Exploring macOS with APOLLO

Sarah Edwards | @iamevltwin | mac4n6.com

for518.com | sarah@blackbagtech.com

Missed OBTS v1.0? No worries!

Apple Pattern of Life Lazy Output'er

- github.com/mac4n6/APOLLO

One lazy python script to run many SQL queries on many databases

Module Based w/ a Python script

- Database Filename
- SQL Query
- Correlation Timestamp

Current Stats:

- 165 Modules
- With macOS support, probably well over 200!

What’s New?

Python3

KMZ Location Output

Many, many, many more iOS modules

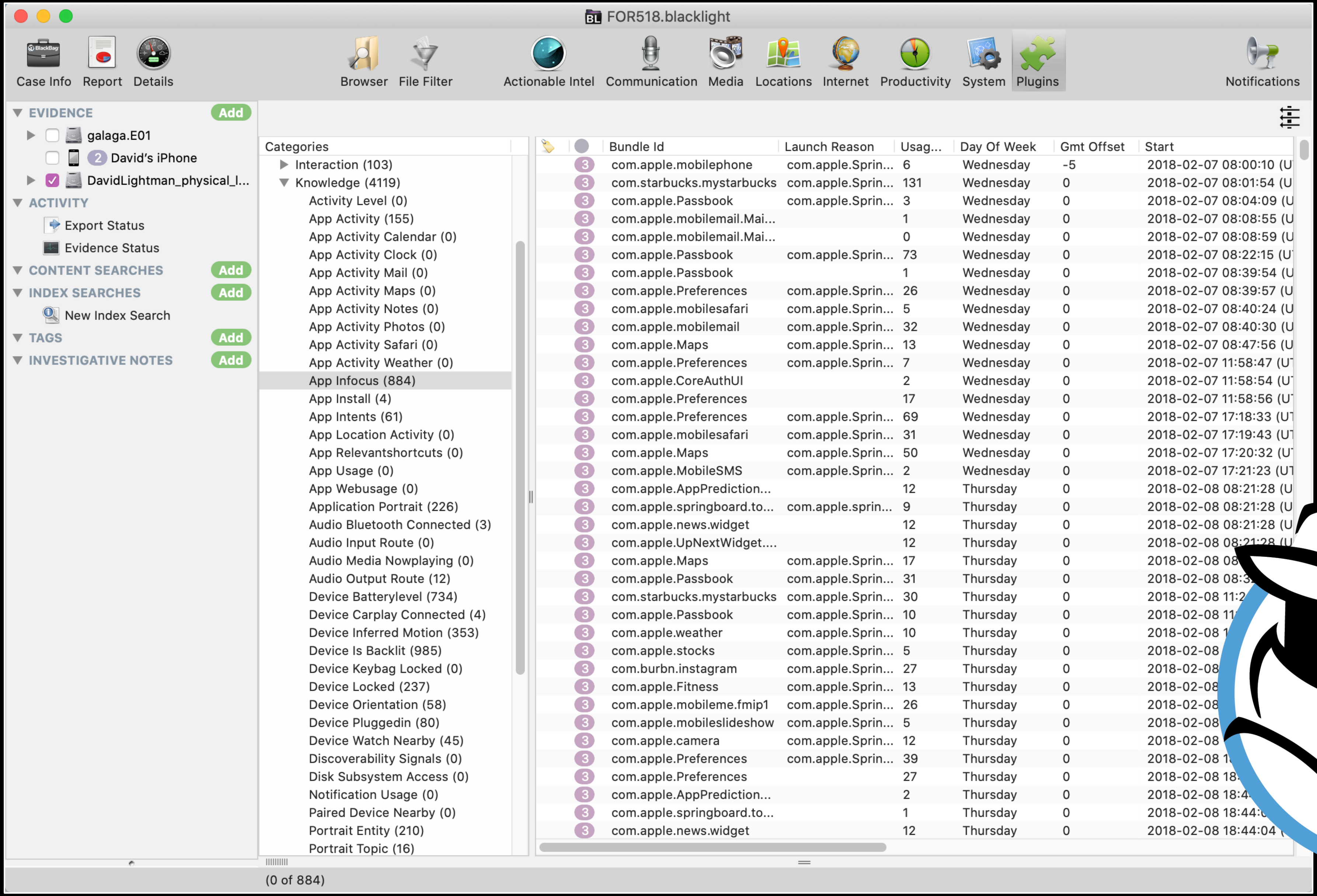
Android Support (ARTEMIS, now supported by iLEAPP)

- github.com/abrignoni/iLEAPP
- github.com/abrignoni/ALEAPP

Commercial Tool Support

…and of course official Mac Support (very, very soon)!

BlackBag BlackLight (blackbagtech.com)



Categories
- Interaction (103)
- Knowledge (4119)
  - Activity Level (0)
  - App Activity (155)
  - App Activity Calendar (0)
  - App Activity Clock (0)
  - App Activity Mail (0)
  - App Activity Maps (0)
  - App Activity Notes (0)
  - App Activity Photos (0)
  - App Activity Safari (0)
  - App Activity Weather (0)
  - App Infocus (884)
  - App Install (4)
  - App Intents (61)
  - App Location Activity (0)
  - App Relevantshortcuts (0)
  - App Usage (0)
  - App Webusage (0)
  - Application Portrait (226)
  - Audio Bluetooth Connected (3)
  - Audio Input Route (0)
  - Audio Media Nowplaying (0)
  - Audio Output Route (12)
  - Device Batterylevel (734)
  - Device Carplay Connected (4)
  - Device Inferred Motion (353)
  - Device Is Backlit (985)
  - Device Keybag Locked (0)
  - Device Locked (237)
  - Device Orientation (58)
  - Device Pluggedin (80)
  - Device Watch Nearby (45)
  - Discoverability Signals (0)
  - Disk Subsystem Access (0)
  - Notification Usage (0)
  - Paired Device Nearby (0)
  - Portrait Entity (210)
  - Portrait Topic (16)

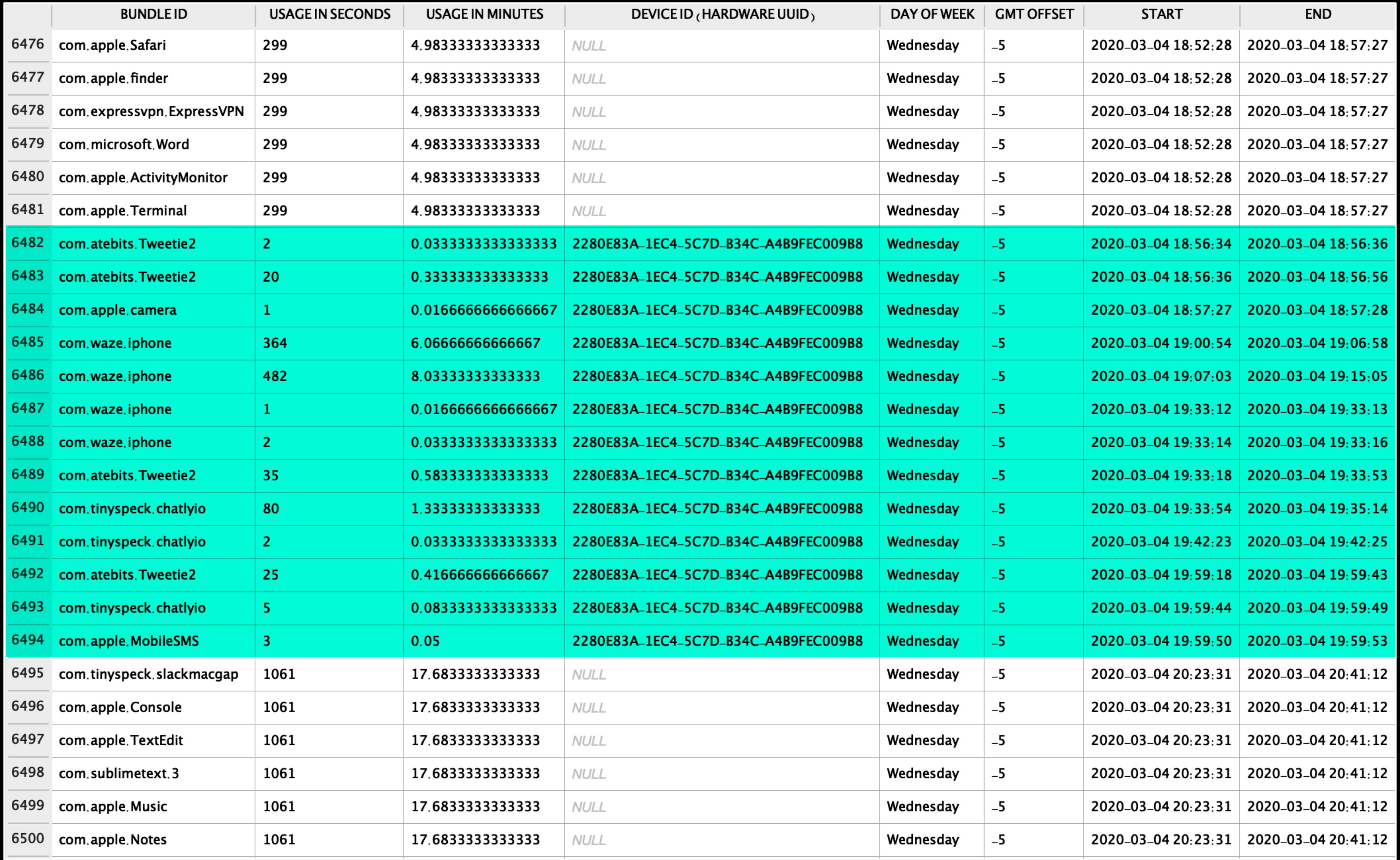
		Bundle Id	Launch Reason	Usag...	Day Of Week	Gmt Offset	Start
	3	com.apple.mobilephone	com.apple.Sprin...	6	Wednesday	-5	2018-02-07 08:00:10 (U
	3	com.starbucks.mystarbucks	com.apple.Sprin...	131	Wednesday	0	2018-02-07 08:01:54 (U
	3	com.apple.Passbook	com.apple.Sprin...	3	Wednesday	0	2018-02-07 08:04:09 (U
	3	com.apple.mobilemail.Mai...		1	Wednesday	0	2018-02-07 08:08:55 (U
	3	com.apple.mobilemail.Mai...		0	Wednesday	0	2018-02-07 08:08:59 (U
	3	com.apple.Passbook	com.apple.Sprin...	73	Wednesday	0	2018-02-07 08:22:15 (U
	3	com.apple.Passbook		1	Wednesday	0	2018-02-07 08:39:54 (U
	3	com.apple.Preferences	com.apple.Sprin...	26	Wednesday	0	2018-02-07 08:39:57 (U
	3	com.apple.mobilesafari	com.apple.Sprin...	5	Wednesday	0	2018-02-07 08:40:24 (U
	3	com.apple.mobilemail	com.apple.Sprin...	32	Wednesday	0	2018-02-07 08:40:30 (U
	3	com.apple.Maps	com.apple.Sprin...	13	Wednesday	0	2018-02-07 08:47:56 (U
	3	com.apple.Preferences	com.apple.Sprin...	7	Wednesday	0	2018-02-07 11:58:47 (UT
	3	com.apple.CoreAuthUI		2	Wednesday	0	2018-02-07 11:58:54 (UT
	3	com.apple.Preferences		17	Wednesday	0	2018-02-07 11:58:56 (UT
	3	com.apple.Preferences	com.apple.Sprin...	69	Wednesday	0	2018-02-07 17:18:33 (UT
	3	com.apple.mobilesafari	com.apple.Sprin...	31	Wednesday	0	2018-02-07 17:19:43 (UT
	3	com.apple.Maps	com.apple.Sprin...	50	Wednesday	0	2018-02-07 17:20:32 (UT
	3	com.apple.MobileSMS	com.apple.Sprin...	2	Wednesday	0	2018-02-07 17:21:23 (UT
	3	com.apple.AppPrediction...		12	Thursday	0	2018-02-08 08:21:28 (U
	3	com.apple.springboard.to...	com.apple.sprin...	9	Thursday	0	2018-02-08 08:21:28 (U
	3	com.apple.news.widget		12	Thursday	0	2018-02-08 08:21:28 (U
	3	com.apple.UpNextWidget....		12	Thursday	0	2018-02-08 08:21:28 (U
	3	com.apple.Maps	com.apple.Sprin...	17	Thursday	0	2018-02-08 08
	3	com.apple.Passbook	com.apple.Sprin...	31	Thursday	0	2018-02-08 08:3
	3	com.starbucks.mystarbucks	com.apple.Sprin...	30	Thursday	0	2018-02-08 11:2
	3	com.apple.Passbook	com.apple.Sprin...	10	Thursday	0	2018-02-08 11
	3	com.apple.weather	com.apple.Sprin...	10	Thursday	0	2018-02-08 1
	3	com.apple.stocks	com.apple.Sprin...	5	Thursday	0	2018-02-08
	3	com.burbn.instagram	com.apple.Sprin...	27	Thursday	0	2018-02-08
	3	com.apple.Fitness	com.apple.Sprin...	13	Thursday	0	2018-02-08
	3	com.apple.mobileme.fmip1	com.apple.Sprin...	26	Thursday	0	2018-02-08
	3	com.apple.mobileslideshow	com.apple.Sprin...	5	Thursday	0	2018-02-08
	3	com.apple.camera	com.apple.Sprin...	12	Thursday	0	2018-02-08
	3	com.apple.Preferences	com.apple.Sprin...	39	Thursday	0	2018-02-08 1
	3	com.apple.Preferences		27	Thursday	0	2018-02-08 18:
	3	com.apple.AppPrediction...		2	Thursday	0	2018-02-08 18:4
	3	com.apple.springboard.to...		1	Thursday	0	2018-02-08 18:44:0
	3	com.apple.news.widget		12	Thursday	0	2018-02-08 18:44:04 (

(0 of 884)

So many new modules, where to start?

