DFRWS

DIGITAL FORENSIC RESEARCH CONFERENCE

An Incomplete Tour of the Windows 10 Activity Timeline

By

Dr. Vico Marziale

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2019 USA

Portland, OR (July 15th - 19th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

https://dfrws.org

An Incomplete Tour of the Windows 10 Activity Timeline

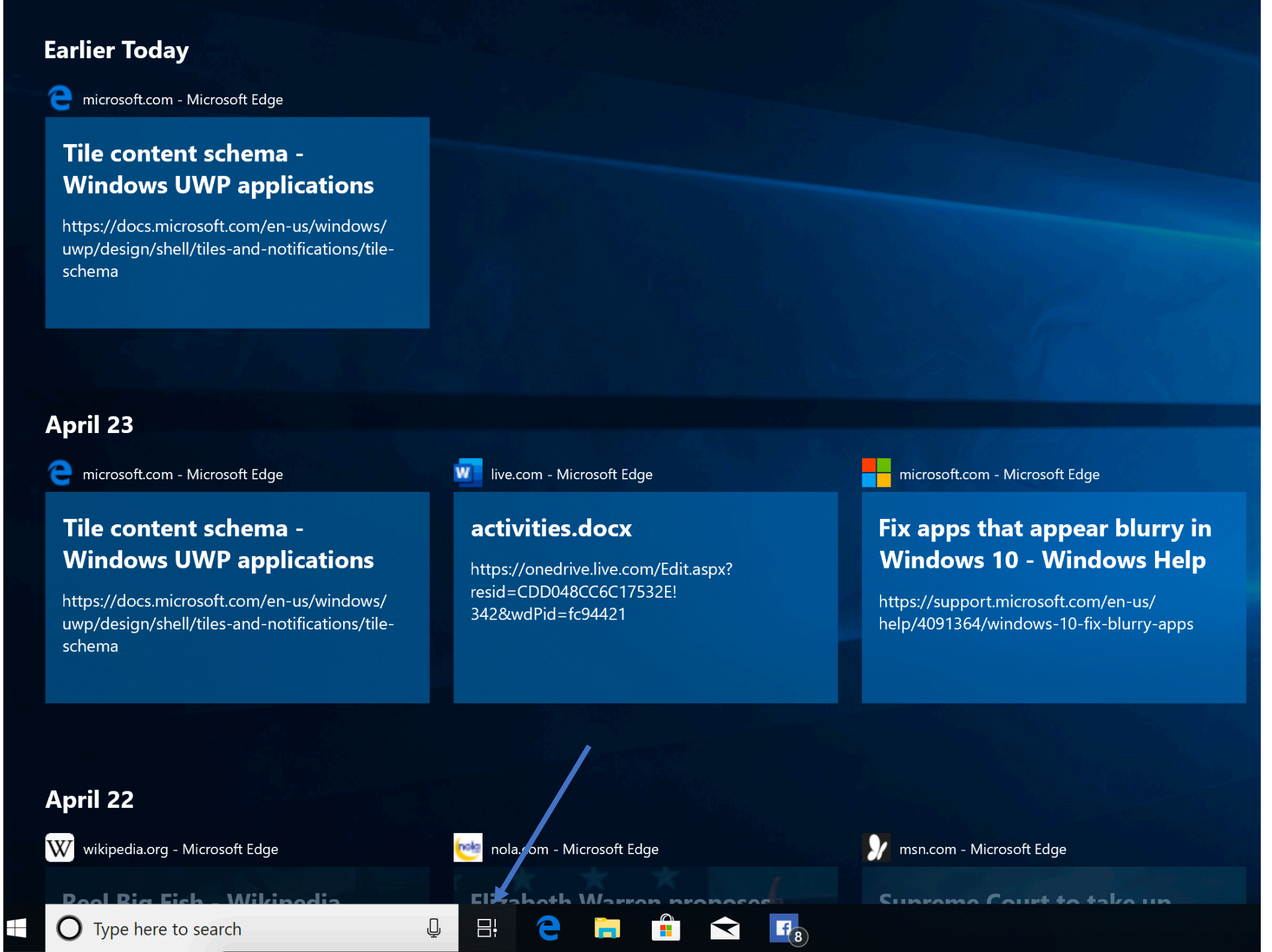
BlackBag®
TECHNOLOGIES

Dr. Vico Marizale
Senior Digital
Forensics Researcher

#whoami

- Researcher: Senior Digital Forensics Researcher, BBT
- Practitioner (formerly): 504ENSICS, mostly civil litigation
- Academic: PhD in CS (Digital Forensics), University of New Orleans
  - Published and presented research and tools at RSA, BlackHat, DOD Cybercrime, a few BSides, DFRWS, ODSFCon, etc.
- Occasional Gatekeeper: Digital Investigation, DFRWS, others
- Organizer: BSidesNOLA, NOLASec
- Tool author: Scalpel, Registry Decoder, Spotlight Inspector, DAMM

