## An examination of Win10 ActivitiesCache.db database

Windows Timeline, is a new feature of Windows 10 introduced with version 1803. It is part of the Connected Devices Platform

- The Connected Devices Platform Service, is a Windows service that provides a way for devices \_ such as PC's and smartphones to discover and send messages between each other.
- Connected Devices Platform Service (CDPSvc) Defaults in Windows 10. -

and the Microsoft Graph's Cross-device experience (Project Rome).

The CDP settings for the Current User are stored in the registry at: NTUSER.DAT -> 'Software\Microsoft\Windows\CurrentVersion\CDP'

> 📙 Clip

Name	Туре	Data			
(Default)	REG_SZ	(value not set)			
CdpSessionUserAuthzPolicy	REG_DWORD	0x0000001 (1)			
CdpUserSettingsVersion	REG_SZ	RS4			
nableRemoteLaunchToast	REG_DWORD	0x0000001 (1)			
nearShareChannelUserAuthzPolic	y REG_DWORD	0x00000000 (0)			
nomeSdkChannelUserAuthzPolic	REG_DWORD	0x0000001 (1)			
and					
CapabilityAccessManager	<ul> <li>Name</li> </ul>				
✓	(Default)				
📙 SettingsPage	100 BluetoothLastD	BluetoothLastDisabledNearShare			
ClickNote	111 NearShareChar	nell IserAuthzPolicy			

11 NearShareChannelUserAuthzPolicy

(value not set) 0x0000000 (0) 0x0000001 (1)

Data

REG\_DWORD

## Before Windows 10 version 1803

The service and the 'ActivitiesCache.db' database existed before the 1803 upgrade (May 2018), but with limited functionality. Another possibly related\* activity store location is at: 'Software\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\\$\$ wind ows.data.taskflow.shellactivities\Current'

\*(considering that the current ActivitiesCache.db uses taskflow to retrieve device information as seen further below in this document)

🔻 🚞 Cache	0	1	2018-05-10 13:57:42
▼ 🚞 DefaultAccount			2018-05-17 20:24:23
\$\$windows.data.bluelightreduction.bluelightreductionstate			2018-05-10 13:57:42
\$\$windows.data.bluelightreduction.settings			2018-05-10 13:57:42
\$\$windows.data.calling.callfavorites			2018-05-10 14:03:05
\$\$windows.data.calling.callhistory			2018-05-10 14:03:05
\$\$windows.data.curatedtilecollection.rootcollection			2018-05-10 13:57:42
▶ 🚞 \$\$windows.data.messaging.settings			2018-05-10 14:03:05
\$\$windows.data.notifications.quiethourssettings			2018-05-10 13:57:48
\$\$windows.data.placeholdertilecollection			2018-05-10 13:57:42
\$\$windows.data.placeholdertilecollectionlocal			2018-05-10 13:57:42
\$\$windows.data.platform.partitioning.activepartitions			2018-05-10 13:58:00
\$\$windows.data.platform.partitioning.systempartitionindex			2018-05-10 13:58:00
▶ 🚞 \$\$windows.data.signals.registrations		1	-05-10 13:58:16
🔻 🚞 \$\$windows.data.taskflow.shellactivities			2013-05-10 13:57:42
🚞 Current			2018-05-10 13:57:42
\$\$windows.data.unifiedtile.localstartglobalproperties			2018-05-10 13:57:42

where there is a value named 'Data':

	Value	Valu	Da	ta														•	Value Slack
۴																			
			02	-00-0	0-00	-D0-E	D-C/	-EB-	63-E8	3-D3-	01-0	0-00-	00-00	)-43-	42-0	1-00-	CB-0		00-00-00-00-00-00-00-00-00-00
_				-	10	_	_	_	_	_	_	=	-	_	_	_	_	_	
T	ype viewe	r Sla	ack v	iewer															
		00	01	02	03	04	05	06	07	08	09	0A	0B	00	0 D	0 E	0 F	10	
00	000000	02	00	00	00	DO	ED	CA	EB	63	E8	D3	01	00	00	00	00	43	Đí ÊēcèÓ C
00	000011	42	01	00	CB	0A	0A	B5	03	D2	0A	30	4D	00	69	00	63	00	B., Ē., μ. Ò. ΟΜί. c.
00	000022	72	00	6F	00	73	00	6F	00	66	00	74	00	2 E	00	4D	00	69	r.o.s.o.f.tMi
00	000033	00	63	00	72	0.0	6F	00	73	00	6F	00	66	00	74	00	53	00	. c. r. o. s. o. f. t. S.
00	000044	74	00	69	00	63	00	6 B	00	79	00	4 E	00	6 F	00	74	00	65	t. i. c. k. y. N. o. t. e
00	000055	00	73	00	5F	00	38	00	77	00	65	00	6B	00	79	00	62	00	. s 8. w. e. k. y. b.

Its value is in hex and it seems to hold interesting information, including the Filetime of last update (which corresponds to the Last Write Timestamp of the registry key).

If Windows is updated to version 1803, this 'log' stops being updated. This can be checked by looking in the SYSTEM hive at the Setup key like:

**Source OS (Updated on 3/25/2018 01:40:42)**Source OS (Updated on 5/10/2018 14:50:04)

## In that case, interestingly,

									Ļ														
Offset	0	1	2	3	4	- 5	6	7	8	9	10	11	12	13	14	15			AN	SI	AS	3CJ	ΓI
00000000	02	00	00	00	D0	ED	CA	EB	63	E8	D3	01	00	00	00	00		Ð	íÊë	cè	ó		
00000016	43	42	01	00	СВ	0A	0A	в5	03	FILE	TIME:	10-0	5-18	16:36	i:37 +	- 3 O	СВ	Ë	μ	ò	40	4 i	Ĺ
00000032	63	00	72	00	6F	00	73	00	6F	00	66	00	74	00	2E	00	c r	0	s	0	ft		
00000048	4D	00	69	00	63	00	72	00	6F	00	73	00	6F	00	66	00	мi	С	r	0	s c	5 f	E
00000064	74	00	53	00	74	00	69	00	63	00	6в	00	79	00	4E	00	t S	t	i	с	k y	71	N
08000000	6F	00	74	00	65	00	73	00	5F	00	38	00	77	00	65	00	o t	е	s	_	8 v	<b>v</b> ∈	в

this Filetime is very close to the date of the ntuser.dat.LOG files (*which coincides with the date the 1803 update occurred*), and that can also be seen from the last entry above:

🥮 NTUSER.DAT	12 Jun 18 1:06 pm
ntuser.dat.LOG1	10 May 18 4:50 pm
ntuser.dat.LOG2	10 May 18 4:50 pm

Further examination shows a consistent pattern:

- 0xD2 14 = Start of Entry
- Next byte = length of block (x2)
- Start of path & executable
- 0xC6 1F = End of block
- Next 4 bytes = unknown
- OxD2 23 = Executable Block
- Next byte = length of block (x2)
- Executable
- OxD2 28 = Payload block
- Next byte = length of block (x2)
- Payload (eg email, URL etc.)
- 0xC6 32 = end of block
- Next 9 bytes = (A) is the same as (B) of the next entry (upwards)
- 0xC6 3C = Pointer to next entry
- Next 9 bytes = (B) is the same as (A) of the next entry (upwards) \*
- Ox CA500000 = End of Entry

\*Top most entry is the newest one, so for the last entry these 9 bytes are all 0xFF

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	02	00	00	00	69	BC	79	90	8F	E9	D3	01	00	00	00	00
00000016	43	42	01	00	CB	0A	0A	91	03	D2	14	25	FILE	TIME:	12-0	5-18
00000032	5C	00	24	00	57	00	49	00	4E	00	44	00	4F	00	57	00
00000048	53	00	2E	00	7E	00	42	00	54	00	5C	00	53	00	6F	00
00000064	75	00	72	00	63	00	65	00	73	00	5C	00	53	00	65	00
0800000	74	00	75	00	70	00	48	00	6F	00	73	00	74	00	2E	00
00000096	65	00	78	00	65	00	C6	1F	80	8D	DC	01	D2	23	0D	53
00000112	00	65	00	74	00	75	00	70	00	48	00	6F	00	73	00	74
00000128	00	2E	00	65	00	78	00	65	00	D2	28	10	57	00	69	00
00000144	6E	00	64	00	6F	00	77	00	73	00	20	00	31	00	30	00
00000160	20	00	53	00	65	00	74	00	75	00	70	00	C6	32	80	9E
00000176	9D	A9	F3	в1	FA	E9	01	C6	3C	FF	FF	FF	FF	FF	FF	FF
00000192	FF	FF	01	CA	5	00	00	D2	14	39	46	00	3A	00	5C	00
00000208	5F	00	46	00	6F	00	72	00	65	00	6E	00	73	00	69	00
00000224	63	00	20	00	54	00	6F	00	6F	00	6C	00	73	00	5C	00
00000240	64	00	6D	00	64	00	65	00	2D	00	70	00	72	00	6F	00
00000256	66	00	2D	00	32	00	21	00	34	00	2E	00	36	00	2E	00
00000272	34	00	34	00	38	00	2D	00	77	00	69	00	6E	00	36	00
00000288	34	00	2D	00	67	00	75	00	69	00	5C	00	64	00	6D	00
00000304	64	00	65	00	2E	00	65	00	78	00	65	00	C6	1F	8E	9D
00000320	9C	01	D2	23	08	64	00	6D	20	64	00	65	00	2E	00	65
00000336	00	78	00	65	00	D2	28	17	44	00	4D	00	44	00	45	00
00000352	20	00	33	00	2E	00	34	00	2E	00	32	00	20	00	46	00
00000368	72	00	65	00	65	00	20	00	45	00	64	00	69	00	74	00
00000384	69	00	6F	00	6E	00	C6	32	E7	81	В1	91	F3	B1	FA	E9
00000400	01	C6	3C	80	9E	9D	A9	F3	B1	FA	E9	01	CA	50	00	00
00000416	D2	14	2C	43	00	3A	00	5C	00	50	00	72	00	6F	00	67
00000432	00	72	00	61	00	6D	00	20	00	46	00	69	00	6C	00	65

With a bit of tweaking in Notepad++, it shows web page titles, email (used in accounts of Outlook), File Explorer paths followed and name of the remote devices accessed with Teamviewer among other.



Back to the 'ActivitiesCache.db' database.

The location of both old and new dBs is at the

"%userprofile%\appdata\local\ConnectedDevicesPlatform" folder.

The old dB table structure was similar to the new dB, but it included 6 tables + the master table (the 'Activity\_PackageId' table was missing, and there were different fields):



The information held was also different:

## E.g. the 'AppSettings' table in the old DB looked like this:

Та	ble: AppSettings			- 😂 🔏
	AppId Filter	SettingsPropertyBag Filter	AppTitle Filter	Logo4141 Filter
1	windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel	BLOB	NULL	NULL
2	Microsoft.SkypeApp_kzf8qxf38zg5c!ppleae38af2e007f4358a809ac99a64a67c1	BLOB		NULL
3	Microsoft.SkypeApp_kzf8qxf38zg5c!App	BLOB	NULL	NULL
4	Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge	BLOB	NULL	NULL
5	AD2F1837.HPPrinterControl_v10z8vjag6ke6!AD2F1837.HPPrinterControl	BLOB	NULL	NULL
6	Microsoft.BingNews_8wekyb3d8bbwe!AppexNews	BLOB	NULL	NULL
7	Microsoft.WindowsCamera_8wekyb3d8bbwe!App	BLOB	NULL	NULL
8	Microsoft.Windows.Photos_8wekyb3d8bbwe!App	BLOB	NULL	NULL
9	VirtualPulse.PlayerforMedia_nh7p8cqfc4t04!App	BLOB	NULL	NULL

## And included UWP (*Universal Windows Platform*) Apps only. The new dB does not have any entries in this table.

## The 'Metadata' table was also different:

Tal	ole: 🔍 Metadata	
	Kev	Value
	Filter	Filter
1	CurrentEtag	5b15de40-92c2-11e7-9117-01020305070d
2	CurrentSettings	{"ActivityTypes":[4,3,2,1,0],"Environment":"prod"}
3	PendingStrongAuth	{"pendingStrongAuth":true}

Looking at the entries in an Lusername folder and a MS account id folder, the username (local account) dB has these entries:

Ta	ble: 🔲 Metadata	
	Key	Value
	Filter	Filter
1	CurrentSettings	{"ActivityTypes":[4,3,2,1,0],"Environment":"prod"}

## And the Microsoft Account dB these:

Ta	ble: 🔲 Metadata		
	Kev		Value
	Filter	Filter	
1	CurrentSettings	{"ActivityTypes":[4,3,2,1,0,5	,6],"Environment":"prod"}
2	CurrentEtag	12c3eb60-189a-11e8-9117-01020	305070d

From this, we can deduce that 'CurrentSettings' is where the Activity Types of the entries populating the database are defined.

The Smartlookup view (query, included in the dB):

select [O].[Id], [O].[AppId], [O].[AppActivityId], [O].[ActivityType], [O].[ParentActivityId], [O].[Tag], [O].[Group], [O].[MatchId], [O].[LastModifiedTime], [O].[ExpirationTime], [O].[Payload], [O].[Priority], [O].[OriginatingDevice], [A].[IsLocalOnly], [A].[PlatformDeviceId], [A].[CreatedInCloud], [O].[StartTime], [O].[EndTime], [O].[LastModifiedOnClient], [O].[ETag] from [ActivityOperation] as [O] left outer join [Activity] as [A] on [O].[Id] = [A].[Id] where [O].[OperationType] <> 3 union select [ld], [Appld], [AppActivityId], [ActivityType], [ParentActivityId], [Tag], [Group], [MatchId], [LastModifiedTime], [ExpirationTime], [Payload], [Priority], [OriginatingDevice], [IsLocalOnly], [PlatformDeviceId], [CreatedInCloud], [StartTime], [EndTime], [LastModifiedOnClient], [ETag] from [Activity] where [Id] not in (select [Id] from [ActivityOperation])

Typical ActivityOperation table entries were of ActivityType 2 :

Т	able:	ActivityOperation				•	
		Id	OperationType Filter	AppId Filter	AppActivityId	ActivityType Filter	<b>ParentActivityId</b> Filter
	1 <b>@</b> e	lx�aM �	1	{"alternateId":"Settings"		2	BLOB
	2 �e	lx�aM �	3	{"alternateId":"Settings"		2	BLOB

# and were in fact Notifications, similar to the ones we can see in %username%\AppData\Local\Microsoft\Windows\Notifications\wpndatabase.db

The AppID was a json blob like this:

Tag	Value
🗸 🏈 <object></object>	
🔤 alternateId	Settings
instanceId	0
🔤 packageId	windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel
🔚 titleId	0
🔤 windows_universal	$windows.immersive control panel\_cw5n1h2txyewy! microsoft.windows.immersive control panel\_cw5n1h2txyewy! mi$

#### And the Payload field

Tag	Group	MatchId	lstModified⊤in	ExpirationTime	Payload
Filter	Filter	Filter	Filter	Filter	Filter
EditionUpgradeTag	EditionUpgradeGroup	NULL	1521896726	1522501525	<toast di…<="" notificationid="107" th=""></toast>
EditionUpgradeTag	EditionUpgradeGroup	NULL	1521896726	1522501525	<toast di<="" notificationid="107" td=""></toast>

#### was an XML blob:

```
<toast NotificationId="107" displayTimestamp="131663703259843007" launch="page=SettingsPageActivate">
    </usual>
    </u
```

From this, another deduction can be made, that ActitivityType 2 is for Toast Notification entries.

The **new** (1803) dB has different fields:

Tał	Table: 🖸 Metadata				
	Key	Value			
	Filter	Filter			
1	CurrentSettings	{"ActivityTypes":[4,3,2,1,0,5,13,6],"Environment":"prod"}			
2	DatabaseInstanceId	38608			
3	DatabaseInstanceIdUpdateTime	2018-05-10T14:00:55.845Z			

After examination of various new 'ActivitiesCache.db' files, any entries seen in the new database have an 'ActivityType' (as *seen above*) of 5 or 6, which appear to represent '*Open App/File/Url*' and '*App In Focus*' respectively – type 13 entries were not observed in any dB yet.

The 'DatabaseInstanceIdUpdateTime' date seen above, is the date & time (in UTC) that the current dB file was created.

A Microsoft Account related DB includes one more field, the 'CurrentEtag' but instead of using an ETAG in the form found elsewhere in the dB, it lists it in the form of a GUID – that is the Cloud ETAG:

	Key	Value
	Filter	Filter
1	CurrentSettings	{"ActivityTypes":[4,3,2,1,0,5,13,6],"Environ
2	DatabaseInstanceId	23919
3	DatabaseInstanceIdUpdateTime	2018-05-10T13:58:59.758Z
4	CurrentEtag	8df03b30-642c-11e8-9117-01020305070d

The 'SmartLookUp' view in the old DB was also different:

1	select	
		[0].[Id],
		[0], [AppId],
		[0]. [AppActivitvId].
		[0].[ActivityType].
		[0].[ParentActivitvId],
		[0].[Tag].
		[0].[Group].
		[O].[MatchTd].
10		[0].[LastModifiedTime].
11		[O]. [ExpirationTime].
12		[O].[Pavload],
13		[O].[Priority],
14		[0].[OriginatingDevice].
15		[A].[IsLocalOnly],
16		[A].[PlatformDeviceId],
17		[A].[CreatedInCloud],
18		[0].[StartTime],
19		[O].[EndTime],
20		[0].[LastModifiedOnClient],
21		[0].[ETag]
22	from	[ActivityOperation] as [0]
23		left outer join [Activity] as [A] on [0].[Id] = [A].[Id]
24	where	[0].[OperationType] <> 3
25	union	
26	select	
		[Id],
		[AppId],
29		[AppActivityId],
		[ActivityType],
31		[ParentActivityId],
32		[Tag],
33		[Group],
34		[MatchId],
		[LastModifiedTime],
36		[ExpirationTime],
37		[Payload],
38		[Priority],
39		[OriginatingDevice],
40		[IsLocalOnly],
41		[PlatformDeviceId],
42		[CreatedInCloud],
43		[StartTime],
44		[EndTime],
45		[LastModifiedOnClient],
46	-	[ETag]
47	irom	
48	where	[Id] not in (select [Id]

## The new Timeline & ActivitiesCache.db

The NEW (updated) database stores information for each user in the %LOCALAPPDATA% \ConnectedDevicesPlatform folder or more commonly familiar as: C:\users\username\appdata\local\ConnectedDevicesPlatform



This folder has a file named 'CDPGlobalSettings.cdp' which is essentially a .json file

and includes information for the service including the store location for the database that holds the windows timeline entries for the current user.



The folder name may include one or more of:

- A Local account starting with an L.UserName, and/or
- folder(s) which appear to be name with random numbers but are the cid's of Microsoft accounts (e.g. Outlook.com, Live.com, Hotmail.com or MSN.com domains).

🗙 📒 ConnectedDevicesPlatform	^	Name	Date modified
Offc25d8321343c3		ActivitiesCache.db	24-Mav-18 10:55
📜 4a7cc0f3b728d240		ActivitiesCache.db-shm	24-May-18 10:54
📕 AAD.e5316abf-be67-4d21-96	5	ActivitiesCache.db-wal	24-May-18 11:00

If a user logs in to Windows with a MS account, then the respective dB is populated. Information as to which online account has this specific ID can be found at: NTUSER.DAT -> 'Software\Microsoft\IdentityCRL\UserExtendedProperties' Under each online account (email) the 'cid' Value contains the respective value for each Microsoft Account & folder.

If a user logs in with a local account, then the "L.UserName" database is populated.

A Microsoft Exchange (Office365 etc.) account starts with 'AAD' and is in the form of AAD.[sid]. AAD denotes a business account (*as in Azure Active Directory*) and information associated with this account 's [sid] can be found in NTUSER.dat at -> 'Software\Microsoft\MSOIdentityCRL\UserExtendedProperties' and/or 'Software\Microsoft\OneDrive\Accounts\Business1'

However, there are two cases when, even if a user continues to use a local account to sign in Windows 10, the activities can still be synchronized across devices:

1. The User has set up a Microsoft Account at "Settings-> Accounts->Email&app accounts" and set it up so that all apps can sign in with this account:



In this case the "L.UserName" folder is removed, and the active folder is the folder that corresponds to this account. All activities are synched across devices.

2. The User has set up a Microsoft Account at "Settings-> Accounts->Email&app accounts" and set it up so that Apps need permission to use this account:



In this case, the local activities are stored in the "L.Username" folder, but any activity on other devices is stored in the respective folder that corresponds to this MS account used on these devices.

