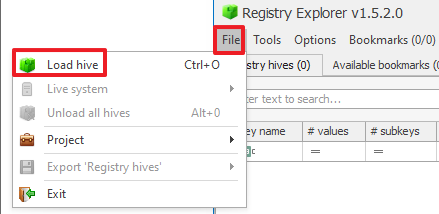
**Step 6:**

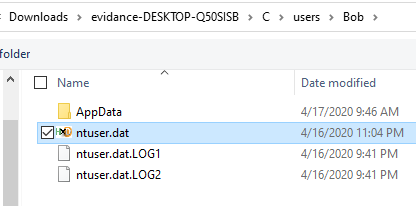
Run Registry Explorer (RegistryExplorer.exe). If prompted about Microsoft Defender SmartScreen, click “More info”.

**Step 7:**

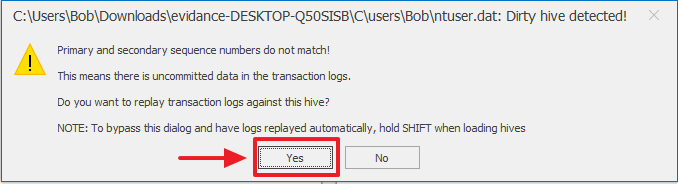
Once Registry Explorer loads, go to File > Load Hive. Browse to the evidence: C:\users\bob\ and select ntuser.dat

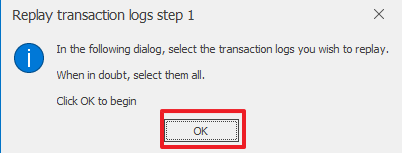




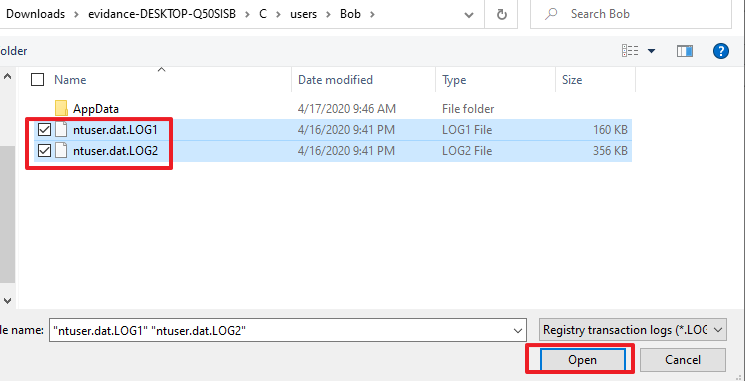
**Step 8:**

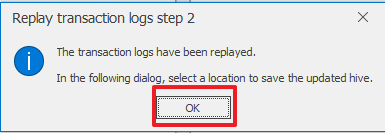
If the ntuser.dat hive is dirty (uncommitted data), press “Yes” to replay the transaction logs against the hive.



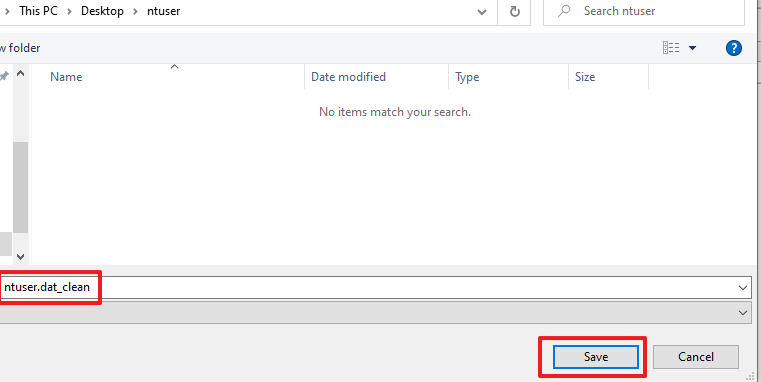


Select both ntuser.dat.LOG1 and ntuser.dat.LOG2 in this case. Then press Open.