Windows Activity Timeline



The Basics

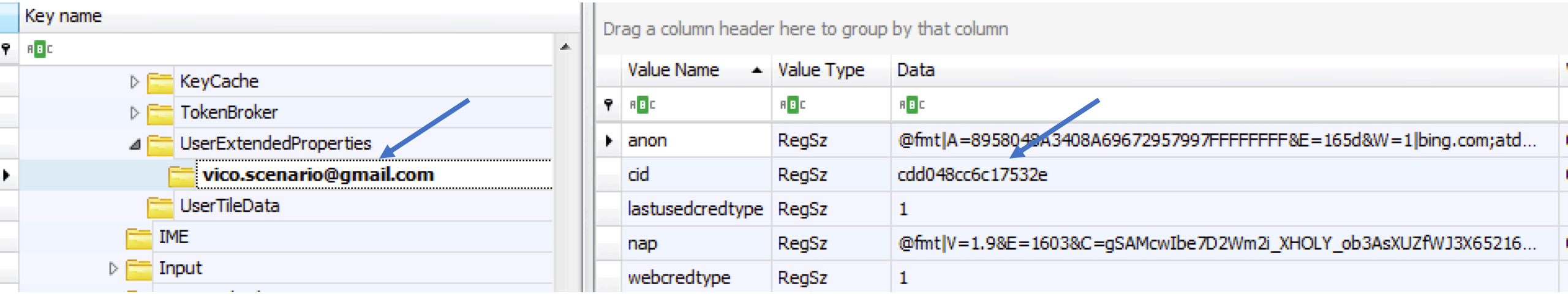
- Activities Cache, Windows Timeline, Activity Feed, etc.
- What is it really for?
  - Remind user what they were doing
  - Allow activities to be picked up across devices
  - Lap -> tablet -> phone, etc.
- How long: about 3 - 30 days depending on settings
- What do we get?
  - Applications run, and when a user was actively engaged
  - URLs, files accessed
  - Way more

Some Details

- What OS versions?
  - 1803 thru 1903 so far
  - With changes just to make life ~~difficult~~ interesting
- /Users/<user>/AppData/Local/ConnectedDevicesPlatform/?/ActivitiesCache.db
  - L.<local user account name> (e.g., L.vico)
  - Microsoft id number (hex string, e.g., cdd048cc6c17532e)
  - AAD.XXXXX (Azure Active Directory)
- File Structure
  - SQLite DB, WAL enabled
- Fully cross platform API support (iOS, Android, etc.)
  - Project Rome
  - MS Graph API
  - Connected Devices Platform

Resolving Microsoft IDs

NTUSER.DAT -> *Software\Microsoft\IdentityCRL\UserExtendedProperties*



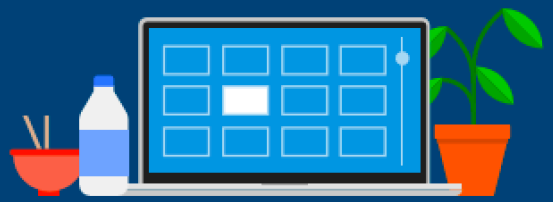
A Note on Configuration

- The behavior of the Activities feature changes depending on several factors
  - Exact version of Windows
  - Type of account used to log in
  - If same account used on multiple machines
  - If sync is turned on
- The “defaults” may be changing
- */Users/…/AppData/Local/ConnectedDevicesPlatform/CDPGlobalSettings.cdp*
- NTUSER.DAT ->*Software/Microsoft/Windows/CurrentVersion/CDP*
- Others related to Group Policy settings

Windows10x64_1903_PRERELEASE

Services

Do more across devices with activity history



If you want timeline and other Windows features to help you continue what you were doing, even when you switch devices, send Microsoft your activity history, which includes info about websites you browse and how you use apps and services. Select **Learn more** to find out how Microsoft products and services use this data to personalize experiences while respecting your privacy.

