

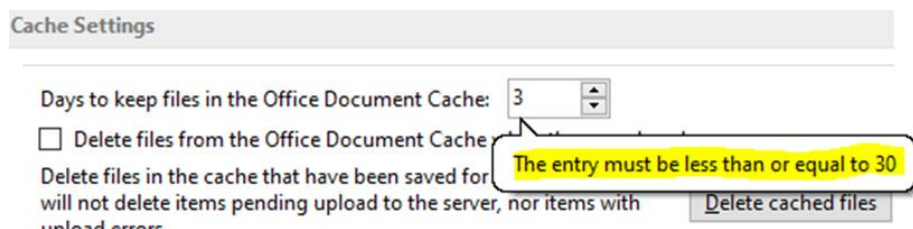
Office Document Cache (ODC)

"..If a user downloaded a 200-KB Microsoft Word document from a SharePoint 2010 document library and then changed just one character in a sentence, the single change between the two files is not saved; instead, two 200-KB files are saved in the content database.

.. When a user modifies one of these documents by using a Microsoft Office 2010 application, using the File Sync via SOAP over HTTP (MS-FSSHTTP) protocol locks portions of a file and downloads the file into the Office 2010 local file cache, the Office Document Cache (ODC). The ODC resides on the user's computer. The Office application opens the document from the ODC. When a user saves the document back to SharePoint, the Office application saves the document into the ODC and then uses the MS-FSSHTTP protocol to upload only the file differentials asynchronously in the background to the SharePoint server. Note: You can access and manage the ODC settings and features through the Upload Center, which is automatically installed with Office 2010."

**Source: "Exploring Microsoft SharePoint 2013: New Features & Functions" by Penelope Coventry.*

The ODC cache settings, by default, are set to delete the cache after 14 days. That value can be changed to anything between 1 and 30 days:



Cache Settings

Days to keep files in the Office Document Cache: 3

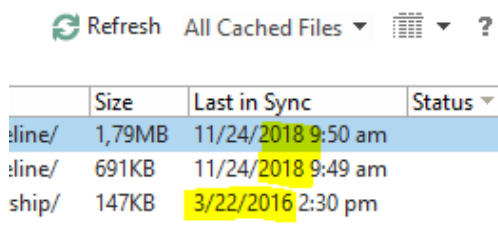
☐ Delete files from the Office Document Cache

Delete files in the cache that have been saved for
will not delete items pending upload to the server, nor items with
upload errors

The entry must be less than or equal to 30

Delete cached files

but that doesn't necessarily mean you won't find older files there:

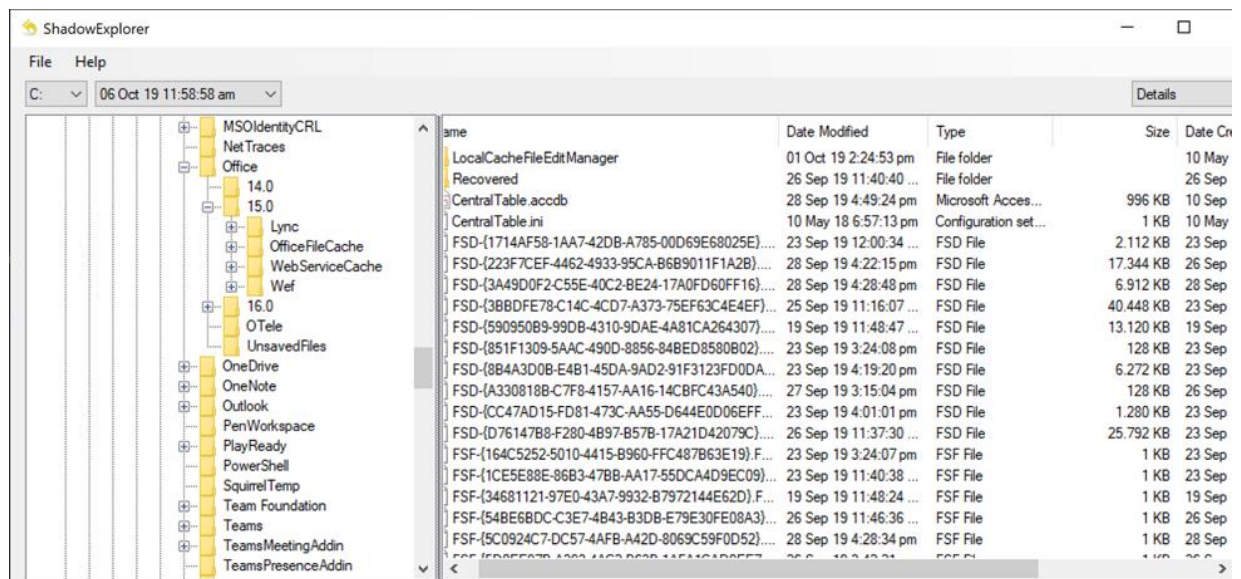


	Size	Last in Sync	Status
line/	1,79MB	11/24/2018 9:50 am	
line/	691KB	11/24/2018 9:49 am	
ship/	147KB	3/22/2016 2:30 pm	

This may be also be relevant: "Files older than the maximum number of days will be removed from the cache only when there are no changes pending upload."

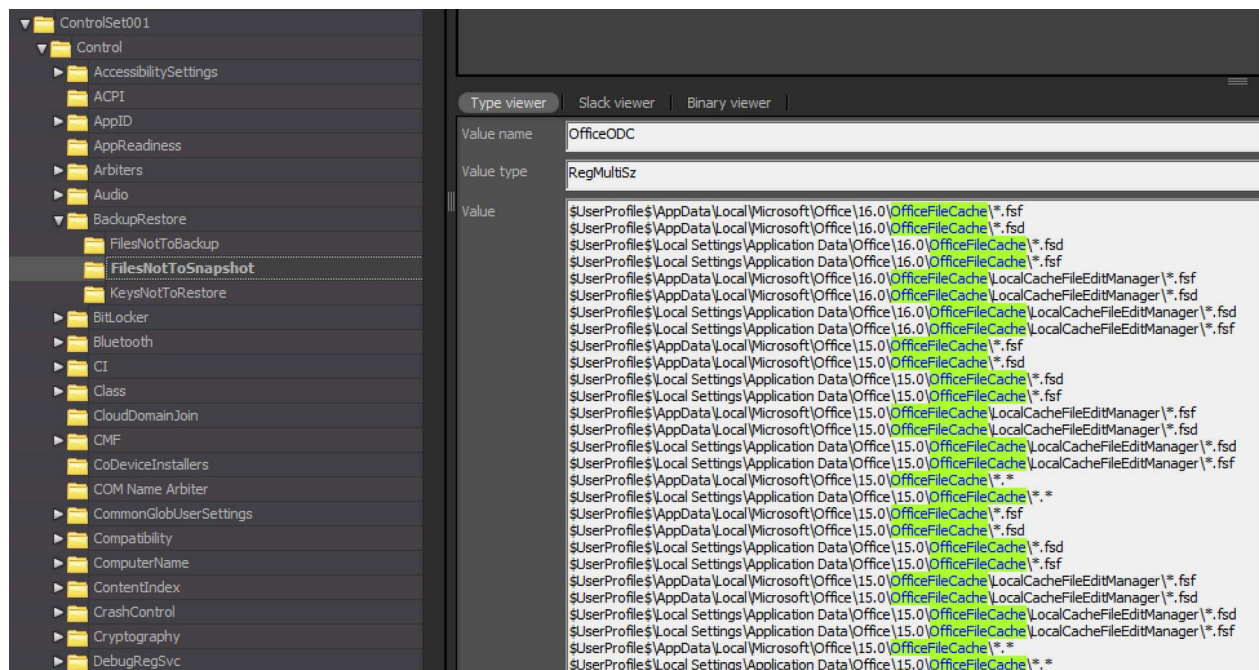
Source: <https://support.office.com/en-us/article/office-document-cache-settings-4b497318-ae4f-4a99-be42-b242b2e8b692>

Volume Shadow copies backup OfficeFileCache (at least in Windows 10 20H1 Insider's edition):