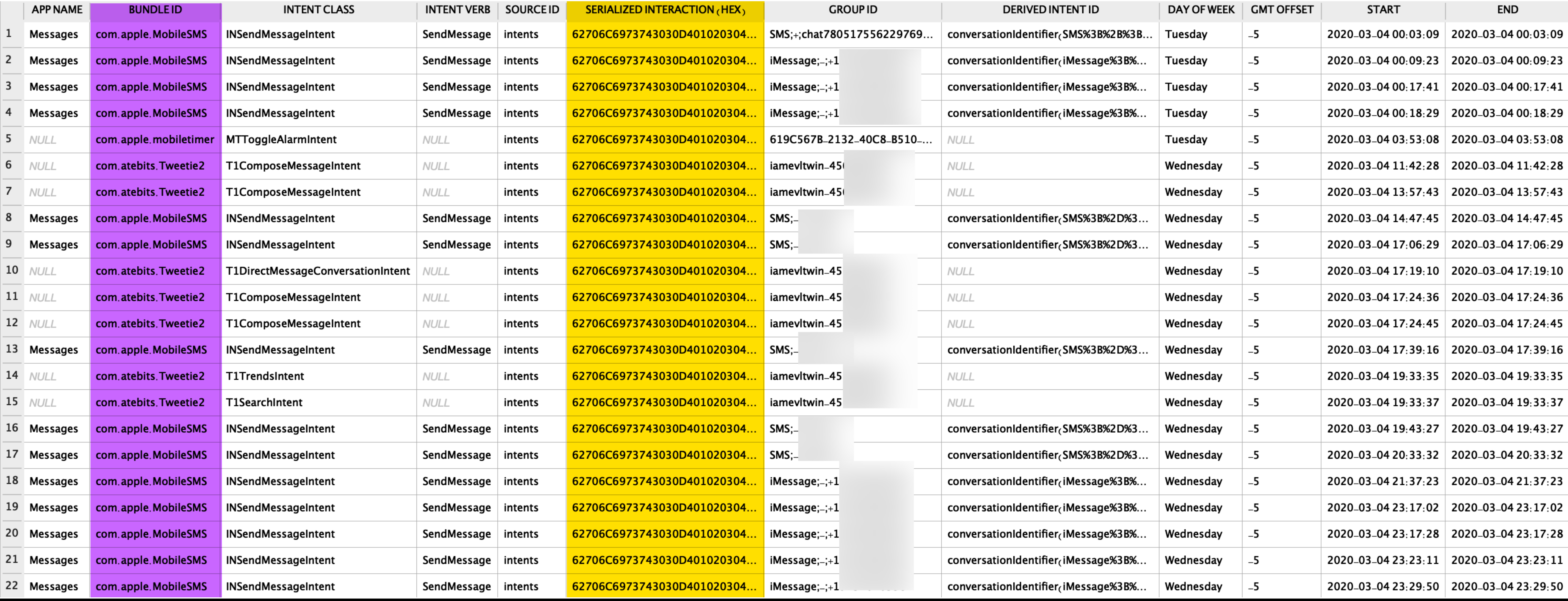
- KnowledgeC
- Net Usage
- InterationsC
- Notifications
- Powerlog
- TCC
- Launch Services Quarantine
- ExecPolicy/KextPolicy

knowledgeC.db – Application Usage



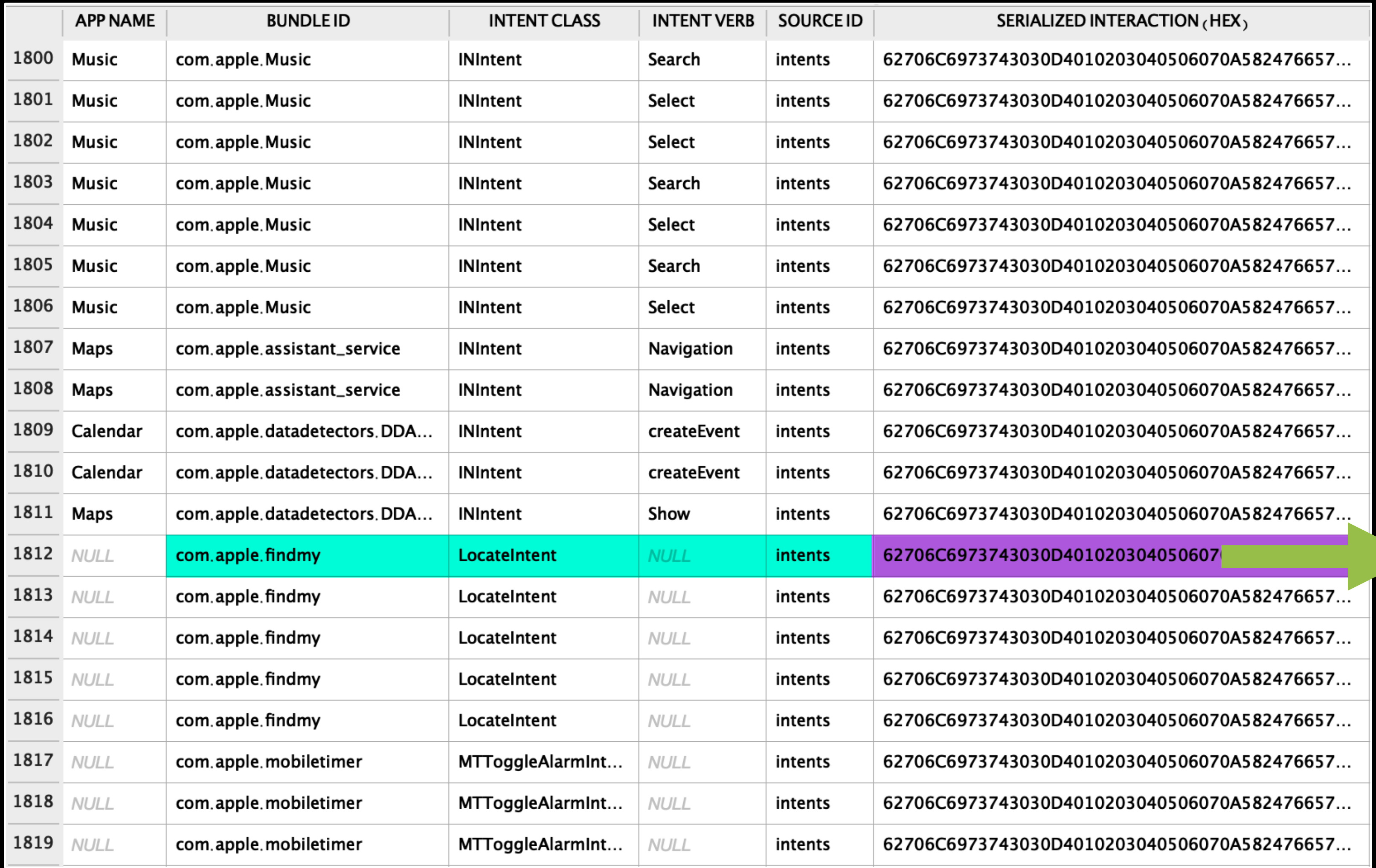
	BUNDLE ID	USAGE IN SECONDS	USAGE IN MINUTES	DEVICE ID (HARDWARE UUID)	DAY OF WEEK	GMT OFFSET	START	END
6476	com.apple.Safari	299	4.98333333333333	NULL	Wednesday	-5	2020-03-04 18:52:28	2020-03-04 18:57:27
6477	com.apple.finder	299	4.98333333333333	NULL	Wednesday	-5	2020-03-04 18:52:28	2020-03-04 18:57:27
6478	com.expressvpn.ExpressVPN	299	4.98333333333333	NULL	Wednesday	-5	2020-03-04 18:52:28	2020-03-04 18:57:27
6479	com.microsoft.Word	299	4.98333333333333	NULL	Wednesday	-5	2020-03-04 18:52:28	2020-03-04 18:57:27
6480	com.apple.ActivityMonitor	299	4.98333333333333	NULL	Wednesday	-5	2020-03-04 18:52:28	2020-03-04 18:57:27
6481	com.apple.Terminal	299	4.98333333333333	NULL	Wednesday	-5	2020-03-04 18:52:28	2020-03-04 18:57:27
6482	com.atebits.Tweetie2	2	0.0333333333333333	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	Wednesday	-5	2020-03-04 18:56:34	2020-03-04 18:56:36
6483	com.atebits.Tweetie2	20	0.333333333333333	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	Wednesday	-5	2020-03-04 18:56:36	2020-03-04 18:56:56
6484	com.apple.camera	1	0.0166666666666667	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	Wednesday	-5	2020-03-04 18:57:27	2020-03-04 18:57:28
6485	com.waze.iphone	364	6.06666666666667	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	Wednesday	-5	2020-03-04 19:00:54	2020-03-04 19:06:58
6486	com.waze.iphone	482	8.03333333333333	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	Wednesday	-5	2020-03-04 19:07:03	2020-03-04 19:15:05
6487	com.waze.iphone	1	0.0166666666666667	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	Wednesday	-5	2020-03-04 19:33:12	2020-03-04 19:33:13
6488	com.waze.iphone	2	0.0333333333333333	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	Wednesday	-5	2020-03-04 19:33:14	2020-03-04 19:33:16
6489	com.atebits.Tweetie2	35	0.583333333333333	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	Wednesday	-5	2020-03-04 19:33:18	2020-03-04 19:33:53
6490	com.tinyspeck.chatlyio	80	1.33333333333333	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	Wednesday	-5	2020-03-04 19:33:54	2020-03-04 19:35:14
6491	com.tinyspeck.chatlyio	2	0.0333333333333333	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	Wednesday	-5	2020-03-04 19:42:23	2020-03-04 19:42:25
6492	com.atebits.Tweetie2	25	0.416666666666667	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	Wednesday	-5	2020-03-04 19:59:18	2020-03-04 19:59:43
6493	com.tinyspeck.chatlyio	5	0.0833333333333333	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	Wednesday	-5	2020-03-04 19:59:44	2020-03-04 19:59:49
6494	com.apple.MobileSMS	3	0.05	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	Wednesday	-5	2020-03-04 19:59:50	2020-03-04 19:59:53
6495	com.tinyspeck.slackmacgap	1061	17.6833333333333	NULL	Wednesday	-5	2020-03-04 20:23:31	2020-03-04 20:41:12
6496	com.apple.Console	1061	17.6833333333333	NULL	Wednesday	-5	2020-03-04 20:23:31	2020-03-04 20:41:12
6497	com.apple.TextEdit	1061	17.6833333333333	NULL	Wednesday	-5	2020-03-04 20:23:31	2020-03-04 20:41:12
6498	com.sublimetext.3	1061	17.6833333333333	NULL	Wednesday	-5	2020-03-04 20:23:31	2020-03-04 20:41:12
6499	com.apple.Music	1061	17.6833333333333	NULL	Wednesday	-5	2020-03-04 20:23:31	2020-03-04 20:41:12
6500	com.apple.Notes	1061	17.6833333333333	NULL	Wednesday	-5	2020-03-04 20:23:31	2020-03-04 20:41:12