Learn more

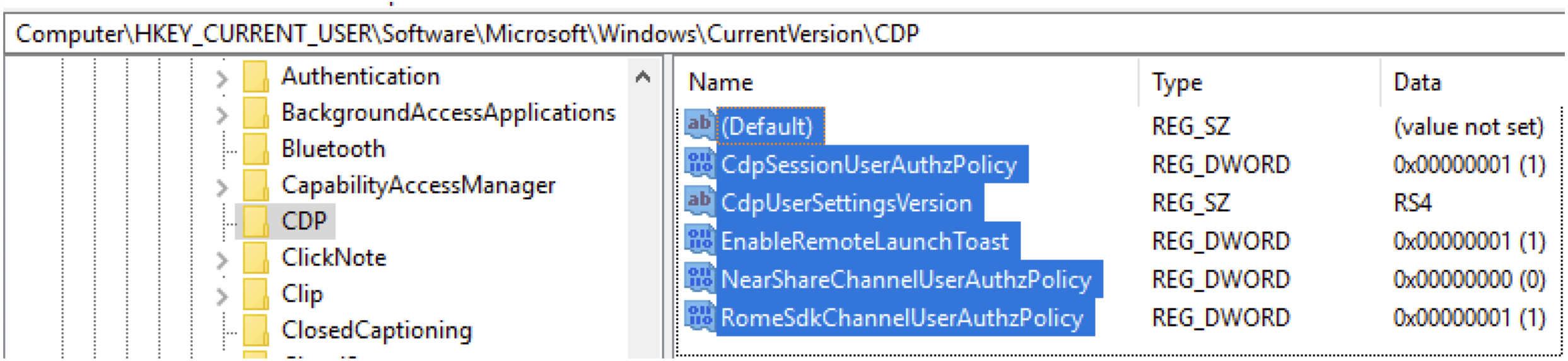
No

Yes

CDPGlobalSettings.cdp

JSON


```
"AfcPrivacySettings" : {
     "ActivityFeed" : 0,
     "CloudSync" : 0,
     "PublishUserActivity" : 0,
    "UploadUserActivity" : 1
  },
…
 "ActivityStoreInfo" : [
    {
      "active" : true,
      "activityStoreId" : "B20070B3-95B6-720F-E9F0-809A388D8DA8",
      "stableUserId" : "e19003d23958b65e"
    }
  ]
```



Structure

There are many fields. Some are not well understood.

There are a few important ones to know.

7 timestamps!
(I'm sure you can't see the column types, so you'll have to trust me.)

Activity		CREATE TABLE [Activity]([Id] GUID PRIMARY KEY
Id	GUID	"Id" GUID NOT NULL
AppId	TEXT	"AppId" TEXT NOT NULL
PackageIdHash	TEXT	"PackageIdHash" TEXT
AppActivityId	TEXT	"AppActivityId" TEXT
ActivityType	INT	"ActivityType" INT NOT NULL
ActivityStatus	INT	"ActivityStatus" INT NOT NULL
ParentActivityId	GUID	"ParentActivityId" GUID
Tag	TEXT	"Tag" TEXT
Group	TEXT	"Group" TEXT
MatchId	TEXT	"MatchId" TEXT
LastModifiedTime	DATETIME	"LastModifiedTime" DATETIME NOT NULL
ExpirationTime	DATETIME	"ExpirationTime" DATETIME
Payload	BLOB	"Payload" BLOB
Priority	INT	"Priority" INT
IsLocalOnly	INT	"IsLocalOnly" INT
PlatformDeviceId	TEXT	"PlatformDeviceId" TEXT
CreatedInCloud	DATETIME	"CreatedInCloud" DATETIME
StartTime	DATETIME	"StartTime" DATETIME
EndTime	DATETIME	"EndTime" DATETIME
LastModifiedOnClient	DATETIME	"LastModifiedOnClient" DATETIME
GroupAppActivityId	TEXT	"GroupAppActivityId" TEXT
ClipboardPayload	BLOB	"ClipboardPayload" BLOB
EnterpriseId	TEXT	"EnterpriseId" TEXT
OriginalPayload	BLOB	"OriginalPayload" BLOB
UserActionState	INT	"UserActionState" INT
IsRead	INT	"IsRead" INT
OriginalLastModifiedOnClient	DATETIME	"OriginalLastModifiedOnClient" DATETIME
GroupItems	TEXT	"GroupItems" TEXT
ETag	INT	"ETag" INT NOT NULL

Important Fields

- **StartTime and EndTime**
- **AppID**: the app that generated the Activity
- **AppActivityID**: app-specific identifier (can have URLs, file paths)
- **ActivityType**
  - 5: user opened an app
  - 6: user engaged with app
- **Payload**
  - Info on how the tile looks in the UI
  - Often contains files the app interacted with
- **Etag**: event ordering integer

PackageIdHash
Filter
nK0OV92yPrJVaQVuIvKdyuQGMDVfKCvHq8Vs/FcJSV8=
k6rI3Te3bxJRvjak0sx3vVZjSTM2c6pZ22Lb+ebZW6A=
FAO6/0eqz6gAo3BfLFqjKN6g3pcMzS+3xWGx07MxKB4=
WmO7oHZWxTMPjRbqWJP0nj4HxdaDGulwqMujnC6Nb0Q=
WmO7oHZWxTMPjRbqWJP0nj4HxdaDGulwqMujnC6Nb0Q=
WmO7oHZWxTMPjRbqWJP0nj4HxdaDGulwqMujnC6Nb0Q=
WmO7oHZWxTMPjRbqWJP0nj4HxdaDGulwqMujnC6Nb0Q=
WmO7oHZWxTMPjRbqWJP0nj4HxdaDGulwqMujnC6Nb0Q=
WmO7oHZWxTMPjRbqWJP0nj4HxdaDGulwqMujnC6Nb0Q=
WmO7oHZWxTMPjRbqWJP0nj4HxdaDGulwqMujnC6Nb0Q=
WmO7oHZWxTMPjRbqWJP0nj4HxdaDGulwqMujnC6Nb0Q=

256-bit
mystery hash

QuickXorHash?

```
[vicos-MacBook-Pro:flashlight vico$ echo "FAO6/0eqz6gAo3BfLFqjKN6g3pcMzS+3xWGx07MxKB4=" | base64 -D | xxd
00000000: 1403 baff 47aa cfa8 00a3 705f 2c5a a328  ....G.....p_,Z.(
00000010: dea0 de97 0ccd 2fb7 c561 b1d3 b331 281e  ....../..a...1(.
```

