

The folder "%user%\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\Settings" has a "settings.dat" file

```

settings.dat
Offset (d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
00000000 72 65 67 66 30 28 00 00 2F 28 00 00 62 EB 51 E0 regf0(../(..bλQŭ
00000016 AD 37 CD 01 01 00 00 00 03 00 00 00 00 00 00 00 .7N.....
  
```

which can be copied, and opened in a registry viewer:

LocalState	20	2018-02-20 09:58:01
AppCache	1	2015-09-27 10:03:23
AppIndexer	8	2018-02-20 09:48:57
AppsConstraintIndex	4	2018-02-20 09:51:38
> collections	0	2017-10-26 13:55:38
> CommitmentExtraction	0	2016-08-03 14:04:00
Configuration	56	2018-02-20 09:58:01
ConstraintIndex	3	2018-02-20 09:48:54
COOBE	0	2015-12-12 22:45:57
CortanaSettingsUpdateService	2	2017-10-26 13:55:38
CSI	5	2017-10-26 13:55:38
debug	0	2015-09-27 10:03:23
> DoNotDisturb	0	2015-09-27 10:02:45
Feedback	1	2017-10-26 13:55:38
HmdsMessages	3	2018-02-15 17:27:58
> IntentExtraction	2	2017-10-26 13:55:38

The ConstrainsIndex key has the following values:

Value Name	Value Type	Data
CurrentConstraintIndexCabPath	RegUnknown	A8-FE-FF-FF-43-00-3A-...
LastDownloadedConstraintIndexCabUrl	RegUnknown	A0-FF-FF-FF-68-00-74-...
LastDownloadedConstraintIndexCabPath	RegUnknown	A8-FE-FF-FF-43-00-3A-...

CurrentConstraintIndexCabPath:

...%user%..\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Input_{a7f50127-550b-4f74-b93e-65c366595b4b}

LastDownloadedConstraintIndexCabUrl: <https://www.bing.com/bcs/ci/18/en-us.cab>

Name	Size	Packed Type	Modified	CRC32
Local Disk				
apps.csg	280	? CSG File	15-Apr-16 8:00 ...	
apps.schema	150	? SCHEMA File	13-Apr-16 8:55 ...	
appsconversions....	31,582	? Text Document	13-Apr-16 8:55 ...	
appsglobals.txt	357,772	? Text Document	15-Apr-16 8:09 ...	
appssynonyms.txt	81,243	? Text Document	15-Apr-16 8:09 ...	
settings.csg	290	? CSG File	15-Apr-16 8:00 ...	
settings.schema	162	? SCHEMA File	13-Apr-16 8:55 ...	
settingsconversio...	31,582	? Text Document	13-Apr-16 8:55 ...	
settingsglobals.txt	40,479	? Text Document	15-Apr-16 8:09 ...	
settingsynonym...	76,566	? Text Document	15-Apr-16 8:09 ...	

which is expanded in the LastDownloadedConstraintIndexCabPath:

LastDownloadedConstraintIndexCabPath:

[ConstraintIndex\Input_{a7f50127-550b-4f74-b93e-65c366595b4b}](#)

Other keys of interest:

Type viewer	Slack viewer
Value name	PrepopulatedVersion
Value type	RegUnknown (0x10C, 268 decimal)
Value	D0-FF-FF-FF-31-00-2E-00-30-00-2E-00-30-00-2E-00-31-00-31-00-5F-00-65-00-6E-00-2D-00-55-00-53-00-00-00-2A-64-A1-BE-0B-F9-D0-01-00-00-00-00-00

AppCache PrepopulatedVersion: 1.0.0.11_en-US

AppsConstraintIndex settings:

LastConstraintIndexBuildAttempted	RegUnknown	E8-FF-FF-FF-4C-67-...	F8-BE-01-00
LatestConstraintIndexFolder	RegUnknown	A8-FE-FF-FF-43-00-...	64-00-73-00
LastConstraintIndexBuildCompleted	RegUnknown	E8-FF-FF-FF-C3-64-...	6E-6B-20-00
CurrentConstraintIndexFolder	RegUnknown	A8-FE-FF-FF-43-00-...	01-00-00-00

SettingsConstraintIndex settings:

LastConstraintIndexBuildAttempted	RegUnknown	E8-FF-FF-FF-F5-3C-...	70-8D-01-00
LatestConstraintIndexFolder	RegUnknown	A0-FE-FF-FF-43-00-...	00-00-00-00
LastConstraintIndexBuildCompleted	RegUnknown	E8-FF-FF-FF-2B-90-...	30-12-01-00
IndexedLanguage	RegUnknown	E8-FF-FF-FF-65-00-...	
IndexedVersion	RegUnknown	C8-FF-FF-FF-31-00-...	5F-54-79-70-65-00
NamespaceSettingsRevision	RegUnknown	A0-FF-FF-FF-7B-00-...	00-00-00-00-00-00
CurrentConstraintIndexFolder	RegUnknown	A0-FE-FF-FF-43-00-...	00-00-00-00

Some of these can also be found (in a live PC) at:

"\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Search\Microsoft.Windows.Cortana_cw5n1h2txyewy\"

AppsConstraintIndex & and SettingsConstraintIndex keys:

- CurrentConstraintIndexCabPath

Value name:

Value data:

- IndexedLanguage

Value name:

Value data:

- LatestConstraintIndexFolder

Value name:

Value data:

followed by the known

\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps" key

The folder

"%user%\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex"

contains 5 subfolders corresponding to the settings we see in the above screenshots of the **settings.dat** file:

Apps_{...current..}
Apps_{...last ..}
Input_{...current...}
Settings_{...current..}
Settings_{...last ..}

The "Apps_{}" folders contain:

0.0.filtertrie.intermediate.txt ----> common phrases and search terms created from apps.index
0.1.filtertrie.intermediate.txt
0.2.filtertrie.intermediate.txt
Apps.ft -----> word list created from apps.index (?)
Apps.index -----> application path list & index from installed apps (?)