The timeline settings ('Settings -> Privacy -> Activity History') enable or not activity to be tracked in the 'ActivitiesCache.db'. In order for the activity to be shared across devices (*via the cloud*) you need to login with a Microsoft account, enable Windows Hello (i.e. create pin and or biometric/photo login).

https://support.microsoft.com/en-us/help/4026102/windows-10-about-sync-settings

To enable cross-device experiences, your app users must login with either a <u>Microsoft Account</u> or an <u>Azure Active Directory</u> account.

https://github.com/Microsoft/project-rome/blob/master/cross-device\_app\_configuration.md

Sync your settings Some Windows features are only available if you are using a Microsoft account or work account.

https://github.com/microsoftgraph/microsoft-graph-docs/blob/master/apireference/beta/resources/intune\_deviceconfig\_windows10generalconfiguration.md

A list of settings that can be roamed or backed up (synced) across devices can be found here: <u>https://docs.microsoft.com/en-us/azure/active-directory/active-directory-windows-enterprise-</u> <u>state-roaming-windows-settings-reference</u>

The 'AfcPrivacySettings' in 'CDPGlobalSettings.cdp' depicts the relative settings in Windows 10 'Settings –> Privacy- >Activity History', for example:

All settings ON:

## Activity history Jump back into what you were doing with apps, docs, or other activities, either on your PC or your phone. Let Windows collect my activities from this PC Let Windows sync my activities from this PC to the cloud

CDPGlobalSe	ettings	
Tag		Value
> 🗮 Act	ivityStoreInfo	
E Afo	DefaultUser	undefined
🗸 🌮 Afc	PrivacySettings	
<b>=</b>	ActivityFeed	0
	CloudSync	0
	PublishUserActivity	0
<b>E</b>	UploadUserActivity	0

Upload to cloud off





Publish off, cloud off



The same settings can also be configured through Group Policy at 'Computer Configuration -> Administrative Templates -> System ->OS Policies'



Opening the respective folder we can see the 'ActivitiesCache.db' (and possibly also the ActivitiesCache.wal and ActivitiesCache.db-sdb files) which is the storage of all timeline activity for the current user. When a user switches from a Local to a MS account, the 'L.UserName' is deleted and a new one is created (if it didn't exist before) under the respective MS account folder. Any previous entries in the 'L.UserName''s 'ActivitiesCache.db' now appear in the new 'ActivitiesCache.db' linked to the MS account, and sync to the cloud. Switching from a MS to a local account, the MS account related db is still available and holds timeline data.

When a user logs in Windows with a MS account, and the relevant check boxes in 'Settings -> Privacy- >Activity History' are set to On,



any activity created with his other MS account(s), is updated in the 'ActivitiesCache.db' in the respective '%LOCALAPPDATA% \ConnectedDevicesPlatform\' SubFolder, and can be seen in his timeline view .

Any -excluded from sync- accounts (*above setting set to off*) can be seen at the registry at: NTUSER.dat

Software\Microsoft\Windows\CurrentVersion\ActivityDataModel\ActivityAccountFilter



The synchronized entries in a MS account related dB will show the 'Device ID' of the machine the entry originated from. The Device Name and Model of the originating machine can be seen in the NTUSER.dat's 'Software\Microsoft\Windows\CurrentVersion\TaskFlow\DeviceCache\':



Even if a user logs in with a local account, when a MS Account was previously used for login, the entries of 'ActivitiesCache.db' of that account will also appear in the user's timeline (for the previous 7 days). So it may be prudent to examine all 'ActivitiesCache.db' databases in a system.

Following is the analysis of the new 'ActivitiesCache.db' file, using <u>DB Browser for SQLite</u>, <u>SQLite</u> <u>Expert Professional</u>, <u>Notepad++</u> and <u>JSON Viewer</u>.

The database has the following structure (7 tables + the master table):



The 'Metadata' table includes the date/time the database was created by the system:

Metadata (main) 🛛 🗴 🗙		
*		
E A Key Text	Key	Value
	Filter	Filter
Value Text		
	1 CurrentSettings	{"ActivityTypes":[4,3,2,1,0,5,13,6],"Environment":"prod"}
	2 DatabaseInstanceId	3428
A	3 DatabaseInstanceIdUpdateTime	2018-05-24T08:16:50.365Z

Note: see page 2 above for the differences with the old database

## The 'ManualSequence' table shows the last Activity (ETAG) recorded in the database:



From the 7 tables above, only three hold information of user activities:

'Activity', 'ActivityOperation' and 'Activity\_PackageID'



The Windows Timeline process looks like this:



Any new application execution or focus change, triggers an entry to the 'Activity' table, and relevant entries in the 'Activity\_PackageID' table.

**Note**: *It should be noted that any new entries/transactions are written first to the write ahead log ('ActivitiesCache.wal')* 

Name	Date modified	Туре	Size
ActivitiesCache.db	27-May-18 5:20 pm	DB File	4.196 KB
ActivitiesCache.db-shm	27-May-18 4:07 pm	DB-SHM File	32 KB
ActivitiesCache.db-wal	27-May-18 5:22 pm	DB-WAL File	528 KB

and the database is updated when the wal file reaches 1000 pages and commits the transactions. The default settings of the database show that each page is 4096 bytes long:

Auto Vacuum	None -
Automatic Index	$\checkmark$
Checkpoint Full FSYNC	
Foreign Keys	$\checkmark$
Full FSYNC	
Ignore Check Constraints	
Journal Mode	WAL -
Journal Size Limit	-1 🗘
Locking Mode	Normal -
Max Page Count	1073741823 🗘
Page Size	4096 🗘
Recursive Triggers	
Secure Delete	
Synchronous	Full -
Temp Store	Default -
User Version	18 🗘
WAL Auto Checkpoint	1000 🗘

The query below (*which is in essence two united queries*) extracts all possible useful information from this database in a readable form. This query will not work properly in any SQLite browser that does not include support for the json1 extension.

1	SELECT This the ActivityOperation Table Query
	ActivityOperation.ETag as 'Etag',
	json extract(ActivityOperation.Payload, ' <b>\$.appDisplayName') as 'Program Name'</b> ,
	case
5	<pre>when ison extract(ActivityOperation.AppId, '\$[0].application') = '308046B0AF4A39CB'</pre>
6	then 'Firefox-308046B0AF4A39CB'
	<pre>when ison extract(ActivityOperation.AppId, '\$[1].application') = '308046B0AF4A39CB'</pre>
8	then 'Firefox-308046B0AF4A39CB'
9	<pre>when length (ison extract(ActivityOperation.AppId, '\$[1].application')) &gt; 17</pre>
10	and length (ison extract(ActivityOperation,AppId, '\$[1],application')) < 22
11	then
12	replace(replace(replace(replace
13	(ison extract(ActivityOperation,AppId, '\$[0].application').
14	'{'  '6D809377-6AF0-444B-8957-A3773F02200E'  '}, '*ProgramFiles (x64)').
15	'{'  '7C5A40EF-A0EB-4BEC-874A-C0E2E0B9EA8E'  '}', '*ProgramFiles (x32)').
16	'{'  '1AC14E77-02E7-4E5D-B744-2EB1AE5198B7' '}', '*System').
17	'{'  'F388F404-1D43-42F2-9305-67DF0828FC23'  '}', '*Windows')
18	(' ')05523180-82F1-4857-A4CF-A8F7C6F47D27' ')', '*Svstem37')
19	else replace(replace(replace(replace(replace(replace)))))))
20	'\$[1].application').
21	<pre>/{! '50809377-56F0-4488-8957-43773E02200E' '}'. '*ProgramFiles (x64)').</pre>
22	'1' ''755406F-40FE-47EC-8740-60F2608648F' '''' '*ProgramFiles ((32)')
23	(1) 14(14F77-02F7-4F50-B744-2FB14F5198B7'  ')' '*System')
24	{\ \\FB8BE404_1D3_42E2_9305_677EB828E(33'\\'}, \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
25	() 15523180-8251-4457-446-88576647071()) (**********************************
26	end as 'Annication'
27	ison extract(ActivityOperation_Payload '\$_displayText')]  ' ('   ison_extract(ActivityOperation_Payload '\$_description')  ')' as 'File/title/nati
	nened
28	case when ison extract(ActivityOperation Payload '\$ shallContentDescription') like '%FileShallLink%'
29	the ison extract(activityOperation Payload, \$ shallContentDescription FileShallink)
30	else joon_extract(ActivityOperation_Payload '5.type')   - '   ion_extract(ActivityOperation_Payload '\$ userTimezone')
31	end as 'bayload/Timezone'
32	case ActivityOperation.ActivityType
33	when 5 then 'Onen Ann/File/Page' when 6 then 'Ann Tn lise/Focus'
34	else 'Inknown vat'
35	end as 'Artivity type'
36	case ison extract/activityOperation_AppId, '\$[0].platform')
37	when 'afs crossilatform' then 'Yes'
38	when 'host' then
39	(case ison extract(ActivityOperation,AppId, '\$[1],platform')
40	when 'afs crossplatform' then 'Yes' else null end)
41	else null
42	end as 'Synced'.
43	case
44	when ison extract(ActivityOperation.AppId, '\$[0].platform') = 'afs crossplatform'
45	then ison extract(ActivityOperation,AppId, '\$[1],platform')
46	else json extract(ActivityOperation.AppId, '\$[0].platform')
47	end as 'Platform'.
48	case ActivityOperation.OperationType
49	when 1 then 'Active' when 2 then 'Updated' when 3 then 'Deleted' when 4 then 'Ignored'
50	end as 'TileStatus',

51	case
52	when ActivityOperation.Id in
53	(select Activity.Id from Activity where Activity.Id = ActivityOperation.Id)
54	then 'Removed'
	end as 'WasRemoved',
56	case
57	when ActivityOperation.Id
58	<pre>in(select Activity.Id from Activity where Activity.Id = ActivityOperation.Id)</pre>
59	then null else 'In Queue'
60	end as 'UploadQueue',
	<pre>coalesce(json extract(ActivityOperation.Payload, '\$.activationUri'),json extract(ActivityOperation.Payload, '\$.reportingApp')) as 'App/Uri',</pre>
62	ActivityOperation.Priority as 'Priority',
63	<pre>time(json extract(ActivityOperation.Payload, '\$.activeDurationSeconds'), 'unixepoch') as 'Active Duration',</pre>
64 🚦	case
65	when cast((ActivityOperation.EndTime - ActivityOperation.StartTime) as integer) < 0 then '-'
66	<pre>else time(cast((ActivityOperation.EndTime - ActivityOperation.StartTime) as integer), 'unixepoch')</pre>
67	end as 'Calculated Duration'.
68	<pre>datetime(ActivityOperation.StartTime, 'unixepoch', 'localtime') as 'StartTime',</pre>
69	<pre>datetime(ActivityOperation.LastModifiedTime, 'unixepoch', 'localtime') as 'LastModified',</pre>
70	case
71	<pre>when ActivityOperation.OriginalLastModifiedOnClient &gt; 0</pre>
72	then datetime(ActivityOperation,OriginalLastModifiedOnClient, 'unixepoch', 'localtime')
73	else ' '
74	end as 'LastModifiedOnClient'.
75	case
76	when ActivityOperation.EndTime > 0
77 🚦	then datetime(ActivityOperation.EndTime, 'unixepoch', 'localtime')
78	else null
79	end as 'EndTime',
80	case
81	when ActivityOperation.CreatedInCloud > 0
82	then datetime(ActivityOperation.CreatedInCloud, 'unixepoch', 'localtime')
83	else null
84	end as 'CreatedInCloud',
85 🛓	<b>cast</b> ((ActivityOperation.ExpirationTime - ActivityOperation.LastModifiedTime)
86	as integer) / '86400' as 'Expires In days',
87	datetime(Activity PackageId.ExpirationTime, 'unixepoch', 'localtime') as 'Expiration on PackageID',
88	datetime(ActivityOperation.ExpirationTime, 'unixepoch', 'localtime') as 'Expiration',
89	ActivityOperation.PlatformDeviceId as 'Device ID',
90	ActivityOperation.PackageIdHash as 'Application Hash',
91	'{'    substr(hex(Activity PackageId, ActivityId), 1, 8)    '-'
92	substr(hex(Activity PackageId.ActivityId), 9, 4)    '-'
93	substr(hex(Activity PackageId.ActivityId), 13, 4)
94	substr(hex(Activity PackageId.ActivityId), 17, 4)
95	<pre>substr(hex(Activity PackageId.ActivityId), 21, 12)    '}' as 'ID',</pre>
96	json extract(ActivityOperation.OriginalPayload, '\$.appDisplayName') as 'Original Displayed Name',
	json extract(ActivityOperation.OriginalPayload, '\$.displayText') as 'Original File/title opened',
98	json extract(ActivityOperation.OriginalPayload, '\$.description') as 'Original Full Path /Url',
99	coalesce(json extract(ActivityOperation.OriginalPayload, '\$.activationUri'), json extract(ActivityOperation.OriginalPayload, '\$.reportingApp')) as
	'Original App/Uri',
100	<pre>time(json_extract(ActivityOperation.OriginalPayload, '\$.activeDurationSeconds'), 'unixepoch') as 'Orig.Duration'</pre>

101	
102	from Activity_PackageId
103	join ActivityOperation on Activity_PackageId.ActivityId = ActivityOperation.Id
104	<pre>where Activity_PackageId.Platform = json_extract(ActivityOperation.AppId, '\$[0].platform')</pre>
105	and Activity_PackageId.ActivityId = ActivityOperation.Id
106	
107	union Join Activity & ActivityOperation Queries to get results from both Tables
108	
109	select This the Activity Table Query
110	Activity.ETag as 'Etag',
111	json_extract(Activity.Payload, '\$.appDisplayName') AS 'Program Name',
112	case
113	<pre>when json_extract(Activity.AppId, '\$[0].application') = '308046B0AF4A39CB'</pre>
114	then 'Firefox-308046B0AF4A39CB'
115	<pre>when json_extract(Activity.Appld, '\$[1].application') = '30804680AF4A39CB' product of a product program (a product program) = '30804680AF4A39CB' </pre>
116	then 'Firefox-30804bB0AF4A39LB'
11/	when length ()son_extract(Activity.Appid, \$[0].application')) > 1/ and
118	<pre>length(json_extract(Activity.Appid, \$[0].appilcation )) &lt; 22</pre>
119	then replace(replace(replace(replace()son_extract(Activity.Appld, `\$[1].application'),
120	{    0L0093/7-0AF0-4440-035/-A3/75F02200E    } , *Programiles (x04) ),
121	{    /LSA40EF-A0FB-4BFL-8/4A-L0F2E0B9FA8E    }, *ProgramFiles (X32) ),
122	{    IAL142//-022/-4530-0/44-2251450/10 } , -3/stem ), { /  1/23025404 1042 425 0262 57750202572    } , -3/stem )
123	{    F30F494-1043-4272-3303-0/DE0026FC23    } , WLINDWS },
124	$\{   U052100^{+}021^{+}403^{+}44C^{+}A0C^{+}0CA(DCA/D2^{+})   \}, 53(2004KP00CA)   3000KF0A20CP   3000KF0A20CP $
125	then Storextract(Activity.Appid, \$(0).appiledtion) = 50004000AP4A55Cb
120	alse renlace(renlace(renlace(renlace)
128	(ison extract (Activity And (15(A) and initiation))
129	()5/(
130	{\ \'7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E' \'}\'*ProgramFiles (X32)').
131	'{'  '1AC14E77-02E7-4E5D-B744-2EB1AE5198B7'  '}'. '*System').
132	'{'  'F38BF404-1D43-42F2-9305-67DE0B28FC23'  '}'. '*Windows').
133	'{'  'D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27'  '}', '*System32')
134	end as 'Application',
135	json_extract(Activity.Payload, '\$.displayText')   ' ('   json_extract(Activity.Payload, '\$.description')  ')' as 'File/title/path opened',
136	<pre>case when json_extract(Activity.Payload, '\$.shellContentDescription') like '%FileShellLink%'</pre>
137	<pre>then json_extract(Activity.Payload, '\$.shellContentDescription.FileShellLink')</pre>
138	<pre>else json_extract(Activity.Payload, '\$.type')  ' - '   json_extract(Activity.Payload,'\$.userTimezone')</pre>
139	end as 'Payload/Timezone',
140	case Activity.ActivityType
141	when 5 then 'Open App/File/Page' when 6 then 'App In Use/Focus'
142	else 'Unknown yet'
143	end as 'Activity_type',
144	<pre>case json_extract(Activity.AppId, '\$[0].platform')</pre>
145	when 'ats_crossplatform' then 'Yes'
146	when 'host' then (case json_extract(Activity.AppId, '\$[].platform')
147	when 'ats_crossplatform' then Yes' else null end) else null
148	end as 'Synced',
149	case
150	when json_extract(Activity.Appid, \$[0].platform ) = afs_crossplatform



An updated version of this query can be found online at: https://kacos2000.github.io/WindowsTimeline/

The above query pulls information from the 'Activity' , 'ActivityOperation' and

'Activity\_PackageId' tables. The 'Activity\_PackageId' table is more or less a 'cache' of the unique IDs of each application execution and its expiration time.

## Some field explanations provided by Microsoft:

Name	Туре	Description
status	EnumType	Set by the server. A status code used to identify valid objects. Values: active, updated, deleted, ignored.
userTimezone	String	Optional. The timezone in which the user's device used to generate the activity was located at activity creation time. Values supplied as Olson IDs in order to support cross-platform representation.
createdDateTime	DateTimeOffset	Set by the server. DateTime in UTC when the object was created on the server.
lastModifiedDateTime	DateTimeOffset	Set by the server. DateTime in UTC when the object was modified on the server.
id	String	Required. Client-set GUID for the historyltem object.
startedDateTime	DateTimeOffset	Required. UTC DateTime when the <b>historyItem</b> (activity session) was started. Required for timeline history.
lastActiveDateTime	DateTimeOffset	Optional. UTC DateTime when the <b>historyItem</b> (activity session) was last understood as active or finished - if null, <b>historyItem</b> status should be Ongoing.
expirationDateTime	DateTimeOffset	Optional. UTC DateTime when the <b>historyItem</b> will undergo hard-delete. Can be set by the client.
activeDurationSeconds	int	Optional. The duration of active user engagement. if not supplied, this is calculated from the <b>startedDateTime</b> and <b>lastActiveDateTime</b> .

## The Activity' table's 'ID' (*Primary key*) field is a unique value: [Activity]([Id] GUID PRIMARY KEY NOT NULL

It is the unique ID of each entry/user activity. The same ID can be seen more than 2 times in the Activity\_PackageID table depending on the 'Platform' field which has the following possible values (*Note: most of project Rome is still undocumented, so not all entries can be defined*):

- "Host" (is listed as many times as the number of entries in the Activity table),
- "packageid"\*\*, (is listed as many times as the number of entries and includes the executable and its path for all x\_exe & windows\_win32 apps, as seen in the Activity\_PackageID's PackageName field)
- "x\_exe\_path" for Programs called from a specific path (e.g. Standalone executables)

\*\* as seen below:

ETag	ID	Activity_PackageId.PackageName	Activity_json_Packageid
41723	3254D1271207F6C50CED	*System\cmd.exe	*System\cmd.exe
41722	2FB37475807AA6C1D3C9	*System\snippingtool.exe	*System\SnippingTool.exe
41721	3A99ABF8D3BA3ABE6B31	microsoft.office.desktop_8wekyb3d8bbwe!powerpoint	NULL
41720	935EB39CF7CE0C170659	*ProgramFiles (x64)\lsoft technologies\active@ disk editor	*ProgramFiles (x64)\LSoft Technologies\Active@ Disk Edi
41719	2922B987D85B0B6FA4ED	*ProgramFiles (x64)\tracker software\pdf viewer\pdfxcview	*ProgramFiles (x64)\Tracker Software\PDF Viewer\PDFXC
41718	F13910B8FE851B13E14D	microsoft.windowscalculator_8wekyb3d8bbwe!app	Microsoft.WindowsCalculator_8wekyb3d8bbwe!App
41717	FF1241976D7A557AEA1E	microsoft.windowscalculator_8wekyb3d8bbwe!app	Microsoft.WindowsCalculator_8wekyb3d8bbwe!App
41715	D222BC19A52035C3398E	*System\snippingtool.exe	*System\SnippingTool.exe
41713	5A61C68F4DE1C99F14A4	*System\snippingtool.exe	*System\SnippingTool.exe
41707	587C1298F7A2D926DBD	microsoft.windows.explorer	Microsoft.Windows.Explorer
41706	68547C5BDBFD068D2F3F	microsoft.windows.explorer	Microsoft.Windows.Explorer
41704	A7B05CED895ABC4DCCF	*System\notepad.exe	*System\notepad.exe