Table: Metadata

New Record | Delete Record

	Key	Value
	Filter	Filter
1	CurrentSettings	{"ActivityTypes":[4,3,2,1,0,5,13,6,11],"Environment":"prod"}
2	DatabaseInstanceId	11229
3	DatabaseInstanceIdUpdateTime	2019-02-28T01:00:58.370Z
4	DatabaseNotificationSubscriptionInfo	{"partialSyncToken":"","publisherFilters":[{"activityTypes":[0,1,2,3,4,5,6,7,13],"application":"*"}],"subscriptionEtag":"\"1211265768
5	DatabaseActivityPolicies	{"AllowedSubscriptionSyncScopes":[{"allowedTypes":[0,1,2,3,4,5,6,7,10,13,15],"application":"*"}],"Policies":[{"BlockedOperationFla
6	CurrentEtag	a35abbd0-3acd-11e9-9117-01020305070d

Torrent App Usage

	ETag	AppId	ActivityType
	Filter	torrent	Filter
1	1575	[{"application":"E:\\uTorrent.exe","platform":"x_exe_path"},{"application":"E:\\uTorrent.exe","platfor…	5
2	1586	[{"application":"C:\\Users\\USSF-JKreese\\AppData\\Roaming\\uTorrent\\uTorrent.exe","platform":…	5
3	1593	[{"application":"C:\\Users\\USSF-JKreese\\AppData\\Roaming\\uTorrent\\uTorrent.exe","platform":…	6
4	1629	[{"application":"C:\\Users\\USSF-JKreese\\AppData\\Roaming\\uTorrent\\uTorrent.exe","platform":…	6
5	1747	[{"application":"C:\\Users\\USSF-JKreese\\AppData\\Roaming\\uTorrent\\uTorrent.exe","platform":…	6
6	1847	[{"application":"C:\\Users\\USSF-JKreese\\AppData\\Roaming\\uTorrent\\uTorrent.exe","platform":…	6

Payload	:ime("StartTime", 'unixep	:time("EndTime", 'unixepc
Filter	Filter	Filter
{"displayText":"uTorrent.exe","activationUri":"ms-shellactivity:","appDisplayName":"uTorrent.ex…	2019-01-25 15:16:16	1970-01-01 00:00:00
{"displayText":"µTorrent","activationUri":"ms-shellactivity:","appDisplayName":"µTorrent","back…	2019-01-25 15:16:49	1970-01-01 00:00:00
{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":345,"shel…	2019-01-25 15:16:49	2019-01-25 15:22:45
{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":3,"shellC…	2019-01-25 15:41:37	2019-01-25 15:41:40
{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":135,"shel…	2019-01-25 16:26:51	2019-01-25 16:33:16
{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":2,"shellC…	2019-01-25 17:03:57	2019-01-25 17:03:59

Torrent App Usage

	ETag	AppId	ActivityType
	Filter	torrent	Filter
1	1575	[{"application":"E:\\uTorrent.exe","platform":"x_exe_path"},{"application":"E:\\uTorrent.exe","platfor...	5
2	1586	[{"application":"C:\\Users\\USSF-JKreese\\AppData\\Roaming\\uTorrent\\uTorrent.exe","platform":...	5
3	1593	[{"application":"C:\\Users\\USSF-JKreese\\AppData\\Roaming\\uTorrent\\uTorrent.exe","platform":...	6
4	1629	[{"application":"C:\\Users\\USSF-JKreese\\AppData\\Roaming\\uTorrent\\uTorrent.exe","platform":...	6
5	1747	[{"application":"C:\\Users\\USSF-JKreese\\AppData\\Roaming\\uTorrent\\uTorrent.exe","platform":...	6
6	1847	[{"application":"C:\\Users\\USSF-JKreese\\AppData\\Roaming\\uTorrent\\uTorrent.exe","platform":...	6

Payload	:ime("StartTime", 'unixep	:time("EndTime", 'unixepc
Filter	Filter	Filter
{"displayText":"uTorrent.exe","activationUri":"ms-shellactivity:","appDisplayName":"uTorrent.ex...	2019-01-25 15:16:16	1970-01-01 00:00:00
{"displayText":"µTorrent","activationUri":"ms-shellactivity:","appDisplayName":"µTorrent","back...	2019-01-25 15:16:49	1970-01-01 00:00:00
{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":345,"shel...	2019-01-25 15:16:49	2019-01-25 15:22:45
{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":3,"shellC...	2019-01-25 15:41:37	2019-01-25 15:41:40
{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":135,"shel...	2019-01-25 16:26:51	2019-01-25 16:33:16
{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":2,"shellC...	2019-01-25 17:03:57	2019-01-25 17:03:59

