**Examining Cloud File Storage Incidents – LAB**

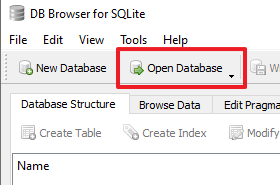
Google Drive

**LAB INSTRUCTIONS**

**Step 1:**

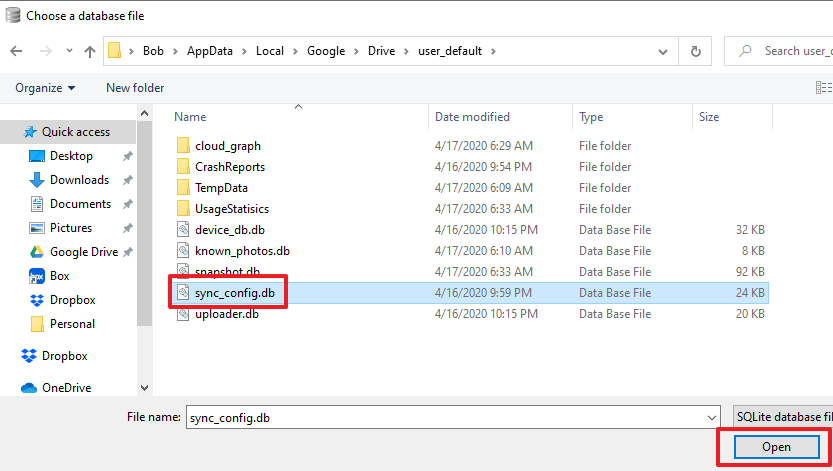
Run DB Browser for SQLite (located in C:\Program Files\DB Browser for SQLite)

Click “Open Database” under the Help menu.



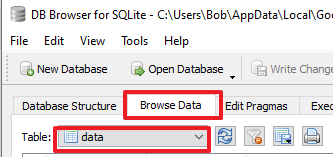
Browse to …C\Users\Bob\Appdata\Local\Google\Drive\user\_default\

Select the sync\_config.db database and press “Open”



Click on the “Browse Data” tab.

Ensure the “data” table is being used.



**Questions**:

What is the data\_value for the following rows?

|  |  |
| --- | --- |
| **entry\_key** | **data\_value** |
| **highest\_app\_version** |  |
| **local\_sync\_root\_path** |  |
| **user\_email** |  |

**Step 2:**

Browse to … evidence-DESKTOP-Q50SISB\C\Users\Bob\Appdata\Local\Google\Drive\user\_default\cloud\_graph\

Select the cloud\_graph.db database and press “Open”

Select the cloud\_graph\_entry table.

**Question**:

What’s the filename for the doc\_type = 6 (Google Doc)?

**Question**:

Look at the modified data for the file identified in the prior question (doc\_type = 6). What time locally (Los Angeles) was the file modified? (HINT: Convert Unix epoch to GMT. Subtract 7 from GMT - https://www.epochconverter.com/)

**Question**:

Further examination of the filename column in the database uncovers additional documents of interest. For example, doc\_id = 1mPsyPP6CW\_CPTdaqRQSVoD3QMdrgYfC8. When was this document last modified locally (Los Angeles)?

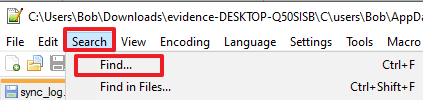
**Question**:

What’s the file hash for the filename “Client List.txt”?

**Step 3**:

In Notepad++ open sync\_log.log (located in… evidance-DESKTOP-Q50SISB\C\users\Bob\AppData\Local\Google\Drive\user\_default\)

NOTE: Ideally, we’d use a better tool for parsing logs (e.g. SumoLogic, ElasticStack, grep, sed, etc.), but for simplicity of the workshop, we’ll sue “Find” within Notepad++ to answer this question. Just keep in mind there are better ways to do this task.



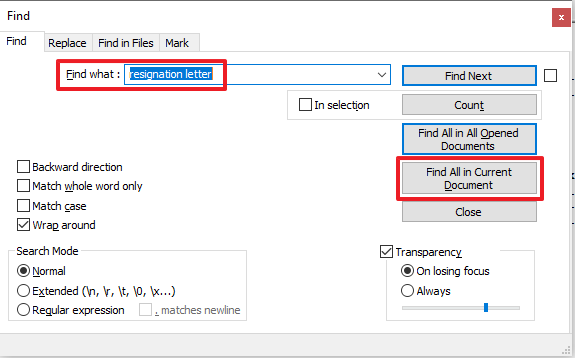
In the “Find what:” field, search for “Resignation Letter”. Look at the Action.CREATE in the event to verify you’re looking at the first create event for this file.