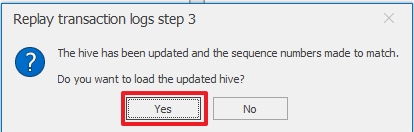




Save the ntuser.dat\_clean file somewhere (e.g. Desktop)



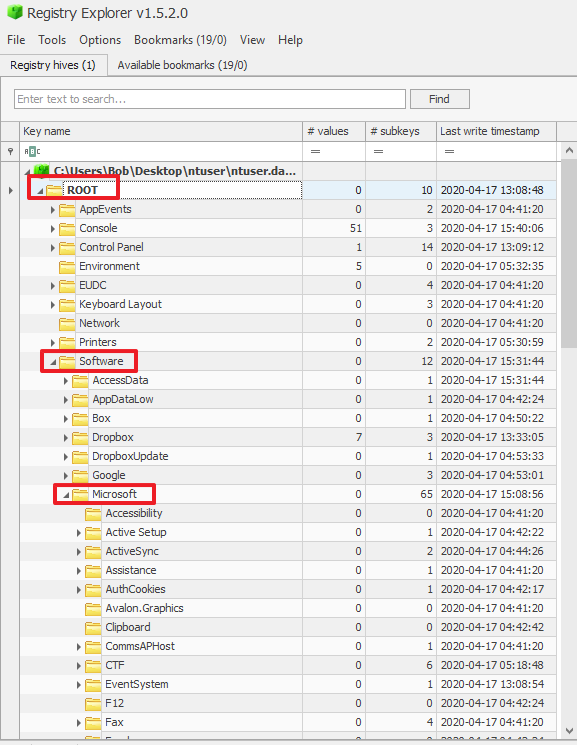
Load the updated ntuser.dat\_clean hive by pressing “Yes”:



If asked to load the dirty have as well, press “NO”.

**Step 9:**

Expand the registry hive until you get to: Software\Microsoft\OneDrive\Accounts\[Personal\



**Question**:

Fill in the data/values for the following:

|  |  |
| --- | --- |
| **UserEmail** |  |
| **cid** |  |
| **NamespaceRootId** |  |
| **UserFolder** |  |
| **LastSignInTime** |  |
| **ClientFirstSignInTimestamp** |  |

**Step 10:**

Navigate to the following registry key within Registry Explorer: HKCU\Software\SyncEngines\Providers\OneDrive\

“Personal” is a default directory.

**Question**:

Aside from “Personal”, what other shared directories does the user have?

**Question**:

Clicking into the Personal and other shared folder keys in the registry hive, what data/value do you see for the CIDs for each shared folder?

**DETAILED WALKTHROUGH**

**Step 1:**

Navigate to the evidence and open the [Cid]-ProfileServiceResponse.txt file with Notepad++:   
…evidence-DESKTOP-Q50SISB\C\Users\Bob\AppData\Local\Microsoft\OneDrive\settings\Personal\[Cid]-ProfileServiceResponse.txt

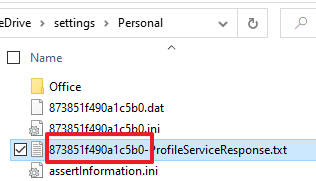
**Question**:

What’s Bob’s Microsoft OneDrive CID?

**Answer**:

873851f490a1c5b0

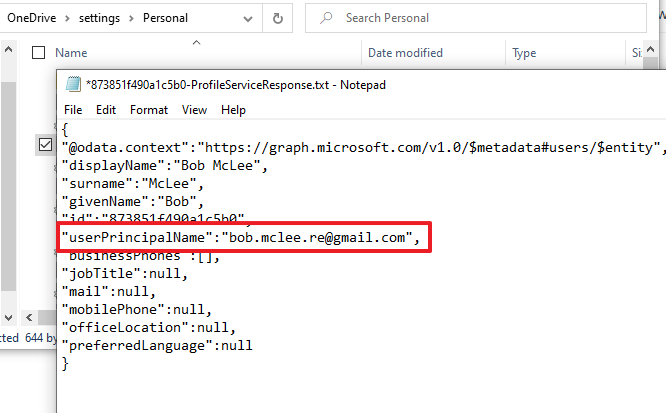
…evidance-DESKTOP-Q50SISB\C\users\Bob\AppData\Local\Microsoft\OneDrive\settings\Personal\



**Question**:

Examine the [Cid]-ProfileServiceResponse.txt file and get the “userPrincipalName” of the authenticated OneDrive account.