Similarly, the "Settings_{}" folders contain:

0.0.filtertrie.intermediate.txt ----> common phrases and search terms created from settings.index
0.1.filtertrie.intermediate.txt
0.2.filtertrie.intermediate.txt
Settings.ft -----> word list created from Settings.index (?)
Settings.index -----> index from Settings (?)

Both the Apps_{ } and Settings_{ } subfolders have a .ft and .index files created respectively from the installed apps and system settings.

The "0.0.filtertrie.intermediate.txt" is a wordlist of common phrases created from the respective index (?) eg.

snippinmg~
snippinh~
snippingtool~
snippingn~
snipping'~
snipping tool~
snipping tools~
snipping toold~
snipping took~
snipping toll~
snippinf~

The Input_ folder has two .schema files:

The Apps.schema:

WindowsSearch
Conversions=AppsConversions.txt name
conversions=market,
spelling
synonyms=AppsSynonyms.txt
gscore=number lscore=number

The Settings.schema :

WindowsSearch
Conversions=SettingsConversions.txt name
conversions=market,
spelling
synonyms=SettingsSynonyms.txt
gscore=number lscore=number

There are also two global.txt files which are prepopulated. The “settingsglobal.txt” (common control panel and other settings) and appsglobal.txt (common application installation folders and executables, which are downloaded automatically as seen above in settings.dat) so Windows Search will know where/how to find them if they exist (?)

From the above files, the appssynonyms.txt (example):

* apple software update	* itunes up	4254
* application manager	* avid	1
* asphalt 8: airborne	* á	6538
* audiowizard	* maxx	4050
* autocad 2016 - english	* acad	4744
* autohotkey	* ahk	3756
* aw command center	* alienware	1927
* b&o play	* bo	1931
* baidu browser	* spark	3692

and settingsynonyms.txt (example):

* add or remove programs	* down	7683
* add or remove programs	* exit	7143
* add or remove programs	* pror	8514
* add or remove programs	* unst	8129
* add or remove programs	* aps	8005
* add or remove programs	* prg	8495
* add, edit, or remove other people	* administrator	4143
* add, edit, or remove other people	* user accounts	4020
* add, edit, or remove other people	* add account	3303
* add, edit, or remove other people	* accounts	3815
* add, edit, or remove other people	* add user	2199
* add, edit, or remove other people	* family	4020
* add, edit, or remove other people	* users	1050

The Apps.csg and Settings.csg files opened with a hex editor show this pattern:

pattern.^launch...pattern.^open...pattern.^start

Going back to the Settings.dat registry file, we can see in the AppIndexer key:

LocalState	15
{D1915118-9D27-4C69-B82E-7955DAF57...}	0
AppIndexer	7
AppsConstraintIndex	4
CommitmentExtraction	0

the “LatestCacheFileName”

Value name	Value type	Data
CurrentScaleFactor	RegUnknown	F0-FF-FF-FF-FA-00-00-00-96-9F-D5-9C-E8-7B-D3-01
HasInitialPushCompleted	RegUnknown	F0-FF-FF-FF-01-34-3D-AF-40-33-5D-D2-01-00-00-00
IconCacheHighContrastScheme	RegUnknown	E0-FF-FF-FF-3C-00-6E-00-6F-00-6E-00-65-00-3E-00-00-00-34-3D-AF-40-33-5D-D2-01-...
IndexedLanguage	RegUnknown	E8-FF-FF-FF-65-00-6E-00-2D-00-55-00-53-00-00-00-5B-95-FB-6B-3B-5D-D2-01
IndexedScaleFactor	RegUnknown	F0-FF-FF-FF-FA-00-00-00-8D-15-9C-A4-E8-7B-D3-01
LastSignalUploadTime	RegUnknown	E8-FF-FF-FF-00-00-00-00-00-00-00-00-00-00-B9-BD-C3-3B-33-5D-D2-01-00-00-00-00
LatestCacheFileName	RegUnknown	B0-FF-FF-FF-41-00-70-00-70-00-43-00-61-00-63-00-68-00-65-00-31-00-33-00-31-00-3...

has a value (translated from HEX) of: "AppCache131636187328178389.txt" which is found at

File Name	Date	Time	Type	Size
AppCache131636192750617377.txt	20-Feb-18	6:54 PM	Text Document	500 KB
AppCache131636187328178389.txt	20-Feb-18	6:45 PM	Text Document	499 KB
AppCache131636185216666425.txt	20-Feb-18	6:42 PM	Text Document	499 KB
AppCache131636183476622632.txt	20-Feb-18	6:39 PM	Text Document	498 KB
AppCache131633582122436911.txt	17-Feb-18	6:23 PM	Text Document	501 KB
SettingsCache.txt	29-Dec-16	3:41 PM	Text Document	276 KB

