**Examining Cloud File Storage Incidents – LAB**

Box

**LAB INSTRUCTIONS**

**Step 1:**

Open the following file in Notepad++: …\evidence-DESKTOP-Q50SISB\C\users\Bob\AppData\Local\Box\Box\logs\ Box\_Streem\_0\_2020-04-16.log

Go to Search > Find and in the “Find what:” field enter: [AddFile]

**Question**:

What’s the first file added to Box?

**Step 2:**

Open the following file in Notepad++: …\evidence-DESKTOP-Q50SISB\C\users\Bob\AppData\Local\Box\Box\logs\ Box\_Streem\_2\_2020-04-16.log

Go to Search > Find and in the “Find what:” field enter: [onCreateFile]

**Question**:

What four (4) files were created and at what time was each file created?

**Question**:

In the same log file as used in the prior question, scroll to the top and search for: [MicrosoftEdge.exe]

What document was opened [onOpenFile] by MicrosoftEdge.exe?

**Step 3:**

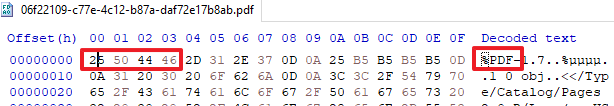
Open HxD hex editor.

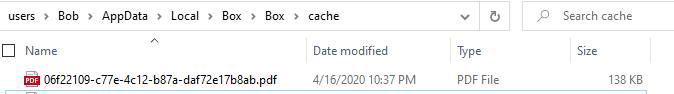
File > Open.

Navigate to: …evidence-DESKTOP-Q50SISB\C\users\Bob\AppData\Local\Box\Box\cache\ to see cached items.

Open each item one-by-one and look at the magic byte changing the file extension and opening the document to view the contents. For example, if you view the contents of 06f22109-c77e-4c12-b87a-daf72e17b8ab in HxD, you’ll see the magic byte: 25 50 44 46 2d (%PDF-), thus change the file name from 06f22109-c77e-4c12-b87a-daf72e17b8ab to 06f22109-c77e-4c12-b87a-daf72e17b8ab.pdf. Type to open the document in a PDF viewer to see the contents.

List of magic bytes: <https://en.wikipedia.org/wiki/List_of_file_signatures>



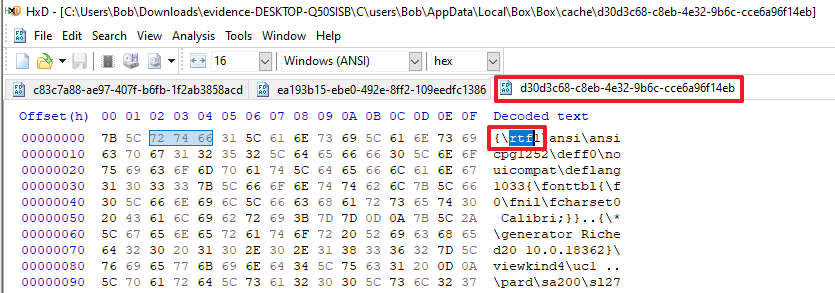


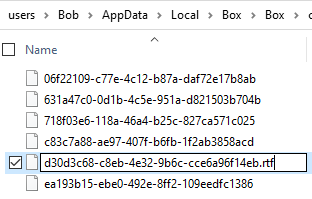
**Question**:

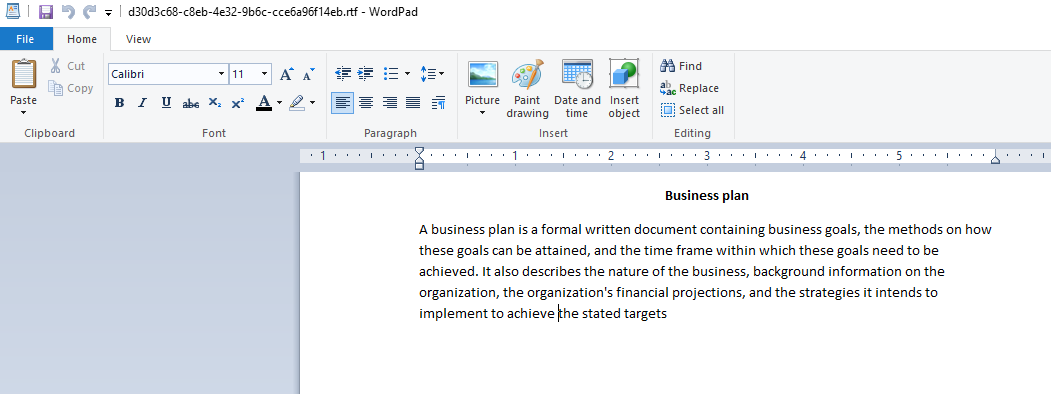
Which cached file is an RTF business plan?