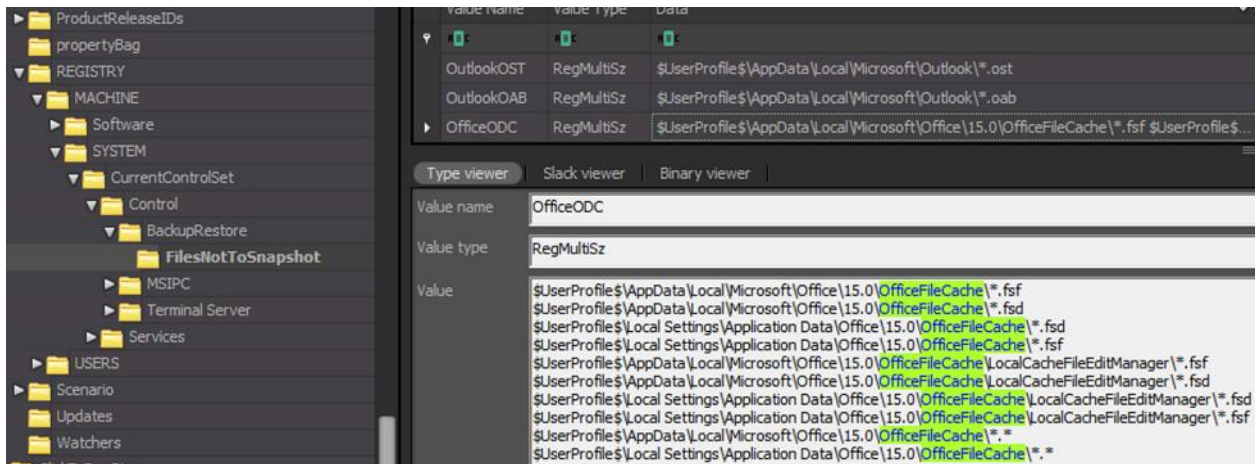
But that contradicts with the default registry settings, which exclude any FSF or FSD files from Snapshots:

in the SYSTEM hive at: "ControlSet001\Control\BackupRestore\FilesNotToSnapshot"



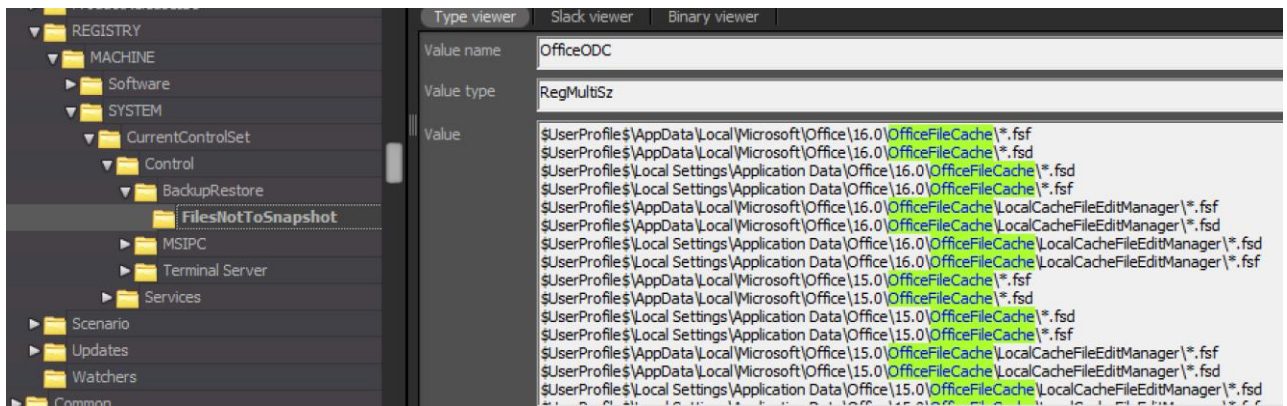
And in the SOFTWARE hive at:

"Microsoft\Office\15.0\ClickToRun\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot"



Of if it's Office 16 at

"Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot"



Another interesting thing is that a user has the ability to change the default location of the "OfficeFileCache" folder from "AppData\Local\Microsoft\Office\version\OfficeFileCache" either via a custom policy, or a registry setting:

If the following path exists In NTuser.dat, check the 'Value' of "msoridofficefilecachelocation":

"software\policies\microsoft\office\version\common\fileio"

source:

https://getadmx.com/?Category=Office2016&Policy=office16.Office.Microsoft.Policies.Windows::L_OfficeDocumentCacheLocation

Note: Also, a user may also manually rename or delete an OfficeFileCache folder. There are numerous forum posts related to OfficeFileCache size or Office Upload sync, problems mentioning this as a solution.