knowledgeC.db – Application Intents

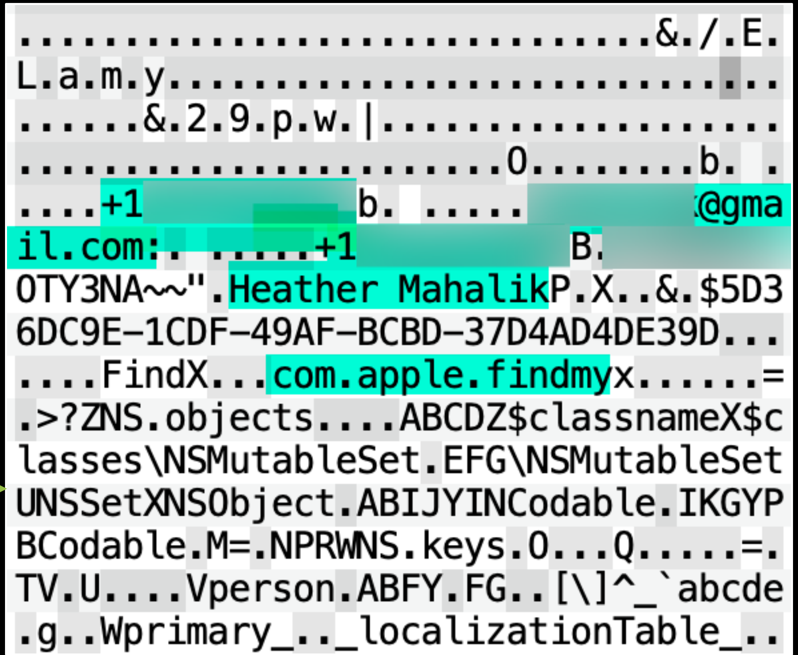


	APP NAME	BUNDLE ID	INTENT CLASS	INTENT VERB	SOURCE ID	SERIALIZED INTERACTION (HEX)	GROUP ID	DERIVED INTENT ID	DAY OF WEEK	GMT OFFSET	START	END
1	Messages	com.apple.MobileSMS	INSendMessageIntent	SendMessage	intents	62706C6973743030D401020304...	SMS;+;chat780517556229769...	conversationIdentifier(SMS%3B%2B%3B...	Tuesday	-5	2020-03-04 00:03:09	2020-03-04 00:03:09
2	Messages	com.apple.MobileSMS	INSendMessageIntent	SendMessage	intents	62706C6973743030D401020304...	iMessage;-;+1 [redacted]	conversationIdentifier(iMessage%3B%...	Tuesday	-5	2020-03-04 00:09:23	2020-03-04 00:09:23
3	Messages	com.apple.MobileSMS	INSendMessageIntent	SendMessage	intents	62706C6973743030D401020304...	iMessage;-;+1 [redacted]	conversationIdentifier(iMessage%3B%...	Tuesday	-5	2020-03-04 00:17:41	2020-03-04 00:17:41
4	Messages	com.apple.MobileSMS	INSendMessageIntent	SendMessage	intents	62706C6973743030D401020304...	iMessage;-;+1 [redacted]	conversationIdentifier(iMessage%3B%...	Tuesday	-5	2020-03-04 00:18:29	2020-03-04 00:18:29
5	NULL	com.apple.mobiletimer	MTToggleAlarmIntent	NULL	intents	62706C6973743030D401020304...	619C567B-2132-40C8-B510-...	NULL	Tuesday	-5	2020-03-04 03:53:08	2020-03-04 03:53:08
6	NULL	com.atebits.Tweetie2	T1ComposeMessageIntent	NULL	intents	62706C6973743030D401020304...	iamevltwin-45 [redacted]	NULL	Wednesday	-5	2020-03-04 11:42:28	2020-03-04 11:42:28
7	NULL	com.atebits.Tweetie2	T1ComposeMessageIntent	NULL	intents	62706C6973743030D401020304...	iamevltwin-45 [redacted]	NULL	Wednesday	-5	2020-03-04 13:57:43	2020-03-04 13:57:43
8	Messages	com.apple.MobileSMS	INSendMessageIntent	SendMessage	intents	62706C6973743030D401020304...	SMS;- [redacted]	conversationIdentifier(SMS%3B%2D%3...	Wednesday	-5	2020-03-04 14:47:45	2020-03-04 14:47:45
9	Messages	com.apple.MobileSMS	INSendMessageIntent	SendMessage	intents	62706C6973743030D401020304...	SMS;- [redacted]	conversationIdentifier(SMS%3B%2D%3...	Wednesday	-5	2020-03-04 17:06:29	2020-03-04 17:06:29
10	NULL	com.atebits.Tweetie2	T1DirectMessageConversationIntent	NULL	intents	62706C6973743030D401020304...	iamevltwin-45 [redacted]	NULL	Wednesday	-5	2020-03-04 17:19:10	2020-03-04 17:19:10
11	NULL	com.atebits.Tweetie2	T1ComposeMessageIntent	NULL	intents	62706C6973743030D401020304...	iamevltwin-45 [redacted]	NULL	Wednesday	-5	2020-03-04 17:24:36	2020-03-04 17:24:36
12	NULL	com.atebits.Tweetie2	T1ComposeMessageIntent	NULL	intents	62706C6973743030D401020304...	iamevltwin-45 [redacted]	NULL	Wednesday	-5	2020-03-04 17:24:45	2020-03-04 17:24:45
13	Messages	com.apple.MobileSMS	INSendMessageIntent	SendMessage	intents	62706C6973743030D401020304...	SMS;- [redacted]	conversationIdentifier(SMS%3B%2D%3...	Wednesday	-5	2020-03-04 17:39:16	2020-03-04 17:39:16
14	NULL	com.atebits.Tweetie2	T1TrendsIntent	NULL	intents	62706C6973743030D401020304...	iamevltwin-45 [redacted]	NULL	Wednesday	-5	2020-03-04 19:33:35	2020-03-04 19:33:35
15	NULL	com.atebits.Tweetie2	T1SearchIntent	NULL	intents	62706C6973743030D401020304...	iamevltwin-45 [redacted]	NULL	Wednesday	-5	2020-03-04 19:33:37	2020-03-04 19:33:37
16	Messages	com.apple.MobileSMS	INSendMessageIntent	SendMessage	intents	62706C6973743030D401020304...	SMS;- [redacted]	conversationIdentifier(SMS%3B%2D%3...	Wednesday	-5	2020-03-04 19:43:27	2020-03-04 19:43:27
17	Messages	com.apple.MobileSMS	INSendMessageIntent	SendMessage	intents	62706C6973743030D401020304...	SMS;- [redacted]	conversationIdentifier(SMS%3B%2D%3...	Wednesday	-5	2020-03-04 20:33:32	2020-03-04 20:33:32
18	Messages	com.apple.MobileSMS	INSendMessageIntent	SendMessage	intents	62706C6973743030D401020304...	iMessage;-;+1 [redacted]	conversationIdentifier(iMessage%3B%...	Wednesday	-5	2020-03-04 21:37:23	2020-03-04 21:37:23
19	Messages	com.apple.MobileSMS	INSendMessageIntent	SendMessage	intents	62706C6973743030D401020304...	iMessage;-;+1 [redacted]	conversationIdentifier(iMessage%3B%...	Wednesday	-5	2020-03-04 23:17:02	2020-03-04 23:17:02
20	Messages	com.apple.MobileSMS	INSendMessageIntent	SendMessage	intents	62706C6973743030D401020304...	iMessage;-;+1 [redacted]	conversationIdentifier(iMessage%3B%...	Wednesday	-5	2020-03-04 23:17:28	2020-03-04 23:17:28
21	Messages	com.apple.MobileSMS	INSendMessageIntent	SendMessage	intents	62706C6973743030D401020304...	iMessage;-;+1 [redacted]	conversationIdentifier(iMessage%3B%...	Wednesday	-5	2020-03-04 23:23:11	2020-03-04 23:23:11
22	Messages	com.apple.MobileSMS	INSendMessageIntent	SendMessage	intents	62706C6973743030D401020304...	iMessage;-;+1 [redacted]	conversationIdentifier(iMessage%3B%...	Wednesday	-5	2020-03-04 23:29:50	2020-03-04 23:29:50

knowledgeC.db – Application Intents

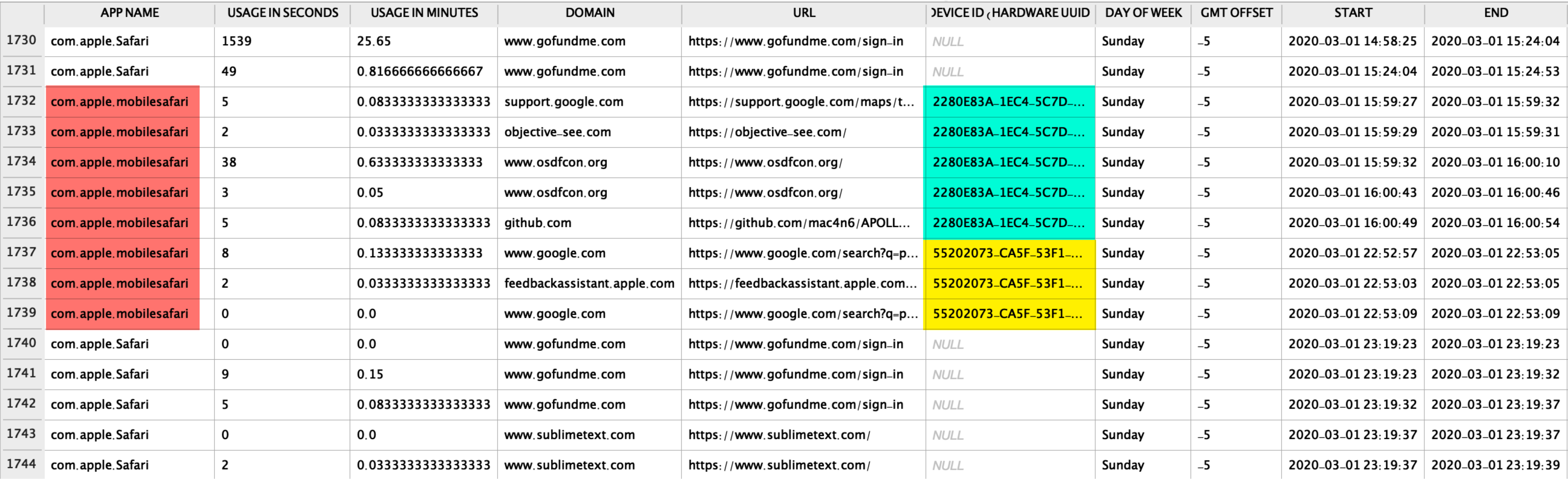


	APP NAME	BUNDLE ID	INTENT CLASS	INTENT VERB	SOURCE ID	SERIALIZED INTERACTION (HEX)
1800	Music	com.apple.Music	INIntent	Search	intents	62706C6973743030D401020304050607 0A582476657...
1801	Music	com.apple.Music	INIntent	Select	intents	62706C6973743030D4010203040506070A582476657...
1802	Music	com.apple.Music	INIntent	Select	intents	62706C6973743030D4010203040506070A582476657...
1803	Music	com.apple.Music	INIntent	Search	intents	62706C6973743030D4010203040506070A582476657...
1804	Music	com.apple.Music	INIntent	Select	intents	62706C6973743030D4010203040506070A582476657...
1805	Music	com.apple.Music	INIntent	Search	intents	62706C6973743030D4010203040506070A582476657...
1806	Music	com.apple.Music	INIntent	Select	intents	62706C6973743030D4010203040506070A582476657...
1807	Maps	com.apple.assistant_service	INIntent	Navigation	intents	62706C6973743030D4010203040506070A582476657...
1808	Maps	com.apple.assistant_service	INIntent	Navigation	intents	62706C6973743030D4010203040506070A582476657...
1809	Calendar	com.apple.datadetectors.DDA...	INIntent	createEvent	intents	62706C6973743030D4010203040506070A582476657...
1810	Calendar	com.apple.datadetectors.DDA...	INIntent	createEvent	intents	62706C6973743030D4010203040506070A582476657...
1811	Maps	com.apple.datadetectors.DDA...	INIntent	Show	intents	62706C6973743030D4010203040506070A582476657...
1812	NULL	com.apple.findmy	LocateIntent	NULL	intents	62706C6973743030D40102030405060 7
1813	NULL	com.apple.findmy	LocateIntent	NULL	intents	62706C6973743030D4010203040506070A582476657...
1814	NULL	com.apple.findmy	LocateIntent	NULL	intents	62706C6973743030D4010203040506070A582476657...
1815	NULL	com.apple.findmy	LocateIntent	NULL	intents	62706C6973743030D4010203040506070A582476657...
1816	NULL	com.apple.findmy	LocateIntent	NULL	intents	62706C6973743030D4010203040506070A582476657...
1817	NULL	com.apple.mobiletimer	MTToggleAlarmInt...	NULL	intents	62706C6973743030D4010203040506070A582476657...
1818	NULL	com.apple.mobiletimer	MTToggleAlarmInt...	NULL	intents	62706C6973743030D4010203040506070A582476657...
1819	NULL	com.apple.mobiletimer	MTToggleAlarmInt...	NULL	intents	62706C6973743030D4010203040506070A582476657...



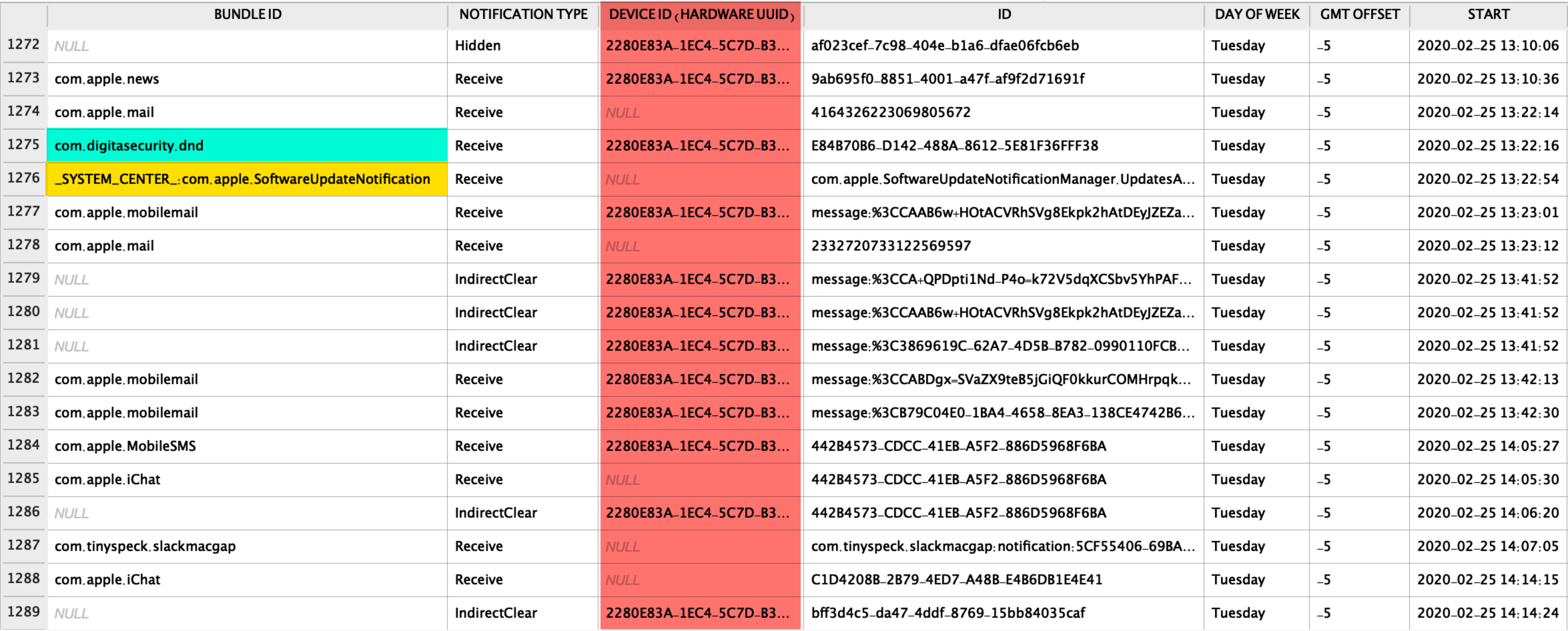
```
..............................&./.E.
L.a.m.y.............................
......&.2.9.p.w.|...................
......................O.........b. .
....+1[redacted]b. .....[redacted]@gma
il.com:[redacted]+1[redacted]B.[redacted]
OTY3NA~~".Heather MahalikP.X..&.$5D3
6DC9E-1CDF-49AF-BCBD-37D4AD4DE39D...
....FindX...com.apple.findmyx......=
.>?ZNS.objects....ABCDZ$classnameX$c
lasses\NSMutableSet.EFG\NSMutableSet
UNSSetXNSObject.ABIJYINCodable.IKGYP
BCodable.M=.NPRWNS.keys.O...Q.....=.
TV.U....Vperson.ABFY.FG..[\]^_`abcde
.g..Wprimary_.._localizationTable_..
```