**Answer**:

d30d3c68-c8eb-4e32-9b6c-cce6a96f14eb







**Question**:

Which cached document seems to have evidence that Bob may have violated his non-solicit clause and poached clients?

**Step 4:**

Open DBrowser for SQLite and open the …\Box\Box\data\streemfs.db database.

Select the cachefiels table.

Locate the row containing a cacheDataId that equals to the evidence found in the …\Box\Box\cache\ directory that may prove Bob poached clients.

**Question**:

What is the inodeId and age (in Los Angles)? The cache age will determine when the item was first cached locally to start our timeline.

**Step 5:**

Change the tables in the streemfs.db to fsnodes.

Look at the inodeId column and find the row for the cached document indicating client solicitation found in prior steps.

**Question:**

What is the actual filename, createdAtTimestamp (Los Angeles), modifiedAtTimestamp (Los Angeles), and accessedAtTimestamp (Los Angeles)?

NOTE: If the timestamps don’t make sense, that can be expected. Different cloud file storage solutions will preserve/inherit different file attributes. In the case of Box, these timestamps are accurate, but this gets into a topic outside the scope of this workshop. In short, we stumbled upon evidence of “file copy”. In a NTFS filesystem, the “file copy” action will modify the file properties as such:

* Modified Date = inherited from the original/source file
* Accessed Date = changed on the second file (however this cannot always be trusted)
* Creation Date = changed on the second file

Images illustrating how a file modified time inherits the creation time of the source file can be found in the detailed walkthrough.

|  |  |
| --- | --- |
| **inodeId** |  |
| **filename** |  |
| **createdAtTimestamp** |  |
| **modifiedAtTimestamp** |  |
| **accessedAtTimestamp** |  |

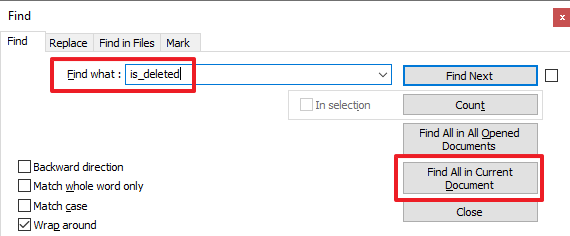
**Step 6**:

Open Box-2.13.518.log (located in …\evidence-DESKTOP-Q50SISB\C\users\Bob\AppData\Local\Box\Box\logs\) in Notepad++.

Go to Search > Find.

In the “Find what:” field, type: is\_deleted

Press the “Find all in current document” button.



The first few entries appears to be changes in the name of Bob’s resignation letter.

**Question**:

What’s more concerning is what happens between 6:00AM – 6:30AM. What file name stands out to you in your investigation? What’s the time stamp of the event?

**DETAILED LAB WALKTHROUGH**

**Step 1:**

Open the following file in Notepad++: …\evidence-DESKTOP-Q50SISB\C\users\Bob\AppData\Local\Box\Box\logs\ Box\_Streem\_0\_2020-04-16.log

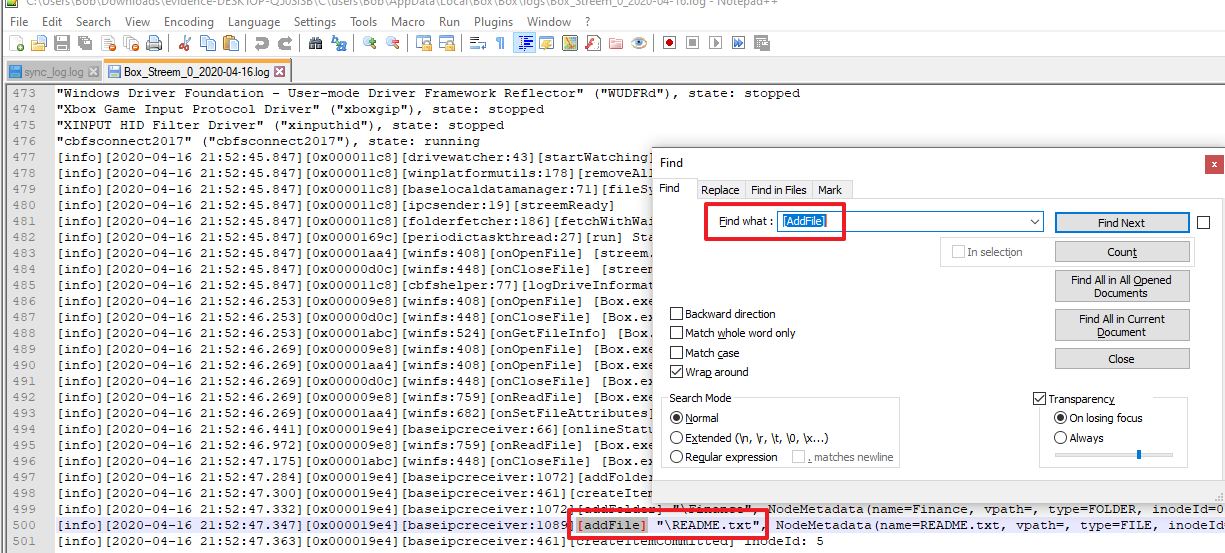
Go to Search > Find and in the “Find what:” field enter: [AddFile]