Torrent App Usage

	ETag	AppId	ActivityType
	Filter	torrent	Filter
1	1575	[{"application":"E:\\uTorrent.exe","platform":"x_exe_path"},{"application":"E:\\uTorrent.exe","platfor…	5
2	1586	[{"application":"C:\\Users\\USSF-JKreese\\AppData\\Roaming\\uTorrent\\uTorrent.exe","platform":…	5
3	1593	[{"application":"C:\\Users\\USSF-JKreese\\AppData\\Roaming\\uTorrent\\uTorrent.exe","platform":…	6
4	1629	[{"application":"C:\\Users\\USSF-JKreese\\AppData\\Roaming\\uTorrent\\uTorrent.exe","platform":…	6
5	1747	[{"application":"C:\\Users\\USSF-JKreese\\AppData\\Roaming\\uTorrent\\uTorrent.exe","platform":…	6
6	1847	[{"application":"C:\\Users\\USSF-JKreese\\AppData\\Roaming\\uTorrent\\uTorrent.exe","platform":…	6

Payload	:ime("StartTime", 'unixep	:time("EndTime", 'unixepc
Filter	Filter	Filter
{"displayText":"uTorrent.exe","activationUri":"ms-shellactivity:","appDisplayName":"uTorrent.ex…	2019-01-25 15:16:16	1970-01-01 00:00:00
{"displayText":"µTorrent","activationUri":"ms-shellactivity:","appDisplayName":"µTorrent","back…	2019-01-25 15:16:49	1970-01-01 00:00:00
{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":345,"shel…	2019-01-25 15:16:49	2019-01-25 15:22:45
{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":3,"shellC…	2019-01-25 15:41:37	2019-01-25 15:41:40
{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":135,"shel…	2019-01-25 16:26:51	2019-01-25 16:33:16
{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":2,"shellC…	2019-01-25 17:03:57	2019-01-25 17:03:59

Timezone

ActivityType 6


```
{
   "activeDurationSeconds": 3,
   "reportingApp": "ShellActivityMonitor",
   "shellContentDescription": {
      "MergedGap": 600
   },
   "type": "UserEngaged",
   "userTimezone": "America/Chicago"
}
```

	ETag	AppId	ActivityType	Payload	:time("StartTime", 'unixepc	:time("EndTime", 'unixepc
	F...	notepad	Filter	Filter	Filter	Filter
1	885	[{"application":"{1AC14E77-02E7-...	5	{"displayText":"Notepad","activationUri":"ms-shellactivity:","appDisplayName":"Notepad","back...	2018-12-18 15:33:59	1970-01-01 00:00:00
2	895	[{"application":"{1AC14E77-02E7-...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":17,"shel...	2019-01-09 19:58:56	2019-01-09 19:59:38
3	901	[{"application":"{1AC14E77-02E7-...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":6,"shell...	2019-01-09 19:59:49	2019-01-09 19:59:55
4	907	[{"application":"{1AC14E77-02E7-...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":11,"shel...	2019-01-09 20:00:00	2019-01-09 20:00:11
5	1327	[{"application":"{1AC14E77-02E7-...	5	{"displayText":"Notepad","activationUri":"ms-shellactivity:","appDisplayName":"Notepad","back...	2019-01-25 14:37:28	1970-01-01 00:00:00
6	1328	[{"application":"{1AC14E77-02E7-...	5	{"displayText":"aSecurity.reg","activationUri":"ms-shellactivity:","appDisplayName":"Notepad","...	2019-01-25 14:37:28	1970-01-01 00:00:00
7	1338	[{"application":"{1AC14E77-02E7-...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":43,"shel...	2019-01-25 14:37:28	2019-01-25 14:38:18
8	1659	[{"application":"{1AC14E77-02E7-...	5	{"displayText":"out.txt","activationUri":"ms-shellactivity:","appDisplayName":"Notepad","descri...	2019-01-25 15:50:52	1970-01-01 00:00:00
9	1663	[{"application":"{1AC14E77-02E7-...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":2,"shell...	2019-01-25 15:50:52	2019-01-25 15:50:54
10	1675	[{"application":"{1AC14E77-02E7-...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":1,"shell...	2019-01-25 15:51:08	2019-01-25 15:51:09
11	1756	[{"application":"{1AC14E77-02E7-...	5	{"displayText":"out.txt","activationUri":"ms-shellactivity:","appDisplayName":"Notepad","descri...	2019-01-25 16:36:12	1970-01-01 00:00:00
12	1760	[{"application":"{1AC14E77-02E7-...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":1,"shell...	2019-01-25 16:36:12	2019-01-25 16:36:13