knowledgeC.db – Safari Web Browsing



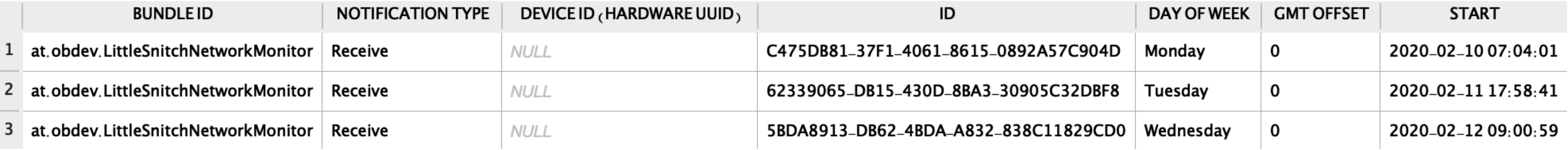
	APP NAME	USAGE IN SECONDS	USAGE IN MINUTES	DOMAIN	URL	DEVICE ID (HARDWARE UUID	DAY OF WEEK	GMT OFFSET	START	END
1730	com.apple.Safari	1539	25.65	www.gofundme.com	https://www.gofundme.com/sign-in	NULL	Sunday	-5	2020-03-01 14:58:25	2020-03-01 15:24:04
1731	com.apple.Safari	49	0.816666666666667	www.gofundme.com	https://www.gofundme.com/sign-in	NULL	Sunday	-5	2020-03-01 15:24:04	2020-03-01 15:24:53
1732	com.apple.mobilesafari	5	0.0833333333333333	support.google.com	https://support.google.com/maps/t...	2280E83A-1EC4-5C7D-...	Sunday	-5	2020-03-01 15:59:27	2020-03-01 15:59:32
1733	com.apple.mobilesafari	2	0.0333333333333333	objective-see.com	https://objective-see.com/	2280E83A-1EC4-5C7D-...	Sunday	-5	2020-03-01 15:59:29	2020-03-01 15:59:31
1734	com.apple.mobilesafari	38	0.633333333333333	www.osdfcon.org	https://www.osdfcon.org/	2280E83A-1EC4-5C7D-...	Sunday	-5	2020-03-01 15:59:32	2020-03-01 16:00:10
1735	com.apple.mobilesafari	3	0.05	www.osdfcon.org	https://www.osdfcon.org/	2280E83A-1EC4-5C7D-...	Sunday	-5	2020-03-01 16:00:43	2020-03-01 16:00:46
1736	com.apple.mobilesafari	5	0.0833333333333333	github.com	https://github.com/mac4n6/APOLL...	2280E83A-1EC4-5C7D-...	Sunday	-5	2020-03-01 16:00:49	2020-03-01 16:00:54
1737	com.apple.mobilesafari	8	0.133333333333333	www.google.com	https://www.google.com/search?q=p...	55202073-CA5F-53F1-...	Sunday	-5	2020-03-01 22:52:57	2020-03-01 22:53:05
1738	com.apple.mobilesafari	2	0.0333333333333333	feedbackassistant.apple.com	https://feedbackassistant.apple.com...	55202073-CA5F-53F1-...	Sunday	-5	2020-03-01 22:53:03	2020-03-01 22:53:05
1739	com.apple.mobilesafari	0	0.0	www.google.com	https://www.google.com/search?q=p...	55202073-CA5F-53F1-...	Sunday	-5	2020-03-01 22:53:09	2020-03-01 22:53:09
1740	com.apple.Safari	0	0.0	www.gofundme.com	https://www.gofundme.com/sign-in	NULL	Sunday	-5	2020-03-01 23:19:23	2020-03-01 23:19:23
1741	com.apple.Safari	9	0.15	www.gofundme.com	https://www.gofundme.com/sign-in	NULL	Sunday	-5	2020-03-01 23:19:23	2020-03-01 23:19:32
1742	com.apple.Safari	5	0.0833333333333333	www.gofundme.com	https://www.gofundme.com/sign-in	NULL	Sunday	-5	2020-03-01 23:19:32	2020-03-01 23:19:37
1743	com.apple.Safari	0	0.0	www.sublimetext.com	https://www.sublimetext.com/	NULL	Sunday	-5	2020-03-01 23:19:37	2020-03-01 23:19:37
1744	com.apple.Safari	2	0.0333333333333333	www.sublimetext.com	https://www.sublimetext.com/	NULL	Sunday	-5	2020-03-01 23:19:37	2020-03-01 23:19:39

knowledgeC.db – Application Notifications

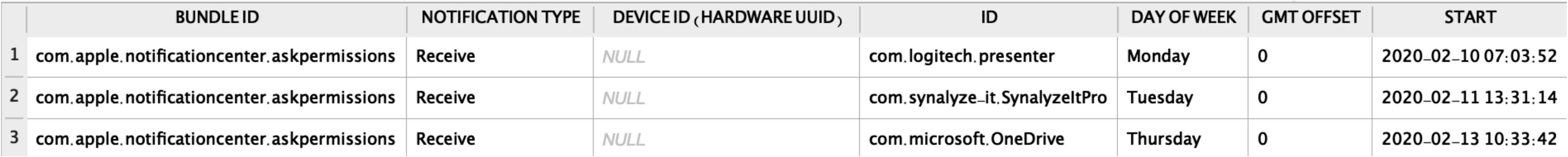


	BUNDLE ID	NOTIFICATION TYPE	DEVICE ID (HARDWARE UUID)	ID	DAY OF WEEK	GMT OFFSET	START
1272	NULL	Hidden	2280E83A-1EC4-5C7D-B3...	af023cef-7c98-404e-b1a6-dfae06fcb6eb	Tuesday	-5	2020-02-25 13:10:06
1273	com.apple.news	Receive	2280E83A-1EC4-5C7D-B3...	9ab695f0-8851-4001-a47f-af9f2d71691f	Tuesday	-5	2020-02-25 13:10:36
1274	com.apple.mail	Receive	NULL	4164326223069805672	Tuesday	-5	2020-02-25 13:22:14
1275	com.digitasecurity.dnd	Receive	2280E83A-1EC4-5C7D-B3...	E84B70B6-D142-488A-8612-5E81F36FFF38	Tuesday	-5	2020-02-25 13:22:16
1276	_SYSTEM_CENTER_:com.apple.SoftwareUpdateNotification	Receive	NULL	com.apple.SoftwareUpdateNotificationManager.UpdatesA...	Tuesday	-5	2020-02-25 13:22:54
1277	com.apple.mobilemail	Receive	2280E83A-1EC4-5C7D-B3...	message:%3CCAAB6w+HOtACVRhSVg8Ekpk2hAtDEyJZEZa...	Tuesday	-5	2020-02-25 13:23:01
1278	com.apple.mail	Receive	NULL	2332720733122569597	Tuesday	-5	2020-02-25 13:23:12
1279	NULL	IndirectClear	2280E83A-1EC4-5C7D-B3...	message:%3CCA+QPDpti1Nd-P4o=k72V5dqXCSbv5YhPAF...	Tuesday	-5	2020-02-25 13:41:52
1280	NULL	IndirectClear	2280E83A-1EC4-5C7D-B3...	message:%3CCAAB6w+HOtACVRhSVg8Ekpk2hAtDEyJZEZa...	Tuesday	-5	2020-02-25 13:41:52
1281	NULL	IndirectClear	2280E83A-1EC4-5C7D-B3...	message:%3C3869619C-62A7-4D5B-B782-0990110FCB...	Tuesday	-5	2020-02-25 13:41:52
1282	com.apple.mobilemail	Receive	2280E83A-1EC4-5C7D-B3...	message:%3CCABDgx=SVaZX9teB5jGiQF0kkurCOMHrpqk...	Tuesday	-5	2020-02-25 13:42:13
1283	com.apple.mobilemail	Receive	2280E83A-1EC4-5C7D-B3...	message:%3CB79C04E0-1BA4-4658-8EA3-138CE4742B6...	Tuesday	-5	2020-02-25 13:42:30
1284	com.apple.MobileSMS	Receive	2280E83A-1EC4-5C7D-B3...	442B4573-CDCC-41EB-A5F2-886D5968F6BA	Tuesday	-5	2020-02-25 14:05:27
1285	com.apple.iChat	Receive	NULL	442B4573-CDCC-41EB-A5F2-886D5968F6BA	Tuesday	-5	2020-02-25 14:05:30
1286	NULL	IndirectClear	2280E83A-1EC4-5C7D-B3...	442B4573-CDCC-41EB-A5F2-886D5968F6BA	Tuesday	-5	2020-02-25 14:06:20
1287	com.tinyspeck.slackmacgap	Receive	NULL	com.tinyspeck.slackmacgap:notification:5CF55406-69BA...	Tuesday	-5	2020-02-25 14:07:05
1288	com.apple.iChat	Receive	NULL	C1D4208B-2B79-4ED7-A48B-E4B6DB1E4E41	Tuesday	-5	2020-02-25 14:14:15
1289	NULL	IndirectClear	2280E83A-1EC4-5C7D-B3...	bff3d4c5-da47-4ddf-8769-15bb84035caf	Tuesday	-5	2020-02-25 14:14:24

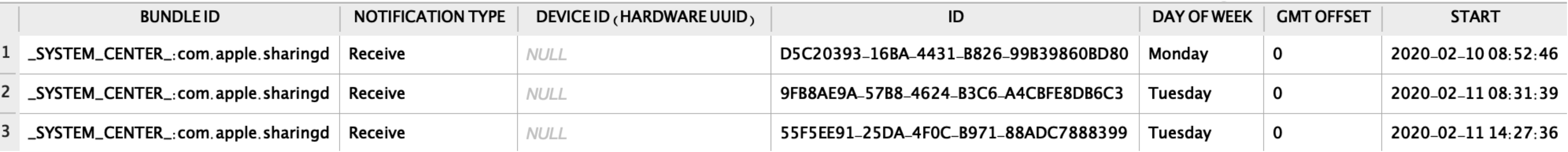
knowledgeC.db – Application Notifications



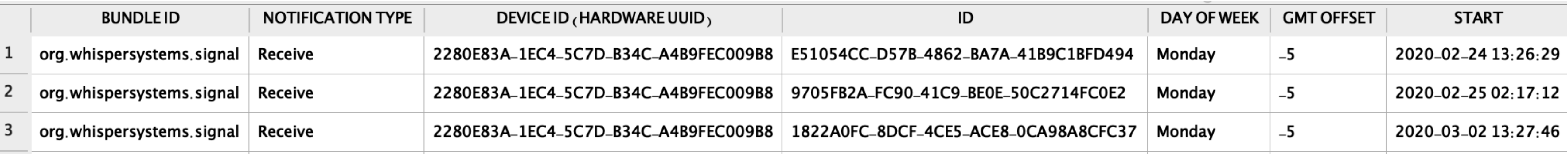
	BUNDLE ID	NOTIFICATION TYPE	DEVICE ID (HARDWARE UUID)	ID	DAY OF WEEK	GMT OFFSET	START
1	at.obdev.LittleSnitchNetworkMonitor	Receive	NULL	C475DB81-37F1-4061-8615-0892A57C904D	Monday	0	2020-02-10 07:04:01
2	at.obdev.LittleSnitchNetworkMonitor	Receive	NULL	62339065-DB15-430D-8BA3-30905C32DBF8	Tuesday	0	2020-02-11 17:58:41
3	at.obdev.LittleSnitchNetworkMonitor	Receive	NULL	5BDA8913-DB62-4BDA-A832-838C11829CD0	Wednesday	0	2020-02-12 09:00:59



	BUNDLE ID	NOTIFICATION TYPE	DEVICE ID (HARDWARE UUID)	ID	DAY OF WEEK	GMT OFFSET	START
1	com.apple.notificationcenter.askpermissions	Receive	NULL	com.logitech.presenter	Monday	0	2020-02-10 07:03:52
2	com.apple.notificationcenter.askpermissions	Receive	NULL	com.synalyze-it.SynalyzeItPro	Tuesday	0	2020-02-11 13:31:14
3	com.apple.notificationcenter.askpermissions	Receive	NULL	com.microsoft.OneDrive	Thursday	0	2020-02-13 10:33:42

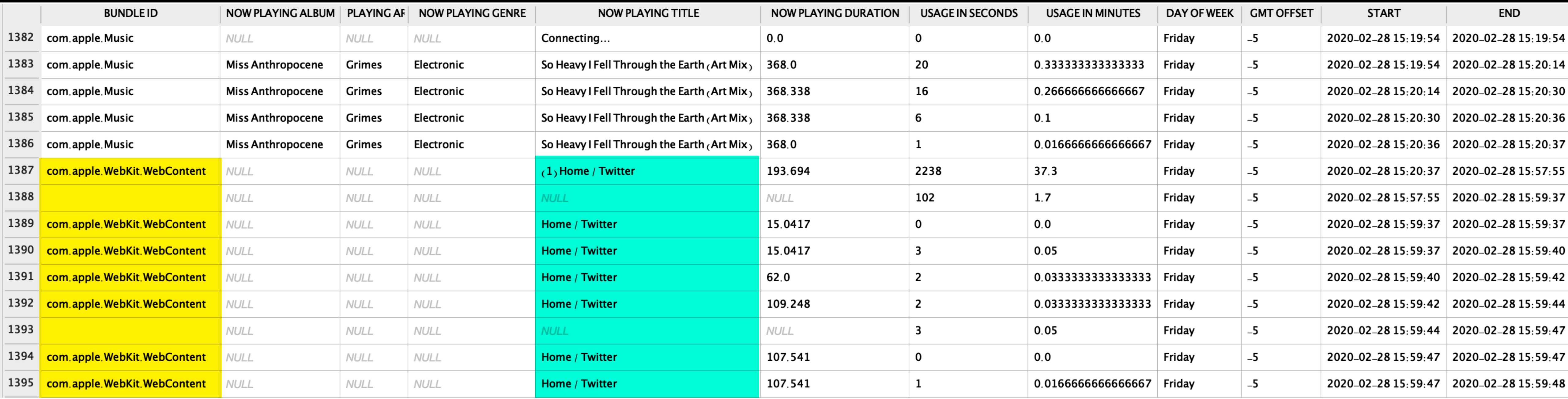


	BUNDLE ID	NOTIFICATION TYPE	DEVICE ID (HARDWARE UUID)	ID	DAY OF WEEK	GMT OFFSET	START
1	_SYSTEM_CENTER_:com.apple.sharingd	Receive	NULL	D5C20393-16BA-4431-B826-99B39860BD80	Monday	0	2020-02-10 08:52:46
2	_SYSTEM_CENTER_:com.apple.sharingd	Receive	NULL	9FB8AE9A-57B8-4624-B3C6-A4CBFE8DB6C3	Tuesday	0	2020-02-11 08:31:39
3	_SYSTEM_CENTER_:com.apple.sharingd	Receive	NULL	55F5EE91-25DA-4F0C-B971-88ADC7888399	Tuesday	0	2020-02-11 14:27:36