#### By running the following query:

select
Activity.ETag,

hex(Activity\_PackageId.ActivityId) as 'ID', replace(replace(replace(replace(replace( replace(replace(
 Activity\_PackageId.PackageName,
 lower('30804680AF4A39CB'), 'Mozilla Firefox'),
 '{'||lower('6D809377-6AF0-444B-8957-A3773F02200E')||'}', '\*ProgramFiles (x64)'),
 '{'|lower('7C5A40EF-A0FB-4BFC-874A-C0F2E089FA8E')||'}', '\*ProgramFiles (x22)'),
 '{'|lower('1AC14E77-02E7-44E5D-8744-2EB1AE5198B7')||'}', '\*System'),
 '{'|lower('F38BF404-1D43-42F2-9305-67DE0028FC23')||'}', '\*Windows'),
 '{'|lower('D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27')||'}', '\*System32') as 'Activity\_PackageId.PackageName', case when json\_extract(Activity.AppId, '\$[0].platform') like '%packageid%' then (json\_extract(Activity.AppId, '\$[0].appIication'), '308046504FA439CG', 'Mozilla Firefox'), '{'||'6D809377-6AF0-444B-8957-A3773F02200E'||'}', '\*ProgramFiles (x64)'), '{'||'7C5A40EF-A0FB-4BFC-874A-C0F220B9FA8E'||'}', '\*ProgramFiles (x32)'), '{'||'17384640-1043-42F2-9305-67DE0828FC23'||'}', '\*System'), '{'||'16532180-82F1-4857-A4CE-A8E7C6EA7D27'|'}', '\*System32') 't'|' 06523180-82F1-4857-A4CE-A8E7C6EA7D27'|'}', '\*System32') 't'|'' 06523180-124560re')' when json\_extract(Activity.AppId, '\$[1].platform') like '%packageid%' then replace(replace(replace(replace(replace) (json\_extract(Activity.AppId, '\$[2].application'), when json\_extract(Activity.AppId, '\$[3].platform') like '%packageid%' then replace(replace(replace(replace(replace))) replace (replace (json\_extract(Activity.AppId, '\$[4].application'), '308046B0AFAA39CB', 'Mozilla Firefox'), '{'|'6D80937-6AF0-444B-8957-A3773F02200E'|'}, '\*ProgramFiles (x64)'), '{'|'17C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E'|'}, '\*ProgramFiles (x32)'), '{'|'17C5A40EF-A0FB-4BFC-874A-2EB1AE519887'|'}, '\*System'), '{'|'17C5A40EF7-4E5D-8744-2EB1AE519887'|'}, '\*System'), '{'|'1753BF404-1D43-42F2-9305-67DE0B28FC23'|'}, '\*Windows'), '{'|'165231B0-B2F1-4857-A4CE-A8E7C6EA7D27'|'}, '\*System32')

when json\_extract(Activity.AppId, '\$[5].platform') like '%packageid%' then replace(replace(replace(replace(replace) (json\_extract(Activity.AppId, '\$[5].application'), '308046B0AF4A39CB', 'Mozilla Firefox'), '{'||'6D809377-6AF0-444B-8957-A3773F02200E '\*ProgramFiles (x64)'), '\*ProgramFiles (x32)'), '7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E' ||'7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E'||'}', '\*ProgramFi ||'1AC14E77-02E7-4E5D-B744-2EB1AE5198B7'||'}', '\*System'), replace(replace(replace(replace(replace) (json\_extract(Activity.AppId, '\$[6].application'), '308046B0AF4A39CB', 'Mozilla Firefox'), 308046B0AF4A39CB', 'Mozilla Firefox'), '{'||'6D809377-6AF0-444B-8957-A3773F02200E'||'}', '\*ProgramFiles (x64)'), || 'bD80937'-bAF0-4448-895'-A3773F02200E'||'}, '\*ProgramFiles (x54)'), |'7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E'|'}, '\*ProgramFiles (x32)'), |'1AC14E77-02E7-4E5D-8744-2EB1AE5198B7'|'}, '\*System'), |'F38BF404-1D43-42F2-9305-67DE0B28FC23'|'}, '\*Windows'), |'D65231B0-82F1-4857-A4CE-A8E7C6EA7D27'|'}, '\*System32') || 'D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27'|| when json\_extract(Activity.AppId, '\$[7].platform') like '%packageid%' then replace(replace(replace(replace(replace (json\_extract(Activity.AppId, '\$[7].application'), 'Mozilla Firefox') 308046B0AF4A39CB', 'Mozilla Firefox'), '{'||'6D809377-6AF0-444B-8957-A3773F02200E'|| '{'||'6D809377-6AF0-4448-8957-A3773F02200E'|'}', '\*ProgramFiles (x64)'), '{'||'7C5A40EF-A0FB-4BFC-874A-C0F2E089FA8E'|'}', '\*ProgramFiles (x32)'), '{'|'1AC14E77-02E7-4E5D-B744-2EB1AE519887'|'}', '\*System'), '{'|'153BF404-1D43-42F2-9305-67DE0828FC23'|'}', '\*Windows'), '{'|'153BF404-1D43-42F2-9305-67DE0828FC23'|'}', '\*System32') when json\_extract(Activity.AppId, '\$[].platform') like '%packageid%' then place(replace(replace(replace replace(replace(replace(replace(replace (json\_extract(Activity.AppId, '\$[8].application'), ,JSUI\_extFact(Activity.Appl, \$[6].appl(attoin), 388046B04FA439CE', 'Mozilla Firefox'), '{'||`6D809377-6AF0-444B-8957-A3773F02200E'||`}', '\*ProgramFiles (x64)'), { || 6DS0937/-bAF0-4448-8957-A37/3F022006 || } , \*ProgramFiles (x64) ), '{'||'7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E'||'}', '\*PorgramFiles (x32)'), '{'||'14C4F7-02E7-4E5D-8744-2EB1AE5198B7'||'}', '\*System'), '{'||'F38BF404-1D43-42F2-9305-67DE0B28FC23'||'}', '\*Windows'), '{'||'D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27'||'}', '\*System32') end as 'Activity\_json\_Packageid' from Activity\_PackageId join Activity on Activity.Id = Activity\_PackageId.ActivityId where Activity\_PackageId.ActivityId = Activity.Id and Activity\_PackageId.Platform = 'packageid' Order by etag desc

plus one or more of the following (platform-specific application IDs):

- "windows\_win32" for Installed Software (non UWP) Applications
- "windows\_universal' for Windows <u>UWP</u> Apps
- "msa",
- "ios",
- "android", and
- "web"

As seen by this MS example:

Example:

```
{"platform":"windows_universal", "application":"Microsoft.Contoso_8wekyb3d8bbwe"},
{"platform":"windows_win32", "application":"DefaultBrowser_NOPUBLISHERID!Microsoft.Contoso.Default"},
{"platform":"android", "application":"com.example.myapp"},
{"platform":"ios", "application":"com.example.myapp"},
{"platform":"web", "application":"https://contoso.com"},
{"platform":"web", "application":"https://chat.contoso.com"},
{"platform":"msa", "application":"0000000603E0BF"},
{"platform":"msa", "application":"48932b46-98b1-4020-9be4-cc7a65643c9e"},
]
```

If the Sync activity is enabled (user logs in with a MS Account) then another entry may also be seen: "afs\_crossplatform" which shows a <u>cloud sync</u> enabled activity, and is an additional entry to the same ones seen when using a local account.

When using a MS account:

5251	\$\$\$% c.	afs_crossplatform	6082723978844556501	1529741627
5252	\$\$\$% co	windows_win32	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\foobar2000\f	1529741627
5253	\$\$\$% co	packageid	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\foobar2000\f	1529741627
5254	000% co	host		1529741627

When using a Local account there is NO 'afs\_crossplatform' entry:

79	e% 📀	@ <b>\$</b> I <b>\$</b>	windows_win32	microsoft.window	1529742843	
80	e% 🔷	@ <b>\$</b> I <b>\$</b>	packageid	microsoft.window	1529742843	
81	e% 🌒	@ <b>\$</b> I <b>\$</b>	host		1529742843	

## As can also be seen below (these are for a single ID of a Microsoft Word entry):

ActivityId	Platform	PackageName	ExpirationTime
CA06838559F87AE076659BF18C593CF9	host	word.activity.windows.com	2018-06-29 16:39:49
CA06838559F87AE076659BF18C593CF9	afs_crossplatform	16883319693718197224	2018-06-29 16:39:49
CA06838559F87AE076659BF18C593CF9	windows_universal	microsoft.office.word_8wekyb3d8bbwe	2018-06-29 16:39:49
CA06838559F87AE076659BF18C593CF9	windows_universal	microsoft.office.desktop_8wekyb3d8bbwe	2018-06-29 16:39:49
CA06838559F87AE076659BF18C593CF9	android	com.microsoft.office.word	2018-06-29 16:39:49
CA06838559F87AE076659BF18C593CF9	ios	com.microsoft.office.word	2018-06-29 16:39:49
CA06838559F87AE076659BF18C593CF9	windows_win32	microsoft.office.winword.exe.15	2018-06-29 16:39:49
CA06838559F87AE076659BF18C593CF9	windows_win32	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\microsoft office\office15\winword.exe	2018-06-29 16:39:49
CA06838559F87AE076659BF18C593CF9	windows_win32	{6d809377-6af0-444b-8957-a3773f02200e}\microsoft office\office15\winword.exe	2018-06-29 16:39:49
CA06838559F87AE076659BF18C593CF9	windows_win32	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\microsoft office\office14\winword.exe	2018-06-29 16:39:49
CA06838559F87AE076659BF18C593CF9	windows_win32	{6d809377-6af0-444b-8957-a3773f02200e}\microsoft office\office14\winword.exe	2018-06-29 16:39:49
CA06838559F87AE076659BF18C593CF9	msa	000000003edf6	2018-06-29 16:39:49

## The above can be seen by using this query:

An example of the entry of Microsoft YourPhone's app:

```
[{"application":"mmxsdktest.azurewebsites.net","platform":"host"},
{"application":"16815419600048394801","platform":"afs_crossplatform"},
{"application":"000000004018945C","platform":"msa"},
{"application":"","platform":"packageId"},
{"application":"","platform":"alternateId"},
{"application":"","platform":"windows_universal"}]
```

The afs\_crossplatform field has been observed to contain a numeric representation of the application used (?), with the exception of MS Office applications and MS Edge:

Activity_json_afs_crossplatform						
9553497022742795366						
9616461484989533944						
9726032056939584244						
972940661883734646						
9751790172484571661						
9792636623328491085						
edge.activity.windows.com						
excel.activity.windows.com						
powerpoint.activity.windows.com						
word.activity.windows.com						
As seen by running the que	ery below:					
select						
when json_extract(Activity.AppId,	'\$[0].platform')	like	'%afs_crossplatform%'	then	json_extract (Activity.AppId,	'\$[0].applicat
when json_extract (Activity.AppId,	'\$[1].platform')	like	'%afs_crossplatform%'	then	json_extract (Activity.AppId,	'\$[0].applicat
when json_extract(Activity.Appid,	'\$[2].platform')	like	'sais_crossplatiorms'	then	json_extract (Activity.Appid,	'\$[0].applicat
when ison extract (Activity, AppId,	'\$[4].platform')	like	'%afs_crossplatform%'	then	ison extract (Activity. AppId.	'\$[0].applicat
when ison extract (Activity. AppId,	'\$[5].platform')	like	'%afs crossplatform%'	then	ison extract (Activity. AppId,	'\$[0].applicat
when json extract (Activity.AppId,	'\$[6].platform')	like	'%afs crossplatform%'	then	json extract (Activity. AppId,	'\$[0].applicat
when json_extract (Activity.AppId,	'\$[7].platform')	like	'%afs_crossplatform%'	then	json_extract (Activity.AppId,	'\$[0].applicat
when json_extract (Activity.AppId,	'\$[8].platform')	like	'%afs_crossplatform%'	then	json_extract(Activity.AppId,	'\$[0].applicat
end as 'Activity_json_afs_crosspl	atform'					
from Activity						
group by Activity_json_afs_crossplatf	orm					

The 'Activity\_Packageld' table seemingly has more information than the 'Activity' table. That is not true though, as the 'Activity' table's 'AppID' field holds this information and a lot more. The 'Activity' and 'ActivityOperation' table 'AppID' fields are in fact Binary Large Objects (BLOB) in 'json array' format e.g.:

'AppID' entry for an Installed Application in Windows:



**Note:** Notice that the path shown above is in the form of a GUID. It is a KNOWNFOLDERID used by windows for standard known folders like 'program files'. In the json file above, this is the GUID for ProgramFilesX86 (C:\Program Files (x86)\) folder. There are various lists of CLSIDs in the internet like https://msdn.microsoft.com/en-us/library/windows/desktop/dd378457(v=vs.85).aspx



#### and 'AppID' entry for a Windows UWP app



-- List all entries in the AppID json array

Since this is a json array, we can do a query to see what values it holds in the 'application' and 'platform' fields. The [x]. depicts the number of the element in the JSON array, and 'platform' or 'application' of the respective field name:

```
select
hex(Activity.ID) as 'ID',
json_extract(Activity.AppId, '$[0].platform') as 'p0',
json_extract(Activity.AppId, '$[0].application') as '0',
json_extract(Activity.AppId, '$[1].platform') as 'p1',
json_extract(Activity.AppId, '$[1].application') as '1',
json_extract(Activity.AppId, '$[2].platform') as 'p2',
json_extract(Activity.AppId, '$[2].application') as 'p2',
json_extract(Activity.AppId, '$[2].application') as 'p3',
json_extract(Activity.AppId, '$[3].platform') as 'p3',
json_extract(Activity.AppId, '$[3].application') as 'p3',
json_extract(Activity.AppId, '$[4].platform') as 'p4',
json_extract(Activity.AppId, '$[4].platform') as 'p4',
json_extract(Activity.AppId, '$[5].platform') as 'p5',
json_extract(Activity.AppId, '$[5].application') as '5',
json_extract(Activity.AppId, '$[6].platform') as 'p6',
```

```
json_extract(Activity.AppId, '$[6].application') as '6' ,
json_extract(Activity.AppId, '$[7].platform') as 'p7' ,
json_extract(Activity.AppId, '$[7].application') as '7' ,
json_extract(Activity.AppId, '$[8].platform') as 'p8' ,
json_extract(Activity.AppId, '$[8].application') as '8'
```

## from Activity order by ID asc

	A0	PO	A1	P1	A2	P2	A3	P3
19	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Acronis\TrueImageHome\TrueImage.exe	x_exe_path	{7C5A40EF-A0FB-4BFC-874A-C0F2	packageld		alternateId		windows_universal
20	Microsoft.Office.OUTLOOK.EXE.15	windows_win32	Microsoft.Office.OUTLOOK.EXE.15	packageld		alternateId		windows_universal
21	{6D809377-6AF0-444B-8957-A3773F02200E}\VOW Software\plist Editor Pro\plistEditor.exe	windows_win32	{6D809377-6AF0-444B-8957-A377	packageld		alternateId		windows_universal
22	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Acronis\TrueImageHome\TrueImage.exe	x_exe_path	{7C5A40EF-A0FB-4BFC-874A-C0F2	packageld		alternateId		windows_universal
23	{6D809377-6AF0-444B-8957-A3773F02200E}\SQLite Expert\Professional 5\SQLiteExpertP	windows_win32	{6D809377-6AF0-444B-8957-A377	packageld		alternateId		windows_universal
24	Microsoft.Office.OUTLOOK.EXE.15	windows_win32	Microsoft.Office.OUTLOOK.EXE.15	packageld		alternateId		windows_universal

### Or

	2	р3	3	p4	4	p5	5	p6	6	p7	7	р8	8
1	osoftEdge_8wekyb3d8bbwe!MicrosoftEdge	msa	f44b1140-bc5e-48c6-8dc0-5cf5a53c0e34	msa	00000004C1BC462	android	com.microsoft.emmx.daily	android	com.microsoft.emmx.selfhost	android	com.microsoft.emmx	ios	com.microsoft.emmx.daily-df
2	osoftEdge_8wekyb3d8bbwe!MicrosoftEdge	msa	f44b1140-bc5e-48c6-8dc0-5cf5a53c0e34	msa	00000004C1BC462	android	com.microsoft.emmx.daily	android	com.microsoft.emmx.selfhost	android	com.microsoft.emmx	ios	com.microsoft.emmx.daily-df
3	osoftEdge_8wekyb3d8bbwe!MicrosoftEdge	msa	f44b1140-bc5e-48c6-8dc0-5cf5a53c0e34	msa	00000004C1BC462	android	com.microsoft.emmx.daily	android	com.microsoft.emmx.selfhost	android	com.microsoft.emmx	ios	com.microsoft.emmx.daily-df
4	osoftEdge_8wekyb3d8bbwe!MicrosoftEdge	msa	f44b1140-bc5e-48c6-8dc0-5cf5a53c0e34	msa	00000004C1BC462	android	com.microsoft.emmx.daily	android	com.microsoft.emmx.selfhost	android	com.microsoft.emmx	ios	com.microsoft.emmx.daily-df
5	osoftEdge_8wekyb3d8bbwe!MicrosoftEdge	msa	f44b1140-bc5e-48c6-8dc0-5cf5a53c0e34	msa	000000004C1BC462	android	com.microsoft.emmx.daily	android	com.microsoft.emmx.selfhost	android	com.microsoft.emmx	ios	com.microsoft.emmx.daily-df

Similarly, the 'Activity' and the 'ActivityOperation' table 'payload' fields (blob) are also in json format with different entries related to the different platform type as follows:

# For "x\_exe\_path", "windows\_win32" and "windows\_universal" it doesn't include duration when an app is first executed:



but includes it in subsequent entries:



Having included my own duration calculation (calculated by subtracting the 'StartTime' from the 'EndTime'), the duration is sometimes different than the one included in the json blob. A longer calculated duration could indicate that the app is in focus but idle i.e. the user does not interact with it.

When "windows\_universal" or "windows\_win32" applications open a file, the 'payload' field includes quite a bit of information.

"windows\_universal" (In this case MS Edge - which uses the <u>Adaptive Card framework</u> - bing search for CDPTraces.log) can be seen below:



And 'windows\_win32' here:



The 'ExpirationTime' fields in both Activity and Activity\_PackageId tables are the same for each 'ID' and 'ActivityId' respectively (Unique field entry GUID).

All Dates/Times are stored by the database in UTC. To get the local times, we can adjust the query by using, 'localtime' e.g. :

```
datetime(Activity.StartTime , 'unixepoch', 'localtime'),
```

The 'ExpirationTime' is exactly 2592000 seconds or 30 Days from the relevant entry's 'LastModified' time, and is easily seen by using the following:

```
Select
(Activity.ExpirationTime - Activity.LastModifiedTime) as 'Expires in'
From Activity
```

Sorting the query by the 'ETAG' field gives a historical list (sort of a timeline) according to the Events recorded in the db, but is not the same as if sorted by Start, End or Expiry datetimes. The ETAG can change for a particular entry's GUID depending on the current action the database has recorded for that ID (e.g. user removed Tile from timeline).

An example that an ID can have multiple ETAGs associated with it, is shown below:

	ID	Program Name	Nr_of_ETAGs_per_ID
1	14A18F08264CCBEEE1F87294159CC174	Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge	12
2	E410C45C9351D584F5FF8771FB79EBE0	Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge	12
3	3850384E31582BB4D7444A87238EBE71	Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge	11
4	7FBCA86B1284531AB13714378DE462BF	Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge	11
5	AF83A1D79E8018D88E34C6DA0367D8D2	Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge	11
6	005A5B3C02AF18D3D743923C12A6A1A4	{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe	4
7	00AEEED61A3676A61C4683F4ADF956DC	{6D809377-6AF0-444B-8957-A3773F02200E}\Windows NT\Accessories\wordpad	4
8	0197B6BDC361072CAE085484AF9E9D13	{6D809377-6AF0-444B-8957-A3773F02200E}\Windows NT\Accessories\wordpad	4
9	019F2517AFD0B40206B668B4B979C5F3	Chrome	4
10	026D393D2A3C851046DD8296FFFFA0C1	Chrome	4

by running this query against a MS account's 'ActivitiesCache.db':

```
1 select
2 hex(Activity.id) as 'ID',
3 json_extract(Activity.AppId, '$[2].application') as 'Program Name',
4 count(activity.etag) as 'Nr_of_ETAGs_per_ID'
5 from Activity
6 join Activity_PackageId on activity.id = Activity_PackageId.ActivityId
7 group by ID
8 order by Nr_of_ETAGs_per_ID desc
```

The 'PlatformDeviceID' seen in the 'Activity' & 'ActivityOperations' tables:

PlatformDeviceId	c^	506 PR	AGMA	ignore_c	check_const
Filter	Fi	507 PR	RAGMA	journal	mode
7it7kvkbMZ9R20MhUL/UCkDTVs44	0	<			
7it7kvkbMZ9R20MhUL/UCkDTVs44	0	Edit Databas	co Coll		
7it7kvkbMZ9R20MhUL/UCkDTVs44	0	CUIL Databas	se cei		
7it7kvkbMZ9R20MhUL/UCkDTVs44	0	Mode: Te	ot •	Impor	rt Expo
7it7kvkbMZ9R20MhUL/UCkDTVs44	0				10
7it7kvkbMZ9R20MhUL/UCkDTVs44	0	7it7kvk	kbMZ9	R20MhUL/	1
7it7kvkbMZ9R20MhUL/UCkDTVs44	0	UCkDT	V\$445	Orje52mr\	WLi1gA=
7it7kvkbMZ9R20MhUL/UCkDTVs44	0				

can be found in the user's NTUSER.dat at

## "Software\Microsoft\Windows\CurrentVersion\TaskFlow\DeviceCache\".

## As seen below:

Key name		# values	00	an a rokenn head	er here to crocio hir	that column
	7it7kvkbMZ9R20MhUL/UCkDTVs4450rj			Value Name	Value Type	Data
	7jBa 1plaSCvrXW 10umfoOZUPoqGRdvzncK4e		۲			
	en8WEeuzdXY4kusjOThS+6fAUNSeU5xorU6c		٠	DeviceName	RegSz	ALIEN
	🛅 ЮкбhyGOHLCgUIuwaRzmpcjqa7+SdY380np5			DeviceType	RegDword	15
	S+3dLRYe2xDz2N0adnS4ou0RDxKWRptZbyf			DeviceMake	RegSz	Alenware
	Yd98tylCyWtQS5jTPjr+weOyQ/ceopRRyL6aX			DeviceModel	RegSz	Alenware 15 R3
	YHgsOGnQYlv1sCENiXZFVgAahHBF3bKutop4					

But it is not fixed - it looks encoded with the <u>QuickXorHash</u> Algorithm, similar to the 'FileShellLink' in the 'Payload' field blob - and it changes occasionally,

#### Device ID

- 190 TDdtGmqdscQk78xppyGhb2yzThGYW8Ldm8tsq+GJ9n4=
- 191 TDdtGmqdscQk78xppyGhb2yzThGYW8Ldm8tsq+GJ9n4=
- 192 TDdtGmqdscQk7BxppyGhb2yzThGYW8Ldm8tsq+GJ9n4=
- 193 TDdtGmqdscQk7BxppyGhb2yzThGYW8Ldm8tsq+GJ9n4=
- 194 Yd9BtyKlyWtQS5jTPjr+weOyQ/ceqpRRyL6aX0XAiro=
- 195 Yd9BtyKlyWtQS5jTPjr+weOyQ/ceqpRRyL6aX0XAiro=
- 196 Yd9BtyKlyWtQS5jTPjr+weOyQ/ceqpRRyL6aX0XAiro=

still depicting the same Machine (as seen at the relevant registry entries). Have not yet found the pattern as to why or when it changes when a user logs in with a local account.

According to <u>Microsoft</u> "..Note that the hardware hash also contains details about when it was generated, so it will change each time it is generated.." which makes sense.