The LocalState\DeviceSearchCache folder along with the SettingsCache.txt:

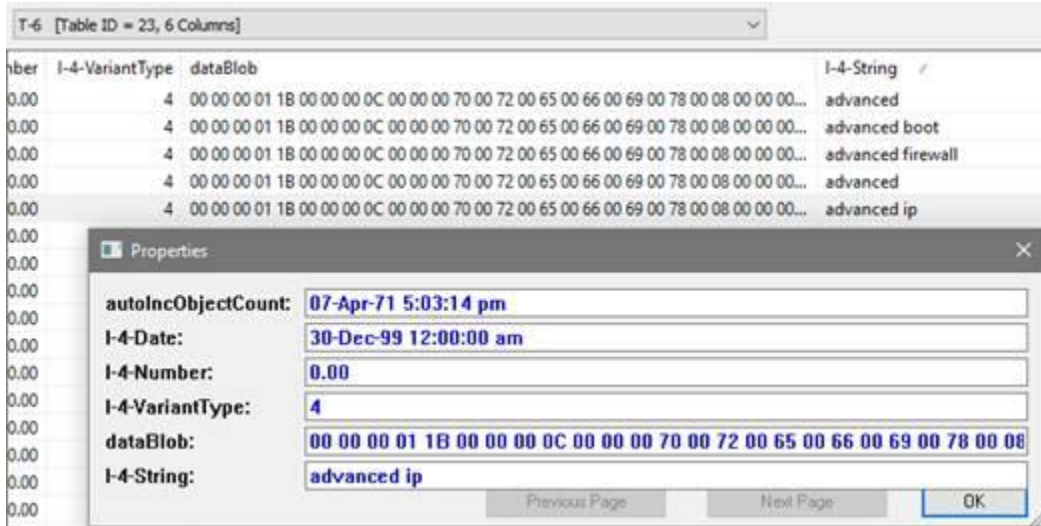
The AppCache****.txt is a list of all applications installed in the system, updated regularly, and has entries in the form of

System.FileExtension (eg exe, pdf,)
System.Software.ProductVersion
System.Kind (eg Program)
System.ParsingName
System.Software.TimesUsed
System.Tile.Background
System.AppUserModel.PackageFullName
System.FileName
System.ConnectedSearch.JumpList
System.ConnectedSearch.VoiceCommandExamples
System.ItemType (eg Trusted Immersive)
System.DateAccessed
System.Tile.EncodedTargetPath
System.Tile.SmallLogoPath
System.ItemNameDisplay

SettingsCache.txt which has entries in the form of

System.ParsingName
System.AppUserModel.ActivationContext
System.Setting.PageID
System.Setting.HostID
System.Comment
System.HighKeywords

Part of indexed.edb is also populated similarly; For example, I opened indexed.edb's T6 table and checked the 'advanced ip' in the I-4 string:



Where the datablob has a value of:

```
00 00 00 01 1B 00 00 00 0C 00 00 00 70 00 72 00 65 00 66 00 69 00 78 00 08 00 00 00 16 00 00 00 61 00 64 00 76 00 61 00 6E 00 63 00 65 00 64 00 20 00 69 00 70 00 00 00 0A 00
00 00 74 00 61 00 73 00 68 00 73 00 00 00 32 00 00 00 01 00 00 00 18 00 00 00 04 00 00 00 69 00 64 00 08 00 00 00 A4 00 00 00 7B 00 37 00 43 00 35 00 41 00 34 00 30 00 45 00
46 00 2D 00 41 00 30 00 46 00 42 00 2D 00 34 00 42 00 46 00 43 00 2D 00 38 00 37 00 34 00 41 00 2D 00 43 00 30 00 46 00 32 00 45 00 30 00 42 00 39 00 46 00 41 00 38 00 45
00 7D 00 5C 00 41 00 64 00 76 00 61 00 6E 00 63 00 65 00 64 00 20 00 49 00 50 00 20 00 53 00 63 00 61 00 6E 00 6E 00 65 00 72 00 5C 00 61 00 64 00 76 00 61 00 6E 00 63 00 65
00 64 00 5F 00 69 00 70 00 5F 00 73 00 63 00 61 00 6E 00 6E 00 65 00 72 00 2E 00 65 00 78 00 65 00 08 00 00 00 74 00 79 00 70 00 65 00 06 00 00 00 01 00 00 00 FF FF FF FF FF
FF FF FF 18 00 00 00 73 00 75 00 70 00 70 00 72 00 65 00 73 00 73 00 69 00 6F 00 6E 00 73 00 32 00 00 00 00 00 00 00 FF FF FF FF 22 00 00 00 65 00 6E 00 67 00 61 00 67 00 65
00 6D 00 65 00 6E 00 74 00 53 00 69 00 67 00 6E 00 61 00 6C 00 73 00 00 00 1B 00 00 00 2A 00 00 00 61 00 64 00 76 00 61 00 6E 00 63 00 65 00 64 00 20 00 69 00 70 00 20 00 73
00 63 00 61 00 6E 00 6E 00 65 00 72 00 09 00 30 00 00 00 1B 00 00 00 1E 00 00 00 53 00 75 00 67 00 67 00 65 00 73 00 74 00 69 00 6F 00 6E 00 47 00 72 00 6F 00 75 00 70 00 00
00 06 00 00 00 00 00 00 2A 00 00 00 50 00 72 00 6F 00 62 00 53 00 75 00 67 00 43 00 6C 00 69 00 63 00 6B 00 47 00 69 00 76 00 65 00 6E 00 50 00 72 00 65 00 66 00 00 00 07
00 00 00 E5 ED 08 A7 05 2F E5 3F FF FF FF 2C 00 00 00 61 00 64 00 76 00 61 00 6E 00 63 00 65 00 64 00 20 00 69 00 70 00 20 00 73 00 63 00 61 00 6E 00 6E 00 65 00 72 00 09
00 31 00 31 00 1B 00 00 00 1E 00 00 00 53 00 75 00 67 00 67 00 65 00 73 00 74 00 69 00 6F 00 6E 00 47 00 72 00 6F 00 75 00 70 00 00 00 06 00 00 00 0B 00 00 00 2A 00 00 00 50
00 72 00 6F 00 62 00 53 00 75 00 67 00 43 00 6C 00 69 00 63 00 6B 00 47 00 69 00 76 00 65 00 6E 00 50 00 72 00 65 00 66 00 00 00 07 00 00 00 27 31 08 AC 1C 5A CC 3F FF FF FF
FF FF FF FF FF FF FF FF 01
```