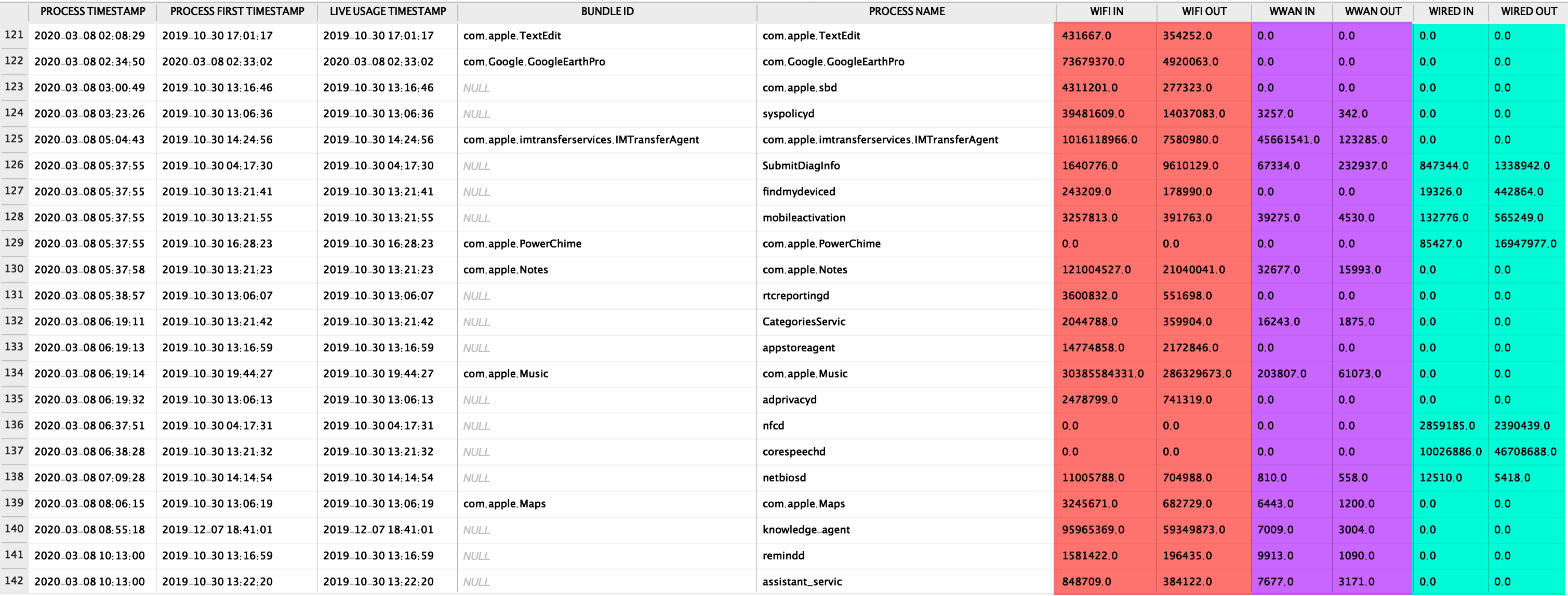
	BUNDLE ID	NOTIFICATION TYPE	DEVICE ID (HARDWARE UUID)	ID	DAY OF WEEK	GMT OFFSET	START
1	org.whispersystems.signal	Receive	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	E51054CC-D57B-4862-BA7A-41B9C1BFD494	Monday	-5	2020-02-24 13:26:29
2	org.whispersystems.signal	Receive	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	9705FB2A-FC90-41C9-BE0E-50C2714FC0E2	Monday	-5	2020-02-25 02:17:12
3	org.whispersystems.signal	Receive	2280E83A-1EC4-5C7D-B34C-A4B9FEC009B8	1822A0FC-8DCF-4CE5-ACE8-0CA98A8CFC37	Monday	-5	2020-03-02 13:27:46

knowledgeC.db – Now Playing



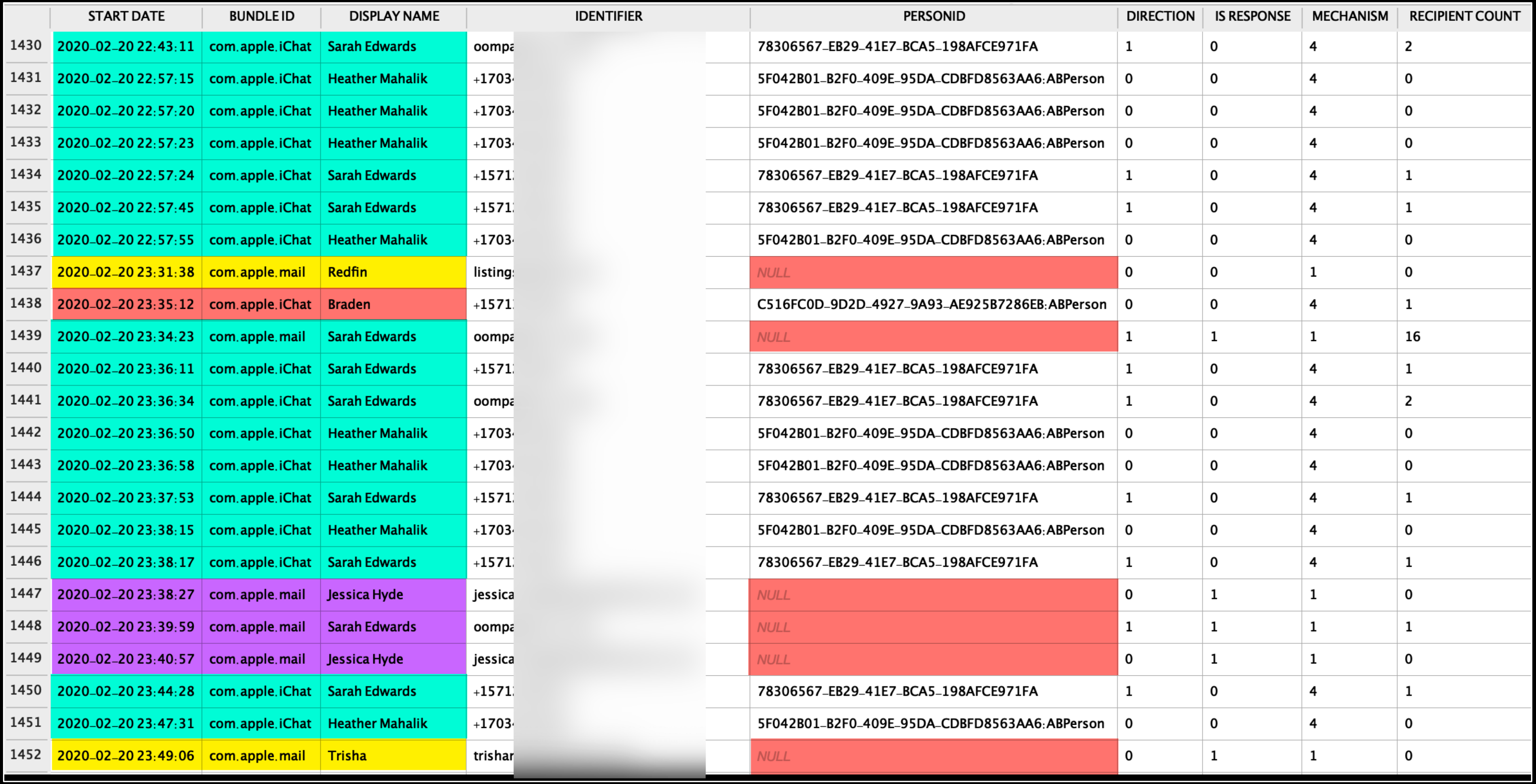
	BUNDLE ID	NOW PLAYING ALBUM	PLAYING AF	NOW PLAYING GENRE	NOW PLAYING TITLE	NOW PLAYING DURATION	USAGE IN SECONDS	USAGE IN MINUTES	DAY OF WEEK	GMT OFFSET	START	END
1382	com.apple.Music	NULL	NULL	NULL	Connecting...	0.0	0	0.0	Friday	-5	2020-02-28 15:19:54	2020-02-28 15:19:54
1383	com.apple.Music	Miss Anthropocene	Grimes	Electronic	So Heavy I Fell Through the Earth (Art Mix)	368.0	20	0.333333333333333	Friday	-5	2020-02-28 15:19:54	2020-02-28 15:20:14
1384	com.apple.Music	Miss Anthropocene	Grimes	Electronic	So Heavy I Fell Through the Earth (Art Mix)	368.338	16	0.266666666666667	Friday	-5	2020-02-28 15:20:14	2020-02-28 15:20:30
1385	com.apple.Music	Miss Anthropocene	Grimes	Electronic	So Heavy I Fell Through the Earth (Art Mix)	368.338	6	0.1	Friday	-5	2020-02-28 15:20:30	2020-02-28 15:20:36
1386	com.apple.Music	Miss Anthropocene	Grimes	Electronic	So Heavy I Fell Through the Earth (Art Mix)	368.0	1	0.0166666666666667	Friday	-5	2020-02-28 15:20:36	2020-02-28 15:20:37
1387	com.apple.WebKit.WebContent	NULL	NULL	NULL	(1) Home / Twitter	193.694	2238	37.3	Friday	-5	2020-02-28 15:20:37	2020-02-28 15:57:55
1388		NULL	NULL	NULL	NULL	NULL	102	1.7	Friday	-5	2020-02-28 15:57:55	2020-02-28 15:59:37
1389	com.apple.WebKit.WebContent	NULL	NULL	NULL	Home / Twitter	15.0417	0	0.0	Friday	-5	2020-02-28 15:59:37	2020-02-28 15:59:37
1390	com.apple.WebKit.WebContent	NULL	NULL	NULL	Home / Twitter	15.0417	3	0.05	Friday	-5	2020-02-28 15:59:37	2020-02-28 15:59:40
1391	com.apple.WebKit.WebContent	NULL	NULL	NULL	Home / Twitter	62.0	2	0.0333333333333333	Friday	-5	2020-02-28 15:59:40	2020-02-28 15:59:42
1392	com.apple.WebKit.WebContent	NULL	NULL	NULL	Home / Twitter	109.248	2	0.0333333333333333	Friday	-5	2020-02-28 15:59:42	2020-02-28 15:59:44
1393		NULL	NULL	NULL	NULL	NULL	3	0.05	Friday	-5	2020-02-28 15:59:44	2020-02-28 15:59:47
1394	com.apple.WebKit.WebContent	NULL	NULL	NULL	Home / Twitter	107.541	0	0.0	Friday	-5	2020-02-28 15:59:47	2020-02-28 15:59:47
1395	com.apple.WebKit.WebContent	NULL	NULL	NULL	Home / Twitter	107.541	1	0.0166666666666667	Friday	-5	2020-02-28 15:59:47	2020-02-28 15:59:48

Network Usage (netusage.sqlite)



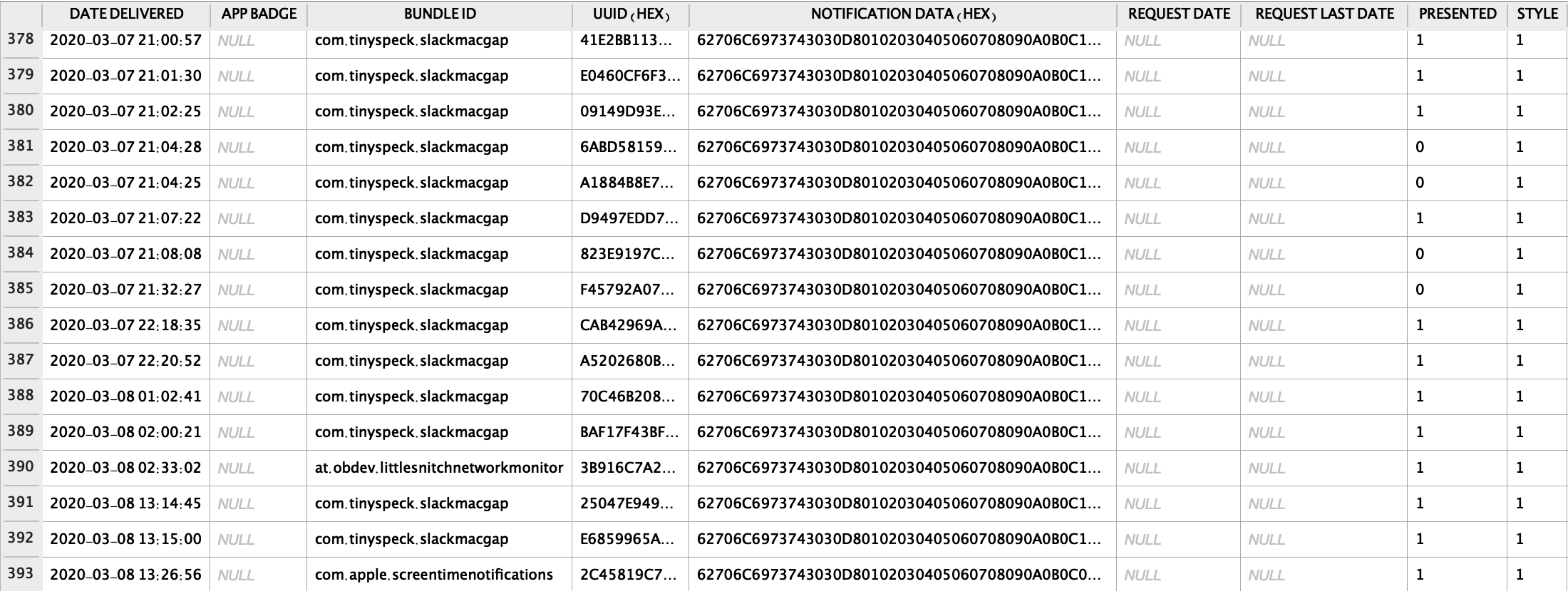
	PROCESS TIMESTAMP	PROCESS FIRST TIMESTAMP	LIVE USAGE TIMESTAMP	BUNDLE ID	PROCESS NAME	WIFI IN	WIFI OUT	WWAN IN	WWAN OUT	WIRED IN	WIRED OUT
121	2020-03-08 02:08:29	2019-10-30 17:01:17	2019-10-30 17:01:17	com.apple.TextEdit	com.apple.TextEdit	431667.0	354252.0	0.0	0.0	0.0	0.0
122	2020-03-08 02:34:50	2020-03-08 02:33:02	2020-03-08 02:33:02	com.Google.GoogleEarthPro	com.Google.GoogleEarthPro	73679370.0	4920063.0	0.0	0.0	0.0	0.0
123	2020-03-08 03:00:49	2019-10-30 13:16:46	2019-10-30 13:16:46	NULL	com.apple.sbd	4311201.0	277323.0	0.0	0.0	0.0	0.0
124	2020-03-08 03:23:26	2019-10-30 13:06:36	2019-10-30 13:06:36	NULL	syspolicyd	39481609.0	14037083.0	3257.0	342.0	0.0	0.0
125	2020-03-08 05:04:43	2019-10-30 14:24:56	2019-10-30 14:24:56	com.apple.imtransferservices.IMTransferAgent	com.apple.imtransferservices.IMTransferAgent	1016118966.0	7580980.0	45661541.0	123285.0	0.0	0.0
126	2020-03-08 05:37:55	2019-10-30 04:17:30	2019-10-30 04:17:30	NULL	SubmitDiagInfo	1640776.0	9610129.0	67334.0	232937.0	847344.0	1338942.0
127	2020-03-08 05:37:55	2019-10-30 13:21:41	2019-10-30 13:21:41	NULL	findmydeviced	243209.0	178990.0	0.0	0.0	19326.0	442864.0
128	2020-03-08 05:37:55	2019-10-30 13:21:55	2019-10-30 13:21:55	NULL	mobileactivation	3257813.0	391763.0	39275.0	4530.0	132776.0	565249.0
129	2020-03-08 05:37:55	2019-10-30 16:28:23	2019-10-30 16:28:23	com.apple.PowerChime	com.apple.PowerChime	0.0	0.0	0.0	0.0	85427.0	16947977.0
130	2020-03-08 05:37:58	2019-10-30 13:21:23	2019-10-30 13:21:23	com.apple.Notes	com.apple.Notes	121004527.0	21040041.0	32677.0	15993.0	0.0	0.0
131	2020-03-08 05:38:57	2019-10-30 13:06:07	2019-10-30 13:06:07	NULL	rtcreportingd	3600832.0	551698.0	0.0	0.0	0.0	0.0
132	2020-03-08 06:19:11	2019-10-30 13:21:42	2019-10-30 13:21:42	NULL	CategoriesServic	2044788.0	359904.0	16243.0	1875.0	0.0	0.0
133	2020-03-08 06:19:13	2019-10-30 13:16:59	2019-10-30 13:16:59	NULL	appstoreagent	14774858.0	2172846.0	0.0	0.0	0.0	0.0
134	2020-03-08 06:19:14	2019-10-30 19:44:27	2019-10-30 19:44:27	com.apple.Music	com.apple.Music	30385584331.0	286329673.0	203807.0	61073.0	0.0	0.0
135	2020-03-08 06:19:32	2019-10-30 13:06:13	2019-10-30 13:06:13	NULL	adprivacyd	2478799.0	741319.0	0.0	0.0	0.0	0.0
136	2020-03-08 06:37:51	2019-10-30 04:17:31	2019-10-30 04:17:31	NULL	nfcd	0.0	0.0	0.0	0.0	2859185.0	2390439.0
137	2020-03-08 06:38:28	2019-10-30 13:21:32	2019-10-30 13:21:32	NULL	corespeechd	0.0	0.0	0.0	0.0	10026886.0	46708688.0
138	2020-03-08 07:09:28	2019-10-30 14:14:54	2019-10-30 14:14:54	NULL	netbiosd	11005788.0	704988.0	810.0	558.0	12510.0	5418.0
139	2020-03-08 08:06:15	2019-10-30 13:06:19	2019-10-30 13:06:19	com.apple.Maps	com.apple.Maps	3245671.0	682729.0	6443.0	1200.0	0.0	0.0
140	2020-03-08 08:55:18	2019-12-07 18:41:01	2019-12-07 18:41:01	NULL	knowledge-agent	95965369.0	59349873.0	7009.0	3004.0	0.0	0.0
141	2020-03-08 10:13:00	2019-10-30 13:16:59	2019-10-30 13:16:59	NULL	remindd	1581422.0	196435.0	9913.0	1090.0	0.0	0.0
142	2020-03-08 10:13:00	2019-10-30 13:22:20	2019-10-30 13:22:20	NULL	assistant_servic	848709.0	384122.0	7677.0	3171.0	0.0	0.0