It is used to show the Device\* origin of a Tile in the Timeline view, such as:

\*(if no device name is seen in one or more tiles in the user's Timeline view, then the activity is local)

The device name seen above is derived from the "DeviceModel" entry in the registry for the specific DeviceID. That information originates from the OEM information value in 'SystemProductName' at "HKLM\SYSTEM\ControlSet001\Control\SystemInformation" which is usually filled by the device manufacturer, or is blank when the computer is user assembled.

The 'AppActivityId' field has 3 possible observed values:

- ECB32AF3-1440-4086-94E3-5311F97F89C4 which looks like a GUID but having checked 4 different computers of different users except my own ones, this GUID remains the same in all of them.
- An alphanumeric identifier (Hash?) following the above GUID, which is specific to a file opened, or
- A URL opened by MS Edge (on MS Account related 'ActivitiesCache.db' databases).

This can be seen by running the following:

```
select
case when Activity.AppActivityId not like '%-%-%-%-%\%' then Activity.AppActivityId
when Activity.AppActivityId not like '%-%-%-%' then Activity.AppActivityId
else substr(Activity.AppActivityId , 38)
end as 'DeviceID',
datetime(Activity.StartTime, 'unixepoch', 'localtime') AS 'StartTime',
json_extract(Activity.Payload, '$.displayText') as 'File_Name'
from Activity
join Activity_PackageId on activity.id = Activity_PackageId.ActivityId
group by File_Name
order by StartTime asc
```

	DeviceID	StartTime	File Name
13	ECB32AF3-1440-4086-94E3-5311F97F89C4	2018-05-01 07:20:10	7-Zip File Manager
4	ECB32AE3-1440-4086-94E3-5311E97E89C4	2018-05-01 07:24:15	SystemPropertiesAdvanced exe
15	ECB32AF3-1440-4086-94E3-5311F97F89C4	2018-05-01 07:28:48	Opera Browser
16	ECB32AF3-1440-4086-94E3-5311F97F89C4	2018-05-01 07:35:45	ESEDatabaseView.exe
7	ECB32AF3-1440-4086-94E3-5311F97F89C4	2018-05-01 07:45:59	ire-8u171-windows-x64.exe
8	4cc59f0fe7ab8e7280b2c4228bcd76193b3e5f3f	2018-05-01 07:58:11	backup.tar
9	fc1379ad2d57897a2013f92a6e5d53e0dbd1e0f8	2018-05-01 08:01:38	tealium db
20	h6o7o75f16f5d0fddf4260ho2o2o1058hcfh619o	2018-05-01 08:05:13	flivster dc2 db

The 'PackageIDHash' field is a unique value related to each application. It appears to be the 'QuickXorHash' of the executable – with this query:

```
select
     Activity.PackageIdHash as 'Hash',
     Activity_PackageId.PackageName as 'Name',
     datetime(Activity.StartTime, 'unixepoch', 'localtime') AS 'StartTime'
     from Activity
     join Activity_PackageId on activity.id = Activity_PackageId.ActivityId
group by Hash
order by StartTime desc
```

we can see that different versions of the same application have a different Hash value:

	Hash	Name	StartTime
1	LpMbiNsalvhwz9RKScqy+21v9qKArm8vsmGRxfqVh8k=	d:\_forensic tools\dmde-3.2.0.692-win32-gui\dmde.exe	2018-05-28 19:44:18
2	83TnlWHEKIgYDl4QLfHkrWYjNrlRwf7OP4R6Djg6TXI=	d:\_forensic tools\dmde-3.0.6.648-win32-gui\dmde.exe	2018-05-28 19:44:00

The 'Activity' table's 'ActivityStatus' and 'ActivityOperation' tables's 'OperationType' have 3 observed values ranging from 1 to 3 and depict the related Tile Status as:

1 -> Active (means it is still an open application)

2-> Updated (means the entry is an update for a previously Active entry)

**3**-> Deleted (means the Tile is removed from the Timeline)

And there <u>could be a  $4^{th}$  entry</u> with a value of **4**, meaning that the entry is 'Ignored'.

When a Tile is removed from the Timeline by the user,

PDF-View	er	Alienware 15 R3
Window	wsTimeline.pdf	
	Open	
	Remove	
	Clear all from Earlier Today	• m• 1

the associated ID(s) to this Tile remain the same, but the entries are copied from the 'Activity' to the 'ActivityOperation' table with a NEW 'Etag' and new type/status value:

1	select						
2	activity.etag as 'Activity Etag',						
3	hex(activity.id) as 'Activity ID',						
4	Activity.Act	ivityStatus <b>as 'Type'</b> ,					
5	ActivityOper	ation.ETag as 'ActivityOperation	n Etag	',			
6	hex (Activity	Operation.Id) as 'ActivityOperat	tion I	D',			
7	ActivityOper	ation.OperationType as 'Type'					
8	from Activit	У					
9	join Activit	"Operation on Activity.Id = Acti	lvityo	Posti un 10			
			-				
	Activity Etag	Activity ID	Type	ActivityOperation Etag	ActivityOperation ID	Туре	
1	19255	942964941C4A1FC75A837A1CFC8CFF92	1	20098	942964941C4A1FC75A837A1CFC8CFF92	3	
2	19264	0DE4C1CFA7AD59E7B9F9A3A0509D21CA	1	20099	0DE4C1CFA7AD59E7B9F9A3A0509D21CA	3	
3	19267	4B8DDEC337073252145BE8B622D2A619	1	20100	4B8DDEC337073252145BE8B622D2A619	3	
4	19270	3704910DA81C809DB04126F03E300092	1	20101	3704910DA81C809DB04126F03E300092	3	
5	19410	289D11B903A8BC64FE6305B96BC46750	1	20102	289D11B903A8BC64FE6305B96BC46750	3	

When the user logs in with a local account, and a tile is removed from the Timeline, the associated entries for that are copied from the 'Activity' to the 'ActivityOperation' table with a different 'ETAG' value, and stay there until expiration time.

An easy way to figure out which entries are User Removed can be derived from viewing the 'SmartLookup' view (*automatically created query included in the database*) which, in essence, is the source of the actual timeline a user observes:



The key here is the line: FROM [Activity] WHERE [Id] NOT IN (SELECT [Id] FROM [ActivityOperation])

If we check the 'SmartLookup' query data view, it lists all 'Activity' table entries plus all 'ActivityOperation' table entries minus the 'Activity' table entries that appear in both tables with the same ID. Why? Because when the ActivityOperation.Id is also found in the Activity.Id then the entry has been (user) removed from the timeline.

What this query also does, is to mark (and list) all entries in the 'Activity' table with a value of 0 in the field [IsInUploadQueue], and all entries in the 'ActivityOperations with a value of 1 in the [IsInUploadQueue]. What this means, is that the entries in the 'ActivityOperations' table are in the 'Upload to Cloud Queue' unless they also appear in the 'Activity' table.

However, when a user is logged in with a MS Account, and the user removes a tile from the Timeline, the respective entries are copied to the 'ActivityOperation' table with a new 'Etag' value and a new type/status of 3 (*Deleted*) momentarily until they are synced, and then they are

moved to the 'Activity' table until they expire. The type/status value 3 tells the other synchronized devices not to display this tile in their Timeline. This may be confusing when examining an offline system:

Table:	ActivityOperation	n		
	OperationOrder	Id	OperationType	AppId
	Filter	Filter	Filter	Filter
1	1	�)d� J �Z	3	{"application"
2	2	<b>��</b> \$ <b>\$</b> Y <b>\$\$</b>	3	{"application"
3	3	K���7 2R	3	application"
4	4	BLOB	3	{"application"
5	5	(� � ��d	3	{"application"

The following query checks every ID on 'Activity\_PackageID' against both 'Activity' and 'ActivityOperation' tables and provides the relevant results:



```
case
                            when Activity_PackageId.ActivityId in
                            (select Activity.Id from activity) and
                            Activity_PackageId.ActivityId not in
                            (select ActivityOperation.Id from ActivityOperation)
                                     then 'New Activity - '||hex(Activity_PackageId.ActivityId)
                                     else
                                     case
                                               when Activity_PackageId.ActivityId
                                               not in (select Activity.Id from Activity)
                                               and Activity_PackageId.ActivityId
                                               in (select ActivityOperation.Id from ActivityOperation)
                                               then
         In Upload Queue - '||hex(Activity_PackageId.ActivityId)
                  end
                  end
         end
end as 'Status_ID', -- This field includes both the Status and the unique ID of the associated activity
Activity_PackageId.PackageName as 'PackageName', -- The program/ associated with the above ID
datetime(Activity_PackageId.ExpirationTime, 'unixepoch', 'localtime') as 'ExpirationTime',
Activity_PackageId.Platform
from Activity PackageId
where Activity_PackageId.Platform in ('windows_win32', 'windows_universal', 'x_exe_path')
group by Status_ID
order by ExpirationTime asc
```

We can see which ID's entry is a:

- 'New activity'

- 'Had the associated timeline tile removed'
- 'In the Upload Queue'

- Archived' (until expiration time)

	Status_ID	PackageName	ExpirationTime Platform
2464	New Activity - FAC3BF8F86CC8D737E2912333C1B480B	microsoft.office.outlook.exe.15	2018-08-21 18:29:32 windows_win32
2465	New Activity - A082487B90E1920C1E794CCE485D46D6	microsoft.office.outlook.exe.15	2018-08-21 18:29:54 windows_win32
2466	Is Archived - AA02B8BF0A259DEAE764099B3E5BCB8B	(6d809377-6af0-444b-8957-a3773f02200e)\db browser for sqlite\db browser for sqlite.exe	2018-08-24 10:30:25 windows_win32
2467	Is Archived - 5D82FFF1A179FFEAC9A59CE52FC48ACA	windows.immersivecontrolpanel_cw5n1h2txyewy	2018-08-24 10:30:44 windows_universa
2468	New Activity - E4D4D3EE8FF161D4D330C2C5FAAEECF2	{6d809377-6af0-444b-8957-a3773f02200e}\db browser for sqlite\db browser for sqlite.exe	2018-08-24 10:30:44 windows_win32
2469	Is Archived - F48D10A0C52199D9D35BDB1EE68CBC4E	windows.immersivecontrolpanel_cw5n1h2txyewy	2018-09-25 23:06:50 windows_universa
2470	Is Archived - 65D2974DC6A859499B8B20FA926146BE	microsoft.office.outlook.exe.15	2018-11-21 17:29:58 windows_win32

2471 Is Archived - 732C5C66B18DBB39B19AAE2D48AA8C65 windows.immersivecontrolpanel\_cw5n1h2txyewy

2018-11-21 17:29:59 windows\_universal

The 'Priority' field has these possible values (and assumed explanations):

- 0 None
- 1 High
- 3 Low

As indicated by <u>MS Graph REST API</u>: "Indicates the priority of a raw user notification. Visual notifications are sent with high priority by default. Valid values are None, High and Low."

Note: The 'userTimezone' information found in 'ActivityType' 6 entries's 'Payload' field is: "..the timezone in which the user's device used to generate the activity was located at activity creation time; values supplied as IATA/Olson ID's in order to support cross-platform representation."

<u>Source</u>

## Changes with Windows 10 version 1809 (October 2018 update)

(The following in based on Win10 Insider's build 17744.rc5\_release.180818-1845)



## The previous (1803) was structured like this:

With the main tables being 'Activities' and 'ActivitiesOperation', while 'Activities\_PackageID' was the link and archive of all the activity entries.

The database structure has changed a bit with the new October 2018 Windows 10 update (version 1809). A new table is introduced:



As well as new fields in both Activity & ActivityOperation tables:

Activity	ActivityOperation
	UploadAllowedByPolicy
UserActionState	UserActionState
IsRead	IsRead
GroupItems	GroupItems

The first 2 ('UserActionState' and 'IsRead ') are most likely related to notifications ('ActivityType' 2), as according to <u>Microsoft</u>:

"..UserNotification class currently provides 2 types of state updates – you can modify the UserNotification<mark>Read</mark>State or the UserNotification<mark>UserActionState</mark> and define your own logic on what should happen when notifications are updated. For example, you can mark <u>UserActionState</u> to be <mark>Activated</mark> or <mark>Dismissed</mark>, and pivot on that value to implement universal dismiss. Alternatively, or at the same time you can mark <u>ReadState</u> as <mark>Read</mark> or <mark>Unread</mark> and based on that determine which notifications should show up in the in-app notification history view..."

Before (1803)		Afte	er (1809)	
Activity	y (main) x	Act	tivity (main) x	
*			*	
🔲 🤌 Id	Guid		P Id Guid	
🔳 Ap	opld Text		Appld Text	
🔳 Pa	ckageldHash Text		PackageldHash Text	
🔳 Ap	pActivityId Text		AppActivityId Text	
🔳 Ac	tivityType Int		ActivityType Int	
🔳 Ac	tivityStatus Int		ActivityStatus Int	
🔲 Pa	rentActivityId Guid		ParentActivityId Guid	
🔲 Ta	g Text		Tag Text	
🔳 Gr	oup Text		Group Text	
🔳 M	atchId Text		MatchId Text	
📃 La	stModifiedTime Datetime		LastModifiedTime Datetime	
Ex Ex	pirationTime Datetime		ExpirationTime Datetime	
📄 Pa	yload Blob		Payload Blob	
📄 Pr	iority Int		Priority Int	
🔳 Isl	.ocalOnly Int		IsLocalOnly Int	
Pla	atformDeviceId Text		PlatformDeviceId Text	
Cr	eatedInCloud Datetime		CreatedInCloud Datetime	
Sta	artTime Datetime		StartTime Datetime	
En En	dTime Datetime		EndTime Datetime	
📃 La	stModifiedOnClient Datetime		LastModifiedOnClient Datetime	
Gr Gr	oupAppActivityId Text		GroupAppActivityId Text	
CI	ipboardPayload Blob		ClipboardPayload Blob	
En En	terpriseld Text		Enterpriseld Text	
Or Or	riginalPayload Blob		OriginalPayload Blob	
Or 📃	riginalLastModifiedOnClient Datetime		OriginalLastModifiedOnClient Datetime	
ET ET	ag Int		ETag Int	
	<u> </u>		UserActionState Int	
1000 C			IsRead Int	
			GroupItems Text	
			<b>A</b>	

ActivityOperation (main) 🛛 🛛 🗴	ActivityOperation (main)
× .	*
OperationOrder Integer	OperationOrder Integer
Id Guid	Id Guid
	OperationType Int
	Appld Text
Appid Text	PackageldHash Text
PackageldHash Text	AppActivityId Text
AppActivityId Text	ActivityType Int
ActivityType Int	■ ParentActivityId Guid
ParentActivityId Guid	Tag Text
Tag Text	Group Text
Group Text	Matchild Text
Matchld Text	LastModifiedTime Datatime
LastModifiedTime Datetime	Expiration Time Datatime
ExpirationTime Datetime	Dayload Plob
Dayload Blob	Priority Int
	Priority Int     Created Time Datations
Created Time D 1 11	Attachments Trit
Created Lime Datetime	Attachments rext     Distribute Day isold Tast
Attachments Text	
PlatformDeviceId Text	CreatedInCloud Datetime
CreatedInCloud Datetime	Start Time Datetime
StartTime Datetime	End I ime Datetime
EndTime Datetime	LastModifiedOnClient Datetime
LastModifiedOnClient Datetime	CorrelationVector Text
CorrelationVector Text	GroupAppActivityId Text
GroupAppActivityId Text	ClipboardPayload Blob
ClipboardPayload Blob	Enterpriseld Text
Enterprised Text	OriginalPayload Blob
OriginalDayload Plab	OriginalLastModifiedOnClient Datetime
	ETag Int
OriginalLastiviodifiedOnClient Datetime	UploadAllowedByPolicy Int
ETag Int	PatchFields Blob
A	UserActionState Int
	IsRead Int
	GroupItems Text
	OperationExpirationTime Datetime
Table: 🔲 ManualSequence	Table: ManualSequence
Key Value	Key Value
Filter Filter	Filter Filter
i itor i incor	1 Activity 127355
1 Activity 126910	
Table: C Metadata	Table: Metadata
Key Value Filter Filter	Key         Value           Filter         Filter           1         CurrentSottinge           /*/stabil/Tungs*/(0.1.2.3.6.5.7.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1
1         CurrentSettings         {"ActivityTypes":[4,3,2,1,0,5,13,6],"Environment":"prod"}           2         DatabaseInstanceId         23919	2011     2011
3 DatabaseInstanceIdUpdateTime 2018-05-10T13:58:59.758Z	4 CurrentEtag         ec9c6840-add6-1184-9117-01020305070d           5 DatabaseNotificationSubscriptionInfo         ("partialSyncToken""," "publisherFilters";{("activityTypes";[0,1,2,3,4,5,6,7,13.151,"application","**").4
4 Currentitag bbaa7770-adbf-11e8-9117-01020305070d	6 DatabaseActivityPolicies {"AllowedSubscriptionSyncScopes":[("allowedTypes":[0,1,2,3,4,5,6,7,10,13,15],"application":"*"),("a 7 PendingActivityTypes {"activityTypes":[]}

The Metadata table is the one major change. The Current Settings key, as previously, is where the allowed Activity Types are listed:

1	CurrentSettings	{"ActivityTypes":[0,1,2,3,4,5,6,7,11,12,13,15],"Environment":"prod		
1	CurrentSettings	{"ActivityTypes":[0,1,2,3,4,5,6,7,13,15],"Environment":"prod"}		

New Keys are introduced:

- DatabaseNotificationSubscriptionInfo,
- DatabaseActivityPolicies and
- PendingActivityTypes

as well as new ActivityTypes & Policies:

Ta	able: 🗉 Metadata				
	Key	Value			
	Filter	Filter			
1	CurrentSettings	{"ActivityTypes":[0,1,2,3,4,5,6,7,11,12,13,15],"Environment":"prod"}			
2	DatabaseInstanceId	23919			
3	DatabaseInstanceIdUpdateTime	2018-05-10T13:58:59.758Z			
4	CurrentEtag	ec9c6840-add6-11e8-9117-01020305070d			
5	DatabaseNotificationSubscriptionInfo	{"partialSyncToken":"","publisherFilters":[{"activityTypes":[0,1,2,3,4,5,6,7,13,15],"application":"*"},{"activit			
6	DatabaseActivityPolicies	{"AllowedSubscriptionSyncScopes":[{"allowedTypes":[0,1,2,3,4,5,6,7,10,13,15],"application":"*"},{"allowed			
7	PendingActivityTypes	{"activityTypes":[]}			

In the 'DatabaseActivityPolicies' key's value (json field), we can see "AllowedSubscriptionSyncScopes" and "Policies" as the main fields:



"AllowedSubscriptionSyncScopes"'s Elements is where the Allowed Activity Types (*to be synched across devices*) are listed as well as the respective application & platform. For example:

Tag	Value
✓ <object></object>	
✓	
✓ <	
✓ allowedTypes	
- = 0	
1	
- = 2	
- = 3	
- = 4	
- = 5	
- = 6	
- 😑 10	
- 😑 13	
- <mark>=</mark> 15	
application	*

ActivityTypes 0-7 and 10, 13 and 15 are allowed for (\*) all applications, but



Activity Types 11 and 12 are only allowed for the application "Microsoft.Credentials.WiFi" and only for the Platform entry "data\_boundary".

The Policies field



Has entries like this in each Element:



Where the PermissionScope is the Application, and Type is the ActivityType blocked for this application. BlockedOperationFlags has seen with values 0, 1 and 7. In the above screenshot, MicrosoftPersonalization and Microsoft.Credentials apps are NOT blocked for ActivityTypes 11 and 12.

BlockedOperationFlags value 1 means that this Element is Blocked for example, ActivityType 8 is blocked (*we can see that in the AllowedTypes as well*):



Whereas value 0 means that this ActivityType is NOT blocked:

✓ < <element #11=""></element>	
BlockedOperationFlags	0
🗸 🌮 Scope	
PermisionScope	
Type	10
Source	4

(ActivityType 10 is listed in the AllowedTypes).

However a BlockedOperationFlags with value 7

∨ 🌮 <element #14=""></element>	
🔤 BlockedOperationFlags	7
🗸 🌮 Scope	
PermisionScope	Microsoft. Accessibility
Type	11
Source	5

Is not yet explained.

The key "DatabaseNotificationSubscriptionInfo" is also a JSON blob:



where in the 'publisherFilters' we see



that ActivitiyTypes 0-7, 13 and 15 are allowed for (\*) all applications.

Finally 'PendingActivityTypes' value is also a JSON blob, but empty at this time.