**Question**:

What’s the first file added to Box?

**Answer**:

README.txt



**Step 2:**

Open the following file in Notepad++: …\evidence-DESKTOP-Q50SISB\C\users\Bob\AppData\Local\Box\Box\logs\ Box\_Streem\_2\_2020-04-16.log

Go to Search > Find and in the “Find what:” field enter: [onCreateFile]

**Question**:

What four (4) files were created and at what time was each file created?

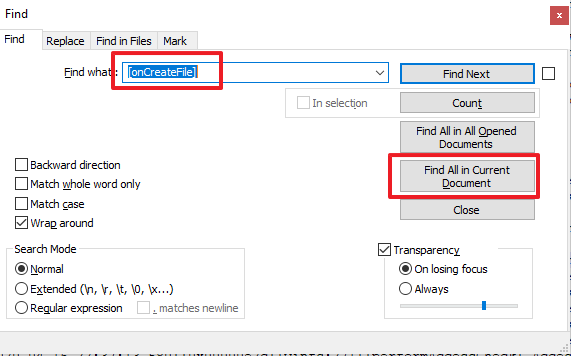
**Answer**:

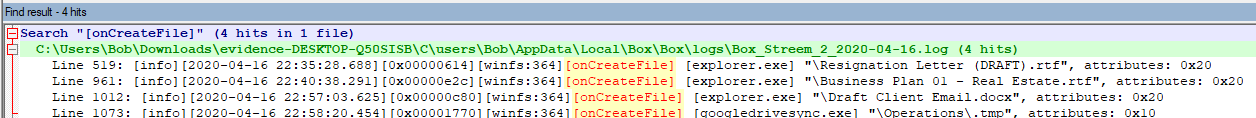
Line 519: [info][2020-04-16 22:35:28.688][0x00000614][winfs:364][onCreateFile] [explorer.exe] "\Resignation Letter (DRAFT).rtf", attributes: 0x20

Line 961: [info][2020-04-16 22:40:38.291][0x00000e2c][winfs:364][onCreateFile] [explorer.exe] "\Business Plan 01 - Real Estate.rtf", attributes: 0x20

Line 1012: [info][2020-04-16 22:57:03.625][0x00000c80][winfs:364][onCreateFile] [explorer.exe] "\Draft Client Email.docx", attributes: 0x20

Line 1073: [info][2020-04-16 22:58:20.454][0x00001770][winfs:364][onCreateFile] [googledrivesync.exe] "\Operations\.tmp", attributes: 0x10