Which roughly translates as:

```
"prefix__advanced ip
tasks2__id_7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Advanced IP
Scanner\advanced_ip_scanner.exe_type__suppressions2"engagementSignals_*advanced ip scanner
  O__SuggestionGroup_*ProbSugClickGivenPref 歛DŽ/译advanced ip scanner 11__SuggestionGroup_
*ProbSugClickGivenPref ""
```

Corresponding to what is seen in the AppGlobals.txt file:

```
{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\cr\advanced_ip_scanner.exe 8859
and to
```

```
"{"1440": [{"7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Advanced IP Scanner\advanced_ip_scanner.exe", "1"]}
```

```
in %Windir%\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\Assets\bcsContent.json"
```

The same can be seen with indexed.edb's table T7 :

T-7 [Table ID = 26, 6 Columns]

0A 00 00 00 74 00 61 00 73 00 6B 00 73 00 00 00 32 00 00 00 04 00 00 00 1B 00 00 00 04 00 00 00 69 00 64 00 08 00 0	I-5-String
65 00 00 00 0A 00 00 00 74 00 61 00 73 00 6B 00 73 00 00 00 32 00 00 00 04 00 00 00 1B 00 00 00 04 00 00 00 69 00 6	add or r
65 00 6D 00 0A 00 00 00 74 00 61 00 73 00 6B 00 73 00 00 00 32 00 00 00 04 00 00 00 1B 00 00 00 04 00 00 00 69 00 6	add or re
65 00 6D 00 6F 00 00 00 0A 00 00 00 74 00 61 00 73 00 6B 00 73 00 00 00 32 00 00 00 05 00 00 00 1B 00 00 00 04 00 0	add or remove
65 00 6D 00 6F 00 76 00 0A 00 00 00 74 00 61 00 73 00 6B 00 73 00 00 00 32 00 00 00 05 00 00 00 1B 00 00 00 04 00 0	add or remov
65 00 6D 00 6F 00 76 00 65 00 00 00 0A 00 00 00 74 00 61 00 73 00 6B 00 73 00 00 00 32 00 00 00 06 00 00 00 1B 00 0	add or remove
65 00 6D 00 6F 00 76 00 65 00 20 00 0A 00 00 00 74 00 61 00 73 00 6B 00 73 00 00 00 32 00 00 00 03 00 00 00 1B 00 0	add or remove
65 00 6D 00 6F 00 76 00 65 00 20 00 70 00 00 00 0A 00 00 00 74 00 61 00 73 00 6B 00 73 00 00 00 32 00 00 00 03 00 0	add or remove p
65 00 6D 00 6F 00 76 00 65 00 20 00 70 00 72 00 0A 00 00 00 74 00 61 00 73 00 6B 00 73 00 00 00 32 00 00 00 04 00 0	add or remove pr
65 00 6D 00 6F 00 76 00 65 00 20 00 70 00 72 00 6F 00 00 00 0A 00 00 00 74 00 61 00 73 00 6B 00 73 00 00 00 32 00 0	add or remove pro
65 00 6D 00 6F 00 76 00 65 00 20 00 70 00 72 00 6F 00 67 00 0A 00 00 00 74 00 61 00 73 00 6B 00 73 00 00 00 32 00 0	add or remove prog
65 00 6D 00 6F 00 76 00 65 00 20 00 70 00 72 00 6F 00 67 00 72 00 61 00 0A 00 00 00 74 00 61 00 73 00 6B 00 73 00 0	add or remove progra
65 00 6D 00 6F 00 76 00 65 00 20 00 70 00 72 00 6F 00 67 00 72 00 61 00 6D 00 00 00 0A 00 00 00 74 00 61 00 73 00 6	add or remove program
65 00 6D 00 6F 00 76 00 65 00 20 00 70 00 72 00 6F 00 67 00 72 00 61 00 6D 00 00 00 0A 00 00 00 74 00 61 00 73 00 6	add or remove programs

Properties

autoIncObjectCount:

I-5-Date:

I-5-Number:

I-5-VariantType:

dataBlob:

I-5-String:

The data blob value:

```
00 00 00 01 1B 00 00 00 0C 00 00 00 70 00 72 00 65 00 66 00 69 00 78 00 08 00 00 00 2C 00 00 00 61 00 64 00 64 00 20 00 6F 00 72 00 20 00 72 00 65 00 6D 00 6F 00 76 00 65 00
20 00 70 00 72 00 6F 00 67 00 72 00 61 00 6D 00 73 00 0A 00 00 00 74 00 61 00 73 00 6B 00 73 00 00 00 32 00 00 00 06 00 00 00 1B 00 00 00 04 00 00 00 69 00 64 00 08 00 00 00
26 00 00 00 41 00 64 00 64 00 4F 00 72 00 52 00 65 00 6D 00 6F 00 76 00 65 00 50 00 72 00 6F 00 67 00 72 00 61 00 6D 00 73 00 00 00 08 00 00 00 74 00 79 00 70 00 65 00 06 00
00 00 02 00 00 00 FF FF FF FF 1B 00 00 00 04 00 00 00 69 00 64 00 08 00 00 00 5C 00 00 00 43 00 6C 00 61 00 73 00 73 00 69 00 63 00 5F 00 7B 00 30 00 34 00 30 00 38 00 37 00
33 00 43 00 42 00 2D 00 34 00 30 00 34 00 41 00 2D 00 34 00 39 00 46 00 45 00 2D 00 41 00 32 00 35 00 34 00 2D 00 41 00 39 00 42 00 42 00 39 00 43 00 45 00 46 00 41 00 45
00 41 00 35 00 7D 00 08 00 00 00 74 00 79 00 70 00 65 00 06 00 00 00 02 00 00 00 FF FF FF FF 1B 00 00 00 04 00 00 00 69 00 64 00 08 00 00 00 5C 00 00 00 43 00 6C 00 61 00 73
00 73 00 69 00 63 00 5F 00 7B 00 45 00 30 00 37 00 46 00 32 00 31 00 35 00 41 00 2D 00 36 00 30 00 32 00 32 00 2D 00 34 00 30 00 45 00 30 00 2D 00 41 00 31 00 30 00 39 00
2D 00 31 00 37 00 30 00 37 00 38 00 39 00 39 00 32 00 45 00 35 00 46 00 39 00 7D 00 08 00 00 00 74 00 79 00 70 00 65 00 06 00 00 00 02 00 00 00 FF FF FF FF 1B 00 00 00 04 00
00 00 69 00 64 00 08 00 00 00 3A 00 00 00 41 00 41 00 41 00 5F 00 53 00 65 00 74 00 74 00 69 00 6E 00 67 00 73 00 47 00 72 00 6F 00 75 00 70 00 41 00 70 00 70 00 53 00 69 00
7A 00 65 00 73 00 4C 00 69 00 73 00 74 00 00 00 08 00 00 00 74 00 79 00 70 00 65 00 06 00 00 00 02 00 00 00 FF FF FF FF 1B 00 00 00 04 00 00 00 69 00 64 00 08 00 00 00 5C 00
00 00 43 00 6C 00 61 00 73 00 73 00 69 00 63 00 5F 00 7B 00 41 00 33 00 43 00 32 00 44 00 36 00 35 00 33 00 2D 00 44 00 44 00 30 00 30 00 2D 00 34 00 30 00 46 00 31 00 2D
00 38 00 45 00 35 00 33 00 2D 00 37 00 39 00 36 00 46 00 39 00 42 00 41 00 31 00 45 00 45 00 30 00 31 00 7D 00 08 00 00 00 74 00 79 00 70 00 65 00 06 00 00 00 02 00 00 00 FF
FF FF FF 1B 00 00 00 04 00 00 00 69 00 64 00 08 00 00 00 5C 00 00 00 43 00 6C 00 61 00 73 00 73 00 69 00 63 00 5F 00 7B 00 39 00 38 00 43 00 43 00 41 00 30 00 42 00 39 00 2D
00 43 00 46 00 36 00 43 00 2D 00 34 00 46 00 46 00 44 00 2D 00 39 00 38 00 45 00 31 00 2D 00 38 00 37 00 42 00 46 00 45 00 44 00 44 00 44 00 34 00 44 00 32 00 31 00 7D 00
08 00 00 00 74 00 79 00 70 00 65 00 06 00 00 00 02 00 00 00 FF FF FF FF 18 00 00 00 73 00 75 00 70 00 70 00 72 00 65 00 73 00 73 00 69 00 6F 00 6E 00 73 00 32 00
00 00 00 00 00 FF FF FF FF 22 00 00 00 65 00 6E 00 67 00 61 00 67 00 65 00 6D 00 65 00 6E 00 74 00 53 00 69 00 67 00 6E 00 61 00 6C 00 73 00 00 00 1B 00 00 00 38 00 00 00
63 00 68 00 61 00 6E 00 67 00 65 00 20 00 6F 00 72 00 20 00 72 00 65 00 6D 00 6F 00 76 00 65 00 20 00 61 00 20 00 70 00 72 00 6F 00 67 00 72 00 61 00 6D 00 09 00 31 00 1B 00
00 00 1E 00 00 00 53 00 75 00 67 00 67 00 65 00 73 00 74 00 69 00 6F 00 6E 00 47 00 72 00 6F 00 75 00 70 00 00 00 06 00 00 00
```