**Answer**:

bob.mclee.re@gmail.com  
  


**Step 2:**

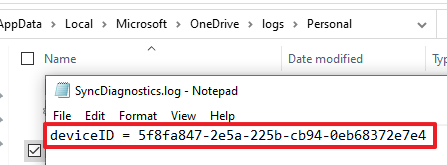
Navigate to …evidence-DESKTOP-Q50SISB\C\Users\Bob\AppData\Local\Microsoft\OneDrive\logs\Personal\ and open SyncDiagnostics.log with Notepad++.

**Question**:

What is the deviceID of the system you’re investigating?

**Answer**:

deviceID = 5f8fa847-2e5a-225b-cb94-0eb68372e7e4



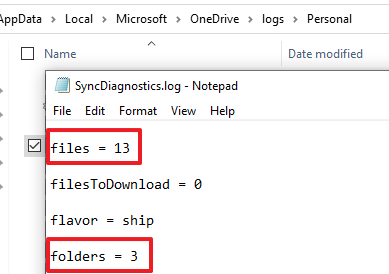
**Question**:

How many files/folders are being synced?

**Answer:**

Files = 13

Folders = 3



**Step 3:**

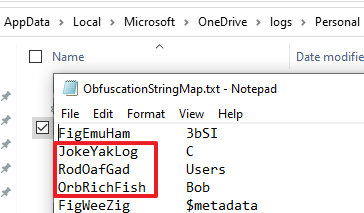
Navigate to …evidence-DESKTOP-Q50SISB\C\Users\Bob\AppData\Local\Microsoft\OneDrive\logs\Personal\ and open ObfuscationStringMap.txt with Notepad++.

**Question**:

Looking at the right column of the text file, identify which keys (left column) would equate to: C\Users\Bob. Example answer: OneTwoThree\MeYouThey\WhoWhatWhere

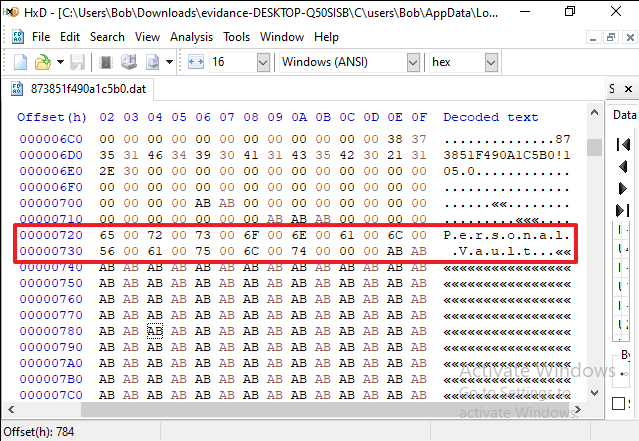
**Answer**:

JokeYakLog\RodOafGad\OrbRichFist



**Step 4**:

Navigate to …evidence-DESKTOP-Q50SISB\C\Users\Bob\AppData\Local\Microsoft\OneDrive\settings\Personal\ and open [cid].dat in HxD hex editor. At offset (h) 00000720 you’ll see “P.e.r.s.o.n.a.l..V.a.u.l.t…” in the Decoded text column.

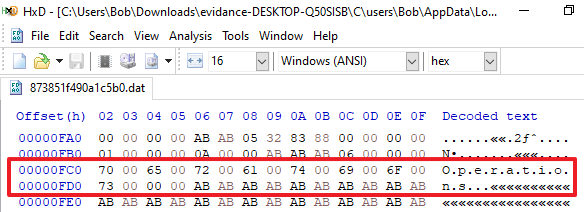


**Question**:

Continue to scroll down in HxD looking for the next human readable folder name. What’s the next folder name you see?