The Microsoft Office “OfficeFileCache” folder contents

1. The MS Access **CentralTable.accdb**
2. Files with extension **FSF**
3. Files with extension **FSD**

CentralTable.accdb

This database tracks all files opened or saved by MS Office applications to and from Onedrive or Sharepoint locations. It has the following 8 tables:

"CacheProperties",
"EventClients",
"EventMetaInfo"
"IncomingEvents",
"MasterFile",
"OutgoingEvents",
"ServerTarget",
"Subcache"

Of which the ‘Masterfile’ table is the most important. This tracks the MS Office documents opened or saved, the Microsoft account used (*email, MS ID etc.*), timestamps of the activity (download/upload/modification etc.), and the “FileEntryFileId” which is the GUID of the respective FSF filename:

FileEntryFileID (GUID)	DocumentLastModifiedTime	DocumentLastAccessedTime	Filename
5D0EE97B-A393-4AC2-B63B-1AFA1CAD9EE7	26/09/19: 15:42:22	27/09/19: 15:15:04	db.xlsx
54BE6BDC-C3E7-4B43-B3DB-E79E30FE08A3	26/09/19: 23:56:22	28/09/19: 16:22:12	Forensic Analysis of OOXML Documents.docx
5C0924C7-DC57-4AFB-A42D-8069C59F0D52	28/09/19: 16:28:35	07/10/19: 15:33:17	Forensic Analysis of OOXML Documents - EDidriksen.docx
24E83A39-9CD8-440A-A6D1-27B443216E55	16/10/19: 19:27:38	16/10/19: 17:48:32	FSD.docx
55A92A02-1DCA-4292-B335-5D459B9B80B8	23/09/19: 17:43:38	06/10/19: 16:19:46	58549343-App-V-Volume-Format-Specification.docx

FSF files

FSF could be dubbed as ‘File Store Filename’. A typical FSF filename looks like this:

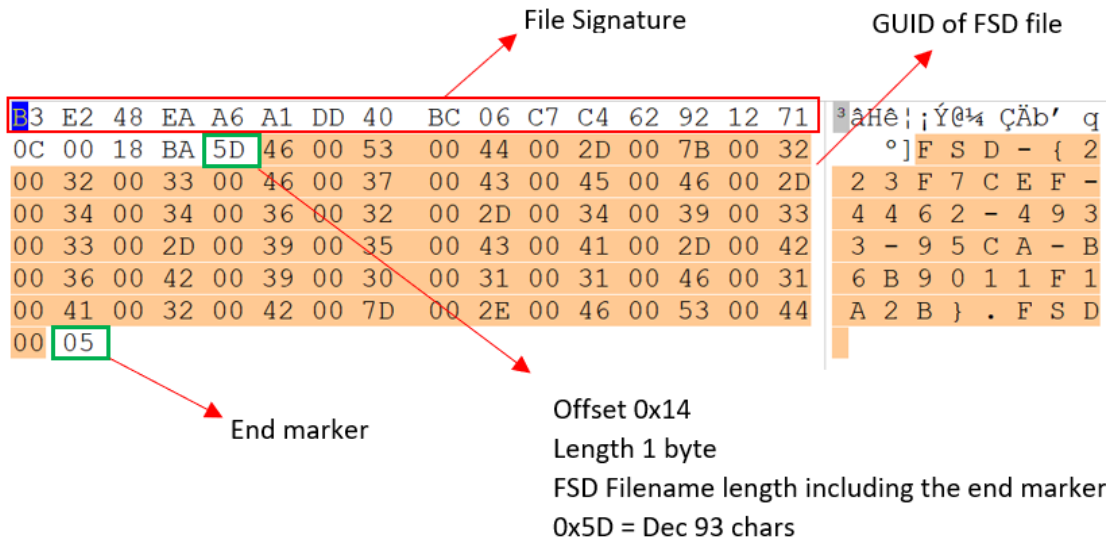
FSF-{54BE6BDC-C3E7-4B43-B3DB-E79E30FE08A3}.FSF