Back to the ActivitiesCaches.db changes, there is also a new table, DataEncryptionKeys:

Da	abase Structure	Browse Data	Edit Pragmas	Execute SQL						
Tab	Table: DataEncryptionKeys									
	KeyVers	sion	Key	/Value	CreatedInCloudTime					
	Filter		Filter		Filter					
1 3362556070382464122		AQAAANCMnd8E	BFdERjHoAwE/Cl	1535762460						

The Smartlookup view (query) view changed:

select         select           [0].ldp,         [0].ldp,           [0].lapid],         [0].lapid],           [0].lapid],         [0].lapkatuityd],           [0].lapkatuityd],         [0].lapkatuityd],           [0].lapkatuityd],         [0].lapkatuityd],           [0].lactivityType],         [0].lactivityType],           [0].lactivityLactivity[],         [0].lactivityLactivity[],           [0].lactivityLactitine],         [0].l	Smartlookup (1803)	Smartlookup (1809)
[0].[a],         [0].[a],           [0].[appid],         [0].[appid],           [0].[appid],         [0].[appid], <td>select</td> <td>select</td>	select	select
[0].[Appid],         [0].[Appid],           [0].[AppActivityId],         [0].[AppActivityId],           [0].[AppActivityId],         [0].[AppActivityId],           [0].[AppActivityId],         [0].[ActivityType],           [0].[ActivityType],         [0].[ActivityType],           [0].[ParentActivityId],         [0].[ParentActivityId],           [0].[ParentActivityId],         [0].[FarentActivityId],           [0].[Group],         [0].[Group],           [0].[Matchid],         [0].[AstModfiedTime],           [0].[ExpirationTime],         [0].[ExpirationTime],           [0].[ExpirationTime],         [0].[ExpirationTime],           [0].[Priority],         [0].[Priority],           [A].[Isticaclonly],         [0].[Priority],           [A].[Isticaclonly],         [0].[EndTime],           [0].[EndTime],         [0].[EndTime],	[O].[Id],	[O].[Id],
[0].[PackageidHash],         [0].[PackageidHash],           [0].[AppActivityId],         [0].[AppActivityId],           [0].[ActivityType],         [0].[ActivityType],           [0].[OperationType] AS [ActivityStatus],         [0].[OperationType] AS [ActivityStatus],           [0].[OperationType] AS [ActivityStatus],         [0].[OperationType] AS [ActivityStatus],           [0].[FarentActivityId],         [0].[FarentActivityId],           [0].[CorpuPapActivityId],         [0].[CorpuPapActivityId],           [0].[CorpuPapActivityId],         [0].[Corp	[O].[AppId],	[O].[AppId],
[0]. AppActivityId].         [0]. AppActivityId].           [0]. ActivityType].         [0]. ActivityType].           [0]. AppactivityId].         [0]. AppActivityId].           [0]. IParemActivityId].         [0]. IParemActivityId].           [0]. IParemActivityId].         [0]. IParemActivityId].           [0]. IParemActivityId].         [0]. IParemActivityId].           [0]. IMatchid].         [0]. IMatchid].           [0]. IMatchid].         [0]. IMatchid].           [0]. IExpirationTime].         [0]. IExpirationTime].           [0]. IParemActivityId].         [0]. IExpirationTime].           [0]. IExpirationTime].         [0]. IExpirationTime].	[O].[PackageIdHash],	[O].[PackageldHash],
[0]. ActivityType],         [0]. ActivityType],           [0]. [OperationType] AS [ActivityStatus],         [0]. [OperationType] AS [ActivityStatus],           [0]. [ParentActivityId],         [0]. [ParentActivityId],           [0]. [FarentActivityId],         [0]. [FarentActivityId],           [0]. [Group],         [0]. [Group],           [0]. [Matchid],         [0]. [Carun],           [0]. [LastModifiedTime],         [0]. [LastModifiedTime],           [0]. [LastModifiedTime],         [0]. [Eavioad],           [0]. [Pavload],         [0]. [Pavload],           [0]. [Pavload],         [0]. [Eavime],           [0]. [StartTime],         [0]. [Cartime],           [0]. [Inatime],         [0]. [Cartime],           [0]. [GroupAppActivityId],         [0]. [Cartime],           [0]. [GroupAppActivityId],         [0]. [Carterprisel],           [0]. [GroupAppActivityId],         [0]. [Carterprisel],           [0]. [GroupAppActivityId],         [0]. [Carterprisel],           [0]. [GroupAppActivityId],         [0]. [Carterprise	[O].[AppActivityId],	[O].[AppActivityId],
[0].[OperationType] AS [ActivityStatus],         [0].[OperationType] AS [ActivityStatus],           [0].[ParentActivityId],         [0].[ParentActivityId],           [0].[Goup],         [0].[Tag],           [0].[Goup],         [0].[Goup],           [0].[Matchid],         [0].[Matchid],           [0].[Matchid],         [0].[Matchid],           [0].[LastModifiedTime],         [0].[ExpirationTime],           [0].[PariotAd],         [0].[ExpirationTime],           [0].[PariotAd],         [0].[PariotAd],           [0].[PariotAd],         [0].[PariotAd],           [0].[PariotAd],         [0].[PariotAd],           [0].[PariotAd],         [0].[PariotAd],           [0].[PariotAd],         [0].[PariotAd],           [0].[PariotAd],         [0].[PariotAd],           [0].[PariotAd],         [0].[ExpirationTime],           [0].[PariotAd],         [0].[PariotAd],           [0].[PariotAd],         [0].[PariotAd],           [0].[PariotAd],         [0].[Enternie],           [0].[LastModifiedOnClient],         [0].[EnterniseId],           [0].[GroupAppActivityId],         [0].[IbboardParioad],           [0].[GroupAppActivityId],         [0].[IbboardParioad],           [0].[CroupAppActivityId],         [0].[IbboardParioad],           [0].[CroupAppActivi	[O].[ActivityType],	[O].[ActivityType],
[0][ParentActivityId].         [0][ParentActivityId].           [0][Tag].         [0][Group].           [0][Group].         [0][Group].           [0][Group].         [0][Group].           [0][BasthadfiedTime].         [0][ExpirationTime].           [0][ParkodfiedTime].         [0][ExpirationTime].           [0][ParkodfiedTime].         [0][ParkodfiedTime].           [0][ParkodfiedTime].         [0][ParkodfiedTime].           [0][ParkodfiedTime].         [0][ParkodfiedTime].           [0][ParkodfiedTime].         [0][ParkodfiedTime].           [0][ParkodfiedTomDeviceId].         [0][ParkomDeviceId].           [0][ParkodfiedTomDeviceId].         [0][ExtratTime].           [0][EastModfiedConClient].         [0][EastModfiedConClient].           [1][StocaIOnk].         [0][Enstime].           [0][IastModfiedConClient].         [0][Enstime].           [0][EastModfiedConClient].         [0][Enstime].           [0][GroupAppActivityId].         [0][CimboardPayload].           [0][CimparPayload].         [0][CimparPayload].           [0][CimparPayload].         [0][CimparPayload].           [0][CimparPayload].         [0][CimparPayload].           [0][CimparPayload].         [0][CimparPayload].           [0][CimparPayload].         [0][CimparPayload].	[O].[OperationType] AS [ActivityStatus],	[O].[OperationType] AS [ActivityStatus],
[0][Tag],         [0][Tag],           [0][Group],         [0][Group],           [0][Matchid],         [0][Matchid],           [0][LastModifiedTime],         [0][ExpirationTime],           [0][Payload],         [0][ExpirationTime],           [0][Payload],         [0][Payload],           [0][Payload],         [0][Payload],           [0][Payload],         [0][Payload],           [0][PlatformDeviceId],         [0][PlatformDeviceId],           [1][Sisca3OhV],         [A][Sisca2OhV],           [2][PlatformDeviceId],         [0].[CastHodifiedOnClient],           [3][CreatedInCloud],         [3][CreatedInCloud],           [4].[Sisca2OhV],         [3][Sisca3OhV],           [5][IndUploadQueue],         1 AS [IsinUploadQueue],           [6].[CastModifiedOnClient],         [0].[LastModifiedOnClient],           [7][CipboardPayload],         [0].[CipboardPayload],           [6].[GroupApActivityId],         [0].[CipboardPayload],           [6].[GroupApActivityId],         [0].[CipboardPayload],           [6].[CipboardPayload],         [0].[CipboardPayload],           [6].[CipboardPayload],         [0].[CipboardPayload],           [6].[CipboardPayload],         [0].[CipboardPayload],           [6].[CipboardPayload],         [0].[CipboardPayload],	[O].[ParentActivityId],	[O].[ParentActivityId],
[0].[Group],         [0].[Group],           [0].[Matchid],         [0].[Matchid],           [0].[ExpirationTime],         [0].[LastModifiedTime],           [0].[ExpirationTime],         [0].[ExpirationTime],           [0].[Payload],         [0].[Payload],           [0].[Priority],         [0].[Priority],           [0].[Priority],         [0].[Priority],           [0].[Priority],         [0].[Priority],           [0].[StartTime],         [0].[Priority],           [0].[StartTime],         [0].[EndTime],           [0].[EndTime],         [0].[EndTime],           [0].[StartTime],         [0].[EndTime],           [0].[EndTime],         [0].[EndTime],           [0].[CirpbardPayloadQueue],         1 AS [IsinUploadQueue],           [1].[AstModifiedOnClient],         [0].[GroupAppActivity]d],           [0].[CirpbardPayload],         [0].[CirpbardPayload],           [	[O].[Tag],	[O].[Tag],
[0].[Matchid],         [0].[Matchid],           [0].[LastModifiedTime],         [0].[ExpirationTime],           [0].[ExpirationTime],         [0].[ExpirationTime],           [0].[Payload],         [0].[Payload],           [0].[Payload],         [0].[Payload],           [0].[Payload],         [0].[Payload],           [0].[PaitormDevicetd],         [0].[PaitormDevicetd],           [0].[PaitormDevicetd],         [0].[CreatedInCloud],           [0].[EastModifiedOnClient],         [0].[LastModifiedOnClient],           [0].[LastModifiedOnClient],         [0].[LastModifiedOnClient],           [0].[EndTime],         [0].[GroupApActivityId],           [0].[EndTime],         [0].[GroupApActivityId],           [0].[GroupApActivityId],         [0].[GroupApActivityId], <td>[0].[Group],</td> <td>[0].[Group],</td>	[0].[Group],	[0].[Group],
[0]. [LastModifiedTime],         [0]. [LastModifiedTime],           [0]. [ExpirationTime],         [0]. [ExpirationTime],           [0]. [Payload],         [0]. [Payload],           [0]. [Payload],         [0]. [Payload],           [0]. [Payload],         [0]. [Payload],           [0]. [Payload],         [0]. [Payload],           [0]. [PatformDeviceld],         [0]. [PatformDeviceld],           [0]. [EatTime],         [0]. [StartTime],           [0]. [EatModifiedOnClient],         [0]. [EatModifiedOnClient],           [0]. [LastModifiedOnClient],         [0]. [EatTime],           [0]. [LastModifiedOnClient],         [0]. [EatTime],           [0]. [CirpopAppActivityId],         [0]. [CirpopAppActivityId],           [0]. [CirpoardPayload],         [0]. [CirpboardPayload],           [0]. [CirpbaardPayload],         [0]. [CirpbaardPayload],           [0]. [CirpbaardPayload],         [0]. [CirpbaardPayload],           [0]. [CirpinalPayload],         [0]. [CirpinalPayload],           [0]. [CirginalPayload],         [0]. [CirpinalPayload], </td <td>[O].[Matchid],</td> <td>[O].[Matchid],</td>	[O].[Matchid],	[O].[Matchid],
[0].[ExpirationTime],         [0].[ExpirationTime],           [0].[Payload],         [0].[Payload],           [0].[Priority],         [0].[Priority],           [0].[PinformDeviceId],         [0].[PatformDeviceId],           [0].[PatformDeviceId],         [0].[PatformDeviceId],           [0].[ExtincalOnly],         [0].[Extince],           [0].[Extince],         [0].[Extince],           [0].[ExtModifiedOnClient],         [0].[ExtModifiedOnClient],           [0].[ExtModifiedOnClient],         [0].[ExtModifiedOnClient],           [1].[Gi_LostModifiedOnClient],         [0].[CipboardPayload],           [0].[GroupAppActivityId],         [0].[CipboardPayload],           [0].[GroupAppActivityId],         [0].[CipboardPayload],           [0].[CirginalPayload],         [0].[CirginalPayload],	[O].[LastModifiedTime],	[0].[LastModifiedTime],
i0].[Payload],         i0].[Prority],           i0].[Prority],         i0].[Prority],           i0].[Prority],         i0].[Prority],           i0].[PlatformDeviceId],         i0].[PlatformDeviceId],           i0].[PlatformDeviceId],         i0].[PlatformDeviceId],           i0].[CreatedInCloud],         i0].[StartTime],           i0].[LastModifiedOnClient],         i0].[LastModifiedOnClient],           i1AS [IsinUploadQueue],         i1AS [IsinUploadQueue],           i0].[GroupAppActivityId],         i0].[CreatedIncPayload],           i0].[CroupAppActivityId],         i0].[CreateDarDeviceId],           i0].[GroupAppActivityId],         i0].[CreateDarDeviceId],           i0].[GroupAppActivityId],         i0].[CreateDarDeviceId],           i0].[CreateDarDeviceId],         i0].[CreateDarDeviceId],           intorind         infl	[O].[ExpirationTime],	[O].[ExpirationTime],
[0].[Priority],         [0].[Priority],           [A].[Ist.ccalOnly],         [A].[Ist.ccalOnly],           [0].[PlatformDeviceId],         [0].[PlatformDeviceId],           [0].[FlatformDeviceId],         [0].[PlatformDeviceId],           [0].[EntTime],         [0].[EntTime],           [0].[EntTime],         [0].[EntTime],           [0].[EntTime],         [0].[EntTime],           [0].[EntpriseId],         [0].[ClipboardPayload],           [0].[ClipboardPayload],         [0].[EnterpriseId],           [0].[ClipboardPayload],         [0].[EnterpriseId],           [0].[ClipboardPayload],         [0].[ClipboardPayload],           [0].[ClipboardPayload],         [0].[Ulipticationstate],           [0].[OriginalEastModifiedOnClient],         [0].[OriginalEastModifiedOnClient],           [0].[OriginalEastModifiedOnClient],         [0].[OriginalEastModifiedOnClient],           [0].[ClipboardPayload],         [0].[OriginalEastModifiedOnClient],           [0].[Itag]         [0].[Itag]           [o].[Itag]         [0].[Itag]           [o].[Itag]         [0].[Itag]           [Itag]         [Itag]           [Itag]         [Itag]           [Itag]         [Itag]           [Itag]         [Itag]           [Itag],         [Itag], <td>[O].[Payload],</td> <td>[O].[Payload],</td>	[O].[Payload],	[O].[Payload],
[A].[istocalOnly],         [A].[istocalOnly],           [Q].[PlatformDeviceId],         [Q].[PlatformDeviceId],           [A].[CreatedInCloud],         [Q].[EndTime],           [Q].[EndTime],         [Q].[EndTime],           [Q].[LastModifiedOnClient],         [Q].[EndTime],           [Q].[LastModifiedOnClient],         [Q].[EndTime],           [Q].[LastModifiedOnClient],         [Q].[CroupAppActivityId],           [Q].[CroupAppActivityId],         [Q].[CroupAppActivityId],           [Q].[CroupAppActivityId],         [Q].[CroupAppActivityId],           [Q].[CroupAppActivityId],         [Q].[CroupAppActivityId],           [Q].[CroupAppActivityId],         [Q].[CroupAppActivityId],           [Q].[CripicalPayload],         [Q].[CripicalPayload],           [Q].[CripicalPayload],         [Q].[CripicalPayload],           [Q].[CriginalPayload],         [Q].[CriginalPayload],           [Q].[CriginalPayload],         [Q].[Cri	[O].[Priority].	[O].[Priority].
Intervention         Intervention	[A].[IsLocalOnly].	[A].[IsLocalOnly].
Litter         Litter           [A].[CreatedInCloud],         [A].[CreatedInCloud],           [O].[StartTime],         [O].[StartTime],           [O].[LastModifiedOnClient],         [O].[LastModifiedOnClient],           1 AS [IsInUploadQueue],         1 AS [IsInUploadQueue],           [O].[GroupAppActivityId],         [O].[CilipboardPayload],           [O].[Istrepriseld],         [O].[CilipboardPayload],           [O].[OriginalLastModifiedOnClient],         [O].[CilipboardPayload],           [O].[OriginalLastModifiedOnClient],         [O].[OriginalLastModifiedOnClient],           [O].[OriginalLastModifiedOnClient],         [O].[OriginalLastModifiedOnClient],           [O].[OriginalLastModifiedOnClient],         [O].[OriginalLastModifiedOnClient],           [O].[OriginalLastModifiedOnClient],         [O].[OriginalLastModifiedOnClient],           [O].[OriginalLastModifiedOnClient],         [O].[OriginalLastModifiedOnClient],           [O].[OriginalLastModifiedOnClient],         [O].[OriginalLastModifiedOnClient],           [O].[CiriginalCiriptActivity] as [A] on [O].[Id] = [A].[Id]         [O].[CiriginalCiriptActivity] as [A] on [O].[Id] = [A].[Id]           [Inion         [O].[CiriginalLastModifiedOnClient],         [O].[Id] = [A].[Id]           [Inion         [O].[CiriptAliptActivity] as [A] on [O].[Id] = [A].[Id]         [O].[CiriptAliptActivity] as [A] on [O].[Id] = [A].[Id]	[O].[PlatformDeviceId].	[O].[PlatformDeviceId].
Difference         Difference           Doi [StartTime],         Difference           [O] [EndTime],         Difference           [O] [LastModifiedOnClient],         Difference           [O] [StartTime],         Difference           [O] [StartTime],         Difference           [O] [LastModifiedOnClient],         Difference           [O] [StartTime],         Difference           [O] [ChipbaardPayload],         Difference           [O] [CoriginalEastModifiedOnClient],         Difference           [O] [CoriginalEastModifiedOnClient],         Difference           [O].[CoriginalEastModifiedOnClient],         Differe	[A].[CreatedInCloud].	[A].[CreatedInCloud].
[D][EndTime],         [D][EndTime],           [O][LastModifiedOnClient],         [O][LastModifiedOnClient],           1 AS [IsinUploadQueue],         1 AS [IsinUploadQueue],           [O][CroupAppActivityId],         [O][CroupAppActivityId],           [O][CroupAppActivityId],         [O][CroupAppActivityId],           [O][CroupAppActivityId],         [O][CroupAppActivityId],           [O][CroupAppActivityId],         [O][CroupAppActivityId],           [O][CriginalPayload],         [O][CriginalPayload],           [O][CriginalIastModifiedOnClient],         [O][CriginalPayload],           [O][CriginalIastModifiedOnClient],         [O][CriginalPayload],           [O][CriginalIastModifiedOnClient],         [O][CriginalPayload],           [O][CriginalIastModifiedOnClient],         [O][CriginalIastModifiedOnClient],           [Id]         [O][Cr	[0].[StartTime].	[O].[StartTime].
ChildChild[0].[LastModifiedOnClient],[0].[LastModifiedOnClient],1 AS [IsInUploadQueue],1 AS [IsInUploadQueue],[0].[GroupAppActivityId],[0].[CilpboardPayload],[0].[CilpboardPayload],[0].[CilpboardPayload],[0].[CirginalPayload],[0].[CinginalPayload],[0].[OriginalLastModifiedOnClient],[0].[UserActionState],[0].[CriginalPayload],[0].[CriginalPayload],[0].[CriginalLastModifiedOnClient],[0].[CriginalPayload],[0].[CriginalLastModifiedOnClient],[0].[GroupItems],[union[0].[CriginalLastModifiedOnClient],[0].[d],[0].[CriginalLastModifiedOnClient],[0].[d],[0].[CriginalLastModifiedOnClient],[0].[d],[0].[CriginalLastModifiedOnClient],[0].[d],[0].[CriginalLastModifiedOnClient],[0].[d],[0].[CriginalLastModifiedOnClient],[0].[d],[0].[CriginalLastModifiedOnClient],[0].[d],[0].[CriginalLastModifiedOnClient],[0].[d],[0].[CriginalLastModifiedOnClient],[0].[d],[0].[CriginalLastModifiedOnClient],[0].[d],[0].[CriginalLastModifiedOnClient],[0].[d],[0].[CriginalLastModifiedOnClient],[1].[d],[0].[CriginalLastModifiedOnClient],[1].[d],[0].[CriginalLastModifiedOnClient],[1].[d],[0].[CriginalLastModifiedOnClient],[2].[d],[1].[d],[2].[d],[2].[d],[3].[d],[3].[d],[4].[d],[4].[d],[4].[d],[4].[d],[4].[d],[4].[d],	[O].[EndTime].	[O].[EndTime].
Instructure         Instructure           1 AS [IsinUploaQueue],         1 AS [IsinUploaQueue],           [0].[GroupAppActivityId],         [0].[GroupAppActivityId],           [0].[ClipboardPayload],         [0].[ClipboardPayload],           [0].[CriginalPayload],         [0].[CheterpriseId],           [0].[OriginalPayload],         [0].[InterpriseId],           [0].[OriginalLastModifiedOnClient],         [0].[InterpriseId],           [0].[OriginalLastModifiedOnClient],         [0].[OriginalLastModifiedOnClient],           [0].[CriginalLastModifiedOnClient],         [0].[OriginalLastModifiedOnClient],           [o].[CriginalLastModifiedOnClient],         [0].[OriginalLastModifiedOnClient],           [eft outer join [Activity] as [A] on [O].[Id] = [A].[Id]         [O].[GroupItems],           union         [O].[Erag]         select           [fd],         [eft outer join [Activity] as [A] on [O].[Id] = [A].[Id]           [appActivityId],         [Id],           [appActivityId],         [Id],           [AppId],         [ActivityType],           [ActivityType],         [AppId],           [ActivityType],         [AppActivityId],           [ActivityType],         [ActivityType],           [Group],         [ActivityType],           [Group],         [ActivityType],	[0].[LastModifiedOnClient].	[0].[LastModifiedOnClient].
Distribution         Distribution           [0].[GroupAppAttivityId],         [0].[GroupAppAttivityId],           [0].[CripinaPayload],         [0].[CripinaPayload],           [0].[CriginalPayload],         [0].[UserActionState],           [0].[OriginalPayload],         [0].[UserActionState],           [0].[CriginalPayload],         [0].[UserActionState],           [0].[OriginalPayload],         [0].[UserActionState],           [0].[CriginalPayload],         [0].[UserActionState],           [0].[CriginalPayload],         [0].[UserActionState],           [0].[CriginalPayload],         [0].[UserActionState],           [0].[CriginalPayload],         [0].[CriginalPayload],           [1].[d]         [0].[CriginalPayload],           [2].[d]         [2].[d]         [2].[d]           [3].[d]         [3].[d]         [3].[d]           [4].[d]         [0].[CreapleTainSing [3] [0]	1 AS [IsInUploadQueue].	1 AS [IsinUploadOueue].
Difference[O].[ClipboardPayload],[O].[ClipboardPayload],[O].[ClipboardPayload],[O].[CriginalPayload],[O].[OriginalPayload],[O].[OriginalPayload],[O].[Erag][O].[Erag][O].[Erag][O].[Erag][O].[Erag][O].[ClipboardPayload],[O].[Erag][O].[Erag][O].[Erag][O].[Erag][O].[Id] = [A].[Id][O].[Erag]union[O].[Erag][Id],<	[0].[GroupAppActivityId].	[0].[GroupAppActivityId].
ID: [D: [D: [D: [D: [D: [D: [D: [D: [D: [	[O].[ClipboardPayload].	[O].[ClipboardPavload].
[O][OriginalPayload],[O][UserActionState],[O].[OriginalLastModifiedOnClient],[O][UserActionState],[O].[OriginalLastModifiedOnClient],[O].[GriginalPayload],from [ActivityOperation] as [O][O].[OriginalLastModifiedOnClient],left outer join [Activity] as [A] on [O].[Id] = [A].[Id][O].[GroupItems],union[O].[ETag]selectfrom [ActivityOperation] as [O][Id],left outer join [Activity] as [A] on [O].[Id] = [A].[Id]union[O].[ETag]selectfrom [ActivityOperation] as [O][Id],left outer join [Activity] as [A] on [O].[Id] = [A].[Id][Appld],union[PackageldHash],select[AppActivityId],[Id],[ActivityStatus],[PackageldHash],[ParentActivityId],[AppActivityId],[Tag],[ActivityType],[Group],[ParentActivityId],[Group],[Tag],[ExpirationTime],[Tag],[ExpirationTime],[Group],[Payload],[MatchId],[Priority],[LastModifiedTime],[IstocalOnly],[Payload],[PlatformDeviceId],[Payload],[CreatedInCloud],[Priority],[StartTime],[IstocalOnly],[StartTime],[IstocalOnly],	[O].[Enterpriseld].	[O].[Enterpriseld].
ID: [O]:[OriginalLastModifiedOnClient],ID: [O]:[IsRead],[O].[CriginalLastModifiedOnClient],[O].[OriginalLastModifiedOnClient],[from [ActivityOperation] as [O][O].[OriginalLastModifiedOnClient],[eft outer join [Activity] as [A] on [O].[Id] = [A].[Id][O].[Grag]selectfrom [ActivityOperation] as [O][Id],[eft outer join [Activity] as [A] on [O].[Id] = [A].[Id][Appld],[eft outer join [Activity] as [A] on [O].[Id] = [A].[Id][Appld],[Id],[Id],[Id],[PackageIdHash],select[AppActivityId],[Id],[ActivityType],[Id],[ActivityType],[AppActivityId],[ParentActivityId],[PackageIdHash],[ParentActivityId],[ParentActivityId],[Tag],[ActivityType],[Group],[ActivityType],[Group],[ActivityStatus],[MatchId],[ParentActivityId],[LastModifiedTime],[Tag],[ExpirationTime],[Group],[Payload],[MatchId],[Priority],[LastModifiedTime],[IsLocalOnly],[Payload],[PatformDeviceId],[Payload],[ParentActivity],[ExpirationTime],[PatformDeviceId],[Payload],[ParentActivity],[ExpirationTime],[PatformDeviceId],[Payload],[CreatedInCloud],[Priority],[StartTime],[IsLocalOnly],	[0] [OriginalPavload]	[O] [UserActionState]
[D][ETag]         [D][Etag]           [O].[ETag]         [O].[OriginalPayload],           from [ActivityOperation] as [O]         [O].[OriginalLastModifiedOnClient],           left outer join [Activity] as [A] on [O].[Id] = [A].[Id]         [O].[GroupItems],           union         [O].[ETag]           select         from [ActivityOperation] as [O]           [Id],         left outer join [Activity] as [A] on [O].[Id] = [A].[Id]           [Appld],         union           [PackageldHash],         select           [AppActivityId],         [Id],           [ActivityType],         [AppActivityId],           [ActivityType],         [AppActivityId],           [ParentActivityId],         [AppActivityId],           [ParentActivityId],         [AppActivityId],           [FarentActivityId],         [AppActivityId],           [FarentActivityId],         [AppActivityId],           [FarentActivityId],         [AppActivityId],           [FarentActivityId],         [AppActivityId],           [FarentActivityId],         [AppActivityId],           [FarentActivityId],         [ParentActivityId],           [FarentActivityId],         [ParentActivityId],           [Itag],         [Group],           [Payload],         [Group],      <	[0].[Originall astModifiedOnClient].	[O].[IsRead].
Top/Let/sp.         Top/Let/sp.         Top/Let/sp.           from         [ActivityOperation] as [0]         [0].[OriginalLastModifiedOnClient],           left outer join [Activity] as [A] on [0].[Id] = [A].[Id]         [0].[GroupItems],           union         [0].[ETag]           select         from [ActivityOperation] as [0]           [Id],         left outer join [Activity] as [A] on [0].[Id] = [A].[Id]           [AppId],         union           [PackageldHash],         select           [AppActivityId],         [Id],           [ActivityType],         [AppId],           [ActivityType],         [AppId],           [ActivityType],         [AppId],           [ActivityType],         [AppId],           [ActivityType],         [AppId],           [ActivityType],         [AppActivityId],           [FarentActivityId],         [ActivityType],           [Group],         [ActivityType],           [Group],         [ActivityStatus],           [Matchid],         [ParentActivityId],           [LastModifiedTime],         [Group],           [ExpirationTime],         [Group],           [Payload],         [Matchid],           [Priority],         [LastModifiedTime],           [IsLocalOnly],		[O] [OriginalPayload]
Interview         Interview         Interview           left outer join [Activity] as [A] on [O].[Id] = [A].[Id]         [O].[GroupItems],           union         [O].[Erag]           select         from [ActivityOperation] as [O]           [Id],         left outer join [Activity] as [A] on [O].[Id] = [A].[Id]           [AppId],         union           [PackageldHash],         select           [AppActivityId],         [Id],           [ActivityType],         [AppId],           [ActivityStatus],         [PackageldHash],           [ParentActivityId],         [AppActivityId],           [Itag],         [ActivityStatus],           [ParentActivityId],         [AppActivityId],           [Group],         [ParentActivityId],           [Group],         [ActivityStatus],           [MatchId],         [ParentActivityId],           [LastModifiedTime],         [Tag],           [ExpirationTime],         [Group],           [Payload],         [MatchId],           [Pariority],         [LastModifiedTime],           [IstocalOnly],         [Payload],           [PatformDeviceId],         [Payload],           [CreatedInCloud],         [Priority],           [StartTime],         [IstocalOnly],	from [ActivityOperation] as [0]	[0] [Originall astModifiedOnClient]
union[O].[ETag]selectfrom [ActivityOperation] as [O][Id],left outer join [Activity] as [A] on [O].[Id] = [A].[Id][AppId],union[PackageldHash],select[AppActivity]d],[Id],[ActivityType],[AppId],[ActivityType],[AppId],[ActivityStatus],[PackageldHash],[ParentActivityId],[Id],[ActivityStatus],[PackageldHash],[ParentActivityId],[AppActivityId],[Tag],[ActivityType],[Group],[ActivityStatus],[MatchId],[ParentActivityId],[LastModifiedTime],[Tag],[ExpirationTime],[Group],[Payload],[MatchId],[Pariot],[LastModifiedTime],[IsLocalOnly],[ExpirationTime],[PlatformDeviceId],[Payload],[StartTime],[IsLocalOnly],[StartTime],[IsLocalOnly],[StartTime],[IsLocalOnly],[StartTime],[IsLocalOnly],	left outer ioin [Activity] as [A] on [O].[Id] = [A].[Id]	[0].[GroupItems].
Image: ConstructionConstructionselectfrom [ActivityOperation] as [O][Id],left outer join [Activity] as [A] on [O].[Id] = [A].[Id][AppId],union[PackageldHash],select[AppActivityId],[Id],[ActivityType],[AppId],[ActivityStatus],[PackageldHash],[ParentActivityId],[AppActivityId],[Tag],[ActivityType],[Group],[ActivityType],[Group],[ActivityStatus],[MatchId],[ParentActivityId],[LastModifiedTime],[Tag],[ExpirationTime],[Group],[IslocalOnly],[LastModifiedTime],[IslocalOnly],[Payload],[CreatedInCloud],[Priority],[StartTime],[IslocalOnly],[StartTime],[IslocalOnly],[StartTime],[IslocalOnly],		
Instruct	select	from [ActivityOperation] as [0]
[Appld],union[PackageldHash],select[AppActivityId],[Id],[ActivityType],[Appld],[ActivityStatus],[PackageldHash],[ParentActivityId],[AppActivityId],[Tag],[ActivityType],[Group],[ActivityStatus],[MatchId],[ParentActivityId],[LastModifiedTime],[Tag],[Payload],[MatchId],[Priority],[LastModifiedTime],[Priority],[LastModifiedTime],[Priority],[LastModifiedTime],[IsLocalOnly],[Payload],[PlatformDeviceld],[Priority],[StartTime],[IsLocalOnly],[StartTime],[IsLocalOnly],		left outer ioin [Activity] as [A] on [O].[Id] = [A].[Id]
[PackageldHash],select[AppActivityId],[Id],[ActivityType],[AppId],[ActivityStatus],[PackageldHash],[ParentActivityId],[AppActivityId],[Tag],[ActivityType],[Group],[ActivityStatus],[MatchId],[ParentActivityId],[LastModifiedTime],[Tag],[ExpirationTime],[Group],[IsLocalOnly],[LastModifiedTime],[IsLocalOnly],[Parjoint],[StartTime],[IsLocalOnly],[StartTime],[IsLocalOnly],		
[AbpActivityId],[Id],[ActivityType],[AppId],[ActivityStatus],[PackageldHash],[ParentActivityId],[AppActivityId],[Tag],[ActivityStatus],[Group],[ActivityStatus],[MatchId],[ParentActivityId],[LastModifiedTime],[Tag],[ExpirationTime],[Group],[Parload],[MatchId],[Parload],[MatchId],[Parload],[MatchId],[Priority],[LastModifiedTime],[Payload],[MatchId],[Priority],[LastModifiedTime],[IsLocalOnly],[ExpirationTime],[PlatformDeviceId],[Payload],[CreatedInCloud],[Priority],[StartTime],[IsLocalOnly],	[PackageldHash]	select
[Appl:display][Appld],[ActivityType],[PackageldHash],[ParentActivityId],[AppActivityId],[Tag],[ActivityType],[Group],[ActivityStatus],[Matchld],[ParentActivityId],[LastModifiedTime],[Tag],[ExpirationTime],[Group],[Payload],[Matchld],[Priority],[LastModifiedTime],[ParentActivity],[LastModifiedTime],[CreatedInCloud],[Payload],[CreatedInCloud],[Priority],[StartTime],[IsLocalOnly],[StartTime],[IsLocalOnly],	[AppActivityId].	
[ActivityStatus],[PackageldHash],[ParentActivityId],[AppActivityId],[Tag],[ActivityType],[Group],[ActivityStatus],[MatchId],[ParentActivityId],[LastModifiedTime],[Tag],[ExpirationTime],[Group],[Payload],[MatchId],[Priority],[LastModifiedTime],[Priority],[LastModifiedTime],[IsLocalOnly],[Payload],[CreatedInCloud],[Priority],[StartTime],[IsLocalOnly],[StartTime],[IsLocalOnly],		[Appld]
[ParentActivityId],[ParentActivityId],[Tag],[ActivityType],[Group],[ActivityStatus],[MatchId],[ParentActivityId],[LastModifiedTime],[Tag],[ExpirationTime],[Group],[Payload],[MatchId],[Priority],[LastModifiedTime],[IsLocalOnly],[ExpirationTime],[CreatedInCloud],[Payload],[CreatedInCloud],[Priority],[StartTime],[IsLocalOnly],	[ActivityStatus]	[PackageldHash].
[reference[Tag],[ActivityType],[Group],[ActivityStatus],[MatchId],[ParentActivityId],[LastModifiedTime],[Tag],[ExpirationTime],[Group],[Payload],[MatchId],[Priority],[LastModifiedTime],[IsLocalOnly],[ExpirationTime],[PatformDeviceId],[Payload],[CreatedInCloud],[Priority],[StartTime],[IsLocalOnly],	[ParentActivityId]	[AnnActivityId]
[Group],[ActivityStatus],[MatchId],[ParentActivityId],[LastModifiedTime],[Tag],[ExpirationTime],[Group],[Payload],[MatchId],[Priority],[LastModifiedTime],[IsLocalOnly],[ExpirationTime],[PlatformDeviceId],[Payload],[CreatedInCloud],[Priority],[StartTime],[IsLocalOnly],	[Tag].	[ActivityType].
[Arterity][Netrity][MatchId],[ParentActivityId],[LastModifiedTime],[Tag],[ExpirationTime],[Group],[Payload],[MatchId],[Priority],[LastModifiedTime],[IsLocalOnly],[ExpirationTime],[PlatformDeviceId],[Payload],[CreatedInCloud],[Priority],[StartTime],[IsLocalOnly],		
[Indefinit][Indefinition][LastModifiedTime],[Tag],[ExpirationTime],[Group],[Payload],[MatchId],[Priority],[LastModifiedTime],[IsLocalOnly],[ExpirationTime],[PlatformDeviceId],[Payload],[CreatedInCloud],[Priority],[StartTime],[IsLocalOnly],	[Matchid]	[ParentActivityId]
[ExpirationTime],[Group],[Payload],[MatchId],[Priority],[LastModifiedTime],[IsLocalOnly],[ExpirationTime],[PlatformDeviceId],[Payload],[CreatedInCloud],[Priority],[StartTime],[IsLocalOnly],	[LastModifiedTime]	
[Payload],       [MatchId],         [Priority],       [LastModifiedTime],         [IsLocalOnly],       [ExpirationTime],         [PlatformDeviceId],       [Payload],         [CreatedInCloud],       [Priority],         [StartTime],       [IsLocalOnly],	[ExpirationTime]	
[Priority],[LastModifiedTime],[IsLocalOnly],[ExpirationTime],[PlatformDeviceId],[Payload],[CreatedInCloud],[Priority],[StartTime],[IsLocalOnly],	[Pavload]	[Matchid]
[Indity],     [Lastroduled Inte],       [IsLocalOnly],     [ExpirationTime],       [PlatformDeviceld],     [Payload],       [CreatedInCloud],     [Priority],       [StartTime],     [IsLocalOnly],	[Priority]	[lastModifiedTime]
[PlatformDeviceld],     [Payload],       [CreatedInCloud],     [Priority],       [StartTime],     [IsLocalOnly],		[ExpirationTime]
[Provided],     [Provided],       [CreatedInCloud],     [Priority],       [StartTime],     [IsLocalOnly],	[PlatformDeviceId]	[Pavload]
[StartTime], [IsLocalOnly],	[CreatedInCloud]	[Priority]
	[StartTime]	
I [PlatformDeviceId]	[FndTime].	[PlatformDeviceId].

