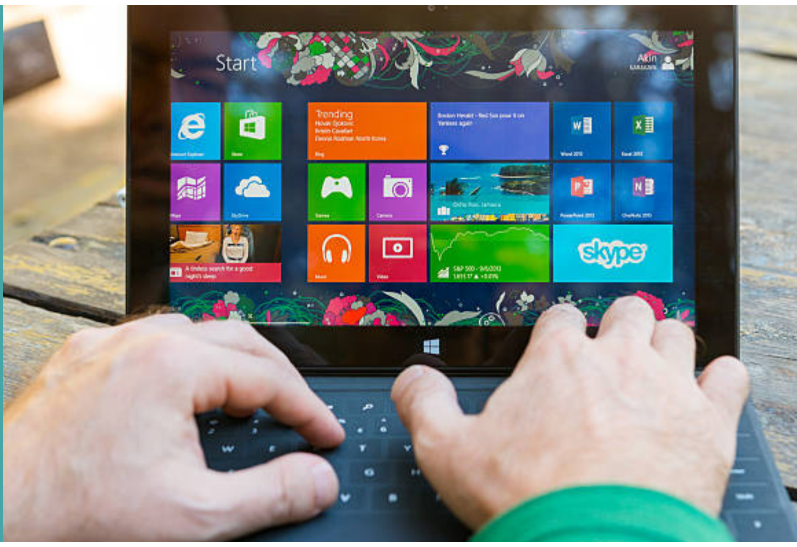
Technical Paper

CCL SOLUTIONS GROUP

incorporating evidencetalks

Windows 10 Timeline Forensic Artefacts

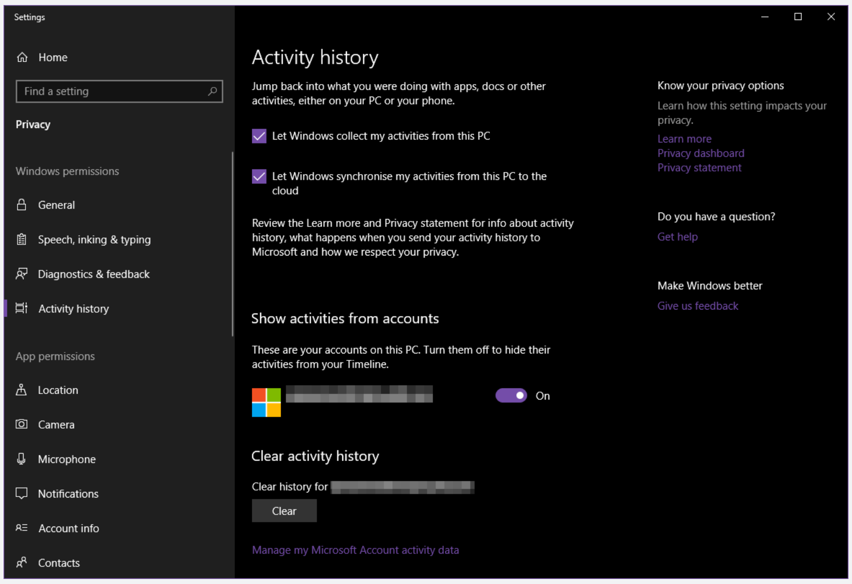
How the Timeline system can be a useful source of analysis



Microsoft's Windows 10 update of April 2018 included a new feature called "Timeline".

Timeline is like a browser history, but for your whole computer; it provides a chronology which not only contains the websites that you visited, but the documents you edited, the games you played, the images you viewed or created and so on. The feature is opt-in with the option to make use of it presented as the April 2018 Feature is applied and subsequently controlled from within the "Privacy" section in the Windows 10 settings.

CCL SOLUTIONS GROUP | incorporating evidencetalks



Settings

Home

Find a setting

Privacy

Windows permissions

General

Speech, inking & typing

Diagnostics & feedback

Activity history

App permissions

Location

Camera

Microphone

Notifications

Account info

Contacts

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 synchronise my activities from this PC to the cloud

Review the Learn more and Privacy statement for info about activity history, what happens when you send your activity history to Microsoft and how we respect your privacy.

Show activities from accounts

These are your accounts on this PC. Turn them off to hide their activities from your Timeline.

[redacted] On

Clear activity history

Clear history for [redacted]

Clear

Manage my Microsoft Account activity data

Know your privacy options

Learn how this setting impacts your privacy.