**Answer**:

Operations



**Step 5:**

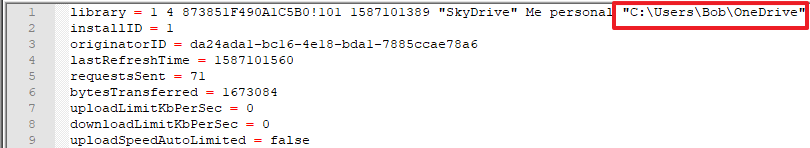
Navigate to …evidence-DESKTOP-Q50SISB\C\Users\Bob\AppData\Local\Microsoft\OneDrive\settings\Personal\ and open [cid].ini in Notepad++.

**Question**:

What’s the local path being used to store files by Microsoft OneDrive?

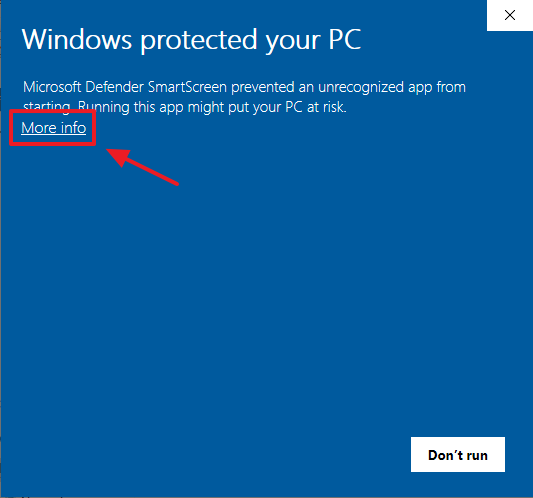
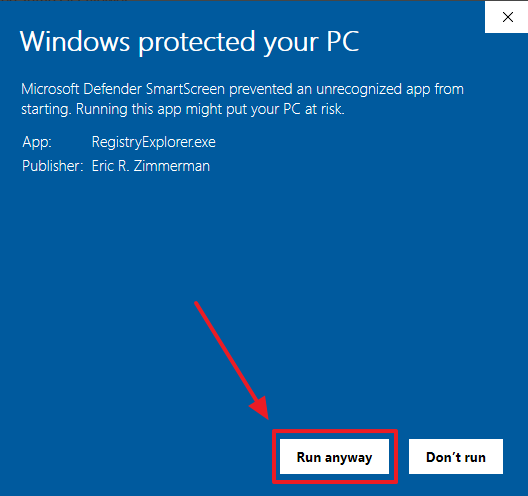
**Answer**:

"C:\Users\Bob\OneDrive"



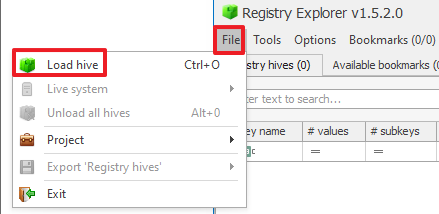
**Step 6:**

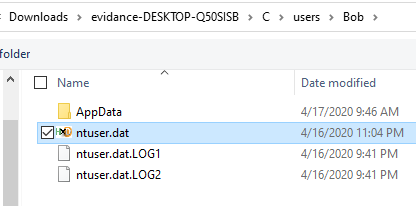
Run Registry Explorer (RegistryExplorer.exe). If prompted about Microsoft Defender SmartScreen, click “More info”.

**Step 7:**

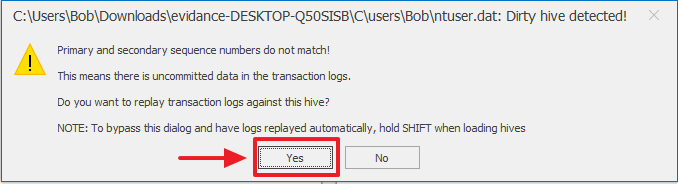
Once Registry Explorer loads, go to File > Load Hive. Browse to the evidence: C:\users\bob\ and select ntuser.dat