Edit Database Cell

Mode: JSON

Import Export Set as NULL


```
{
    "activationUri": "ms-shellactivity:",
    "appDisplayName": "Notepad",
    "backgroundColor": "black",
    "contentUri": "file:%7B0762D272-C50A-4BB0-A382-697DCD729B80%7D/USSF-JKreese/Documents/aSecurity.reg",
    "description": "C:\\Users\\USSF-JKreese\\Documents\\aSecurity.reg",
    "displayText": "aSecurity.reg",
    "shellContentDescription": {
        "FileShellLink": "MBAAAEAFCAAAAAAAADAAAAAAAY0gAAAAgAAAA8buY31u0SdAo0HZmtLtUHAAPrkjzSL1BlkAAAAAAAAABAAAAAAAAAAAAAAAAAAAA8cAUAwHQB+
    }
```

```
00000000: 3010 0000 4005 0800 0000 0000 0030 0000  0...@........0..
00000010: 0000 018d 2000 0000 8000 0000 0317 cc92  .... ............
00000020: 7a59 2740 020f 121f aa25 5070 00db f3f9  zY'@.....%Pp....
00000030: d582 7507 48a4 0000 0000 0000 0400 0000  ..u.H...........
00000040: 0000 0000 0000 0000 0000 0003 4480 500c  ............D.P.
00000050: 0740 1f93 4038 baea 4184 8a23 4202 c08c  .@..@8..A..#B...
00000060: c346 4603 c891 eb01 4000 0000 0000 0000  .FF.....@.......
00000070: 0000 0000 0000 0000 0000 0058 140c 0000  ...........X....
00000080: 0000 0824 3551 9f40 0410 0d15 5507 1d14  ...$5Q.@....U...
00000090: 0001 0024 0001 03cb af4b 6524 f496 5302  ...$.....Ke$..S.
000000a0: 088b 0000 0000 3030 0000 0000 0000 0000  ......00........
000000b0: 0000 0000 0000 0000 0000 0000 0000 0410  ................
000000c0: 00c1 80d0 141d 0041 80b0 1c1c 0000 0058  .......A.......X
000000d0: 002a 0080 c0b4 8240 0046 53c0 c248 0048  .*.....@.FS..H.H
000000e0: cba8 1dd9 0300 c024 0001 03cb af4b 6524  .......$.....Ke$
000000f0: f496 5302 088b 0000 0080 41b0 0000 0000  ..S.......A.....
00000100: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000110: 0000 040c 0380 80a8 101c 01c1 8000 0005  ................
00000120: 0201 4000 0806 03cb af08 0410 0001 c0c0  ..@.............
00000130: 1016 0100 c0cc 001a 0381 80e0 101d 0081  ................
00000140: 80e4 141e 0001 c0cc 180d 0080 c0a8 101a  ................
```

	ETag	AppId	ActivityType	Payload	:time("StartTime", 'unixepc	:time("EndTime", 'unixepc
	F...	notepad	Filter	Filter	Filter	Filter
1	885	[{"application":"{1AC14E77-02E7-...	5	{"displayText":"Notepad","activationUri":"ms-shellactivity:","appDisplayName":"Notepad","back...	2018-12-18 15:33:59	1970-01-01 00:00:00
2	895	[{"application":"{1AC14E77-02E7-...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":17,"shel...	2019-01-09 19:58:56	2019-01-09 19:59:38
3	901	[{"application":"{1AC14E77-02E7-...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":6,"shell...	2019-01-09 19:59:49	2019-01-09 19:59:55
4	907	[{"application":"{1AC14E77-02E7-...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":11,"shel...	2019-01-09 20:00:00	2019-01-09 20:00:11
5	1327	[{"application":"{1AC14E77-02E7-...	5	{"displayText":"Notepad","activationUri":"ms-shellactivity:","appDisplayName":"Notepad","back...	2019-01-25 14:37:28	1970-01-01 00:00:00
6	1328	[{"application":"{1AC14E77-02E7-...	5	{"displayText":"aSecurity.reg","activationUri":"ms-shellactivity:","appDisplayName":"Notepad","...	2019-01-25 14:37:28	1970-01-01 00:00:00
7	1338	[{"application":"{1AC14E77-02E7-...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":43,"shel...	2019-01-25 14:37:28	2019-01-25 14:38:18
8	1659	[{"application":"{1AC14E77-02E7-...	5	{"displayText":"out.txt","activationUri":"ms-shellactivity:","appDisplayName":"Notepad","descri...	2019-01-25 15:50:52	1970-01-01 00:00:00
9	1663	[{"application":"{1AC14E77-02E7-...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":2,"shell...	2019-01-25 15:50:52	2019-01-25 15:50:54
10	1675	[{"application":"{1AC14E77-02E7-...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":1,"shell...	2019-01-25 15:51:08	2019-01-25 15:51:09
11	1756	[{"application":"{1AC14E77-02E7-...	5	{"displayText":"out.txt","activationUri":"ms-shellactivity:","appDisplayName":"Notepad","descri...	2019-01-25 16:36:12	1970-01-01 00:00:00
12	1760	[{"application":"{1AC14E77-02E7-...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":1,"shell...	2019-01-25 16:36:12	2019-01-25 16:36:13

Edit Database Cell

Mode: JSON

Import | Export | Set as NULL


```
{
    "activationUri": "ms-shellactivity:",
    "appDisplayName": "Notepad",
    "backgroundColor": "black",
    "contentUri": "file:///E:/Outgoing/out.txt",
    "description": "E:\\Outgoing\\out.txt",
    "displayText": "out.txt",
    "shellContentDescription": {
        "FileShellLink": "MBAAAEAFCAAAAAAAADAAAAAAAY0gAAAAgAAAAAO7e0cx0SdAAUY6MXMtUHAA8oWvFTL1BkeAAAAAAAAABAAAAAAAAAAAAAAAAAAA0PAUAwHC
```