[LastModifiedOnClient],	[CreatedInCloud],
0 AS [IsInUploadQueue],	[StartTime],
[GroupAppActivityId],	[EndTime],
[ClipboardPayload],	[LastModifiedOnClient],
[EnterpriseId],	0 AS [IsInUploadQueue],
[OriginalPayload],	[GroupAppActivityId],
[OriginalLastModifiedOnClient],	[ClipboardPayload],
[ETag]	[EnterpriseId],
from [Activity]	[UserActionState],
where [Id] not in (select [Id]	[IsRead],
from [ActivityOperation])	[OriginalPayload],
	[OriginalLastModifiedOnClient],
	[GroupItems],
	[ETag]
	from [Activity]
	where [Id] not in (select [Id]
	from [ActivityOperation])

## We also see a new PlatformID entry: "data\_boundary"

ETag	р0	р1	p2	р3	
127201	data_boundary	packageld	alternateId	NULL	
127203	data_boundary	packageId	alternateId	NULL	
127205	data_boundary	packageld	alternateId	NULL	
127207	data_boundary	packageId	alternateId	NULL	
127209	data_boundary	packageId	alternateId	NULL	
127211	data_boundary	packageld	alternateld	NULL	
127213	data_boundary	packageId	alternateId	NULL	

## Associated with Activity types 11 and 12:

Appld	PackageldHash	AppActivityId	Activity type	ActivityStatus
[{"application":"Microsoft.Credentials.WiFi","platform":"data_boundary"},	YNLZe4hPeNt2TsD3m2/J	default\$windows.data.nl	11	Active
[{"application":"Microsoft.Credentials.WiFi","platform":"data_boundary"},	YNLZe4hPeNt2TsD3m2/J	default\$windows.data.nl	11	Active
[{"application":"Microsoft.Credentials.WiFi","platform":"data_boundary"},	YNLZe4hPeNt2TsD3m2/J	default\$windows.data.nl	11	Active
[{"application":"Microsoft.Credentials.WiFi","platform":"data_boundary"},	YNLZe4hPeNt2TsD3m2/J	default\$windows.data.nl	11	Active
[{"application":"Microsoft.Credentials.WiFi","platform":"data_boundary"},	YNLZe4hPeNt2TsD3m2/J	default\$windows.data.nl	11	Active
[{"application":"Microsoft.Credentials.WiFi","platform":"data_boundary"},	YNLZe4hPeNt2TsD3m2/J	default\$windows.data.wifi	12	Updated
[{"application":"Microsoft.Credentials.WiFi","platform":"data_boundary"},	YNLZe4hPeNt2TsD3m2/J	default\$windows.data.wifi	12	Updated

## Whose payload is encoded/encrypted.

And one entry associated with Activity type 15:

AppId	PackageldHash	AppActivityId	Activity type
[{"application":"dek.encrypted.settings", "platform":"alternateId"}, {"application":"", "	aFEhkMTLDtGKXWcGe0U		15

whose Payload field is encoded with Base64, and encrypted. Using <u>https://gchq.github.io/CyberChef/#recipe=From\_Base64('A-Za-z0-9%2B/%3D',true)</u> I was able to see the email (*Microsoft account*) associated with this Win 10 installation.

In the ActivityOperation table, a new column (field) named "UploadAllowedByPolicy" is introduced:

ETag	UploadAllowedByPolicy
Filter	Filter
130207	1
130208	1

With observed values 0 and 1. The obvious deduction is that entries with value 1 are Yes and entries with value 0 are No. The Metadata table is where these policies are defined.

# **Note:** The encryption (?) certificates are stored at C:\Users\%Username%\AppData\Roaming\Microsoft\Crypto\Keys



de7cf8a7901d2ad13e5c67c29e5d1662\_e3e3b692-477f-4ddd-a280-655665776d42

Offset(h)	00 01	. 02	03	04 05	06	07	08	09	<b>0</b> A	0B	0C	0D	0E	0F	Decoded text
00000000	01 00	00	00	00 00	00	00	6F	00	00	00	04	00	03	00	n
00000010	88 00	00	ŏŏ .	42 01	ŏŏ	ŏŏ	šč	ŏĭ	ŏŏ	ŏŏ	čà	ŏŏ	ŏŏ	ŏŏ	
00000020	00 00	00	ŏŏ -	00 00	ŏŏ	ŏŏ	őõ	ŏō	ŏŏ	ŏŏ			-	ňő	Mi
00000030	63 00	72	õõ	6F 00	73	ŏŏ	6Ĕ	ŏŏ	66	õõ	74	00-		ъŏ	crosoft
00000040	43 00	6F	õõ	6F 00	6F	ŏŏ	65	ŏŏ	63	õõ	74	õõ	65	õõ	Connecte
00000050	64 00	20	00	44 00	65	õõ	76	õõ	69	õõ	63	õõ	65	õõ	d. D.e.v.i.c.e.
00000060	73 00	20	õõ	50 00	- 6C	õõ	61	õõ	74	õõ	66	õõ	6F	õõ	sP.l.a.t.f.o.
00000070	72 00	6D	00	20 00	64	00	65	00	76	00	69	00	63	00	r.md.e.v.i.c.
00000080	65 00	20	00	63 00	65	00	72	00	74	00	69	00	66	00	ec.e.r.t.i.f.
00000090	69 00	63	00	61 00	74	00	65	00	2C	00	00	00	00	00	i.c.a.t.e
000000A0	00 00	00	00	00 00	10	00	00	00	08	00	00	00	4D	00	M.
000000B0	6F 00	64	00	69 00	66	00	69	00	65	00	64	00	FD	01	o.d.i.f.i.e.d.v.
000000C0	B5 F7	94	4D	D4 01	5C	00	00	00	0A	00	00	00	00	00	μχ"MT.\
000000D0	00 00	00	00	00 00	48	00	00	00	45	43	53	31	20	00	HECS1 .
000000E0	00 00	7E	86	DA 2B	38	59	59	CE	80	D2	F2	52	EF	F8	~†Ϊ+8ΥΥΞ€□ςRoψ
000000F0	OC 43	D9	33	3A 13	9A	20	6F	8D	В5	30	F5	B6	9C	FE	.CΩ3: o.µ0υ¶.ώ
00000100	27 D4	2F	78	30 F8	F1	47	6B	DF	94	21	74	в0	08	5A	'T/x0ψρGki"!t°.Ζ
00000110	E9 89	C5	EE	3E 99	4E	74	8D	1D	ΒA	0C	ΕA	01	3E	E8	ι‰Eξ>™NtΊ.κ.>θ
00000120	69 62	01	00	00 00	D0	8C	9D	DF	01	15	D1	11	8C	7A	ibПіРz
00000130	00 CC	4F	C2	97 EB	01	00	00	00	D5	F7	ED	6E	03	BE	.ΐ0Β–λΥχνη.Ύ
00000140	02 4E	8F	4D	ED 4B	18	4A	8A	8A	00	00	00	00	2E	00	.N.MvK.J
00000150	00 00	50	00	72 00	69	00	76	00	61	00	74	00	65	00	P.r.i.v.a.t.e.
00000160	20 00	4B	00	65 00	-79	00	20	00	50	00	72	00	6F	00	.K.e.y. P.r.o.
00000170	70 00	65	00	72 00	-74	00	69	00	65	00	73	00	00	00	p.e.r.t.i.e.s
00000180	10 66	00	00	00 01	00	00	20	00	00	00	1A	48	D4	58	.tHTX
00000190	FA 0E	89	9F	16 55	E1	82	19	CD	8D	24	85	EF	BC	D9	τ.‰υα,.Ν.\$…οΌΩ
000001A0	B2 E5	1E	7F	C3 7E	- 25	1C	E8	FA	03	FE	00	00	00	00	²εΓ~%.θϊ.ώ

## Update (Win 10 version 1903 OS Build 18875.1000)

In the latest update, we have a new "ActivityType" -> 10 which is clipboard data (I have only observed clipboard text).