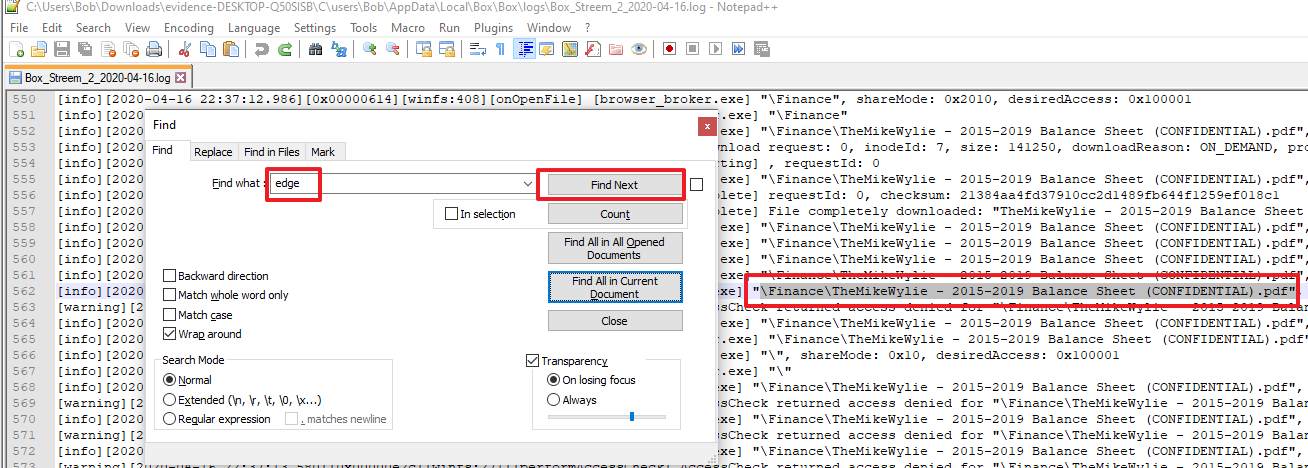
**Question**:

In the same log file as used in the prior question, scroll to the top and search for: [MicrosoftEdge.exe]

What document was opened [onOpenFile] by MicrosoftEdge.exe?

**Answer**:

“\Finance\TheMikeWylie - 2015-2019 Balance Sheet (CONFIDENTIAL).pdf"



**Step 3:**

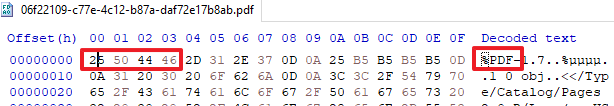
Open HxD hex editor.

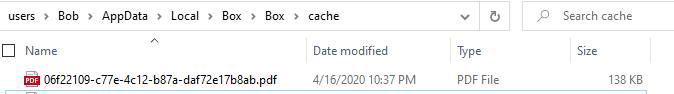
File > Open.

Navigate to: …evidence-DESKTOP-Q50SISB\C\users\Bob\AppData\Local\Box\Box\cache\ to see cached items.

Open each item one-by-one and look at the magic byte changing the file extension and opening the document to view the contents. For example, if you view the contents of 06f22109-c77e-4c12-b87a-daf72e17b8ab in HxD, you’ll see the magic byte: 25 50 44 46 2d (%PDF-), thus change the file name from 06f22109-c77e-4c12-b87a-daf72e17b8ab to 06f22109-c77e-4c12-b87a-daf72e17b8ab.pdf. Type to open the document in a PDF viewer to see the contents.

List of magic bytes: <https://en.wikipedia.org/wiki/List_of_file_signatures>



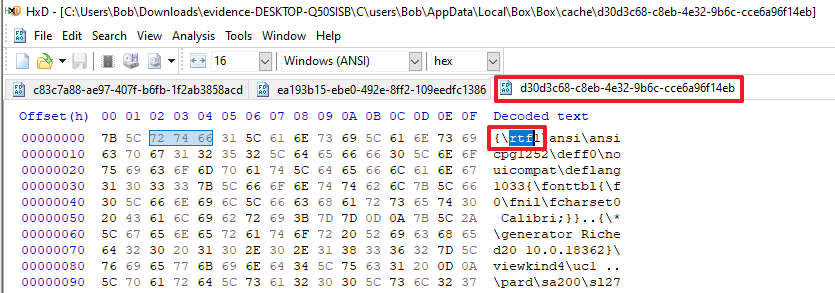


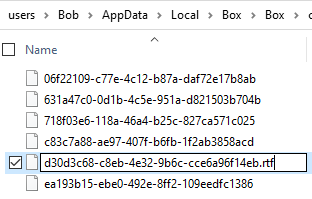
**Question**:

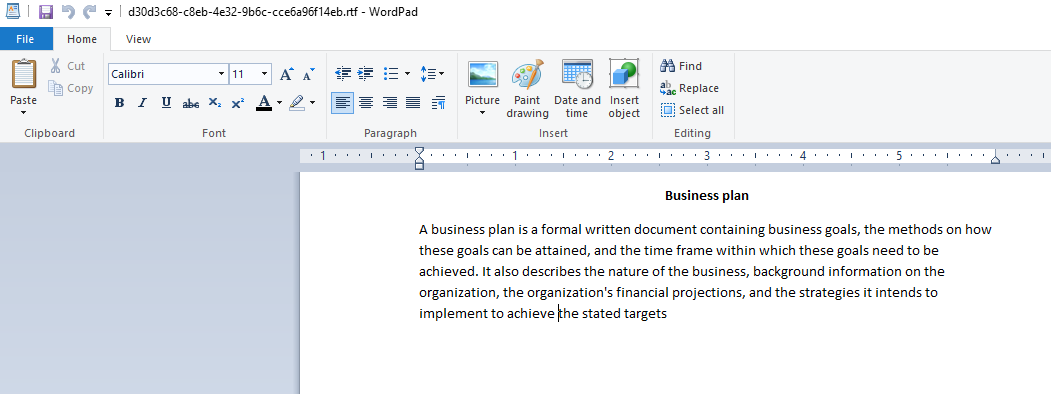
Which cached file is an RTF business plan?

**Answer**:

d30d3c68-c8eb-4e32-9b6c-cce6a96f14eb





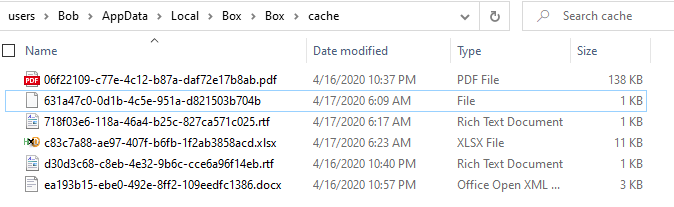


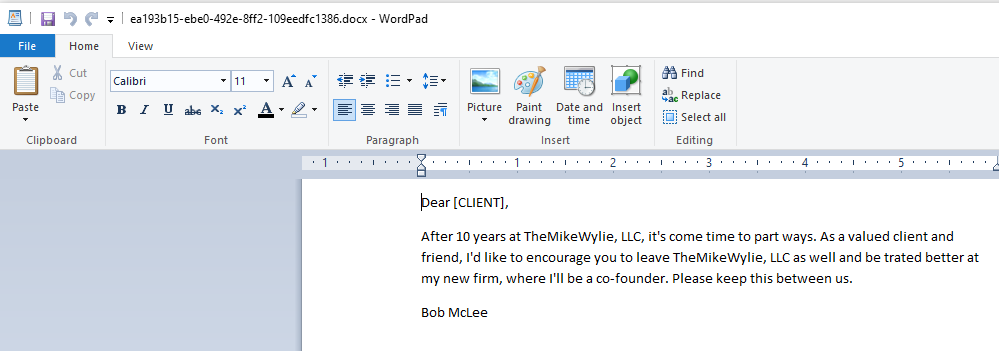
**Question**:

Which cached document seems to have evidence that Bob may have violated his non-solicit clause and poached clients?

**Answer**:

ea193b15-ebe0-492e-8ff2-109eedfc1386.docx





**Step 4:**

Open DBrowser for SQLite and open the …\Box\Box\data\streemfs.db database.

Select the cachefiels table.

Locate the row containing a cacheDataId that equals to the evidence found in the …\Box\Box\cache\ directory that may prove Bob poached clients.

**Question**:

What is the inodeId and age (in Los Angles)? The cache age will determine when the item was first cached locally to start our timeline.

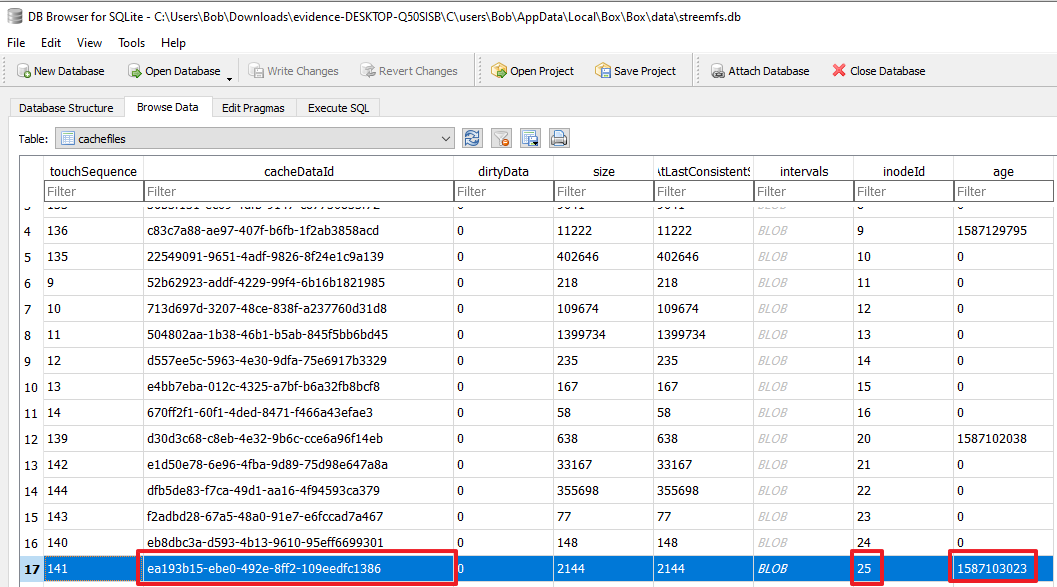
**Answer**:

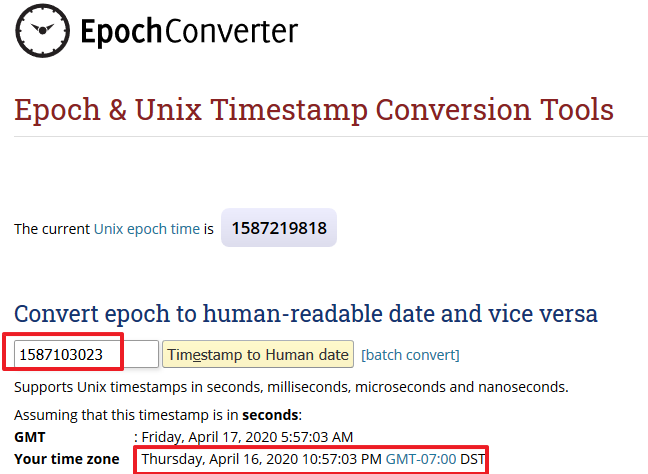
inodeId = 25

age = 1587103023

GMT: Friday, April 17, 2020 5:57:03 AM

Los Angeles: Thursday, April 16, 2020 10:57:03 PM GMT-07:00 DST





**Step 5:**

Change the tables in the streemfs.db to fsnodes.

Look at the inodeId column and find the row for the cached document indicating client solicitation found in prior steps.

**Question:**

What is the actual filename, createdAtTimestamp (Los Angeles), modifiedAtTimestamp (Los Angeles), and accessedAtTimestamp (Los Angeles)?

NOTE: If the timestamps don’t make sense, that can be expected. Different cloud file storage solutions will preserve/inherit different file attributes. In the case of Box, these timestamps are accurate, but this gets into a topic outside the scope of this workshop. In short, we stumbled upon evidence of “file copy”. In a NTFS filesystem, the “file copy” action will modify the file properties as such:

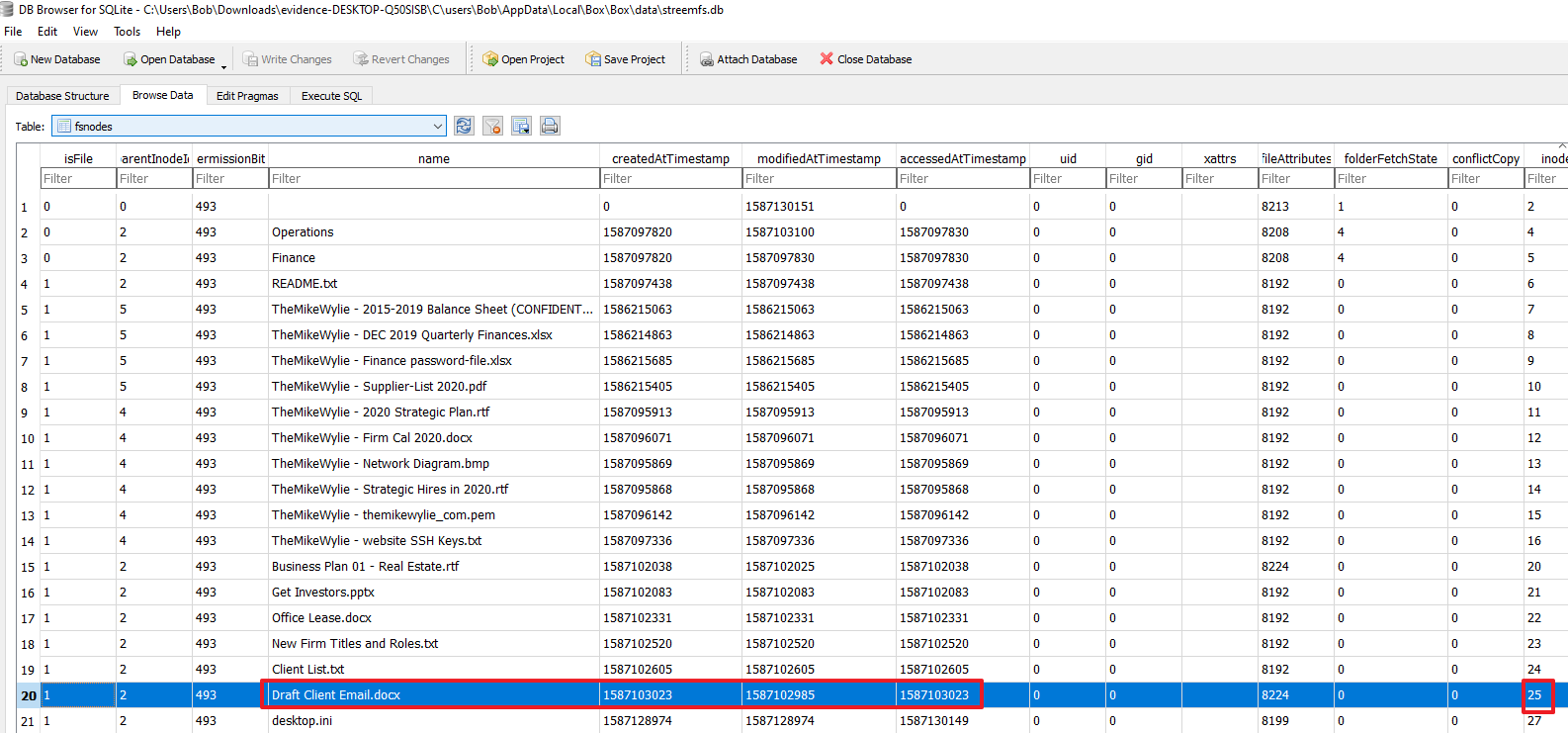
* Modified Date = inherited from the original/source file
* Accessed Date = changed on the second file (however this cannot always be trusted)
* Creation Date = changed on the second file

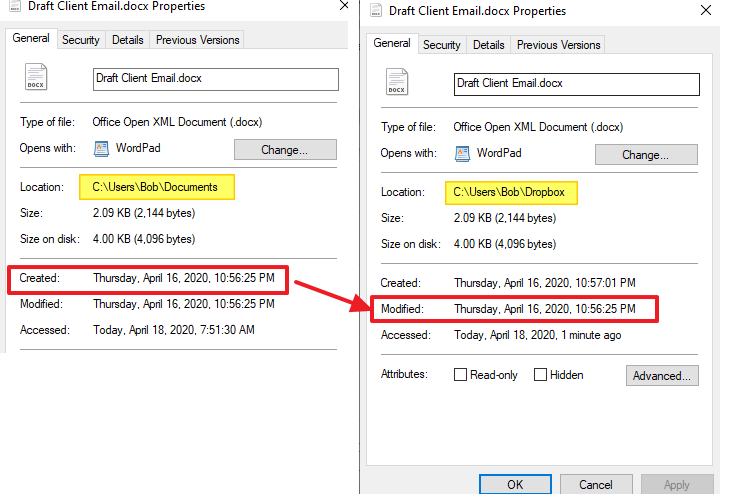
Images illustrating how a file modified time inherits the creation time of the source file can be found in the detailed walkthrough.

|  |  |
| --- | --- |
| **inodeId** |  |
| **filename** |  |
| **createdAtTimestamp** |  |
| **modifiedAtTimestamp** |  |
| **accessedAtTimestamp** |  |

**Answer**:

|  |  |
| --- | --- |
| **inodeId** | 25 |
| **filename** | Draft Client Email.docx |
| **createdAtTimestamp** | 1587103023 (Thursday, April 16, 2020 10:57:03 PM GMT-07:00 DST) |
| **modifiedAtTimestamp** | 1587102985 (Thursday, April 16, 2020 10:56:25 PM GMT-07:00 DST) |
| **accessedAtTimestamp** | 1587103023 (Thursday, April 16, 2020 10:57:03 PM GMT-07:00 DST) |





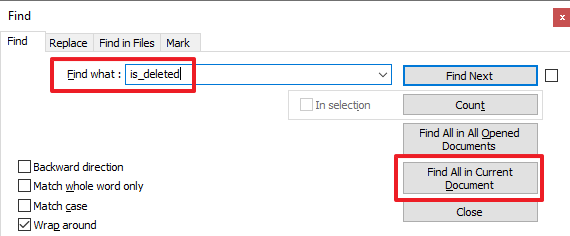
**Step 6**:

Open Box-2.13.518.log (located in …\evidence-DESKTOP-Q50SISB\C\users\Bob\AppData\Local\Box\Box\logs\) in Notepad++.