**Question**:

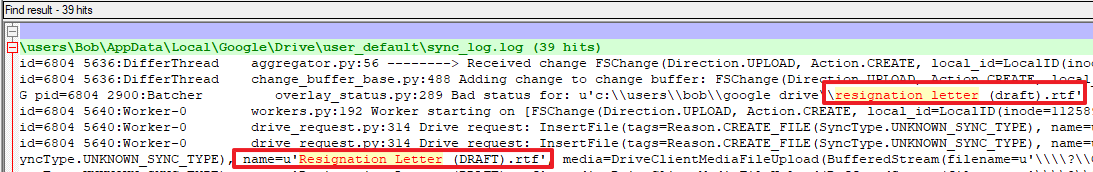
Where did the file originate from? E.g. (Direction.UPLOAD = local. Direction.DOWNLOAD = cloud)

**Question**:

The filename appears to be different from what was displayed earlier. Rather than “Find Next”, click “Find All in Current Document” in the Find box.



Look at all the instances in the log file where the file name appears.



At what time does the filename change and was the change made in the cloud or locally?

**Step 4:**

Run DB Browser for SQLite (located in C:\Program Files\DB Browser for SQLite)

Click “Open Database” under the Help menu.

Browse to …C\Users\Bob\Appdata\Local\Google\Drive\user\_default\

Select the snapshot.db database and press “Open”

Click on the “Browse Data” tab.

Ensure the “cloud\_entry” table is being used.

**Question**:

What is the inode for the “Office Lease.docx” file?

**Step 5**:

Switch to the local\_relations table within snapshot.db

Locate the inode ID found in the prior step used for “Office Lease.docx” within the local\_relations table.

**Question**:

What’s the parent\_inode for “Office Lease.docx”?

**Question**:

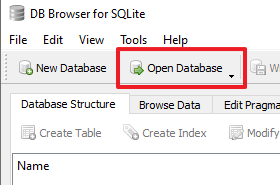
Map the parent\_inode back to the human readable name in the local\_entry table. What’s the human readable folder’s name / path?

**DETAILED LAB WALKTHROUGH**

**Step 1:**

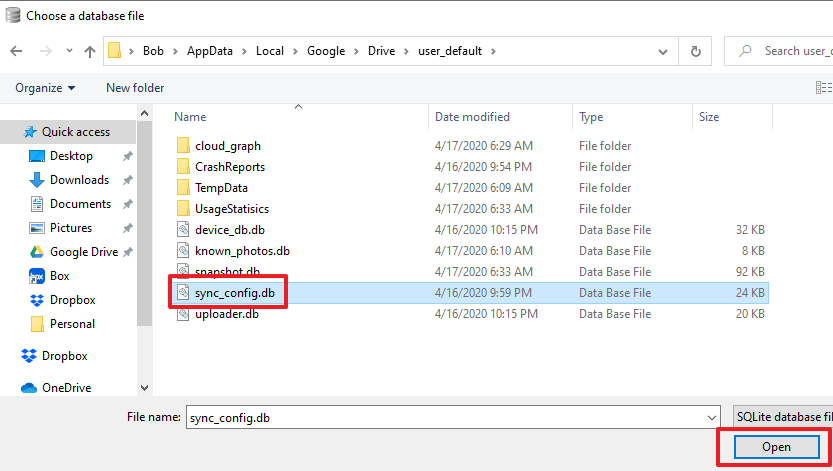
Run DB Browser for SQLite (located in C:\Program Files\DB Browser for SQLite)

Click “Open Database” under the Help menu.



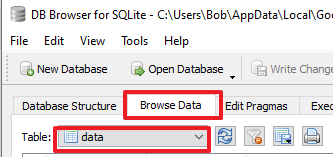
Browse to …C\Users\Bob\Appdata\Local\Google\Drive\user\_default\

Select the sync\_config.db database and press “Open”



Click on the “Browse Data” tab.

Ensure the “data” table is being used.