Learn more

Privacy dashboard

Privacy statement

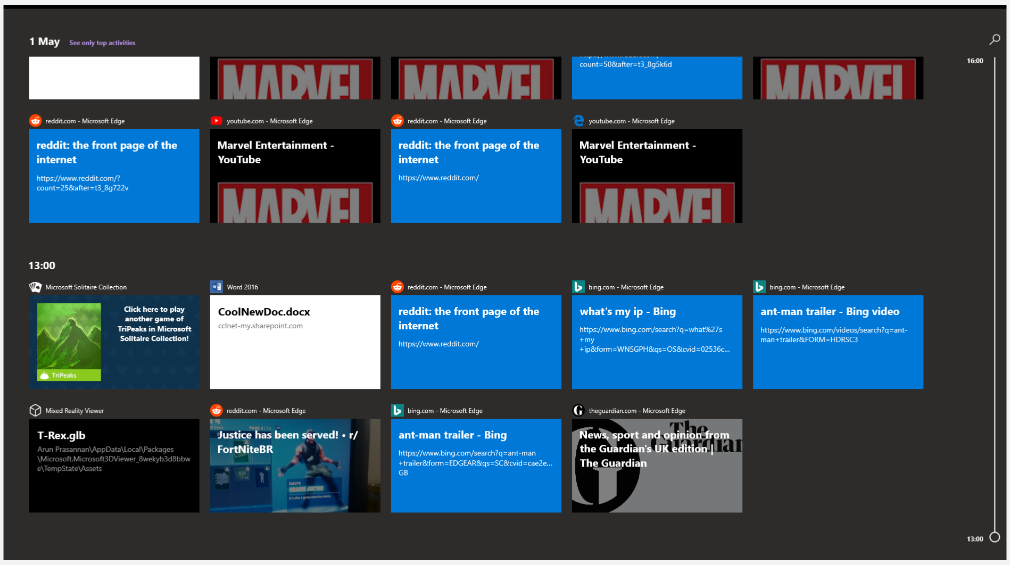
Do you have a question?

Get help

Make Windows better

Give us feedback

For the user, the Timeline lives within the Task View, which by default is accessed by hitting Win+Tab. Prior to this update, the Task View was somewhat like the classic "Alt+Tab" application switching, but augmented (and prettier). Now however, if you scroll down from the open apps you are also presented with a timeline of prior activities. The timeline is broken down by day, and you can dig down even more granularly to see your activity hour by hour.