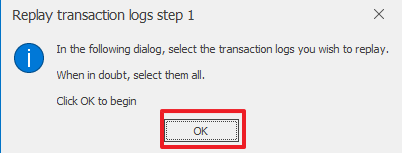




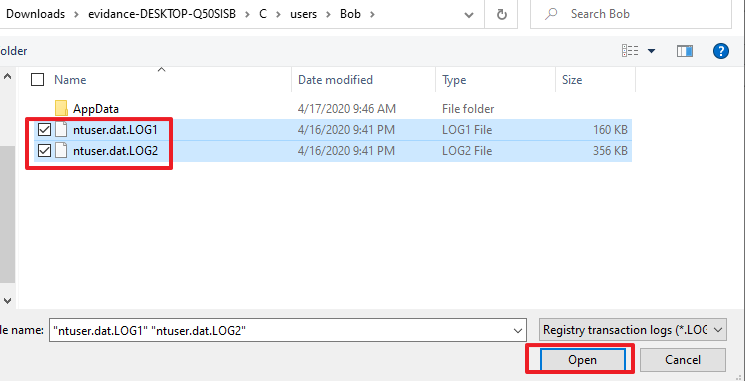
**Step 8:**

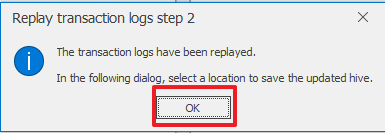
If the ntuser.dat hive is dirty (uncommitted data), press “Yes” to replay the transaction logs against the hive.



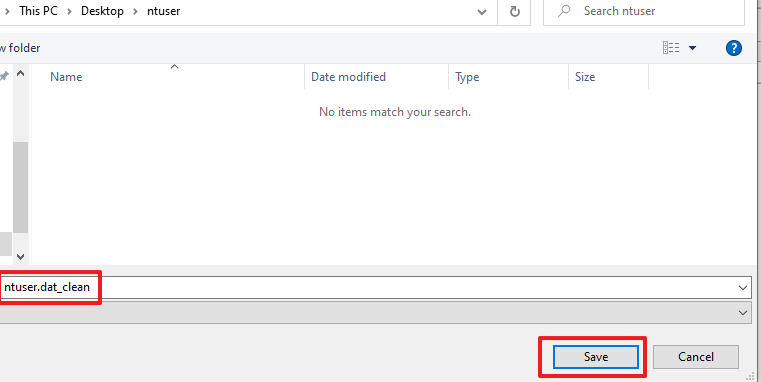


Select both ntuser.dat.LOG1 and ntuser.dat.LOG2 in this case. Then press Open.

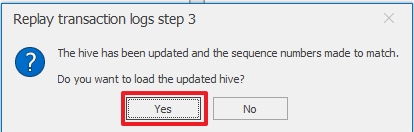




Save the ntuser.dat\_clean file somewhere (e.g. Desktop)



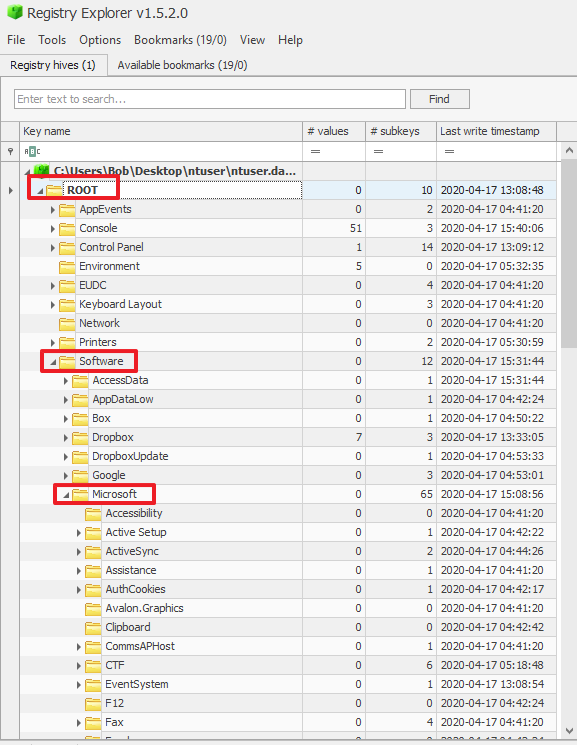
Load the updated ntuser.dat\_clean hive by pressing “Yes”:



If asked to load the dirty have as well, press “NO”.