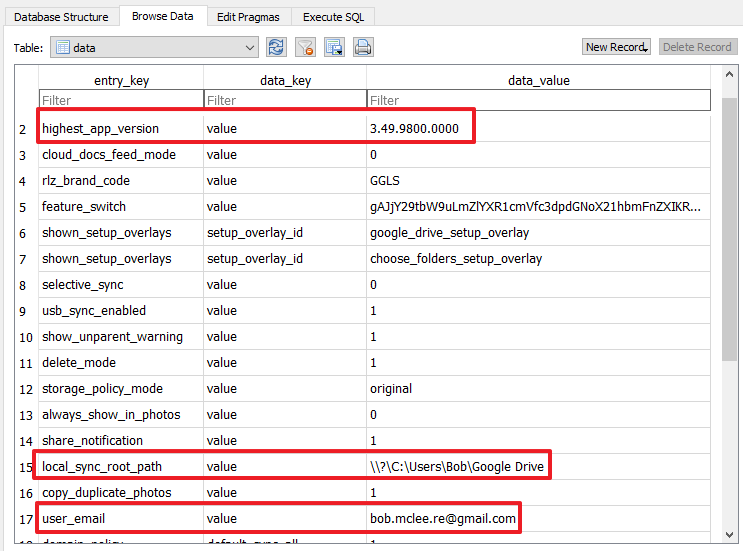
**Questions**:

What is the data\_value for the following rows?

|  |  |
| --- | --- |
| **entry\_key** | **data\_value** |
| **highest\_app\_version** | 3.49.9800.0000 |
| **local\_sync\_root\_path** | \\?\C:\Users\Bob\Google Drive |
| **user\_email** | bob.mclee.re@gmail.com |

**Answer**:

|  |  |
| --- | --- |
| **entry\_key** | **data\_value** |
| **highest\_app\_version** | 3.49.9800.0000 |
| **local\_sync\_root\_path** | \\?\C:\Users\Bob\Google Drive |
| **user\_email** | bob.mclee.re@gmail.com |



**Step 2:**

Browse to … evidence-DESKTOP-Q50SISB\C\Users\Bob\Appdata\Local\Google\Drive\user\_default\cloud\_graph\

Select the cloud\_graph.db database and press “Open”

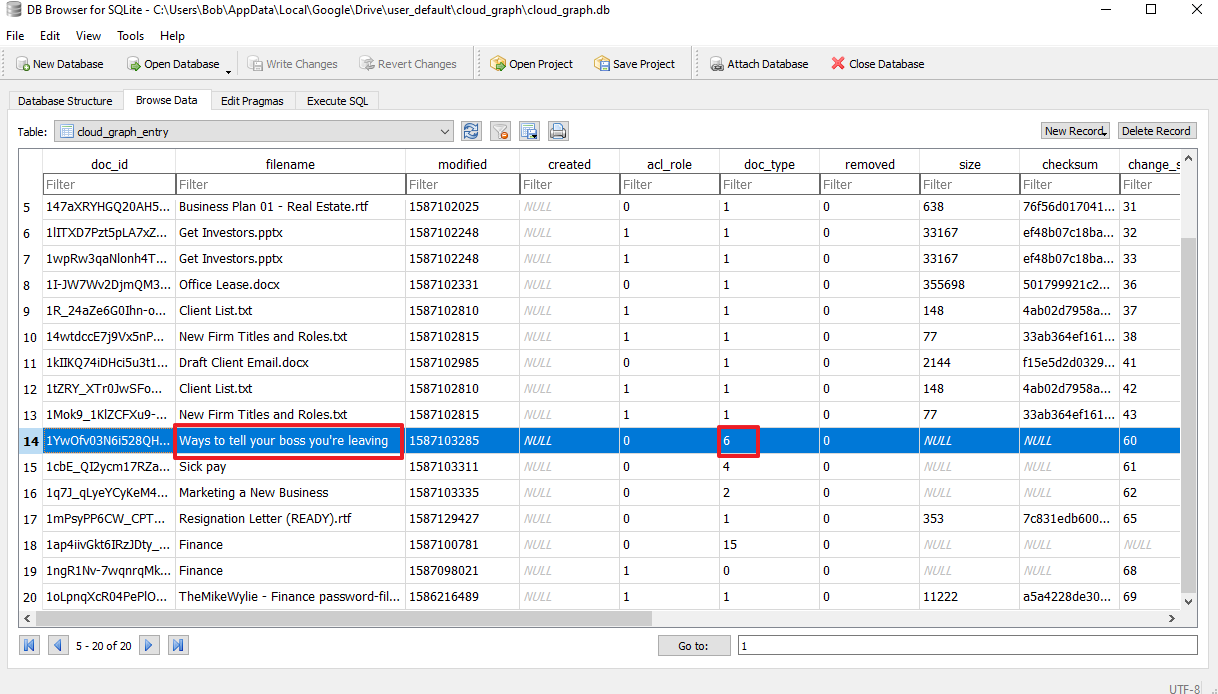
Select the cloud\_graph\_entry table.