“FileEntryFileId” GUID

The FSF file signature is: 0x B3 E2 48 EA A6 A1 DD 40 BC 06 C7 C4 62 92 12 71

Each FSF file contains the GUID of an FSD file:



Typical FSF file sizes:

Office 15 = 114 bytes

Office 16+ = 122 bytes

The reason for the size difference, seems to be that with Office 16 and above the FSD filename has an extra 4 characters after the GUID (or 8 including \0x00), and looks like this:

FSD-{6693522D-931D-4198-9383-0B645ACF96E0}-0-1.FSD

FSD-{CAB9F2BD-B7B6-44FF-B399-FE1A8A9596EC}-0-1.FSD

FSD-{DD0F54C1-141D-474D-B082-FFBC4A0C99E9}-0-1.FSD

FSD Files

These could also be called 'File Store Data' files and are the files with the most interest. They are cache container files, holding the actual document file transferred (or to be transferred), in an unbelievably complex form.

A typical FSD filename looks like this:

Office 15 -> FSD-{223F7CEF-4462-4933-95CA-B6B9011F1A2B}.FSD

Office 16 -> FSD-{CAB9F2BD-B7B6-44FF-B399-FE1A8A9596EC}-0-1.FSD

As you can see, the above (Office 15) FSD filename is an exact match to the one contained in the FSF (screenshot above), so there is a 'link' pattern that looks like this:



With Office 16+, there is a change to this pattern. The FSD filename GUID matches the FSF filename GUID:

FSF Name	FSD Name
FSF-{0ECC9915-DC47-4B62-BE53-9445306DCD4F}.FSF	FSD-{0ECC9915-DC47-4B62-BE53-9445306DCD4F}-0-1.FSD
FSF-{1069C0BB-FDE0-4F35-A3FE-55018EEC8B53}.FSF	FSD-{1069C0BB-FDE0-4F35-A3FE-55018EEC8B53}-0-1.FSD
FSF-{16E8762F-4488-44CF-A17C-0F7446CDC3D4}.FSF	FSD-{16E8762F-4488-44CF-A17C-0F7446CDC3D4}-0-2.FSD
FSF-{21F43D1E-44FD-4C47-B467-C79326A52240}.FSF	FSD-{21F43D1E-44FD-4C47-B467-C79326A52240}-0-1.FSD
FSF-{241A70A6-2D08-43AB-8391-C83A911CB54C}.FSF	FSD-{241A70A6-2D08-43AB-8391-C83A911CB54C}-0-1.FSD
FSF-{40A11809-3C0B-4A0E-AF8F-350BD995E390}.FSF	FSD-{40A11809-3C0B-4A0E-AF8F-350BD995E390}-0-1.FSD
FSF-{4C327AC4-24A0-459D-818C-3E81516F1135}.FSF	FSD-{4C327AC4-24A0-459D-818C-3E81516F1135}-0-1.FSD
FSF-{75CCC875-DF13-4432-81CF-B28E5C0DF206}.FSF	FSD-{75CCC875-DF13-4432-81CF-B28E5C0DF206}-0-1.FSD
FSF-{88D7CAF6-C0F8-48C4-A79B-D19E3EB6DE14}.FSF	FSD-{88D7CAF6-C0F8-48C4-A79B-D19E3EB6DE14}-0-1.FSD
FSF-{902886A3-DAD5-471C-9AA4-AF5B68C4768A}.FSF	FSD-{902886A3-DAD5-471C-9AA4-AF5B68C4768A}-0-1.FSD
FSF-{BB5D0745-7BA1-445F-8006-90EC33584617}.FSF	FSD-{BB5D0745-7BA1-445F-8006-90EC33584617}-0-1.FSD
FSF-{C5B6638E-280F-456D-81C6-826B5E6B89C6}.FSF	FSD-{C5B6638E-280F-456D-81C6-826B5E6B89C6}-0-1.FSD
FSF-{E27A2994-5BE8-47EF-9DE9-975CAF2A82C6}.FSF	FSD-{E27A2994-5BE8-47EF-9DE9-975CAF2A82C6}-0-1.FSD
FSF-{F1DF4645-4617-47D3-99D3-E8BEBA10C29E}.FSF	FSD-{F1DF4645-4617-47D3-99D3-E8BEBA10C29E}-0-1.FSD