Snipping Tool Usage

ETag	AppId	ActivityType	Payload	:time("StartTime", 'unixepc	etime("EndTime", 'u
Filter	Snipping	Filter	Filter	Filter	Filter
1159	[{"application":"{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\\SnippingTool.exe",...	5	{"displayText":"Snipping Tool","activationUri":"ms-shellactivity:","appDisplayName":"Snip...	2019-01-24 19:17:02	1970-01-01 00:00
1160	[{"application":"{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\\SnippingTool.exe",...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":3,...	2019-01-24 19:17:02	2019-01-24 19:17
1166	[{"application":"{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\\SnippingTool.exe",...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":22...	2019-01-24 19:17:26	2019-01-24 19:17
1172	[{"application":"{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\\SnippingTool.exe",...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":26...	2019-01-24 19:18:00	2019-01-24 19:18
1175	[{"application":"{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\\SnippingTool.exe",...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":6,...	2019-01-24 19:18:28	2019-01-24 19:18
1184	[{"application":"{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\\SnippingTool.exe",...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":12...	2019-01-24 19:18:42	2019-01-24 19:18
1203	[{"application":"{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\\SnippingTool.exe",...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":4,...	2019-01-24 19:19:12	2019-01-24 19:19
1206	[{"application":"{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\\SnippingTool.exe",...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":22...	2019-01-24 19:19:20	2019-01-24 19:19
1212	[{"application":"{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\\SnippingTool.exe",...	6	{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":13...	2019-01-24 19:19:53	2019-01-24 19:20

What files?

```
1  {
2      "activationUri": "ms-shellactivity:",
3      "appDisplayName": "Snipping Tool",
4      "backgroundColor": "black",
5      "displayText": "Snipping Tool"
2 6  }
```

Captures

	ETag	AppId	ActivityType	Payload	atetime("StartTime", 'unixepoch
	Filter	Filter	Filter	capture	Filter
1	1222	[{"application":"{7C5A40EF-A0FB-4BFC-874A-C...	5	{"displayText":"Capture3.PNG","activationUri":"ms-shellac...	2019-01-24 19:20:27
2	1232	[{"application":"{7C5A40EF-A0FB-4BFC-874A-C...	5	{"displayText":"Capture2.PNG","activationUri":"ms-shellac...	2019-01-24 19:20:31
3	1242	[{"application":"Microsoft.Windows.Photos_8weky...	5	{"displayText":"Capture1.PNG","activationUri":"ms-shellac...	2019-01-24 19:20:42


```
{
    "activationUri": "ms-shellactivity:",
    "appDisplayName": "Photos",
    "backgroundColor": "black",
    "contentUri": "file:%7BF38BF404-1D43-42F2-9305-67DE0B28FC23%7D/debug/WIA/Logs/Extract/Other/Capture1.PNG",
    "description": "C:\\Windows\\debug\\WIA\\Logs\\Extract\\Other\\Capture1.PNG",
    "displayText": "Capture1.PNG",
    "shellContentDescription": {
        "FileShellLink": "MBAAAEAFCAAAAAAAADAAAAAAAY0gAAAAgAAAAkYzxBZG0SdAB3ngQmBtUHQw9JIkZQL1B8FzPAAAAAAAB
```

Webmail


```
"items": [
   {
      "maxLines": 3,
      "size": "large",
      "text": "Inbox (11) - vico.scenario@gmail.com - Gmail",
      "type": "TextBlock",
      "weight": "bolder",
      "wrap": true
   },
   {
      "maxLines": 3,
      "size": "normal",
      "text": "https://mail.google.com/mail/u/0/",
      "type": "TextBlock",
      "wrap": true
   }
],
"type": "Container"
```

OneDrive


```
"items": [
    {
      "maxLines": 3,
      "size": "large",
      "text": "Pick up test.docx",
      "type": "TextBlock",
      "weight": "bolder",
      "wrap": true
    },
    {
      "maxLines": 3,
      "size": "normal",
      "text": "https://onedrive.live.com/edit.aspx?cid=cdd048cc6c17532e&
              page=view&resid=cdd048cc6c17532e!334&
              parId=cdd048cc6c17532e!104&app=Word",
      "type": "TextBlock",
      "wrap": true
    }
 ],
```

Web Search (Terms)