**Question**:

What’s the filename for the doc\_type = 6 (Google Doc)?

**Answer**:

“Ways to tell your boss you’re leaving”

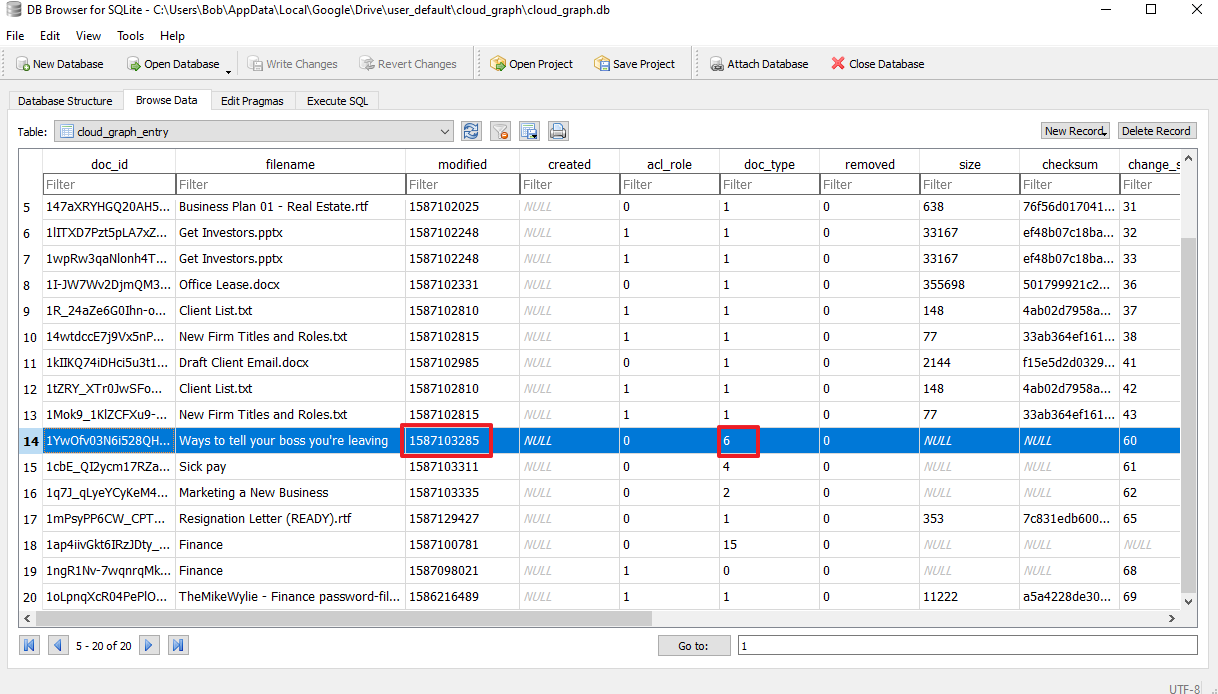


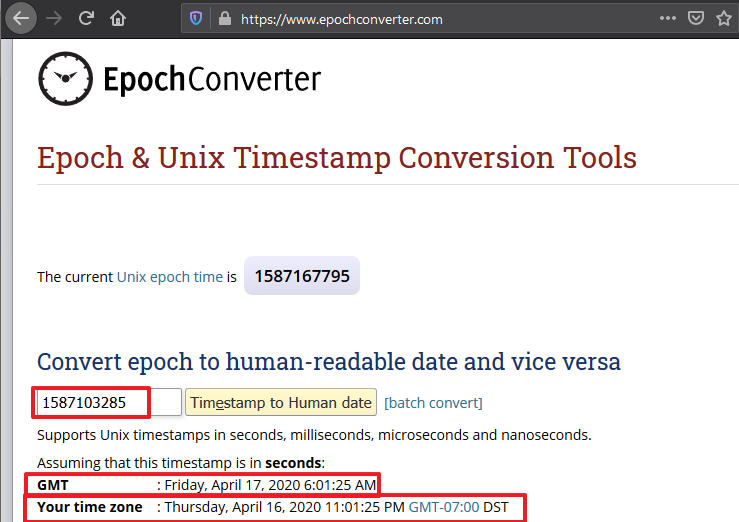
**Question**:

Look at the modified data for the file identified in the prior question (doc\_type = 6). What time locally (Los Angeles) was the file modified? (HINT: Convert Unix epoch to GMT. Subtract 7 from GMT - https://www.epochconverter.com/)

**Answer**:

1587103285 > Friday, April 17, 2020 6:01:25 AM GMT > Thursday, April 16, 2020 11:01:25 PM GMT-07:00 DST