## The Metadata table now includes ActivityType 10 :

Ta	ole: 🗏 Metadata 🗸 😒	
	Key	
	Filter	Filter
1	DatabaseNotificationSubscriptionInfo	{"ddsDeviceId":"","partialSyncToken":"","publisherFilters":[{"activityTyp
2	PendingActivityTypes	{"activityTypes":[]}
3	DatabaseActivityPolicies	<pre>{"AllowedSubscriptionSyncScopes":[{"activityTypes":[0,1,2,3,4,5,6,7,10,13]</pre>
4	CurrentSettings	{"ActivityTypes":[0,1,2,3,4,5,6,7,10,11,13,15],"Environment":"prod"}
5	PendingFirstDEKUpload	false
6	CurrentEtag	cbacde20-5d0e-11e9-9117-01020305070d
7	DatabaseInstanceId	23919
8	DatabaseInstanceIdUpdateTime	2018-05-10T13:58:59.758Z



## **Clipboard History**

The field "ClipboardPayload" (JSON blob) associated to entries of 'ActivityType' 10 (Clipboard text) contain the copied text, Base64 encoded, in the form:

[{"content":"eyJBbGxvd2VkU3Vic2NyaXB0aW9uU3luY1Njb3BlcyI6W3siYWN0aXZpdHlUeXBlcyI6 WzAsMSwyLDMsNCw1LDYsNywxMCwxMywxNV0sImFwcGxpY2F0aW9uIjoiKiJ9LHsiYWN0aXZpd HIUeXBlcyI6WzExLDEyXSwiYXBwbGljYXRpb24iOiJNaWNyb3NvZnQuQ3JIZGVudGlhbHMuVmF1bH QiLCJwbGF0Zm9ybSl6ImRhdGFfYm91bmRhcnkifSx7ImFjdGl2aXR5VHIwZXMiOlsxMSwxMl0sImF wcGxpY2F0aW9uIjoiTWIjcm9zb2Z0LkNyZWRIbnRpYWxzLldpRmkiLCJwbGF0Zm9ybSI6ImRhdGFfY m91bmRhcnkifSx7ImFjdGl2aXR5VHIwZXMiOlsxMV0sImFwcGxpY2F0aW9uIjoibWljcm9zb2Z0LmR IZmF1bHQuZGVmYXVsdCIsInBsYXRmb3JtljoiZGF0YV9ib3VuZGFyeSJ9XSwiUG9saWNpZXMiOlt7IkJ sb2NrZWRPcGVyYXRpb25GbGFncyI6MCwiU2NvcGUiOnsiUGVybWlzaW9uU2NvcGUiOiliLCJUeXBI IjoxMX0sIINvdXJjZSI6MX0seyJCbG9ja2VkT3BlcmF0aW9uRmxhZ3MiOjAsIINjb3BIIjp7IIBlcm1pc2lv blNjb3BlljoiTWljcm9zb2Z0LkNyZWRlbnRpYWxzliwiVHlwZSI6MTF9LCJTb3VyY2UiOjF9LHsiQmxvY2 tlZE9wZXJhdGlvbkZsYWdzIjowLCJTY29wZSI6eyJQZXJtaXNpb25TY29wZSI6lk1pY3Jvc29mdC5QZXJ zb25hbGl6YXRpb24iLCJUeXBlljoxMX0sIlNvdXJjZSl6MX0seyJCbG9ja2VkT3BlcmF0aW9uRmxhZ3Mi OjAsIINjb3BIIjp7IIBlcm1pc2lvbINjb3BIIjoiIiwiVHIwZSI6MTJ9LCJTb3VyY2UiOjF9LHsiQmxvY2tlZE9w ZXJhdGlvbkZsYWdzIjowLCJTY29wZSI6eyJQZXJtaXNpb25TY29wZSI6Ik1pY3Jvc29mdC5DcmVkZW5 0aWFscyIsIIR5cGUiOjEyfSwiU291cmNIIjoxfSx7lkJsb2NrZWRPcGVyYXRpb25GbGFncyI6MCwiU2Nv cGUiOnsiUGVybWlzaW9uU2NvcGUiOiJNaWNyb3NvZnQuUGVyc29uYWxpemF0aW9uliwiVHlwZS I6MTJ9LCJTb3VyY2Ui0jF9LHsiQmxyY2tlZE9wZXJhdGlvbkZsYWdzIjowLCJTY29wZSI6eyJQZXJtaXNp b25TY29wZSI6IiIsIIR5cGUiOjExfSwiU291cmNlljoyfSx7lkJsb2NrZWRPcGVyYXRpb25GbGFncyI6MC wiU2NvcGUiOnsiUGVybWlzaW9uU2NvcGUiOiliLCJUeXBlljoxMn0sllNvdXJjZSI6Mn0seyJCbG9ja2V kT3BlcmF0aW9uRmxhZ3MiOjcsIINjb3Blljp7llBlcm1pc2lvblNjb3BlljoiliwiVHlwZSI6MTB9LCJTb3Vy

Y2UiOjN9LHsiQmxvY2tlZE9wZXJhdGlvbkZsYWdzIjo3LCJTY29wZSl6eyJQZXJtaXNpb25TY29wZSl6lil sIIR5cGUiOjEyfSwiU291cmNlljozfSx7lkJsb2NrZWRPcGVyYXRpb25GbGFncyI6NywiU2NvcGUiOnsi UGVybWlzaW9uU2NvcGUiOiliLCJUeXBlljoxNX0sllNvdXJjZSI6M30seyJCbG9ja2VkT3BlcmF0aW9uR mxhZ3MiOjAsIINjb3BIIjp7IIBIcm1pc2lvbINjb3BIIjoiIiwiVHIwZSI6MTB9LCJTb3VyY2UiOjR9LHsiQmx vY2tlZE9wZXJhdGlvbkZsYWdzIjowLCJTY29wZSl6eyJQZXJtaXNpb25TY29wZSl6liIsllR5cGUiOjEwfSw iU291cmNlljo1fSx7lkJsb2NrZWRPcGVyYXRpb25GbGFncyI6MCwiU2NvcGUiOnsiUGVybWlzaW9u U2NvcGUiOiliLCJUeXBIIjoxMX0sIINvdXJjZSI6NX0seyJCbG9ja2VkT3BIcmF0aW9uRmxhZ3MiOjcsIIN jb3Blljp7llBlcm1pc2lvblNjb3BlljoiTWljcm9zb2Z0LkFjY2Vzc2liaWxpdHkiLCJUeXBlljoxMX0sllNvdXJj ZSI6NX0seyJCbG9ja2VkT3BlcmF0aW9uRmxhZ3MiOjcsIlNjb3BlIjp7llBlcm1pc2lvblNjb3BlIjoiTWljc m9zb2Z0LkNyZWRlbnRpYWxzliwiVHIwZSI6MTF9LCJTb3VyY2UiOjV9LHsiQmxvY2tlZE9wZXJhdGlv bkZsYWdzIjowLCJTY29wZSI6eyJQZXJtaXNpb25TY29wZSI6lk1pY3Jvc29mdC5EZWZhdWx0liwiVHlw ZSI6MTF9LCJTb3VyY2UiOjV9LHsiQmxvY2tlZE9wZXJhdGlvbkZsYWdzIjo3LCJTY29wZSI6eyJQZXJtaX Npb25TY29wZSI6Ik1pY3Jvc29mdC5MYW5ndWFnZSIsIIR5cGUiOjExfSwiU291cmNlljo1fSx7IkJsb2N rZWRPcGVyYXRpb25GbGFncyI6NywiU2NvcGUiOnsiUGVybWlzaW9uU2NvcGUiOiJNaWNyb3NvZn QuUGVyc29uYWxpemF0aW9uIiwiVHIwZSI6MTF9LCJTb3VyY2UiOjV9LHsiQmxvY2tlZE9wZXJhdGlv bkZsYWdzIjowLCJTY29wZSI6eyJQZXJtaXNpb25TY29wZSI6liIsIIR5cGUiOjEyfSwiU291cmNlIjo1fSx7I kJsb2NrZWRPcGVyYXRpb25GbGFncyI6NywiU2NvcGUiOnsiUGVybWlzaW9uU2NvcGUiOiJNaWNy b3NvZnQuQWNjZXNzaWJpbGl0eSIsIIR5cGUiOjEyfSwiU291cmNlljo1fSx7lkJsb2NrZWRPcGVyYXRp b25GbGFncyI6NywiU2NvcGUiOnsiUGVybWlzaW9uU2NvcGUiOiJNaWNyb3NvZnQuQ3JlZGVudGl hbHMiLCJUeXBIIjoxMn0sIINvdXJjZSI6NX0seyJCbG9ja2VkT3BIcmF0aW9uRmxhZ3MiOjAsIINjb3BIIj p7llBlcm1pc2lvblNjb3BlljoiTWljcm9zb2Z0LkRlZmF1bHQiLCJUeXBlljoxMn0sllNvdXJjZSI6NX0seyJC bG9ja2VkT3BlcmF0aW9uRmxhZ3MiOjcsIINjb3Blljp7IIBlcm1pc2lvblNjb3BlljoiTWljcm9zb2Z0Lkxhb md1YWdlliwiVHlwZSI6MTJ9LCJTb3VyY2UiOjV9LHsiQmxvY2tlZE9wZXJhdGlvbkZsYWdzIjo3LCJTY2 9wZSI6eyJQZXJtaXNpb25TY29wZSI6Ik1pY3Jvc29mdC5QZXJzb25hbGl6YXRpb24iLCJUeXBlljoxMn0 sIINvdXJjZSI6NX0seyJCbG9ja2VkT3BlcmF0aW9uRmxhZ3MiOjEsIINjb3Blljp7IIBlcm1pc2lvblNjb3Bll joiliwiVHIwZSI6OH0sIINvdXJjZSI6N30sevJCbG9ia2VkT3BlcmF0aW9uRmxhZ3MiOjEsIINjb3Blljp7II Blcm1pc2lvblNjb3BlIjoiliwiVHIwZSI6OX0sIINvdXJjZSI6N30seyJCbG9ja2VkT3BlcmF0aW9uRmxhZ3 MiQjAsIlNjb3Blljp7llBlcm1pc2lvblNjb3BlljoiliwiVHlwZSI6MTB9LCJTb3VyY2UiQjd9LHsiQmxvY2tlZE 9wZXJhdGlvbkZsYWdzIjowLCJTY29wZSI6eyJQZXJtaXNpb25TY29wZSI6IiIsIIR5cGUiOjExfSwiU291c mNlljo3fSx7lkJsb2NrZWRPcGVyYXRpb25GbGFncyI6MCwiU2NvcGUiOnsiUGVybWlzaW9uU2NvcG UiOiliLCJUeXBIIjoxMn0sIINvdXJjZSI6N30seyJCbG9ja2VkT3BlcmF0aW9uRmxhZ3MiOjAsIINjb3BIIjp 7IIBlcm1pc2lvblNjb3BlIjoiliwiVHlwZSI6MTV9LCJTb3VyY2UiOjd9LHsiQmxvY2tlZE9wZXJhdGlvbkZs YWdzIjowLCJTY29wZSI6eyJQZXJtaXNpb25TY29wZSI6liIsIIR5cGUiOjV9LCJTb3VyY2UiOjh9LHsiQmx vY2tlZE9wZXJhdGlvbkZsYWdzIjowLCJTY29wZSl6eyJQZXJtaXNpb25TY29wZSl6lilsllR5cGUiOjZ9LCJ Tb3VyY2UiOjh9LHsiQmxvY2tlZE9wZXJhdGlvbkZsYWdzIjowLCJTY29wZSI6eyJQZXJtaXNpb25TY29 wZSI6lilsIIR5cGUiOjh9LCJTb3VyY2UiOjh9LHsiQmxvY2tlZE9wZXJhdGlvbkZsYWdzIjowLCJTY29wZSI 6eyJQZXJtaXNpb25TY29wZSI6IiIsIIR5cGUiOjl9LCJTb3VyY2UiOjh9LHsiQmxvY2tIZE9wZXJhdGlvbkZ sYWdzIjowLCJTY29wZSI6eyJQZXJtaXNpb25TY29wZSI6IiIsIIR5cGUiOjEwfSwiU291cmNlljo5fV19"," ormatName":"Text"}]

content	Т	W3siY29udGVudCI6ImV5SkJiR3h2ZDJWa1UzVmljMk55YVhC
formatName	Т	Text

(Translated below:)

Recipe	ī	Input	start: end: length:	0 2 2	length: 47 lines:	12 1	Ð 1			
From Base64	I	<mark>ey</mark> JBbGxvd2VkU3Vic2NyaXB0aW9uU3luY1Njb3BlcyI6W3siYWN0aXZpdHlUeXB xNV0sImFwcGxpY2F0aW9uIjoiKiJ9LHsiYWN0aXZpdHlUeXBlcyI6WzExLDEyXS	lcyI6Wz wiYXBwb	AsMS GljY	wyLDMsNC XRpb24i0	1LDY	sNywxMCu Nyb3NvZi	vxMyw nQuQ3		
Alphabet A-Za-z0-9+/=	r	LZGVudGlhbHMuVmF1bHQiLCJwbGF0Zm9ybSI6ImRhdGFfYm91bmRhcnkifSx7ImFjdGl2aXR5VHlwZXMi01sxMS (pY2F0aW9uIjoiTWljcm9zb2Z0LkNyZWRlbnRpYWxzLldpRmkiLCJwbGF0Zm9ybSI6ImRhdGFfYm91bmRhcnkif (R5VHlwZXMi01sxMV0sImFwcGxpY2F0aW9uIjoibWljcm9zb2Z0LmRlZmF1bHQuZGVmYXVsdCIsInBsYXRmb3Jt b3VuZGFve5J9XSwiUG9saWNpZXMi01t7IkJsb2NrZWRPcGVvYXRpb25GbGFncvI6MCwiU2NvcGUiOnsiUGVvbWl								
Remove non-alphabet chars		ib3VuZGFyeSJ9XSwiUG9saWNpZXMiOlt7IkJsb2NrZWRPcGVyYXRpb25GbGFncy UiOiIiLCJUeXBIIjoxMX0sIlNvdXJjZSI6MX0seyJCbG9ja2VkT3BlcmF0aW9uR	I6MCwiU mxhZ3Mi	2Nvc OjAs	GUiOnsiU IlNjb3Bl	WybW Ijp7I	lzaW9uU 1Blcm1p	2NvcG c2lvb		
		Output start: 0 end: 1 length: 1	time length line:	: 5m : 353	s 4 1	D	f) 🗠	- 0		
		<pre>{"AllowedSubscriptionSyncScopes":[{"activityTypes":[0,1,2,3,4,5 {"activityTypes":[11,12],"application":"Microsoft.Credentials.V {"activityTypes":[11,12],"application":"Microsoft.Credentials.W {"activityTypes": [11],"application":"microsoft.default.default", "platform":"data [{"BlockedOperationFlags":0,"Scope": {"PermisionScope":"","Type" {"BlockedOperationFlags":0,"Scope": {"PermisionScope":"Microsoft.Credentials", "Type":11}, "Source":1 {"BlockedOperationFlags":0,"Scope": {"PermisionScope":"Microsoft.Credentials", "Type":11}, "Source":1 {"BlockedOperationFlags":0,"Scope": {"PermisionScope":"Microsoft.Credentials", "Type":11}, "Source":1 {"BlockedOperationFlags":0,"Scope": {"PermisionScope":"Microsoft.Credentials", "Type":12}, "Source":1 {"BlockedOperationFlags":0,"Scope": {"PermisionScope":"Microsoft.Personalization", "Type":12}, "Source": {"BlockedOperationFlags":0,"Scope": {"PermisionScope":", "Type": {"BlockedOperationFlags":0,"Scope::{"PermisionScope":", "Type": {"BlockedOperationFlags":0,"Scope::{"PermisionScope":", "Type": {"BlockedOperationFlags:0,"Scope::{"PermisionScope":", "Type": {"BlockedOperationFlags:0,"Scope::{"PermisionScope":", "Type": {"BlockedOperationFlags:0,"Scope::{"PermisionScope":", "Type": {"BlockedOperationFlags:0,"Scope::{"PermisionScope":", "Type": {"BlockedOperationFlags:0,"Scope::{"PermisionScope::", "Type": {"BlockedOperationFlags:0,"Scope::{"PermisionScope::", "Type": {"BlockedOperationFlags:0,"Scope::{"PermisionScope::", "Type": {"BlockedOperationFlags:0,"Scope::{"PermisionScope::", "Type":{", "Type":{", "Type::{", "Type::{", "Type::{", "Type::{", "Type::{"</pre>	<pre>,6,7,10 ault"," iFi","p _bounda :11},"S }, e":1}, 12},"Sc }, e":1}, 11},"Sc 12},"Sc 10},"Sc 10},"Sc </pre>	urce urce urce	<pre>15],"app form":"da iorm":"da ],"Polic e":1}, ":1}, ":2}, ":2}, ":3), " - 2</pre>	icat. :ta_bo	ion":"* oundary" undary"	'}, '}, b		

# Another new 'ActivityType' 16 contains data on the application from where data was copied/pasted from/to, and the 'Group' field shows what action was operated:

AppActivityId	ActivityType	ActivityStatus	arentActivityI	Tag	Group
Filter	Filter	Filter	Filter	Filter	Filter
ECB32AF3-1440	<mark>16</mark>	1	BLOB	NULL	Сору
ECB32AF3-1440	6	2	BLOB	NULL	NULL

And where it was pasted:

AppId	PackageIdHash	AppActivityId	ActivityType	ActivityStatus	arentActivityI	Tag	Group
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
[{"applicatio…	RgBDLH4/nR45L		10	1	BLOB	NULL	NULL
[{"applicatio…	deglsgqOfpSkY	ECB32AF3-1440	6	1	BLOB	NULL	NULL
[{"applicatio…	bwfyZ5c003AQa	ECB32AF3-1440	16	1	BLOB	NULL	Paste
[{"applicatio…	Ts0+SH7DZfSHh	ECB32AF3-1440	6	1	BLOB	NULL	NULL

We can now see copy pasted operations:

Group	GroupAppActivityId	GroupItems	Is_Read	EnterpriseId	ParentActivityId	
Paste			No		4233DA52CE1FF43168B53	1
Сору			No		EF261D0B550FC22F26BD2	1
Сору			No		EF261D0B550FC22F26BD2	1
Paste			No		4233DA52CE1FF43168B53	I
Сору			No		EF261D0B550FC22F26BD2	I
Сору			No		EF261D0B550FC22F26BD2	1
Paste			No		4233DA52CE1FF43168B53	I
Сору			No		EF261D0B550FC22F26BD2	I
Сору			No		EF261D0B550FC22F26BD2	I
Сору			No		EF261D0B550FC22F26BD2	1
Сору			No		EF261D0B550FC22F26BD2	1
Сору			No		EF261D0B550FC22F26BD2	1
Paste			No		4233DA52CE1FF43168B53	1
Сору			No		EF261D0B550FC22F26BD2	1
Сору			No		EF261D0B550FC22F26BD2	1

The copy paste operations can be linked via the 'clipboardDataId' value of the 'Payload' field (JSON) eg:

{"gdprType":"ProductAndServiceUsage","clipboardDataId":"{BA306A6E-2B7B-483B-B9B6-76BB7AF64D12}"}

Activity_type	Group	GroupAppActivityId	GroupItems	ParentActivityId	DdsDeviceId	Device ID	Expires In days	clipboardDataId
Copy/Paste	Paste			A7A0DBC58DD13A75E991D	NULL	dpRc3VX485JVH95n3ZaaJ	31	{BA306A6E-2B7B-483B-B9B6-76BB7AF64D1
Clipboard	NULL			0000000000000000000000	NULL	dpRc3VX485JVH95n3ZaaJ	0	NULL
Copy/Paste	Сору			9B1C816547035726A2181	NULL	dpRc3VX485JVH95n3ZaaJ	31	{BA306A6E-2B7B-483B-B9B6-76BB7AF64D1
Clipboard	NULL			000000000000000000000000	NULL	dpRc3VX485JVH95n3ZaaJ	0	NULL
Copy/Paste	Сору			A7A0DBC58DD13A75E991D	NULL	dpRc3VX485JVH95n3ZaaJ	31	{91FAD9DC-6A43-475C-8034-7929148F41E
Clipboard	NULL			000000000000000000000000	NULL	dpRc3VX485JVH95n3ZaaJ	0	NULL
Copy/Paste	Сору			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31	{4BA8B44B-6EF6-49F7-8742-A0BAF8F8D35
Copy/Paste	Paste			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31	{3DB5D8D1-0518-4B03-AD8D-082F6BF3451
Copy/Paste	Paste			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31	{3DB5D8D1-0518-4B03-AD8D-082F6BF3451
Copy/Paste	Paste			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31	{3DB5D8D1-0518-4B03-AD8D-082F6BF3451
Copy/Paste	Paste			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31	{3DB5D8D1-0518-4B03-AD8D-082F6BF3451
Copy/Paste	Paste			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31	{3DB5D8D1-0518-4B03-AD8D-082F6BF3451
Copy/Paste	Paste			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31	{3DB5D8D1-0518-4B03-AD8D-082F6BF3451
Clipboard	NULL			00000000000000000000000	NULL	dpRc3VX485JVH95n3ZaaJ	0	NULL
Copy/Paste	Сору			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31	{3DB5D8D1-0518-4B03-AD8D-082F6BF3451