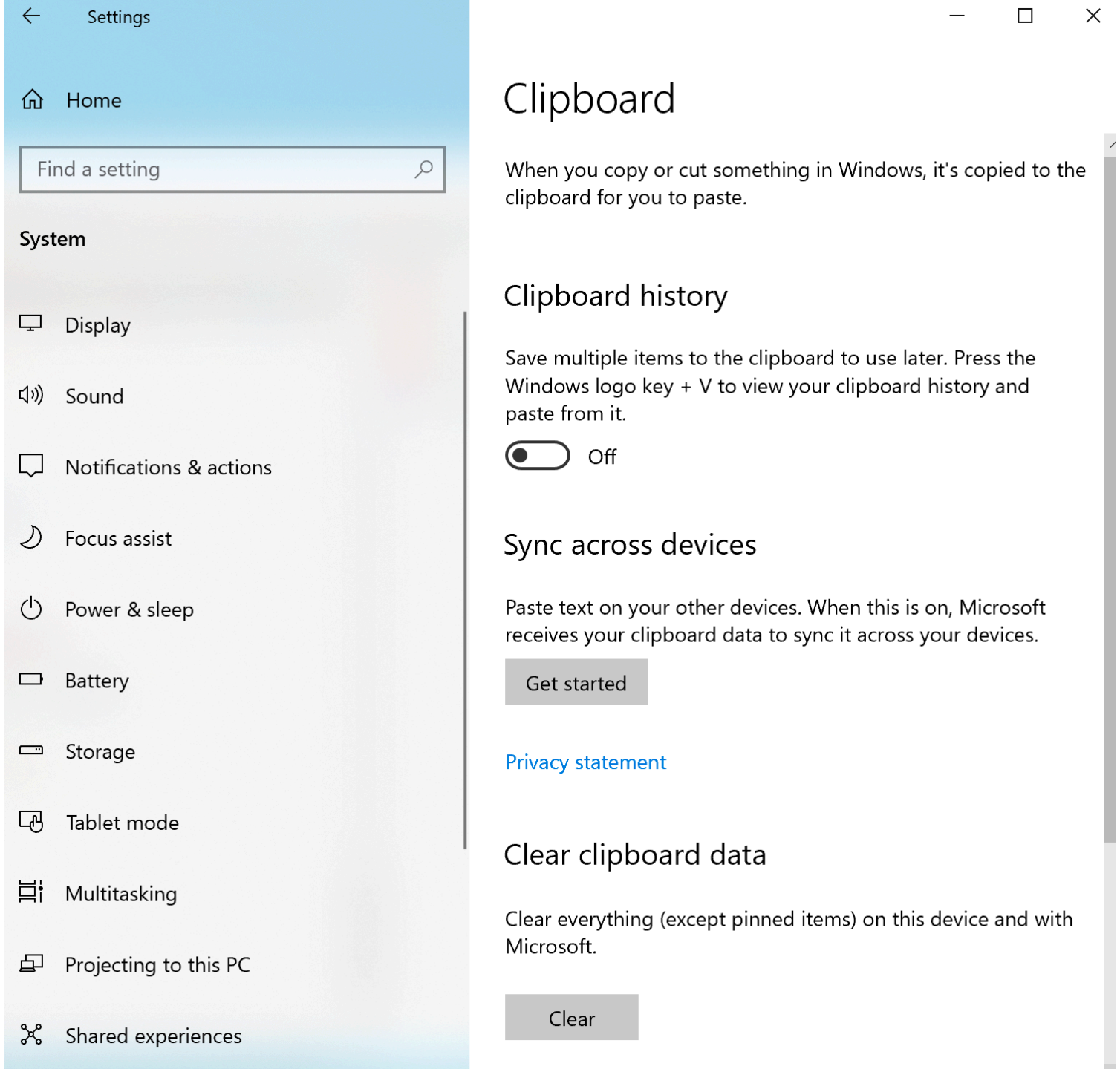

```
"items": [
    {
       "maxLines": 3,
       "size": "large",
       "text": "base64 decode online - Bing",
       "type": "TextBlock",
       "weight": "bolder",
       "wrap": true
    },
    {
       "maxLines": 3,
       "size": "normal",
       "text": "https://www.bing.com/search?q=base64+decode+online&
              form=EDGTCT&qs=SC&cvid=8654972fa47f47c293dc89d100cb1ef1&
              refig=176c2a807192404fce1a5cee03326522&cc=US&setlang=en-US&plvar=0",
       "type": "TextBlock",
       "wrap": true
    }
 ],
```

Windows Live Docs


```
{
   "activationUri": "ms-shellactivity:",
   "appDisplayName": "Word",
   "backgroundColor": "light",
   "contentUri": "https://d.docs.live.net/cdd048cc6c17532e/Documents/activities.docx",
   "description": "https://d.docs.live.net/cdd048cc6c17532e/Documents/activities.docx",
   "displayText": "activities.docx"
}
```

Don’t Forget Syncing

- If the user has an MS account
- Logs into multiple machines
- Has the right configuration
- Timeline of all Activities shows on all machines
- Leverages OneDrive



ActivityType 10: Copy/Paste

- Saw after enabling CloudClipboard
- Sometimes has Payload field populated, sometimes not
- Always has ClipboardPayload field populated:


```
 {
        "content":
"SSBoYXZlIHNlbGVjdGVkIHRoaXMgdGV4dCBhbmQgY29waWVkIGl
0Lg==",
        "formatName": "Text"
    }
```


Decodes to: "I have selected this text and copied it."

Wrap Up

- New feature in Windows 10 from 1803
- Tracks Activities
  - Info on files and URLs accessed
  - Actual user engagement time
  - User time zone
- Can be synced across devices
  - More kinds of devices than you may think
- Only saved for 30 days
  - Don’t forget VSCs
- There’s way more work to do!

BlackBag®
TECHNOLOGIES

Questions
?

Dr. Vico Marziale
vico@blackbagtech.com
@vicomarziale