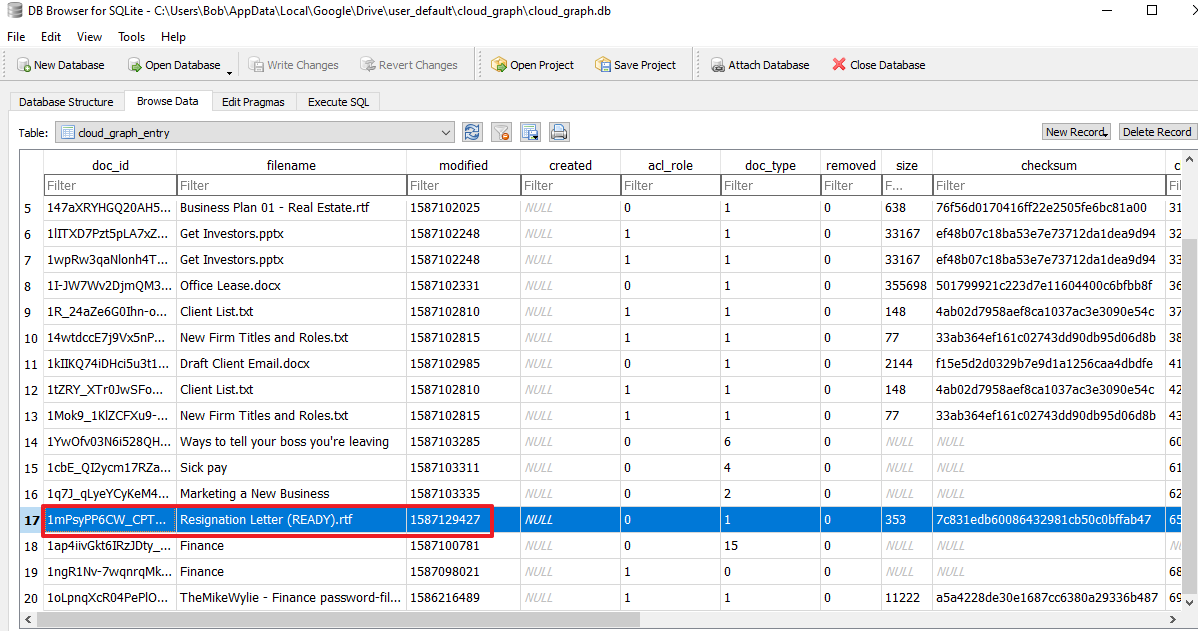


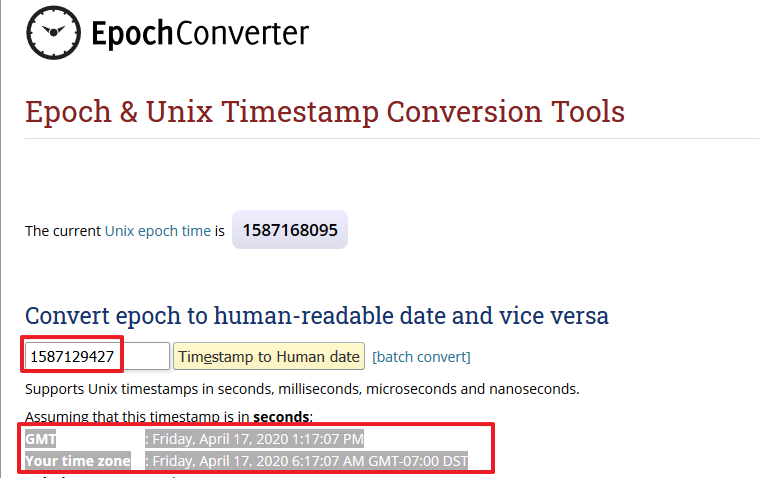
**Question**:

Further examination of the filename column in the database uncovers additional documents of interest. For example, doc\_id = 1mPsyPP6CW\_CPTdaqRQSVoD3QMdrgYfC8. When was this document last modified locally (Los Angeles)?