The FSD file signature is 0x 0C 83 D2 91 AE 1B D4 4D AA 65 46 79 FB DA DD 7A. There is no specific marker indicating the end of the file. However, we can get the byte length (size) of an FSD at offset 0xAC for 4 bytes in Little Endian, which helps if one wants to carve out a deleted FSD, hoping it is not fragmented.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	0C	83	D2	91	AE	1B	D4	4D	AA	65	46	79	FB	DA	DD	7A
00000010	CD	55	EA	3C	97	F6	CB	4A	96	3F	C5	8E	C7	96	32	79
00000020	53	2C	96	B6	D2	58	B3	46	AB	FC	14	46	61	CF	B5	71
00000030	05	00	00	00	05	00	00	00	05	00	00	00	05	00	00	00
00000040	FSD file signature							FF	FF	00	00	00	00	03	56	C7
00000050	FC	1D	7D	40	97	37	E3	E6	FA	A0	B9	7D	B1	00	00	00
00000060	00	00	00	00	E6	FA	1F	D8	5C	05	F3	43	A7	2D	C7	62
00000070	83	7B	7D	65	00	FD	0D	01	00	00	00	00	00	04	00	00
00000080	03	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	00	00	00	00
00000090	00	00	00	00	00	00	00	00	28	5D	0E	01	00	00	00	00
000000A0	00	02	00	00	00	00	00	00	00	04	00	00	00	00	00	00
000000B0	00	00	00	00	04	00	00	00	F5	3F	A1	0F	F5	3F	A1	0F
000000C0	F5	3F	A1	0F	F5	3F	A1	0F	51	03	00	00	00	00	00	00
000000D0	EC	22	0C	01	00	00	00	00	00	00	00	00	00	00	00	00

0x00000F01 =

0x010F0000 in LE

HEX	10F 0000
DEC	17.760.256

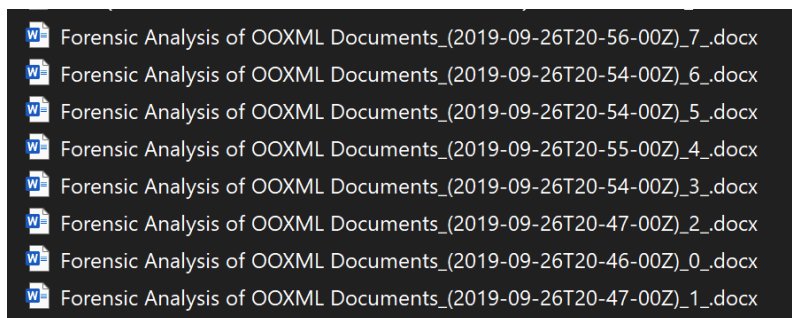
The above file length value matches the Filesystem reported file size:

FSD-(D76147B8-F280-4B97-B57B-17A21D42079C).FSD	25.792 KB
FSD-(223F7CEF-4462-4933-95CA-B6B9011F1A2B).FSD	17.344 KB
FSD-(3A49D0F2-C55E-40C2-BE24-17A0FD60FF16).FSD	13.888 KB

(17.344KB * 1024 = 17.760.256 bytes)

Each FSD file contains any revisions the user made, as long as they were made on the same Computer where the FSD resides. These revisions can be recovered:

Exporting to: ..\ODCrecon\Forensic Analysis of OOXML Documents_(2019-09-26T20-46-00Z)_0_.docx
Exporting to: ..\ODCrecon\Forensic Analysis of OOXML Documents_(2019-09-26T20-47-00Z)_1_.docx
Exporting to: ..\ODCrecon\Forensic Analysis of OOXML Documents_(2019-09-26T20-47-00Z)_2_.docx
Exporting to: ..\ODCrecon\Forensic Analysis of OOXML Documents_(2019-09-26T20-54-00Z)_3_.docx
Exporting to: ..\ODCrecon\Forensic Analysis of OOXML Documents_(2019-09-26T20-55-00Z)_4_.docx
Exporting to: ..\ODCrecon\Forensic Analysis of OOXML Documents_(2019-09-26T20-54-00Z)_5_.docx
Exporting to: ..\ODCrecon\Forensic Analysis of OOXML Documents_(2019-09-26T20-54-00Z)_6_.docx
Exporting to: ..\ODCrecon\Forensic Analysis of OOXML Documents_(2019-09-26T20-56-00Z)_7_.docx



If a document stored in OneDrive was opened from a workstation for the first time, read and closed, then a new FSD would be created on that workstation, which would contain only the latest version of that document.