interactionC.db – Contact Interactions



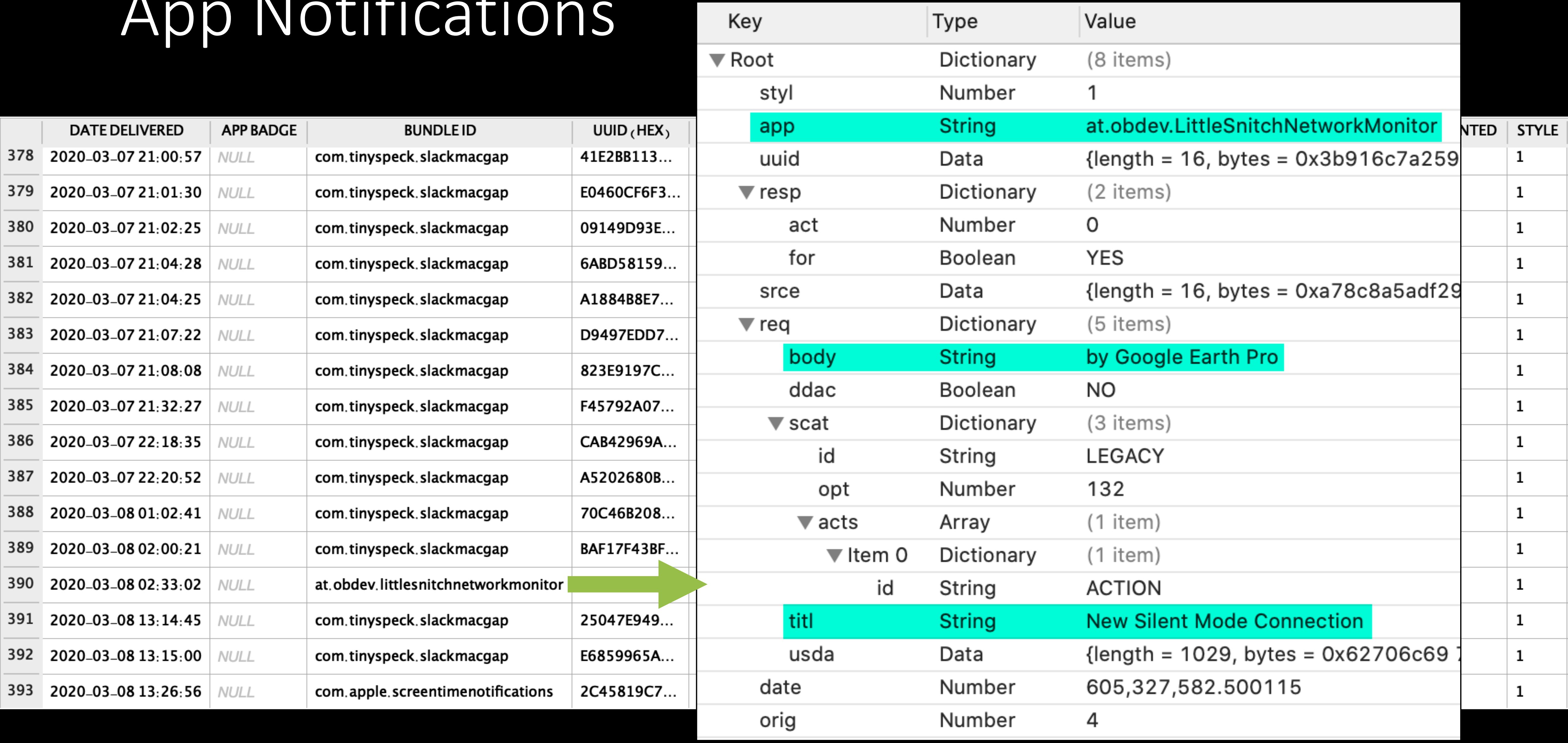
	START DATE	BUNDLE ID	DISPLAY NAME	IDENTIFIER	PERSONID	DIRECTION	IS RESPONSE	MECHANISM	RECIPIENT COUNT
1430	2020-02-20 22:43:11	com.apple.iChat	Sarah Edwards	oompa[redacted]	78306567-EB29-41E7-BCA5-198AFCE971FA	1	0	4	2
1431	2020-02-20 22:57:15	com.apple.iChat	Heather Mahalik	+1703[redacted]	5F042B01-B2F0-409E-95DA-CDBFD8563AA6:ABPerson	0	0	4	0
1432	2020-02-20 22:57:20	com.apple.iChat	Heather Mahalik	+1703[redacted]	5F042B01-B2F0-409E-95DA-CDBFD8563AA6:ABPerson	0	0	4	0
1433	2020-02-20 22:57:23	com.apple.iChat	Heather Mahalik	+1703[redacted]	5F042B01-B2F0-409E-95DA-CDBFD8563AA6:ABPerson	0	0	4	0
1434	2020-02-20 22:57:24	com.apple.iChat	Sarah Edwards	+1571[redacted]	78306567-EB29-41E7-BCA5-198AFCE971FA	1	0	4	1
1435	2020-02-20 22:57:45	com.apple.iChat	Sarah Edwards	+1571[redacted]	78306567-EB29-41E7-BCA5-198AFCE971FA	1	0	4	1
1436	2020-02-20 22:57:55	com.apple.iChat	Heather Mahalik	+1703[redacted]	5F042B01-B2F0-409E-95DA-CDBFD8563AA6:ABPerson	0	0	4	0
1437	2020-02-20 23:31:38	com.apple.mail	Redfin	listing[redacted]	NULL	0	0	1	0
1438	2020-02-20 23:35:12	com.apple.iChat	Braden	+1571[redacted]	C516FC0D-9D2D-4927-9A93-AE925B7286EB:ABPerson	0	0	4	1
1439	2020-02-20 23:34:23	com.apple.mail	Sarah Edwards	oompa[redacted]	NULL	1	1	1	16
1440	2020-02-20 23:36:11	com.apple.iChat	Sarah Edwards	+1571[redacted]	78306567-EB29-41E7-BCA5-198AFCE971FA	1	0	4	1
1441	2020-02-20 23:36:34	com.apple.iChat	Sarah Edwards	oompa[redacted]	78306567-EB29-41E7-BCA5-198AFCE971FA	1	0	4	2
1442	2020-02-20 23:36:50	com.apple.iChat	Heather Mahalik	+1703[redacted]	5F042B01-B2F0-409E-95DA-CDBFD8563AA6:ABPerson	0	0	4	0
1443	2020-02-20 23:36:58	com.apple.iChat	Heather Mahalik	+1703[redacted]	5F042B01-B2F0-409E-95DA-CDBFD8563AA6:ABPerson	0	0	4	0
1444	2020-02-20 23:37:53	com.apple.iChat	Sarah Edwards	+1571[redacted]	78306567-EB29-41E7-BCA5-198AFCE971FA	1	0	4	1
1445	2020-02-20 23:38:15	com.apple.iChat	Heather Mahalik	+1703[redacted]	5F042B01-B2F0-409E-95DA-CDBFD8563AA6:ABPerson	0	0	4	0
1446	2020-02-20 23:38:17	com.apple.iChat	Sarah Edwards	+1571[redacted]	78306567-EB29-41E7-BCA5-198AFCE971FA	1	0	4	1
1447	2020-02-20 23:38:27	com.apple.mail	Jessica Hyde	jessica[redacted]	NULL	0	1	1	0
1448	2020-02-20 23:39:59	com.apple.mail	Sarah Edwards	oompa[redacted]	NULL	1	1	1	1
1449	2020-02-20 23:40:57	com.apple.mail	Jessica Hyde	jessica[redacted]	NULL	0	1	1	0
1450	2020-02-20 23:44:28	com.apple.iChat	Sarah Edwards	+1571[redacted]	78306567-EB29-41E7-BCA5-198AFCE971FA	1	0	4	1
1451	2020-02-20 23:47:31	com.apple.iChat	Heather Mahalik	+1703[redacted]	5F042B01-B2F0-409E-95DA-CDBFD8563AA6:ABPerson	0	0	4	0
1452	2020-02-20 23:49:06	com.apple.mail	Trisha	trishar[redacted]	NULL	0	1	1	0

Application Notifications (com.apple.notificationcenter/db2/)



	DATE DELIVERED	APP BADGE	BUNDLE ID	UUID (HEX)	NOTIFICATION DATA (HEX)	REQUEST DATE	REQUEST LAST DATE	PRESENTED	STYLE
378	2020-03-07 21:00:57	NULL	com.tinyspeck.slackmacgap	41E2BB113...	62706C6973743030D80102030405060708090A0B0C1...	NULL	NULL	1	1
379	2020-03-07 21:01:30	NULL	com.tinyspeck.slackmacgap	E0460CF6F3...	62706C6973743030D80102030405060708090A0B0C1...	NULL	NULL	1	1
380	2020-03-07 21:02:25	NULL	com.tinyspeck.slackmacgap	09149D93E...	62706C6973743030D80102030405060708090A0B0C1...	NULL	NULL	1	1
381	2020-03-07 21:04:28	NULL	com.tinyspeck.slackmacgap	6ABD58159...	62706C6973743030D80102030405060708090A0B0C1...	NULL	NULL	0	1
382	2020-03-07 21:04:25	NULL	com.tinyspeck.slackmacgap	A1884B8E7...	62706C6973743030D80102030405060708090A0B0C1...	NULL	NULL	0	1
383	2020-03-07 21:07:22	NULL	com.tinyspeck.slackmacgap	D9497EDD7...	62706C6973743030D80102030405060708090A0B0C1...	NULL	NULL	1	1
384	2020-03-07 21:08:08	NULL	com.tinyspeck.slackmacgap	823E9197C...	62706C6973743030D80102030405060708090A0B0C1...	NULL	NULL	0	1
385	2020-03-07 21:32:27	NULL	com.tinyspeck.slackmacgap	F45792A07...	62706C6973743030D80102030405060708090A0B0C1...	NULL	NULL	0	1
386	2020-03-07 22:18:35	NULL	com.tinyspeck.slackmacgap	CAB42969A...	62706C6973743030D80102030405060708090A0B0C1...	NULL	NULL	1	1
387	2020-03-07 22:20:52	NULL	com.tinyspeck.slackmacgap	A5202680B...	62706C6973743030D80102030405060708090A0B0C1...	NULL	NULL	1	1
388	2020-03-08 01:02:41	NULL	com.tinyspeck.slackmacgap	70C46B208...	62706C6973743030D80102030405060708090A0B0C1...	NULL	NULL	1	1
389	2020-03-08 02:00:21	NULL	com.tinyspeck.slackmacgap	BAF17F43BF...	62706C6973743030D80102030405060708090A0B0C1...	NULL	NULL	1	1
390	2020-03-08 02:33:02	NULL	at.obdev.littlesnitchnetworkmonitor	3B916C7A2...	62706C6973743030D80102030405060708090A0B0C1...	NULL	NULL	1	1
391	2020-03-08 13:14:45	NULL	com.tinyspeck.slackmacgap	25047E949...	62706C6973743030D80102030405060708090A0B0C1...	NULL	NULL	1	1
392	2020-03-08 13:15:00	NULL	com.tinyspeck.slackmacgap	E6859965A...	62706C6973743030D80102030405060708090A0B0C1...	NULL	NULL	1	1
393	2020-03-08 13:26:56	NULL	com.apple.screentimenotifications	2C45819C7...	62706C6973743030D80102030405060708090A0B0C0...	NULL	NULL	1	1