**Answer**:

1587129427 > GMT: Friday, April 17, 2020 1:17:07 PM > Friday, April 17, 2020 6:17:07 AM GMT-07:00 DST



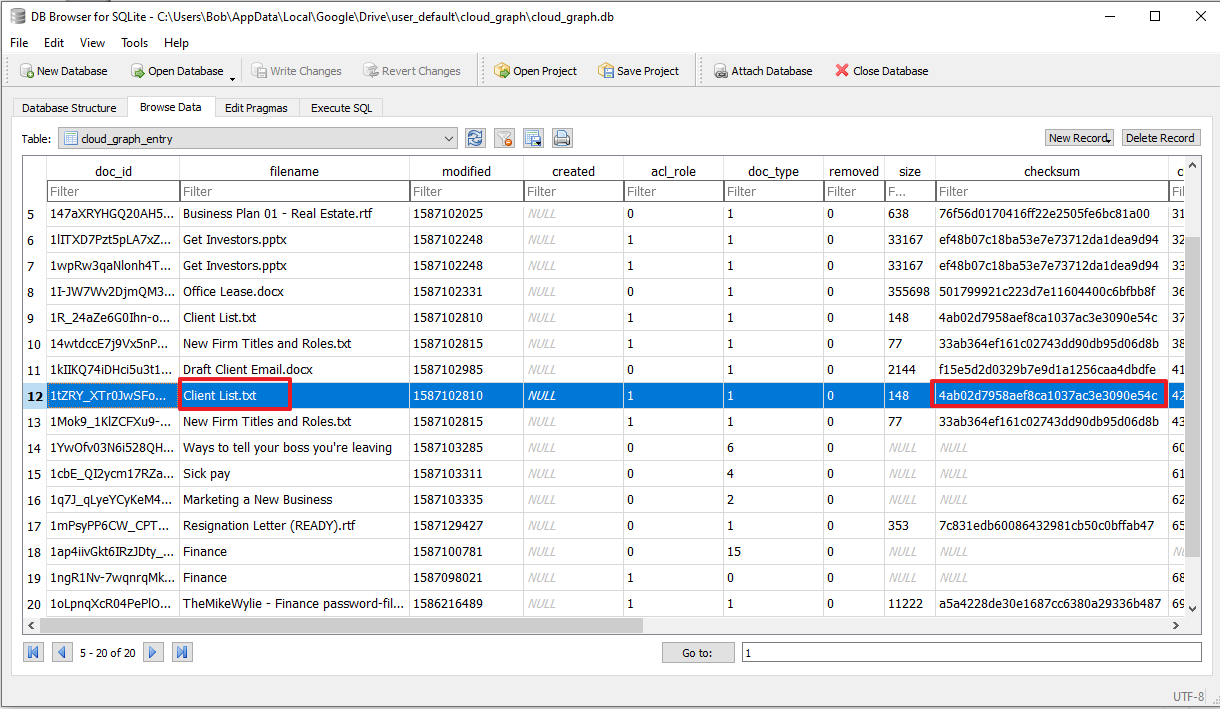


**Question**:

What’s the file hash for the filename “Client List.txt”?

**Answer**:

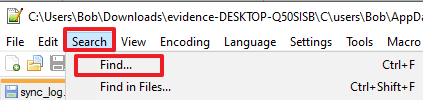
4ab02d7958aef8ca1037ac3e3090e54c



**Step 3**:

In Notepad++ open sync\_log.log (located in… evidance-DESKTOP-Q50SISB\C\users\Bob\AppData\Local\Google\Drive\user\_default\)

NOTE: Ideally, we’d use a better tool for parsing logs (e.g. SumoLogic, ElasticStack, grep, sed, etc.), but for simplicity of the workshop, we’ll sue “Find” within Notepad++ to answer this question. Just keep in mind there are better ways to do this task.



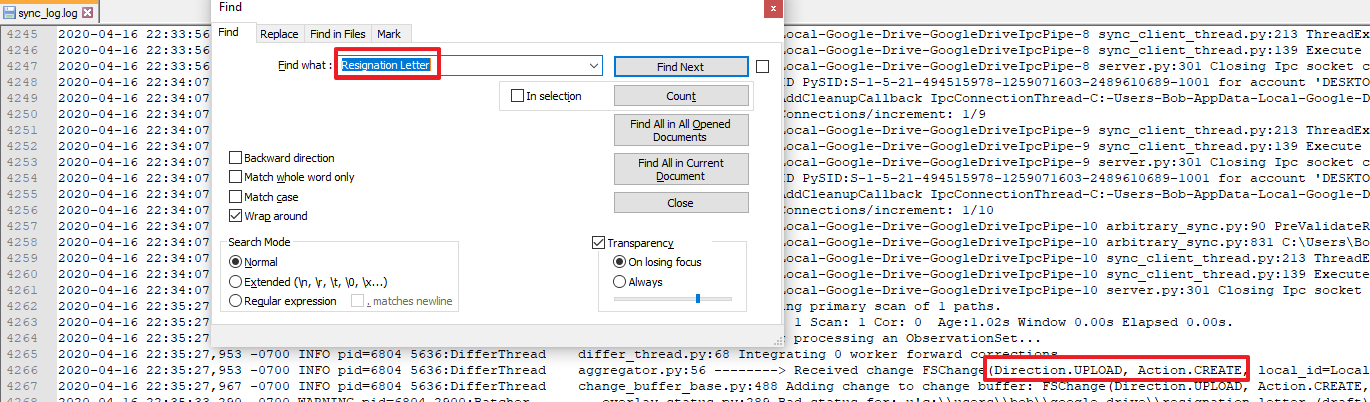
In the “Find what:” field, search for “Resignation Letter”. Look at the Action.CREATE in the event to verify you’re looking at the first create event for this file.