**Step 9:**

Expand the registry hive until you get to: Software\Microsoft\OneDrive\Accounts\[Personal\



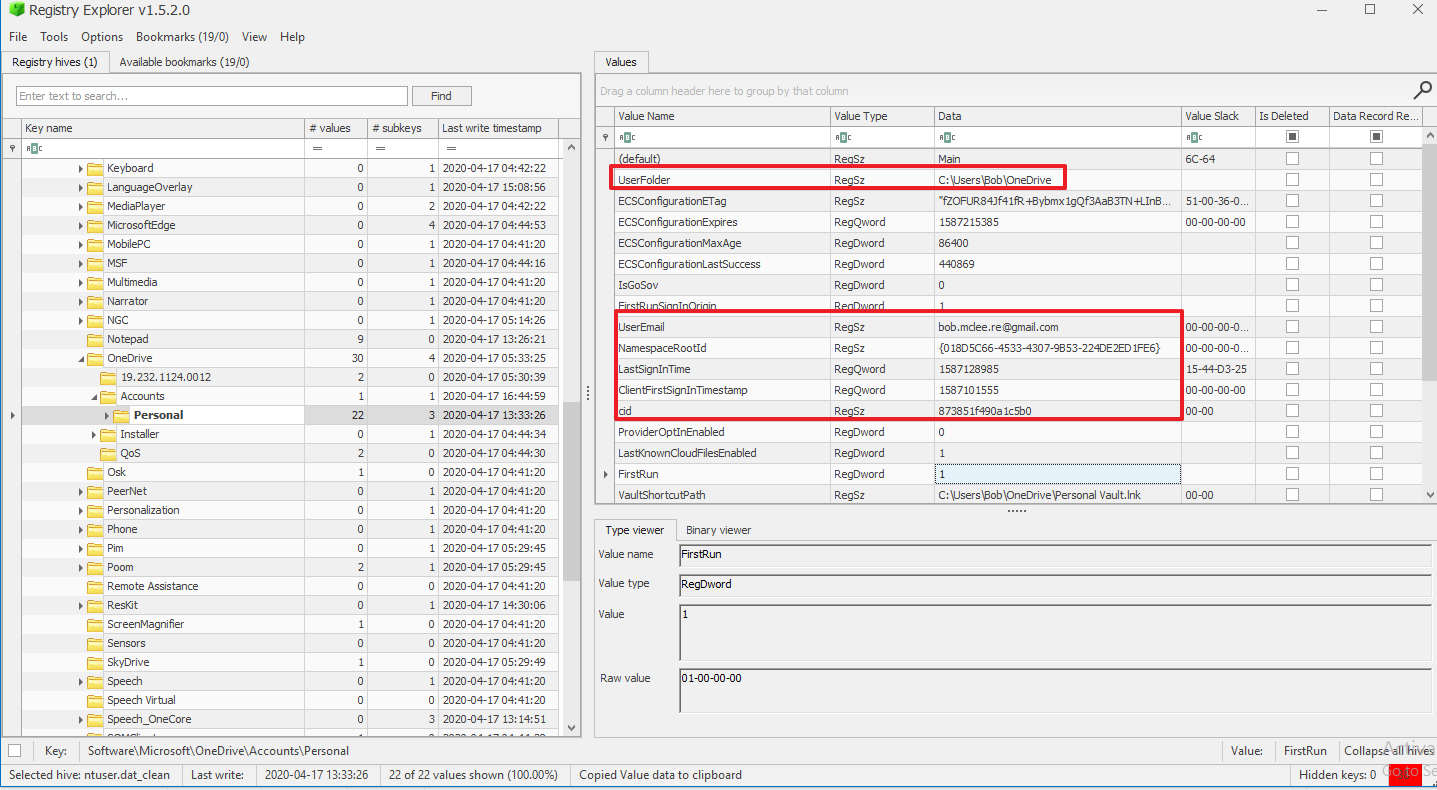
**Question**:

Fill in the data/values for the following:

|  |  |
| --- | --- |
| **UserEmail** |  |
| **cid** |  |
| **NamespaceRootId** |  |
| **UserFolder** |  |
| **LastSignInTime** |  |
| **ClientFirstSignInTimestamp** |  |

**Answer**:

|  |  |
| --- | --- |
| **UserEmail** | bob.mclee.re@gmail.com |
| **cid** | 873851f490a1c5b0 |
| **NamespaceRootId** | {018D5C66-4533-4307-9B53-224DE2ED1FE6} |
| **UserFolder** | C:\Users\Bob\OneDrive |
| **LastSignInTime** | 1587128985 |
| **ClientFirstSignInTimestamp** | 1587101555 |



**Step 10:**

Navigate to the following registry key within Registry Explorer: HKCU\Software\SyncEngines\Providers\OneDrive\

“Personal” is a default directory.