Go to Search > Find.

In the “Find what:” field, type: is\_deleted

Press the “Find all in current document” button.



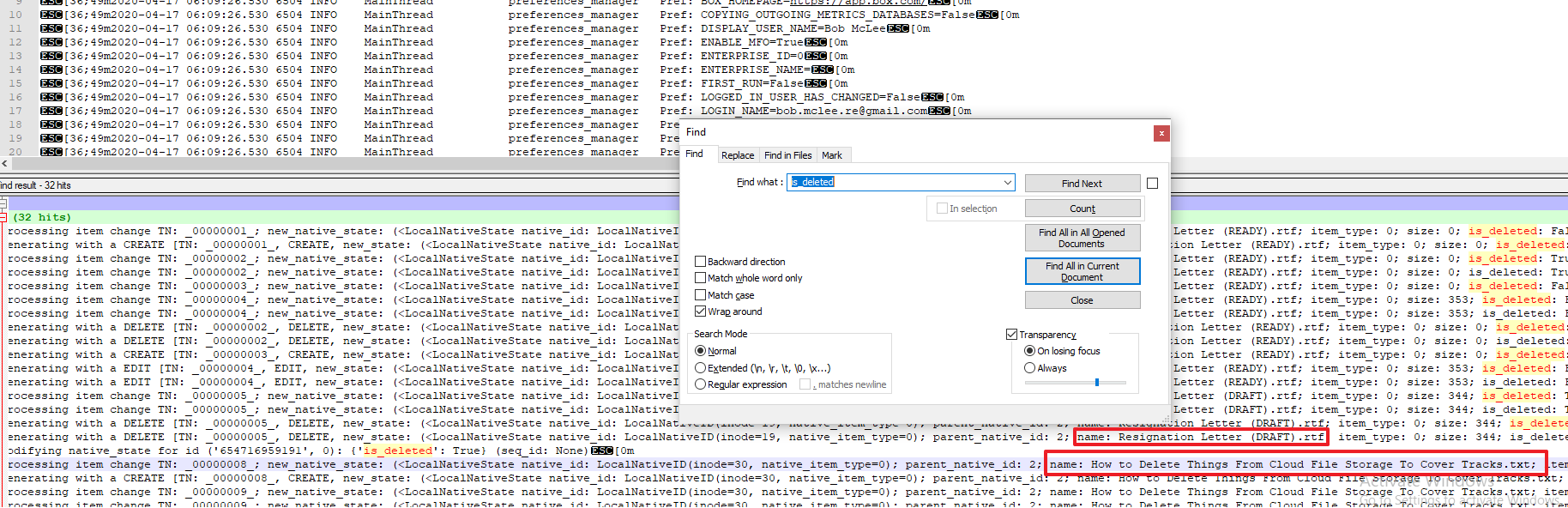
The first few entries appears to be changes in the name of Bob’s resignation letter.

**Question**:

What’s more concerning is what happens between 6:00AM – 6:30AM. What file name stands out to you in your investigation? What’s the time stamp of the event?

**Answer**:

Line 318  
2020-04-17 06:26:31.575 6504 INFO LocalFSMonitor fs\_monitor Processing item change TN: \_00000008\_; new\_native\_state: (<LocalNativeState native\_id: LocalNativeID(inode=30, native\_item\_type=0); parent\_native\_id: 2; name: How to Delete Things From Cloud File Storage To Cover Tracks.txt; item\_type: 0; size: 0; is\_deleted: False; syncability: SYNCABLE; checksum: None; content\_created\_at: 1587129991; content\_updated\_at: 1587129991; attributes: set(); package\_folder\_transition: None>) based on scanned item StreemLocalScannedItem(scanned\_item\_type='NEW\_STATE', native\_id=LocalNativeID(inode=30, native\_item\_type=0), native\_state=<box.sync.adapter.local.local\_native\_state.LocalNativeState object at 0x000001EBEDAB8AE8>, path='\\How to Delete Things From Cloud File Storage To Cover Tracks.txt', old\_native\_state=None, stream\_position=17, key\_value\_pairs=None)[0m



**END OF LAB**