**Question**:

Where did the file originate from? E.g. (Direction.UPLOAD = local. Direction.DOWNLOAD = cloud)

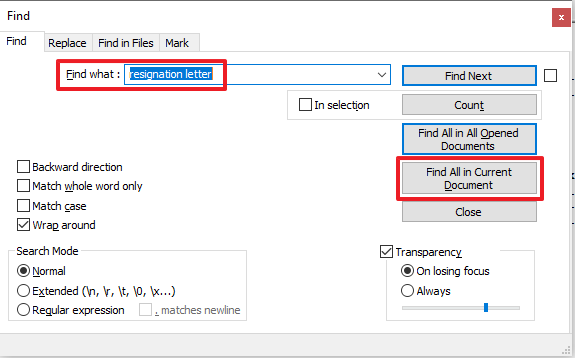
**Answer**:

Direction.UPLOAD

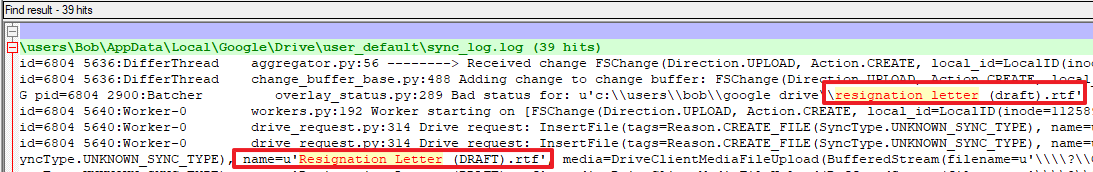


**Question**:

The filename appears to be different from what was displayed earlier. Rather than “Find Next”, click “Find All in Current Document” in the Find box.



Look at all the instances in the log file where the file name appears.



At what time does the filename change and was the change made in the cloud or locally?

**Answer**:

Line 4347: ([ItemChange(item=File(size=344L, md5\_checksum=u'67a6446c1e0fc25f3607f2545a40e3fd', mime\_type=u'application/rtf', photos\_storage\_policy=<StoragePolicyMode.ORIGINAL: 'original'>, modified=1587101582.0, trashed=False, acl\_role=<AclRole.OWNER: 0>, reader\_download\_restricted=False, version=1L, shared=False, file\_extension=u'rtf', doc\_id=u'1h0OmRiI3I\_350z3p\_aw2W9Udq7BEnGue', parent\_doc\_ids=frozenset([u'0AKQBL1meBeCqUk9PVA']), title=u'Resignation Letter (DRAFT).rtf'), change\_id=26L)], None)

Line 6806: **2020-04-17 06:17:08**,533 -0700 INFO pid=4248 1952:DifferThread aggregator.py:56 --------> Received change FSChange(**Direction.UPLOAD**, Action.CREATE, local\_id=LocalID(inode=5348024557595993L, volume='serial:2290299397'), path=u'\\\\?\\C:\\Users\\Bob\\Google Drive', name=u'Resignation Letter (READY).rtf', parent\_local\_id=LocalID(inode=5066549580887987L, volume='serial:2290299397'), is\_folder=False, modified=1587129427, size=353, generator\_module=Generator.LOCAL\_EVENT\_GENERATOR, shared=False)

**Step 4:**

Run DB Browser for SQLite (located in C:\Program Files\DB Browser for SQLite)

Click “Open Database” under the Help menu.

Browse to …C\Users\Bob\Appdata\Local\Google\Drive\user\_default\

Select the snapshot.db database and press “Open”

Click on the “Browse Data” tab.