Is roughly translated as:

"prefix_add or remove programs

```
tasks2__id_&AddOrRemovePrograms_type__id_ \Classic_{040873CB-404A-49FE-A254-A9BB9CEFAEAS}_type__i
d_ \Classic_{E07F215A-6022-40E0-A109-17078992E5F9}_type__id_ :AAA_SettingsGroupAppSizesList_type__id_ \Cl
assic_{A3C2D653-DD00-40F1-8E53-796F9BA1EE01}_type__id_ \Classic_{98CCA0B9-CF6C-4FFD-98E1-87BFEDDD4D2
1}_type__suppressions2"engagementSignals_8change or remove a program 1__SuggestionGroup_"
```

Corresponding to what is seen in the SettingsGlobals.txt file:

```
Classic_{E07F215A-6022-40E0-A109-17078992E5F9} 10637
```

And to {"592" : ["Classic_{E07F215A-6022-40E0-A109-17078992E5F9}", "2"]}









```

590={"589": ["Classic_{DD338333-7000-45CC-A84D-64680D6E683D}", "2"]}
591={"590": ["Classic_{DF7B19EF-DEA5-47D7-BBA5-9FCBE400A59D}", "2"]}
592={"591": ["Classic_{E00117F3-53BA-4E06-B9BF-B8E22A1469E6}", "2"]}
593={"592": ["Classic_{E07F215A-6022-40E0-A109-17078992E5F9}", "2"]}
594={"593": ["Classic_{E2394C16-F45A-496F-83CC-49E163281662}", "2"]}
595={"594": ["Classic_{E4B554C8-B067-4540-A478-0565BB1F76B9}", "2"]}
596={"595": ["Classic_{E5907A23-4A25-4D75-A16E-16822E2FA38B}", "2"]}
597={"596": ["Classic_{E6243488-3449-4D4D-98AA-FFC14E3FF0F8}", "2"]}

```

As seen in the %Windir%\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\Assets\bcsContent.json" file.

The bcsContent.json file is located at "%Windir%\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\Assets" hasn't been updated since 16 Jul 2016.

	reminder.gif	16-Jul-16 2:43 PM	GIF File	139 KB
	search.gif	16-Jul-16 2:43 PM	GIF File	83 KB
	speech.gif	16-Jul-16 2:43 PM	GIF File	177 KB
	bcsContent.json	16-Jul-16 2:43 PM	JSON File	518 KB
	badge.png	16-Jul-16 2:43 PM	PNG File	2 KB
	call.white.png	16-Jul-16 2:43 PM	PNG File	1 KB
	complete.white.png	16-Jul-16 2:43 PM	PNG File	1 KB

After a quick examination, it looks like bcsContent.json was replaced with the appsglobals.txt and settingsglobal.txt files, as its entries seem to include the similar contents to both of these files:

```

438={"1437": [{"7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\Adobe\\Reader 11.0\\Reader\\AcroRd32.exe", "1"]}
439={"1438": [{"7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\Advanced Combat Tracker\\ACTx86.exe", "1"]}
440={"1439": [{"7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\Advanced Combat Tracker\\Advanced Combat Tracker.exe", "1"]}
441={"1440": [{"7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\Advanced IP Scanner\\advanced_ip_scanner.exe", "1"]}
442={"1441": [{"7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\Agoge Technology\\AiM\\AIM.exe", "1"]}
443={"1442": [{"7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\AirDroid\\Launcher.exe", "1"]}
444={"1443": [{"7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\AirPort\\APUtil.exe", "1"]}
445={"1444": [{"7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\Allway Sync\\Bin\\syncappw.exe", "1"]}
446={"1445": [{"7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\AltiGen\\MaxCommunicator\\MaxCommunicator.exe", "1"]}
501={"500": ["Classic_{58e3c745-d971-4081-9034-86e34b30836a}", "2"]}
502={"501": ["Classic_{5902614C-D9C7-4902-9F7F-BAF85454D0B2}", "2"]}
503={"502": ["Classic_{5BB16858-F647-465E-BCFD-010EE9DD41B7}", "2"]}
504={"503": ["Classic_{5D611F64-7985-459B-BDFF-AEC069CB2625}", "2"]}
505={"504": ["Classic_{5DE5B491-2CEA-4AD9-824A-982A22C0B64E}", "2"]}
506={"505": ["Classic_{5FFAA809-0961-40CF-90A4-58037867FA50}", "2"]}
507={"506": ["Classic_{5ea4f148-308c-46d7-98a9-49041b1dd468}", "2"]}
508={"507": ["Classic_{60AC7FA0-A928-4D45-B4DD-AC70A6175E67}", "2"]}

```

It also has entries like

```

478={"whi": {"LL": [], "TSK": [], "SUP": [190,191,192]}}
479={"windows 7": {"LL": [{"windows 7 usb dvd download tool",0,0.15}, {"backup and restore (windows 7)",1,0.45}, {"windows 7 download",
["250,876,661"], "SUP": [751]}]}
480={"windows ba": {"LL": [{"windows backup",11,0.212}, {"file history settings",1,0.075}, {"backup and restore (windows 7)",1,0.553}]}
481={"windows de": {"LL": [{"windows defender settings",1,0.514}, {"windows defender",0,0.424}], "TSK": [169,1369], "SUP": [256]}}
482={"windows defe": {"LL": [{"windows defender",0,0.427}, {"windows defender settings",1,0.54}], "TSK": [169,1369,828], "SUP": []}}