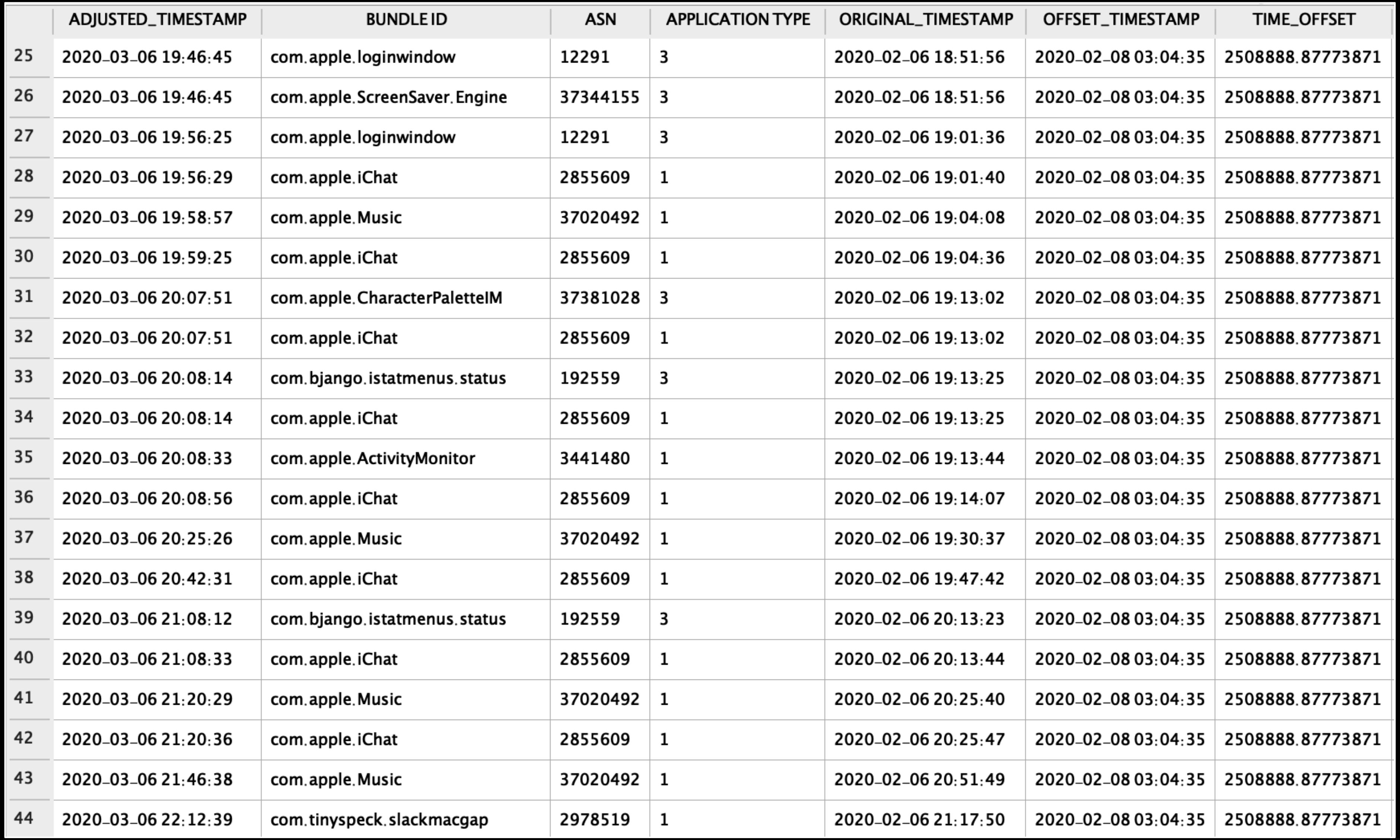
App Notifications



	DATE DELIVERED	APP BADGE	BUNDLE ID	UUID (HEX)	NTED	STYLE
378	2020-03-07 21:00:57	NULL	com.tinyspeck.slackmacgap	41E2BB113...		1
379	2020-03-07 21:01:30	NULL	com.tinyspeck.slackmacgap	E0460CF6F3...		1
380	2020-03-07 21:02:25	NULL	com.tinyspeck.slackmacgap	09149D93E...		1
381	2020-03-07 21:04:28	NULL	com.tinyspeck.slackmacgap	6ABD58159...		1
382	2020-03-07 21:04:25	NULL	com.tinyspeck.slackmacgap	A1884B8E7...		1
383	2020-03-07 21:07:22	NULL	com.tinyspeck.slackmacgap	D9497EDD7...		1
384	2020-03-07 21:08:08	NULL	com.tinyspeck.slackmacgap	823E9197C...		1
385	2020-03-07 21:32:27	NULL	com.tinyspeck.slackmacgap	F45792A07...		1
386	2020-03-07 22:18:35	NULL	com.tinyspeck.slackmacgap	CAB42969A...		1
387	2020-03-07 22:20:52	NULL	com.tinyspeck.slackmacgap	A5202680B...		1
388	2020-03-08 01:02:41	NULL	com.tinyspeck.slackmacgap	70C46B208...		1
389	2020-03-08 02:00:21	NULL	com.tinyspeck.slackmacgap	BAF17F43BF...		1
390	2020-03-08 02:33:02	NULL	at.obdev.littlesnitchnetworkmonitor			1
391	2020-03-08 13:14:45	NULL	com.tinyspeck.slackmacgap	25047E949...		1
392	2020-03-08 13:15:00	NULL	com.tinyspeck.slackmacgap	E6859965A...		1
393	2020-03-08 13:26:56	NULL	com.apple.screentimenotifications	2C45819C7...		1

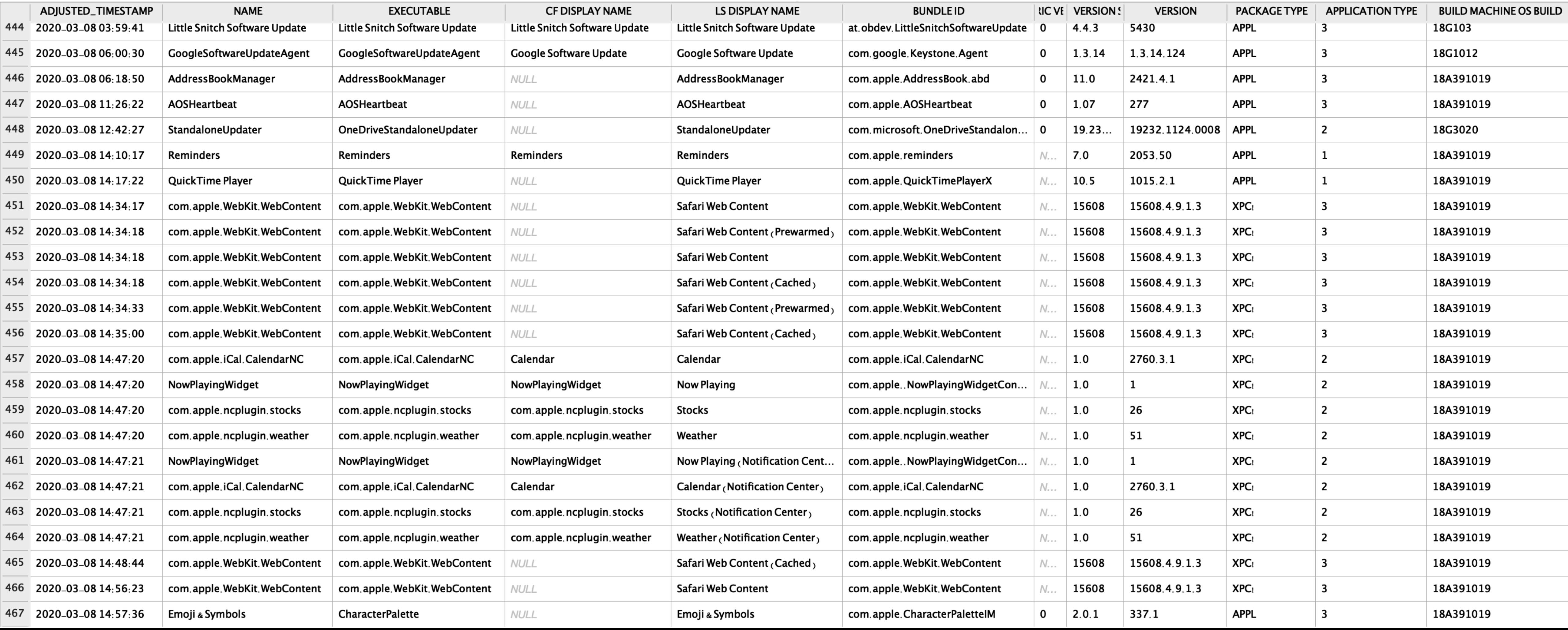
Key	Type	Value
▼ Root	Dictionary	(8 items)
styl	Number	1
app	String	at.obdev.LittleSnitchNetworkMonitor
uuid	Data	{length = 16, bytes = 0x3b916c7a259
▼ resp	Dictionary	(2 items)
act	Number	0
for	Boolean	YES
srce	Data	{length = 16, bytes = 0xa78c8a5adf29
▼ req	Dictionary	(5 items)
body	String	by Google Earth Pro
ddac	Boolean	NO
▼ scat	Dictionary	(3 items)
id	String	LEGACY
opt	Number	132
▼ acts	Array	(1 item)
▼ Item 0	Dictionary	(1 item)
id	String	ACTION
titl	String	New Silent Mode Connection
usda	Data	{length = 1029, bytes = 0x62706c69
date	Number	605,327,582.500115
orig	Number	4

CurrentPowerlog.PLSQL – Front Most App



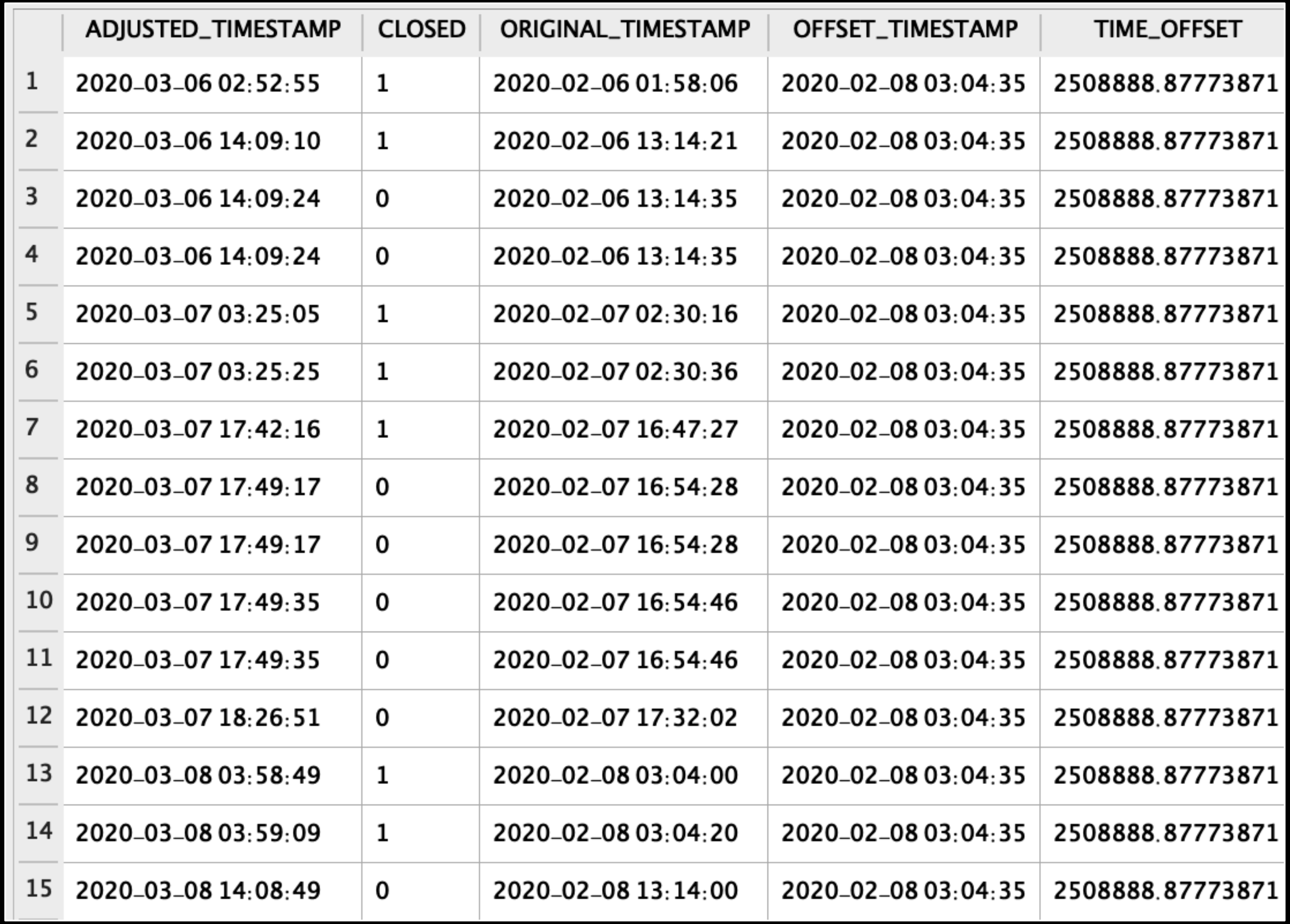
	ADJUSTED_TIMESTAMP	BUNDLE ID	ASN	APPLICATION TYPE	ORIGINAL_TIMESTAMP	OFFSET_TIMESTAMP	TIME_OFFSET
25	2020-03-06 19:46:45	com.apple.loginwindow	12291	3	2020-02-06 18:51:56	2020-02-08 03:04:35	2508888.87773871
26	2020-03-06 19:46:45	com.apple.ScreenSaver.Engine	37344155	3	2020-02-06 18:51:56	2020-02-08 03:04:35	2508888.87773871
27	2020-03-06 19:56:25	com.apple.loginwindow	12291	3	2020-02-06 19:01:36	2020-02-08 03:04:35	2508888.87773871
28	2020-03-06 19:56:29	com.apple.iChat	2855609	1	2020-02-06 19:01:40	2020-02-08 03:04:35	2508888.87773871
29	2020-03-06 19:58:57	com.apple.Music	37020492	1	2020-02-06 19:04:08	2020-02-08 03:04:35	2508888.87773871
30	2020-03-06 19:59:25	com.apple.iChat	2855609	1	2020-02-06 19:04:36	2020-02-08 03:04:35	2508888.87773871
31	2020-03-06 20:07:51	com.apple.CharacterPaletteIM	37381028	3	2020-02-06 19:13:02	2020-02-08 03:04:35	2508888.87773871
32	2020-03-06 20:07:51	com.apple.iChat	2855609	1	2020-02-06 19:13:02	2020-02-08 03:04:35	2508888.87773871
33	2020-03-06 20:08:14	com.bjango.istatmenus.status	192559	3	2020-02-06 19:13:25	2020-02-08 03:04:35	2508888.87773871
34	2020-03-06 20:08:14	com.apple.iChat	2855609	1	2020-02-06 19:13:25	2020-02-08 03:04:35	2508888.87773871
35	2020-03-06 20:08:33	com.apple.ActivityMonitor	3441480	1	2020-02-06 19:13:44	2020-02-08 03:04:35	2508888.87773871
36	2020-03-06 20:08:56	com.apple.iChat	2855609	1	2020-02-06 19:14:07	2020-02-08 03:04:35	2508888.87773871
37	2020-03-06 20:25:26	com.apple.Music	37020492	1	2020-02-06 19:30:37	2020-02-08 03:04:35	2508888.87773871
38	2020-03-06 20:42:31	com.apple.iChat	2855609	1	2020-02-06 19:47:42	2020-02-08 03:04:35	2508888.87773871
39	2020-03-06 21:08:12	com.bjango.istatmenus.status	192559	3	2020-02-06 20:13:23	2020-02-08 03:04:35	2508888.87773871
40	2020-03-06 21:08:33	com.apple.iChat	2855609	1	2020-02-06 20:13:44	2020-02-08 03:04:35	2508888.87773871
41	2020-03-06 21:20:29	com.apple.Music	37020492	1	2020-02-06 20:25:40	2020-02-08 03:04:35	2508888.87773871
42	2020-03-06 21:20:36	com.apple.iChat	2855609	1	2020-02-06 20:25:47	2020-02-08 03:04:35	2508888.87773871
43	2020-03-06 21:46:38	com.apple.Music	37020492	1	2020-02-06 20:51:49	2020-02-08 03:04:35	2508888.87773871
44	2020-03-06 22:12:39	com.tinyspeck.slackmacgap	2978519	1	2020-02-06 21:17:50	2020-02-08 03:04:35	2508888.87773871