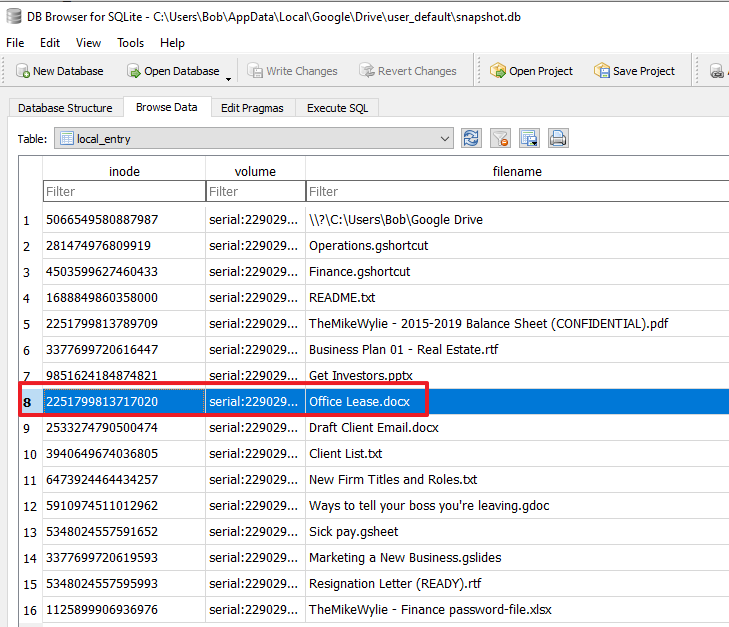
Ensure the “cloud\_entry” table is being used.

Question:

What is the inode for the “Office Lease.docx” file?

Answer:

2251799813717020



**Step 5**:

Switch to the local\_relations table within snapshot.db

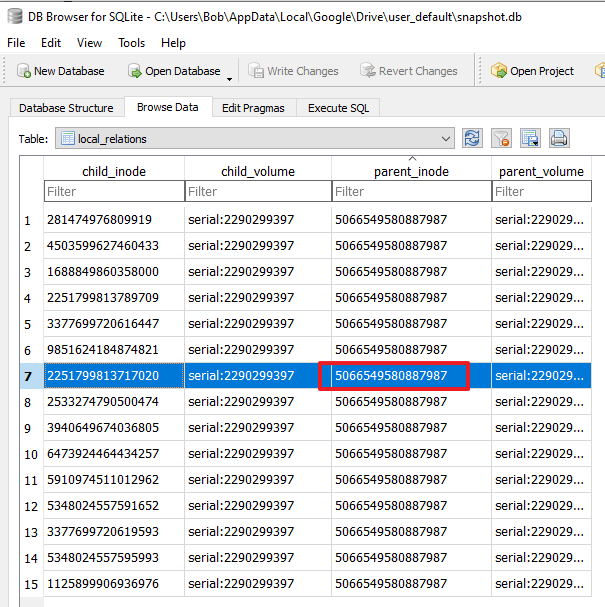
Locate the inode ID found in the prior step used for “Office Lease.docx” within the local\_relations table.

**Question**:

What’s the parent\_inode for “Office Lease.docx”?

**Answer**:

5066549580887987

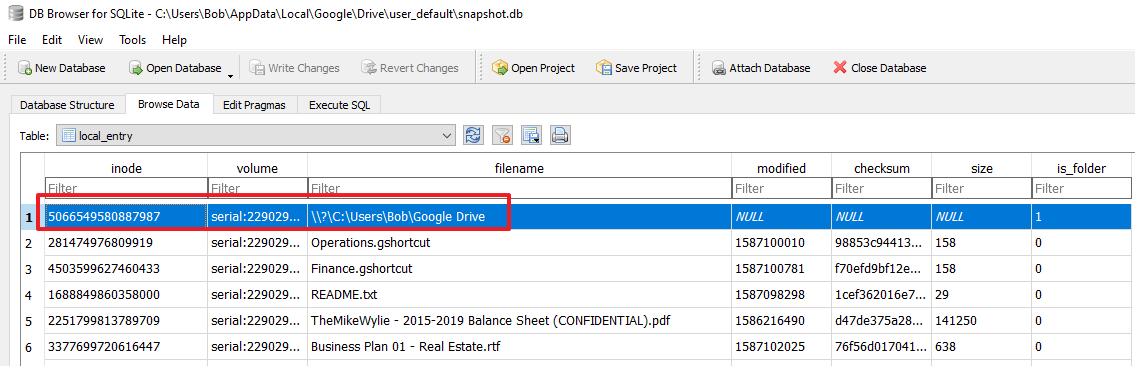


**Question**:

Map the parent\_inode back to the human readable name in the local\_entry table. What’s the human readable folder’s name / path?

**Answer**:

Google Drive



**END OF LAB**