Curiously, while 'ActivityType' 16 is not always listed in the Metadata tables's 'Current Settings' list of Activities, it does sync across devices 😕

The Clipboard text has a duration (ExpirationTime - LastModifiedTime) of 43200 seconds or 12 hours exactly:

Text(Base64)	ClipboardPayload	Activity_type	Group	GroupAppActivityId	GroupItems	ParentActivityId	DdsDeviceId	Device ID	Expires In days
	NULL.	Copy/Paste	Paste			A7A0DBC58DD13A75E991D	NULL	dpRc3VX485JVH95n3ZaaJ	31
U09GVFdBUkVcQ2xpZW50c	[{"content":"U09GVFdB	Clipboard	NULL			000000000000000000000	NULL	dpRc3VX485JVH95n3ZaaJ	0
	NULL	Copy/Paste	Сору			9B1C816547035726A2181	NULL	dpRc3VX485JVH95n3ZaaJ	31
MzA4MDQ2QjBBRjRBMz1DQ	[{"content":"MzA4MDQ2	Clipboard	NULL			000000000000000000000	NULL	dpRc3VX485JVH95n3ZaaJ	0
	NULL	Copy/Paste	Сору			A7A0DBC58DD13A75E991D	NULL	dpRc3VX485JVH95n3ZaaJ	31
PGJyPg==	[{"content":"PGJyPg==	Clipboard	NULL			000000000000000000000	NULL	dpRc3VX485JVH95n3ZaaJ	0
	NULL	Copy/Paste	Сору			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31
	NULL	Copy/Paste	Paste			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31
	NULL	Copy/Paste	Paste			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31
	NULL	Copy/Paste	Paste			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31
	NULL	Copy/Paste	Paste			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31
	NULL	Copy/Paste	Paste			78009A0829A4BAD23D5A8	NUL I,	dpRc3VX485JVH95n3ZaaJ	31
	NULL	Copy/Paste	Paste			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31
PGJyPg==	[{"content":"PGJyPg==	Clipboard	NULL			0000000000000000000000	NULL	dpRc3VX485JVH95n3ZaaJ	0
	NULL	Copy/Paste	Сору			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31
	NULL	Copy/Paste	Paste			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31
DQogICAgV2luZG93cyBJb	[{"content":"DQogICAg	Clipboard	NULL			0000000000000000000000	NULL	dpRc3VX485JVH95n3ZaaJ	0
	NULL	Copy/Paste	Сору			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31
	NULL.	Copy/Paste	Paste			78009A0829A4BAD23D5A8	NULL	dpRc3VX485JVH95n3ZaaJ	31
Q1NleDJTWTFocHBkNWxOT	[{"content":"Q1NleDJT	Clipboard	NULL			00000000000000000000000	NULL	dpRc3VX485JVH95n3ZaaJ	0

After that 'ActivityType' 10 entries are deleted.

**Note** (*Aug 2020*): However, quite a few of them can be recovered, even going back months. Try <u>ClipboardTextEntries.exe</u>

The Copied text can also be seen by the user by pressing the <u>Windows key + V</u>. Pointing the mouse arrow to one of the copied text items, one can see the Last Synced time of that item in a tooltip:

CopiedText	uration	CalculatedDuration	Expires In	LastModifiedOnClient	LastModifiedTime	ExpirationTime	StartTime	EndTime	CreatedInCloud	TimeZone	Dev
	0:44:23	01:10:30	29 days		2020-07-30T11:31:01	2020-08-29T10:22:22	2020-07-30T10:20:20	2020-07-30T11:30:50	2020-07-30T10:22:22	Europe/Bucharest	Wir
db_propertystore			12 hours		2020-07-30T11:24:01	2020-07-30T23:24:01	2020-07-30T11:24:01		2020-07-30T11:24:01		Win
			7 days		2020-07-30T11:24:01	2020-08-06T11:24:01	2020-07-30T11:24:01	2020-07-30T11:24:01	2020-07-30T11 24:01		Wir
			3054 days	2020-07-29T17:32:51	2019-03-18T13:37:21	2027-07-29T11:17:20	2019-03-18T13:37:21				Win
	00:02:36	00:06:07	29 days		2020-07-30T11:17:51	2020-08-29T11:11:52	2020-07-30T11:11:34	2020-07-30T1			
	00:01:04	00:01:04	7 days		2020-07-30T11:14:08	2020-08-06T11:14:08	2020-07-30T11:12:54	2020-07-30TT Cli	pboard 🔥 🔪		
	00:01:12	00:01:12	30 days		2020-07-30T11:13:05	2020-08-29T11:13:05	2020-07-30T11:11:42	2020-07-30T1			
foreach(\$r in \$xml.xmlD			12 hours		2020-07-30T11:03:47	2020-07-30T23:03:47	2020-07-30T11:03:47		th property tore		
			7 days		2020-07-30T11:03:47	2020-08-06T11:03:47	2020-07-30T11:03:46	2020-07-30T1	in-bioheirite		
PS C:\Users\Costas Kats			12 hours		2020-07-30T11:03:02	2020-07-30T23:03:02	2020-07-30T11:03:02				
			7 days		2020-07-30T11:03:02	2020-08-06T11:03:02	2020-07-30T11:03:02	2020-07-30T1			
	00:09:40	00:18:56	29 days		2020-07-30T11:02:39	2020-08-29T10:46:50	2020-07-30T10:43:33	2020-07-30T1	Last syn	ced at 11:24:01 an	
			12 hours		2020-07-30T10:59:37	2020-07-30T22:59:37	2020-07-30T10:59:37				

*Note:* Images, as they aren't syncing (yet), do not behave this way. I.e. if you point the mouse arrow to a copied image, there is no 'Last synced' timestamp tooltip.

Clipboard settings can be seen in the user's NTUser.dat at "SOFTWARE\Microsoft\Clipboard":

Value Name	Value Type	Data
A <mark>8</mark> c	<b>#</b> B¢	# B C
EnableClipboardHistory	RegDword	1
ShellHotKeyUsed	RegDword	1
${\it HistoryOldItemsLastCleanupTimestamp}$	RegQword	132411803816852926
PastedFromClipboardUI	RegDword	1
ClipboardTipRequired	RegDword	0

EnableClipboardHistory: (obviously 0 = No, 1 = Yes) ShellHotKeyUsed: if the +V key has been used by the user (0 = No, 1 = Yes) PastedFromClipboardUI = if the user has ever used +V Clipboard UI to paste items The important entry here is: 'HistoryOldItemsLastCleanupTimestamp' which is a Filetime value of the last UTC time Clipboard History was cleared:

 Original
 date
 format

 132411803816852926
 06 Aug 20 9:39:41 am
 FileTime

This is the last UTC time when expired Clipboard History items were purged from memory (RAM).

*Note*: That could normally (unless the user manually triggers a Clear Clipboard History option) coincide with the Last shutdown time, but it seems my PC has a mind of its own (a):

**ShutdownTime** (SYSTEM: *ControlSet001\Control\Windows*): 0x5EB5F6C6C170D601 = Windows Filetime = 2020-08-12 19:01:02.3064414 +03:00

HistoryOldItemsLastCleanupTimestamp (NTUser.dat: SOFTWARE\Microsoft\Clipboard): 132417276562334760 = Windows Filetime = 2020-08-12 20:40:56.2334760 +03:00

In my test, Clipboard History UI (++V key) had a few more entries beyond that timestamp, BUT pointing the mouse arrow to one of these older entries did not display a last synced timestamp.

These were pinned entries, cached in the user's profile: '\AppData\Local\Microsoft\Windows\Clipboard\Pinned' folder:



Where the metadata.json file shows that the content is encrypted



And "VGV4dA==" which is "Text" Base64 encoded



contains the <u>encrypted</u> text string among other info.

Note1: Similarly, any pinned copied images are also in the same folder & encrypted.

*Note2:* The purpose of the 'AppData\Local\Microsoft\Windows\Clipboard\HistoryData' folder remains (yet) unknown. In a recent Win10 beta I noticed that it was populated, and entries were not encrypted, but haven't yet managed to replicate this

🗸 📙 Clipboard	^	^ Date	modified
<ul> <li>HistoryData</li> <li>41F1D1BD-B28E-42D2-9FC7-B818BA75FF64}</li> </ul>		21 Ju 2841D996-A446-4FC9-9E33-99A2D6FE4DFA} 21 Ju 126DB2EF-F34D-44F8-B651-B924619C395F} 21 Ju	l 20 8:41 pm l 20 8:41 pm
✓ ↓ {0C30DE03-0371-4AB2-8533-78C73941CE66	3	[] {1956817F-6A9B-4D01-930D-18F9DB0A1DDA} 21 Ju	l 20 8:41 pm
ResourceMap			
[1431ED0B-52B1-4CD8-B310-2EA3BFFE4EE8]			
ResourceMap			
C:\Users\Costas \AppData\Local\Microsoft\\	Nindo	ws\Clipboard\HistoryData\{41F1D1BD-B28E-42D2-9FC7-B818	3A75FF64}\{1A31ED0B-
dit Search View Analysis Tools Window Help			
🕞 🔳 💐 🖻 🔹 🖬 16 🔹 Windows (ANSI)		• dec •	
17F-6A9B-4D01-930D-18F9DB0A1DDA}			Special editors
t(d) 00 01 02 03 04 05 06 07 08 09	) 10	11 12 13 14 15 Decoded text	Data inspector
000 FF D8 FF E0 00 10 4A 46 49 46 016 00 C0 00 00 FF DB 00 43 00 0A	6 00 07	01 01 01 00 C0 🖗ØÿàJFIFA 07 09 07 06 0A .Aÿ0.C	14 4 1 1
032 09 08 09 0B 0B 0A 0C 0F 19 10 048 17 12 19 24 20 26 25 23 20 23	) 0F	0E 0E 0F 1E 16 28 2D 39 30 28 \$ 8%# #"(-90(	Binary (8 bit)
064 2A 36 2B 22 23 32 44 32 36 3B	3D	40 40 40 26 30 *6+"#2D26;=@@@&0	Int8
080 46 4B 45 3E 4A 39 3F 40 3D FF	DB	00 43 01 0B 0B FKE>J9?@=ÿ0.c	UInt8
112 JP	23	$29 30 30 30 30 \dots = )#)====$	Int16

*Note3*: Clipboard History UI (**4**+V key) only shows the last 25 copied items + pinned items. A new clipboard entry pushes the last one out.

*Note4*: When Clipboard History is set to not sync, Clipboard items show in the UI are most likely only stored in RAM.

*Note5:* Changing the Clipboard sync setting to NOT Sync across devices



Results in immediate deletion of any ActivitiesCache.db 'ActivityType' 10 entries:

1	SELECT
2	ActivityType,
3	🛛 case ActivityStatus
4	when 1 then 'Active'
5	when 2 then 'Updated'
6	when 3 then 'Deleted'
7	when 4 then 'Ignored'
8	end as ActivityType
9	
10	from SmartLookup
1	<pre>where ActivityType = 10</pre>

	ActivityType	ActivityType	
61	10	Deleted	
62	10	Deleted	
63	10	Deleted	
64	10	Deleted	
65	10	Deleted	
66	10	Deleted	
67	10	Deleted	
68	10	Deleted	
69	10	Deleted	
70	10	Deleted	
71	10	Deleted	
72	10	Deleted	
73	10	Deleted	
74	10	Deleted	
75	10	Deleted	
76	10	Deleted	

Execution finished without errors. Result: 76 rows returned in 10ms

## *Note6:* Changing the Automatic Sync to Never sync automatically:



If you now copy some text and check ActivitiesCache.db, there won't be any related 'ActivityType' 10 entry. Pressing the +V and selecting a copied item's three dots (options), you are now presented with a Sync option:



Which when clicked, a new 'ActivityType' 10 appears in ActivitiesCache.db with a 'ClipboardPayload' of:

[{"content":"QWxsb3cgdGV4dCB0byBzeW5j","formatName":"Text"}]

Recipe	8	Î	Input
From Base64	0	П	QWxsb3cgdGV4dCB0byBzeW5j
Alphabet A-Za-z0-9+/=		*	Output
Remove non-alphabet	t chars		Allow text to sync

(which is the text I copied)

*Note7:* The next Win10 update will probably allow syncing of HTML & Images – I will update this section accordingly.

## Another location with full CDP info

C:\Windows\ServiceProfiles\LocalService\AppData\Local\ConnectedDevicesPlatform

Name	Date modified	Туре	Size
0ffc25d8321343c3.cdp	29 Feb 20 9:58 pm	CDP File	30 KB
3d9ee62b8d4d007f.cdp	29 Feb 20 9:58 pm	CDP File	33 KB
4a7cc0f3b728d240.cdp	29 Feb 20 9:58 pm	CDP File	44 KB
AAD.e5316abf-be67-4d21-9662-d64159c3608a	29 Feb 20 9:58 pm	CDP File	13 KB
CDPGlobalSettings.cdp	29 Feb 20 9:58 pm	CDP File	53 KB
Connected Devices Platform certificates.sst	30 May 18 12:41 pm	Microsoft Serialized	25 KB
📃 L.Costas Katsavounidis.cdp	29 Feb 20 9:58 pm	CDP File	1 KB



## Full Device Info:

Children: 22 Level: 2		
<object> &gt; Devices &gt;</object>	element #5>	
Name	Value	
ApplicationDisplayName		
ApplicationId		
Applications	(array)	
BluetoothClassicMacA		
CcsTicket	.eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6ImVpSlpCc JodHRwOi8vZGRzIiwiaXNzIjoiQ049and0c2lnbmluZy0yLmRkcy wLCJleHAiOjE1OTc5NDU1MzAsInNwc2kiOiJRd20wbndXN0N5	
CcsTicketExpiration	2020-08-20T17:45:30.916Z	
DeduplicationHint		
E DeviceDdsClientId	530a8b79-f55a-5d7a-897a-36603253771d	
E DeviceThumbprint	g3dnHVFMiVc6l3Zt531jiysStZfPDRxNAuCc//Ceer0=	
IpV4Address	192.168.1.143	
ManufacturerName	DellInc.	
E ModelName	Venue 8 Pro 5830	
ShortOSVersion	10.0.19041.330	
😑 UserDeviceThumbprint	DFw3s8u7srTt1N++HfHJkrdN+RPuR+D6EnPdhJRHv40=	
connectionModes	4	
😑 deviceId	g3dnHVFMiVc6l3Zt531jiysStZfPDRxNAuCc//Ceer0=	
endpoints	(array)	
extendedDeviceStatus	0	
isMyDevice	true	
= name	Dell_Venue8	
= status	3	
😑 type	16	

## And capability info:



## A quick PackageIdHash test:

I made a copy of an executable on my desktop & renamed it. Here are the hashes of the two apps, showing they are identical:

Filename 🧳	MD5	SHA1	CRC32
DDC FSD info test app.exe	9DBFF96D5CF7FDC4CD0C5285D3CB1844	861ED00E54296AAE27AC66F8EAAED103249	733EF785
- ODCFSDinfo.exe	9DBFF96D5CF7FDC4CD0C5285D3CB1844	861ED00E54296AAE27AC66F8EAAED103249	733EF785

## And here is the relevant info from ActivitiesCache.db

	ETag	Application	Display Name	File Opened
	809375	D:\Costas\Desktop\ODCFSDinfo.exe		
	809374	D:\Costas\Desktop\ODCFSDinfo.exe	ODCFSDinfo.exe	ODCFSDinfo.exe
	809373	D:\Costas\Desktop\ODC FSD info test app.exe		
	809369	D:\Costas\Desktop\ODC FSD info test app.exe		
⊳	809368	D:\Costas\Desktop\ODC FSD info test app.exe	ODC FSD info test app.exe	ODC FSD info test app.exe

Showing a mismatch in the PackageIdHash value:



Note, the original app's PackageIdHash is "OOSIgddmGo2acCj6LWmJ61RsdMpKy5UH8/AeED0hoCA="

I deleted the original ODCFSDinfo.exe and renamed the second app as "ODCFSDinfo.exe". I run that app a few times to make sure I won't confuse the entries with the previous ones

ETag	Application	PackageldHash
809587	D:\Costas\Desktop\ODCFSDinfo.exe	O0SlgddmGo2acCj6LWmJ61RsdMpKy5UH8/AeED0hoCA=
809577	D:\Costas\Desktop\ODCFSDinfo.exe	O0SlgddmGo2acCj6LWmJ61RsdMpKy5UH8/AeED0hoCA=
809575	D:\Costas\Desktop\ODCFSDinfo.exe	00SlgddmGo2acCj6LWmJ61RsdMpKy5UH8/AeED0hoCA=
809571	D:\Costas\Desktop\ODCFSDinfo.exe	O0SlgddmGo2acCj6LWmJ61RsdMpKy5UH8/AeED0hoCA=

Now that PackageIdHash is the same as the original file's.

## Copied the original app to another folder:

Full Path	MD5	SHA1
D:\Costas\Desktop\ODCFSDinfo.exe	9DBFF96D5CF7FDC4CD0C5285D3CB1844	861ED00E54296AAE27AC66F8EAAED103249
D:\Temp\ODCFSDinfo.exe	9DBFF96D5CF7FDC4CD0C5285D3CB1844	861ED00E54296AAE27AC66F8EAAED103249

## executed it

ETag	Application	Display Name	File Opened
809828	D:\Temp\ODCFSDinfo.exe	ODCFSDinfo.exe	ODCFSDinfo.exe

## And got a totally different PackageIdHash this time:

PackageldHash

KaSajPw+fmzFuXVPSLWHzyMTkMH6P93d1RhcG+NNDXg=

## So, the path is as important as is the filename for the hash.

## Edited 2 bytes of the file

Filename /	Full Path	MD5	SHA1
🔏 ODCFSDinfo.exe	D:\Costas\Desktop\ODCFSDinfo.exe	9DBFF96D5CF7FDC4CD0C5285D3CB1844	861ED00E54296AAE27AC66F8EAAED103249

#### in WinHex, saved it (*obviously the MD5/SHA1 hashes are now different*):

Filename 🧳	Full Path	MD5	SHA1
🐌 ODCFSDinfo.exe	D:\Costas\Desktop\ODCFSDinfo.exe	3E24338CF560C553A9218975789BBC1B	62B5DB078B370E651CD31A895956D07CAE8

#### and executed it:

ETag	Application	PackageldHash
825030	D:\Costas\Desktop\ODCFSDinfo.exe	O0SlgddmGo2acCj6LWmJ61RsdMpKy5UH8/AeED0hoCA=
825026	D:\Costas\Desktop\ODCFSDinfo.exe	O0SlgddmGo2acCj6LWmJ61RsdMpKy5UH8/AeED0hoCA=

And the 'PackageIdHash' is still the same! So, it appears that 'PackageIdHash' is <u>not hashing the</u> <u>contents</u> of the file. Just the full path (including filename).

I highly suspect that 'PackageIdHash' is the hash of the info of the application (see below) and then is encoded in Base64:

: 33322BoxInc.Box Name Publisher : CN=D1F7D9E8-004F-4357-8F99-A820EE1E0308 Architecture : Neutral ResourceId : split.scale-400 Version : 2.1.68.0 PackageFullName : 33322BoxInc.Box\_2.1.68.0\_neutral\_split.scale-400\_dbfg57zya1ymg InstallLocation : C:\Program Files\WindowsApps\33322BoxInc.Box\_2.1.68.0\_neutral\_split.scale-400\_dbfg57zya1ymg IsFramework : False PackageFamilyName : 33322BoxInc.Box\_dbfg57zya1ymg PublisherId : dbfg57zya1ymg IsResourcePackage : True IsBundle : False IsDevelopmentMode : False NonRemovable : False IsPartiallyStaged : False SignatureKind : Store : Ok Status

#### such as obtained by Get-AppxPackage 33322BoxInc.Box

#### Or

Mode : -a----VersionInfo : File: D:\Costas\Desktop\ODCFSDinfo.exe InternalName: OriginalFilename: ODC-FSD FileVersion: 1.0.8.0 FileDescription:

Product: ODCFSDinfo ProductVersion: 1.0.8.0 Debug: False Patched: False PreRelease: False PrivateBuild: False SpecialBuild: False Language: Language Neutral : ODCFSDinfo BaseName Target : {} LinkType : Name : ODCFSDinfo.exe Length : 124472 DirectoryName : D:\Costas\Desktop Directory : D:\Costas\Desktop IsReadOnly : False Exists : True : D:\Costas\Desktop\ODCFSDinfo.exe FullName Extension :.exe CreationTime : 07 Jul 20 9:40:58 pm CreationTimeUtc : 07 Jul 20 6:40:58 pm LastAccessTime : 26 Jul 20 2:39:26 pm LastAccessTimeUtc : 26 Jul 20 11:39:26 am LastWriteTime : 25 Jul 20 9:47:24 pm LastWriteTimeUtc : 25 Jul 20 6:47:24 pm Attributes : Archive

#### Obtained by:

(get-item "D:\Costas\Desktop\ODCFSDinfo.exe")|select -Property \* ExcludeProperty PS\*

Not sure how this works with apps like

"Microsoft.Office.Word\_8wekyb3d8bbwe!microsoft.word" or "E7CF176E110C211B" (*Mozilla Firefox*) or "OperaSoftware.OperaWebBrowser.1402082470" etc.

## \*To be updated\*