```

which are similar to the settingsynonyms.txt:

```
*|autoplay settings *|autorun 4653
*|autoplay settings *|drive 5578
*|autoplay settings *|dvd 1167
*|backup and restore (windows 7) *|windows backup 3490
*|backup and restore (windows 7) *|window 7 6005
*|backup and restore (windows 7) *|recover 5523
*|backup settings *|file history settings 5543
*|backup settings *|file history drive 5209
*|backup settings *|windows backup 4528
*|backup settings *|system backup 4944
*|backup settings *|system image 3748
*|backup settings *|file backup 5440
*|backup settings *|back up 2667
*|backup settings *|history 5038
```

and

```
016={"phot": {"LL": [{"photos",0,0.294},["adobe photoshop cc 2015",0,0.272]], "TSK": [656,835,1134,1135,1136,1435], "SUP": [1094]}}
017={"photo": {"LL": [{"photos",0,0.276},["adobe photoshop cc 2015",0,0.278]], "TSK": [702,1135,1136,1435,92,207,282,656,835,1134,80], "SUP": []}}
018={"photoshop": {"LL": [{"adobe photoshop express",10,0.106},["adobe photoshop cc 2014",0,0.057},["adobe photoshop cc 2015",0,0.398},["photoshop",2,0.088},["adobe photoshop cs6",0,0.077]], "TSK": [656,1134,1135,1136,1435], "SUP": []}}
```

similar to the appssynonyms.txt

```
*|adobe creative cloud *|adobe cc 6062
*|adobe photoshop cc 2015 *|فوتوشوب 7451
*|adobe photoshop cs6 (64 bit) *|phôt 6536
*|adobe reader touch *|pdf 2199
*|adobe reader x *|acro 3405
*|adobe reader xi *|acro 3405
*|adobe reader xi *|pdf 2458
```

and the relevant entries in Indexedb.edb

prefix photo

tasks2

__id_pFileManager_cw5n1h2txyewy\Microsoft.Windows.PhotoManager_type_..._id_x{6D809377-6AF0-444B-8957-A3773F02200E}\Adobe\Adobe Photoshop CC

2015\Photoshop.exe_type_..._id_®{6D809377-6AF0-444B-8957-A3773F02200E}\Adobe\Adobe Photoshop CS6 (64

Bit)\Photoshop.exe_type_..._id_®{7C5A0EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Adobe\Adobe Photoshop

CS6\Photoshop.exe_type_..._id_DAAA_SettingsGroupLockScreenPreview_type_..._id_JAAA_SystemSettings_D

I-3-Date	I-3-Number	I-3-VariantType	dataBlob	I-3-String
30-Dec-99 12:00:00 AM	0.00	4	00 00 00 01 18 00 00 00 0C 00 00 00 70 00 72 00 65...	phot
30-Dec-99 12:00:00 AM	0.00	4	00 00 00 01 18 00 00 00 0C 00 00 00 70 00 72 00 65...	photoshop
30-Dec-99 12:00:00 AM	0.00	4	00 00 00 01 18 00 00 00 0C 00 00 00 70 00 72 00 65...	photosh
30-Dec-99 12:00:00 AM	0.00	4	00 00 00 01 18 00 00 00 0C 00 00 00 70 00 72 00 65...	photo
30-Dec-99 12:00:00 AM	0.00	4	00 00 00 01 18 00 00 00 0C 00 00 00 70 00 72 00 65...	photosho
30-Dec-99 12:00:00 AM	0.00	4	00 00 00 01 18 00 00 00 0C 00 00 00 70 00 72 00 65...	photos

Properties

autoIncObjectCount: 4295

I-3-Date: 30-Dec-99 12:00:00 AM

I-3-Number: 0.00

I-3-VariantType: 4

dataBlob: 00 65 00 6D 00 53 00 65 00 74 00 74 00 69 00 6E 00 67 00 73 00 5F 00 44 00

I-3-String: photo

The {D1915118-9D27-4C69-B82E-7955DAF57201} key in the settings.dat registry file:

LocalState	15
{D1915118-9D27-4C69-B82E-7955DAF57201}	0
Files	1

corresponds to: SpUncompressedLexicon Class

(%SystemRoot%\System32\Speech_OneCore\Common\sapi_onecore.dll)

Name	Type	Data
(Default)	REG_SZ	SpUncompressedLexicon Class

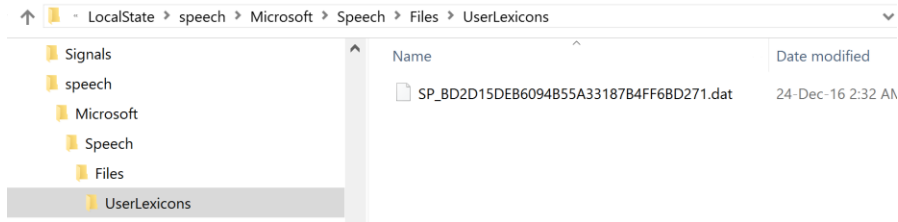
and has a value of:

Value name	Datafile
Value type	RegUnknown
Stack	20-00
Value	50-FF-FF-FF-25-00-31-00-61-00-25-00-5C-00-4D-00-69-00-63-00-72-00-6F-00-73-00-6F-00-66-00-74-00-5C-00-53-00-70-00-65-00-65-00-63-00-68-00-5C-00-46-00-69-00-6C-00-65-00-73-00-5C-00-55-00-73-00-65-00-72-00-4C-00-65-00-78-00-69-00-63-00-6F-00-6E-00-73-00-5C-00-53-00-50-00-5F-00-42-00-44-00-32-00-44-00-31-00-35-00-44-00-45-00-42-00-36-00-30-00-39-00-34-00-42-00-35-00-35-00-41-00-33-00-33-00-31-00-38-00-37-00-42-00-34-00-46-00-46-00-36-00-42-00-44-00-32-00-37-00-31-00-2E-00-64-00-61-00-74-00-00-00-E6-AC-A5-2E-7D-5D-D2-01-20-00

"\Microsoft\Speech\Files\UserLexicons\SP_BD2D15DEB6094B55A33187B4FF6BD271.dat"

Accordingly, the user speech lexicon can be found at:

"%user%\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\speech\Microsoft\Speech\Files\UserLexicons"



Looking at the DatabaseAndObjectStoreCatalog table of IndexedDB.dat, we see the application containerID "S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-2659745135-2630312742"

logicalDatabaseId	idDifferentiator	isObjectStore	versionNumber	lastOpenTimestamp	pseudoPrimaryIndexId	applicationContainerId
1002	4	255	303828725919...	30-Dec-99 12:00:0...	3	
1002	3	42	2	22-Dec-17 1:02:31 ...		S-1-15-2-1861897761-1695161497-2927542615-...
1005	8	255	303828725919...	30-Dec-99 12:00:0...	6	
1005	7	42	05-May-29 11:50:03 PM	20-Feb-18 5:57:18 ...		S-1-15-2-1861897761-1695161497-2927542615-...

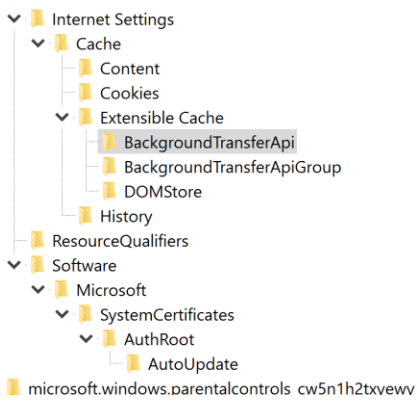
Property	Value
logicalDatabaseId:	1005
idDifferentiator:	7
isObjectStore:	42
versionNumber:	05-May-29 11:50:03 PM
lastOpenTimestamp:	20-Feb-18 5:57:18 PM
pseudoPrimaryIndexId:	
applicationContainerId:	S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-
domainName:	05-May-29 11:50:03 PM
siteOrigin:	68 74 74 70 73 3A 77 77 77 2E 62 69 6E 67 2E 63 6F 6D 04 00 00 61
logicalDatabaseName:	mruWithIndex
friendlyObjectStoreName:	

This corresponds to the current version of Cortana as seen at

"\SOFTWARE\Microsoft\SecurityManager\CapAuthz\ApplicationsEx\Microsoft.Windows.Cortana_1.7.0.14393_neutral_neutral_cw5n1h2txyewy"

Microsoft.Windows.Apprep.ChxApp_1000.14393.2068.0_neutral_neutral_cw5n1h2txyewy	CapSids	REG_BINARY	16 00 00 00 01 0a 00 00 00 00 0f 03 00 00 00 00
Microsoft.Windows.AssignedAccessLockApp_1000.14393.2068.0_neutral_neutral_cw5n1h2txyewy	DeviceCapSids	REG_BINARY	0a 00 00 00 01 05 00 00 00 00 0f 03 00 00 00 00
Microsoft.Windows.CloudExperienceHost_10.0.14393.0_neutral_neutral_cw5n1h2txyewy	EnterpriseID	REG_DWORD	0x00000000 (0)
Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neutral_cw5n1h2txyewy	PackageSid	REG_SZ	S-1-15-2-1861897761-1695161497-2927542615-
Microsoft.Windows.ContentDeliveryManager_10.0.14393.0_neutral_neutral_cw5n1h2txyewy			
Microsoft.Windows.Cortana_1.7.0.14393_neutral_neutral_cw5n1h2txyewy			
Microsoft.Windows.ParentalControls_1000.14393.0.0_neutral_neutral_cw5n1h2txyewy			
Microsoft.Windows.ParentalControls_1000.14393.2068.0_neutral_neutral_cw5n1h2txyewy			

\USER_GUID\SOFTWARE\Classes\Local
 Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\Internet Settings\Cache\Extensible Cache



CacheLimit	REG_DWORD	0x000000
CacheOptions	REG_DWORD	0x000000
CachePath	REG_SZ	C:\Users\...
CachePrefix	REG_SZ	:Backgrou...
CacheRelativePath	REG_SZ	INetHisto...
CacheRepair	REG_DWORD	0x000000

Value name:

Value data:

OK Cancel

Cache locations:

Background Transfer API: "\\AC\INetHistory\BackgroundTransferApi"
 BackgroundTransferApiGroup: "\\AC\INetHistory\BackgroundTransferApiGroup"
 DOMStore: "\\AC\Microsoft\Internet Explorer\DOMStore"