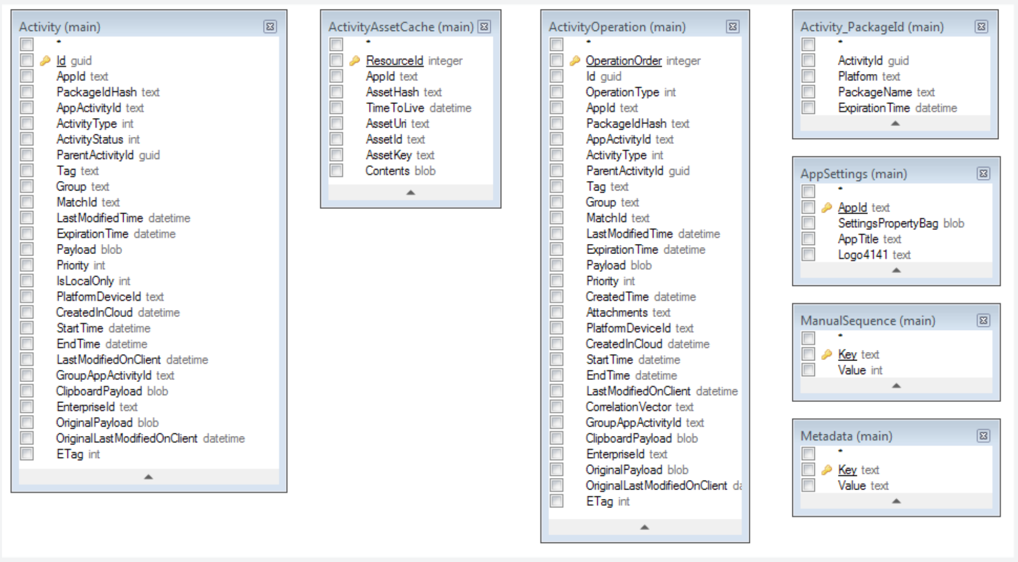

1 May
See only top activities
count=50&after=t3_8g5k6d
16:00
reddit.com - Microsoft Edge
reddit: the front page of the internet
https://www.reddit.com/?count=25&after=t3_8g722v
youtube.com - Microsoft Edge
Marvel Entertainment - YouTube
reddit.com - Microsoft Edge
reddit: the front page of the internet
https://www.reddit.com/
youtube.com - Microsoft Edge
Marvel Entertainment - YouTube
13:00
Microsoft Solitaire Collection
Click here to play another game of TriPeaks in Microsoft Solitaire Collection!
TriPeaks
Word 2016
CoolNewDoc.docx
cclnet-my.sharepoint.com
reddit.com - Microsoft Edge
reddit: the front page of the internet
https://www.reddit.com/
bing.com - Microsoft Edge
what's my ip - Bing
https://www.bing.com/search?q=what%27s+my+ip&form=WNSGPH&qs=OS&cvid=02536c...
bing.com - Microsoft Edge
ant-man trailer - Bing video
https://www.bing.com/videos/search?q=ant-man+trailer&FORM=HDRSC3
Mixed Reality Viewer
T-Rex.glb
Arun Prasannan\AppData\Local\Packages\Microsoft.Microsoft3DViewer_8wekyb3d8bbwe\TempState\Assets
reddit.com - Microsoft Edge
Justice has been served! • r/FortNiteBR
bing.com - Microsoft Edge
ant-man trailer - Bing
https://www.bing.com/search?q=ant-man+trailer&form=EDGEAR&qs=SC&cvid=cae2e...GB
theguardian.com - Microsoft Edge
News, sport and opinion from the Guardian's UK edition | The Guardian
13:00

At the time of writing, not every application contributes data to the timeline that the user sees. Some of the applications we found that currently provide data to the Timeline are: Edge (browsing history); the Office 2016 suite (files accessed); Windows' Photo viewer (photos viewed); the XBox app (games played); Paint 3D (drawings drawn).

All very useful for the user (personally I think I'll be making use of this – "what was I doing 2 days ago" is a question I often need answering), but what artefacts does this system leave for the pioneering analyst? Let's take a look:

Our initial exploration made use of the fantastic ProcMon utility in the **Sysinternals** suite, to hone in on a file which seemed to be at the centre of most interactions with the timeline. This file was found in `"%APPDATA%\ConnectedDevicesPlatform\AAD.xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx\ActivitiesCache.db".`

ActivitiesCache.db is a nice SQLite database with a fairly straightforward schema:



```
Activity (main)
*
Id guid
AppId text
PackageIdHash text
AppActivityId text
ActivityType int
ActivityStatus int
ParentActivityId guid
Tag text
Group text
MatchId text
LastModifiedTime datetime
ExpirationTime datetime
Payload blob
Priority int
IsLocalOnly int
PlatformDeviceId text
CreatedInCloud datetime
StartTime datetime
EndTime datetime
LastModifiedOnClient datetime
GroupAppActivityId text
ClipboardPayload blob
EnterpriseId text
OriginalPayload blob
OriginalLastModifiedOnClient datetime
ETag int
```

```
ActivityAssetCache (main)
*
ResourceId integer
AppId text
AssetHash text
TimeToLive datetime
AssetUri text
AssetId text
AssetKey text
Contents blob
```

```
ActivityOperation (main)
*
OperationOrder integer
Id guid
OperationType int
AppId text
PackageIdHash text
AppActivityId text
ActivityType int
ParentActivityId guid
Tag text
Group text
MatchId text
LastModifiedTime datetime
ExpirationTime datetime
Payload blob
Priority int
CreatedTime datetime
Attachments text
PlatformDeviceId text
CreatedInCloud datetime
StartTime datetime
EndTime datetime
LastModifiedOnClient datetime
CorrelationVector text
GroupAppActivityId text
ClipboardPayload blob
EnterpriseId text
OriginalPayload blob
OriginalLastModifiedOnClient d
ETag int
```

```
Activity_PackageId (main)
*
ActivityId guid
Platform text
PackageName text
ExpirationTime datetime
```

```
AppSettings (main)
*
AppId text
SettingsPropertyBag blob
AppTitle text
Logo4141 text
```

```
ManualSequence (main)
*
Key text
Value int
```

```
Metadata (main)
*
Key text
Value text
```

The table which jumps out as being the most important initially is "Activity", as it appears to contain data directly related to the entries displayed in the timeline and how that data is displayed. Much of the data in the Activity table (and indeed the database as a whole) is serialised as **JSON**. There are some complications caused by the fact that the JSON is sometimes stored as text (as in the "AppId" field) and other times as a binary data in a BLOB field, with the text encoded as UTF-8 (for example in the "Payload" field); one feasible explanation for this is that Microsoft may store other types of payload in the future, but in our testing, we only encountered JSON.