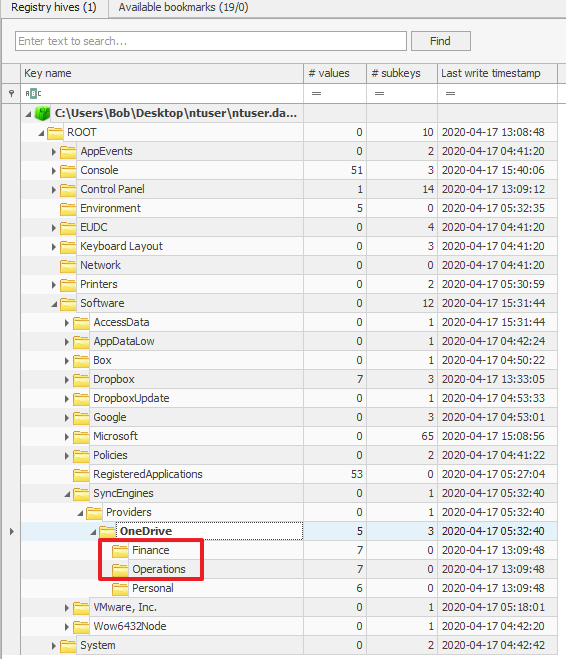
**Question**:

Aside from “Personal”, what other shared directories does the user have?

**Answer**:

Operations

Finance



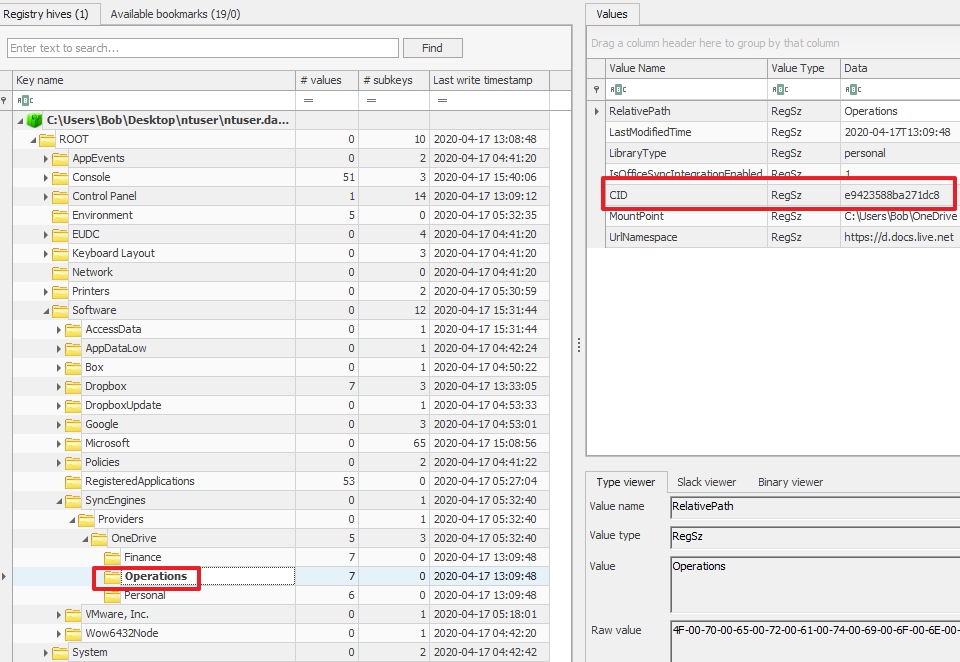
**Question**:

Clicking into the Personal and other shared folder keys in the registry hive, what data/value do you see for the CIDs for each shared folder?

**Answer**:

Finance / Operations = e9423588ba271dc8

Personal = 873851f490a1c5b0



**END OF LAB**