Things to note:

A OneDrive sync error can cause a massive dump of FSD files – in my case, I got a dump of 940+ FSDs from a Sharepoint sync error. Removing a synched Sharepoint folder from 'OneDrive for business' almost instantly deleted ~600 FSD files from the 'OfficeFileCache' folder.

In the 'Masterfile' table of the 'CentralTable.accdb', the items under the field 'DocumentUserTypedUrl' were opened by the user. If there are entries in the 'DisplayURL' field but with null 'DocumentUserTypedUrl' values, these could have been created by OneDrive sync. I got a lot of such entries when I tried to open a 'Team' shared folder from Sharepoint with Word 2013. These files were also listed in the 'OutgoingEvents' table.

Further artifacts

Identities

in the user's NTuser.dat at:

"Software\Microsoft\office\{version}\Common\Roaming\Identities"

you can find a list of MS IDs in the system and available to MS Office. Any IDs linked to MS Office can hold more information in other sub-keys. Under each ID key, you may find the following info:

EmailAddress	RegSz
FriendlyName	RegSz
Initials	RegSz
LibraryType	RegDw...
IdP	RegDw...
ProviderId	RegSz
FlowUrl	RegSz
CompanyName	RegSz
PhoneNumber	RegSz
ProfileUrl	RegSz
Picture	RegSz
LastName	RegSz
FirstName	RegSz
FederationProvider	RegSz
SignInName	RegSz

Roaming Identities ListItems

Further related artifacts can be found at:

`"Software\Microsoft\office\{version}\Common\Roaming\Identities\{MS Id}\Settings*\{00000000-0000-0000-0000-000000000000}\ListItems*\{*\}"`

You can find entries like this:

LastModified	RegBinary	E3-07-0A-00-00-00-06-00-11-0...
ItemKey	RegBinary	68-00-74-00-74-00-70-00-73-00...
ItemData	RegBinary	3C-00-4D-00-65-00-74-00-61-0...
SortKey	RegQword	132141505460000000
LastOperation	RegBinary	00-00-00-00

Where "LastModified" Value is a [128-bit System](#) Timestamp:

E307 => 07E3 = 2019 (year)
0A00 => 000A = 10 (Month)
0300 => 0003 = 03 (day of week -> Wednesday)
1000 => 0010 = 16 (day)
0A00 => 000A = 10 (Hour)
0300 => 0003 = 03 (Minute)
3200 => 0032 = 50 (Seconds)
BE03=> 03BE = 958 (milliseconds)

the "ItemKey" Value contains the Document URL,
and the "ItemData" Value contains an XML with metadata:

▼ Metadata	
ServiceName	WLINBOX_SKYDRIVE
DocOwnerID	
FriendlyPath	
DocTitle	Forensic Analysis of OOXML Documents
DocExtension	docx
FileSizeInBytes	6825021
ResourceId	13529
StorageHost	1

There is one entry for each file/folder accessed from OneDrive/Sharepoint by MS Office applications.

The "SortKey" timestamp in the above entry

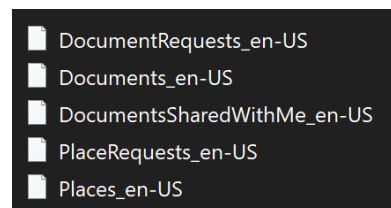
`w32tm /ntte 132141505460000000 => 28 Sep 19 4:22:26 pm`

matches the "DocumentAccessedTime" of the 'Masterfile' table in the dB:

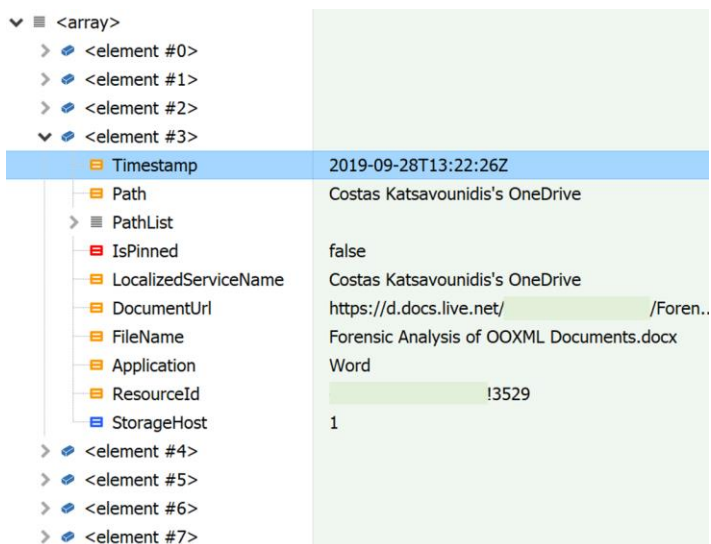
DocumentLastAccessedTime	Filename
27/09/19: 15:15:04	db.xlsx
28/09/19: 16:22:12	Forensic Analysis of OOXML Documents.docx
07/10/19: 15:33:17	Forensic Analysis of OOXML Documents - EDidriksen.docx

MruServiceCache

In MS Office 16 and above (Office 2016, 2019, 365), at the location:
 “AppData\Local\Microsoft\Office\16.0\MruServiceCache\{MS Id}\{MS Office app}” you may find any of these files:



which are JSON files with no file extension. Each one is updated when the respective MS Office app (e.g. Word) - linked to a Microsoft account - starts, and contains the Most Recently Used cloud stored ooxml (*docx or pptx or xlsx etc.*) files:



The above “Documents_en-US” shows the Timestamp of the .docx file we’ve seen in the previous locations. This is the last time this file was accessed. Note, that this JSON file was in a different computer which did not access this .docx document.

BackstageInAppNavCache

Backstage is Microsoft’s term for the interface where you can load recently accessed documents before picking a document and after loading Microsoft Office program. This location was

described at <http://www.learndfir.com/2018/10/18/daily-blog-510-office-2016-backstage-artifacts/>.

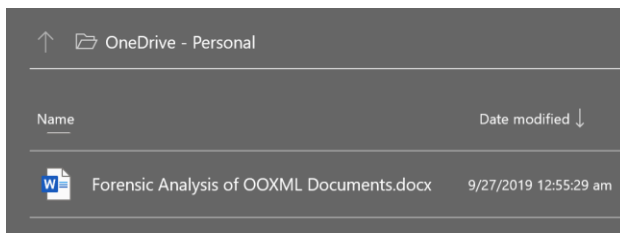
Only in Office 16 and above, at the location:

"AppData\Local\Microsoft\Office\16.0\BackstageInAppNavCache\{MS Id}"

you can find JSON files in the form of:

FD482C0888392B541C2485223D7B782DF834B4D14A0E6FEB99F6D65BBCAB87D4.json

Listing all available files at each location as seen from the application's Open File screen:



And the contents of the JSON file look like this:

LCID	#	1033
ContainerUrl	T	D:\\Costas\\OneDrive
ContainerResourceId	T	
Metadata		
FolderCreationAllowed	B	true
FileCreationAllowed	B	true

Url	T	D:\\Costas\\OneDrive\\Forensic Analysis of OOXML Documents.docx
DisplayName	T	Forensic Analysis of OOXML Documents.docx
Author	T	
ResourceId	T	
RootResourceId	T	
LastModified	#	132140085290000000
SharingLevelDescription	T	
OneNoteItem	B	false

"LCID", which is often used in MS Office applications, is the language identifier. In this case:

1033 = "English United States en-us "**

**Source: <https://docs.microsoft.com/en-us/deployoffice/office2016/language-identifiers-and-optionstate-id-values-in-office-2016>

The "LastModified" timestamp is Windows Filetime:

w32tm /ntte 132140085290000000 => 27 Sep 19 12:55:29 am