Each row in the table represents an "activity". These activities have a number of timestamps: "Last Modified"; "Created In Cloud" (because of course this data is synchronised in the cloud); "Start Time"; "End Time"; "Last Modified on Client"; and "Expiration Time"; the timestamps are stored as the number of seconds since 01/01/1970 - a Unix epoch timestamp. In our testing, the Expiration Time appeared to be set 30 days after the initial event. Whether or not "expired" records are removed from the database immediately requires some further research, but given that this is an SQLite database a tool such as Epilog may still be able to recover deleted records.

The activities also have an associated "App ID", which is stored as a JSON object in the "AppId" field in the table. The App ID field is slightly tricky: it does not absolutely record the application which generated the activity, rather it lists applications which are suitable for picking up and continuing this activity across multiple platforms (or even multiple options on the same platform). As an example, an activity related to accessing an Excel Spreadsheet lists 2 different versions of Excel on (native, Win32) Windows, the Universal App version of Excel and both the Android and iOS versions of Excel. Clearly, we didn't open the spreadsheet with all of these Apps at once, so we should be very careful how we interpret this field. It does, however, highlight something very interesting: it seems that Microsoft have aspirations for the Timeline to operate cross-platform, through the cloud. The opportunities and potential pitfalls provided by cross-device synchronisation was something I discussed in another **recent blog**.

It seems that many of these "Activities" can relate to the same application or system, and can be grouped together by examining the "AppActivityId" field – where this field matches another entry in the Activity table, they appear to relate to one another.

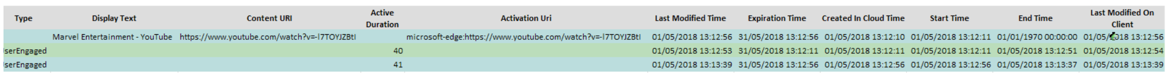
Given that overview of the structure of the database table, the meat of the information resides in the Payload field (which as mentioned previously is JSON stored in a BLOB field). The structure and content of the JSON data will vary based on the data it is representing, but what types of information did we observe during our exploration?

As expected, we found records which directly related back to the tiles seen in the Timeline itself; this includes the URLs of websites, the details of documents opened, games that were played, etc. and of course these entries are all timestamped.

More interestingly, there is significant information stored in this database table which is not otherwise displayed to the user in the Timeline view.

One such example is what seems to be a comprehensive list of applications that have been launched by the user – not just the applications which we noted above as contributing to the timeline, but all applications; native, UWP (universal) apps – it doesn't seem to matter, they all make their way into the Activity table. This is another potential source to demonstrate that a program was launched – but wait, it gets better!

Most of the types of entries we've mentioned so far have associated activities (by way of the matching "AppActivityId") where the Payload has the type "UserEngaged". This is a fascinating artefact which contains an "activeDurationSeconds" field which, from our testing so far, seems to provide a duration not of an application's (or part of an application's) execution, but rather the period of time that the user actively interacted with it. Furthermore it is possible to have multiple instances of "UserEngaged" activities related to an activity.



Type	Display Text	Content URI	Active Duration	Activation Uri	Last Modified Time	Expiration Time	Created In Cloud Time	Start Time	End Time	Last Modified On Client
	Marvel Entertainment - YouTube	https://www.youtube.com/watch?v=-l7TOYJZBtI		microsoft-edge:https://www.youtube.com/watch?v=-l7TOYJZBtI	01/05/2018 13:12:56	31/05/2018 13:12:56	01/05/2018 13:12:10	01/05/2018 13:12:11	01/01/1970 00:00:00	01/05/2018 13:12:56
serEngaged			40		01/05/2018 13:12:53	31/05/2018 13:12:11	01/05/2018 13:12:11	01/05/2018 13:12:11	01/05/2018 13:12:51	01/05/2018 13:12:54
serEngaged			41		01/05/2018 13:13:39	31/05/2018 13:12:56	01/05/2018 13:12:56	01/05/2018 13:12:56	01/05/2018 13:13:37	01/05/2018 13:13:39

As an example, a user might browse to a site in a tab within the Edge browser. This creates a record in the timeline relating to that site's URL; interacting with that tab also creates a "UserEngaged" record for the time that they are browsing that page. They then follow link on that page and open it in a new tab; this creates a new entry in the for the URL they opened and as they interact with the tab, a new "UserEngaged" record is created for the new URL. Finally closing the new tab, they return to the previous tab, which creates a second "UserEngaged" record in the timeline for the original URL. This "UserEngaged" artefact may be a new way for us to "put hands on the keyboard" when examining Windows 10 machines with a high level of specificity.

There is still more work to be done to more exhaustively analyse and understand this artefact in Windows 10, and we look forward to sharing more details with you, but in the meantime, if you have any questions email contact@cclsolutionsgroup.com or call 01789 261 200.

Alex Caithness, Principal Analyst (Research & Development)

May 2018