CurrentPowerlog.PLSQL – App Info



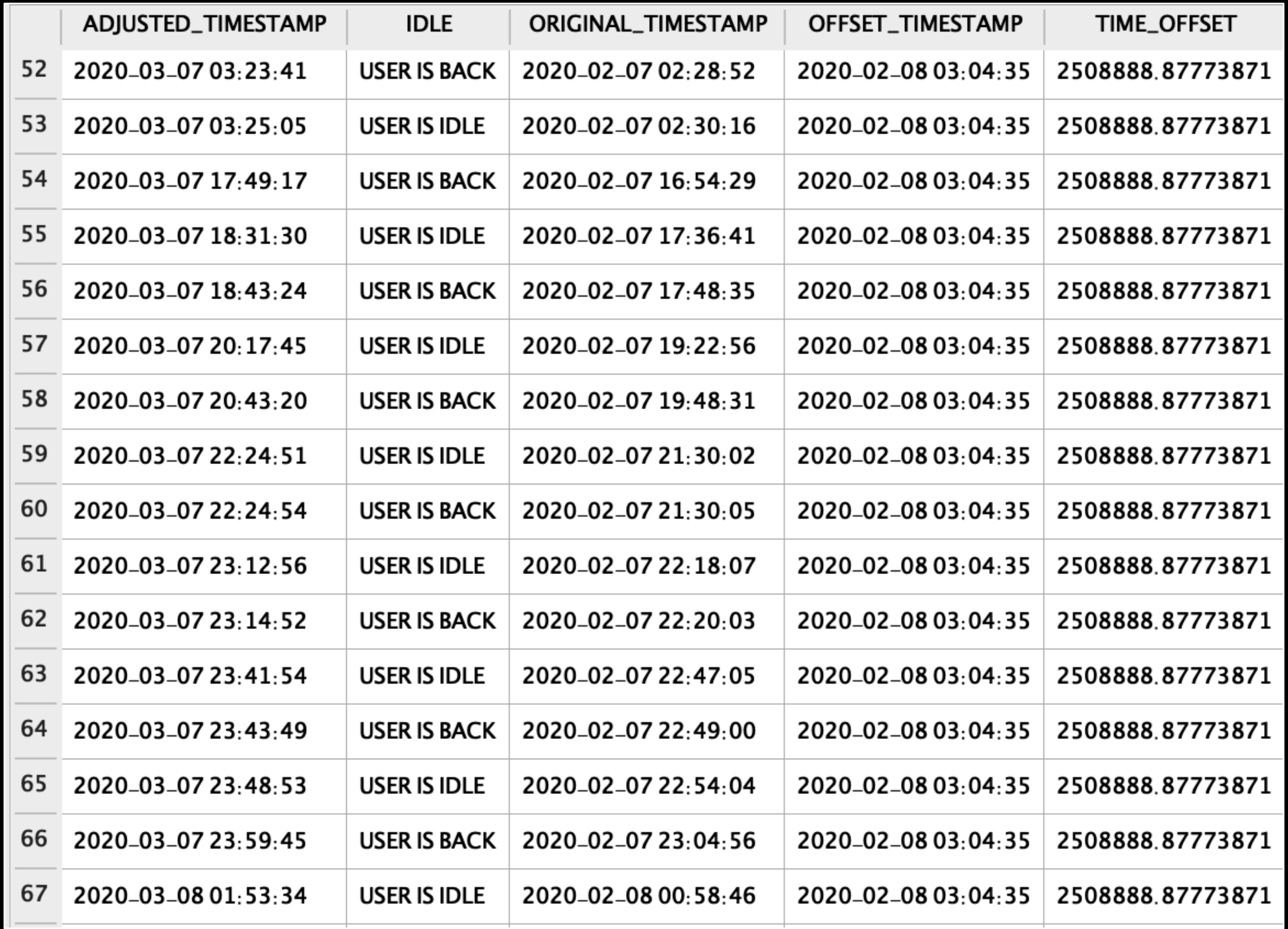
	ADJUSTED_TIMESTAMP	NAME	EXECUTABLE	CF DISPLAY NAME	LS DISPLAY NAME	BUNDLE ID	RIC VE	VERSION S	VERSION	PACKAGE TYPE	APPLICATION TYPE	BUILD MACHINE OS BUILD
444	2020-03-08 03:59:41	Little Snitch Software Update	Little Snitch Software Update	Little Snitch Software Update	Little Snitch Software Update	at.obdev.LittleSnitchSoftwareUpdate	0	4.4.3	5430	APPL	3	18G103
445	2020-03-08 06:00:30	GoogleSoftwareUpdateAgent	GoogleSoftwareUpdateAgent	Google Software Update	Google Software Update	com.google.Keystone.Agent	0	1.3.14	1.3.14.124	APPL	3	18G1012
446	2020-03-08 06:18:50	AddressBookManager	AddressBookManager	NULL	AddressBookManager	com.apple.AddressBook.abd	0	11.0	2421.4.1	APPL	3	18A391019
447	2020-03-08 11:26:22	AOSHeartbeat	AOSHeartbeat	NULL	AOSHeartbeat	com.apple.AOSHeartbeat	0	1.07	277	APPL	3	18A391019
448	2020-03-08 12:42:27	StandaloneUpdater	OneDriveStandaloneUpdater	NULL	StandaloneUpdater	com.microsoft.OneDriveStandalon...	0	19.23...	19232.1124.0008	APPL	2	18G3020
449	2020-03-08 14:10:17	Reminders	Reminders	Reminders	Reminders	com.apple.reminders	N...	7.0	2053.50	APPL	1	18A391019
450	2020-03-08 14:17:22	QuickTime Player	QuickTime Player	NULL	QuickTime Player	com.apple.QuickTimePlayerX	N...	10.5	1015.2.1	APPL	1	18A391019
451	2020-03-08 14:34:17	com.apple.WebKit.WebContent	com.apple.WebKit.WebContent	NULL	Safari Web Content	com.apple.WebKit.WebContent	N...	15608	15608.4.9.1.3	XPC!	3	18A391019
452	2020-03-08 14:34:18	com.apple.WebKit.WebContent	com.apple.WebKit.WebContent	NULL	Safari Web Content (Prewarmed)	com.apple.WebKit.WebContent	N...	15608	15608.4.9.1.3	XPC!	3	18A391019
453	2020-03-08 14:34:18	com.apple.WebKit.WebContent	com.apple.WebKit.WebContent	NULL	Safari Web Content	com.apple.WebKit.WebContent	N...	15608	15608.4.9.1.3	XPC!	3	18A391019
454	2020-03-08 14:34:18	com.apple.WebKit.WebContent	com.apple.WebKit.WebContent	NULL	Safari Web Content (Cached)	com.apple.WebKit.WebContent	N...	15608	15608.4.9.1.3	XPC!	3	18A391019
455	2020-03-08 14:34:33	com.apple.WebKit.WebContent	com.apple.WebKit.WebContent	NULL	Safari Web Content (Prewarmed)	com.apple.WebKit.WebContent	N...	15608	15608.4.9.1.3	XPC!	3	18A391019
456	2020-03-08 14:35:00	com.apple.WebKit.WebContent	com.apple.WebKit.WebContent	NULL	Safari Web Content (Cached)	com.apple.WebKit.WebContent	N...	15608	15608.4.9.1.3	XPC!	3	18A391019
457	2020-03-08 14:47:20	com.apple.iCal.CalendarNC	com.apple.iCal.CalendarNC	Calendar	Calendar	com.apple.iCal.CalendarNC	N...	1.0	2760.3.1	XPC!	2	18A391019
458	2020-03-08 14:47:20	NowPlayingWidget	NowPlayingWidget	NowPlayingWidget	Now Playing	com.apple..NowPlayingWidgetCon...	N...	1.0	1	XPC!	2	18A391019
459	2020-03-08 14:47:20	com.apple.ncplugin.stocks	com.apple.ncplugin.stocks	com.apple.ncplugin.stocks	Stocks	com.apple.ncplugin.stocks	N...	1.0	26	XPC!	2	18A391019
460	2020-03-08 14:47:20	com.apple.ncplugin.weather	com.apple.ncplugin.weather	com.apple.ncplugin.weather	Weather	com.apple.ncplugin.weather	N...	1.0	51	XPC!	2	18A391019
461	2020-03-08 14:47:21	NowPlayingWidget	NowPlayingWidget	NowPlayingWidget	Now Playing (Notification Cent...	com.apple..NowPlayingWidgetCon...	N...	1.0	1	XPC!	2	18A391019
462	2020-03-08 14:47:21	com.apple.iCal.CalendarNC	com.apple.iCal.CalendarNC	Calendar	Calendar (Notification Center)	com.apple.iCal.CalendarNC	N...	1.0	2760.3.1	XPC!	2	18A391019
463	2020-03-08 14:47:21	com.apple.ncplugin.stocks	com.apple.ncplugin.stocks	com.apple.ncplugin.stocks	Stocks (Notification Center)	com.apple.ncplugin.stocks	N...	1.0	26	XPC!	2	18A391019
464	2020-03-08 14:47:21	com.apple.ncplugin.weather	com.apple.ncplugin.weather	com.apple.ncplugin.weather	Weather (Notification Center)	com.apple.ncplugin.weather	N...	1.0	51	XPC!	2	18A391019
465	2020-03-08 14:48:44	com.apple.WebKit.WebContent	com.apple.WebKit.WebContent	NULL	Safari Web Content (Cached)	com.apple.WebKit.WebContent	N...	15608	15608.4.9.1.3	XPC!	3	18A391019
466	2020-03-08 14:56:23	com.apple.WebKit.WebContent	com.apple.WebKit.WebContent	NULL	Safari Web Content	com.apple.WebKit.WebContent	N...	15608	15608.4.9.1.3	XPC!	3	18A391019
467	2020-03-08 14:57:36	Emoji & Symbols	CharacterPalette	NULL	Emoji & Symbols	com.apple.CharacterPaletteIM	0	2.0.1	337.1	APPL	3	18A391019

CurrentPowerlog.PLSQL – Clamshell State



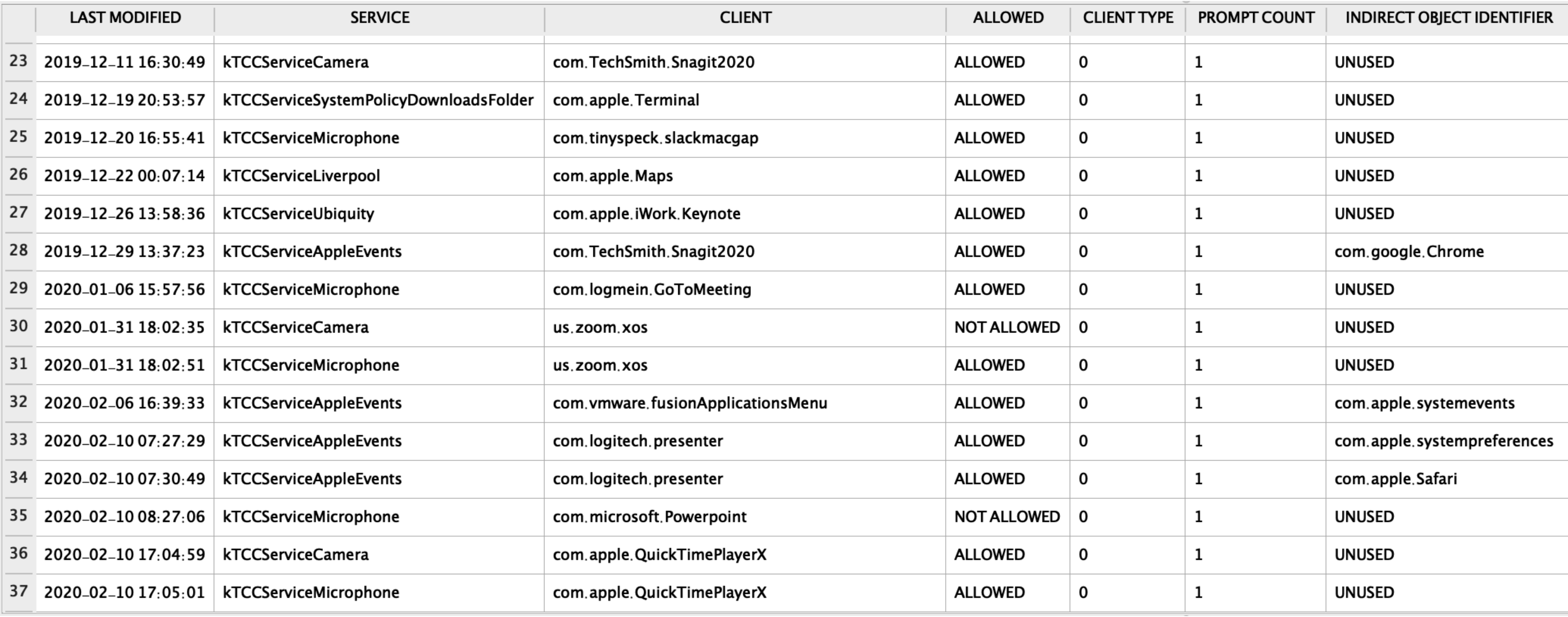
	ADJUSTED_TIMESTAMP	CLOSED	ORIGINAL_TIMESTAMP	OFFSET_TIMESTAMP	TIME_OFFSET
1	2020-03-06 02:52:55	1	2020-02-06 01:58:06	2020-02-08 03:04:35	2508888.87773871
2	2020-03-06 14:09:10	1	2020-02-06 13:14:21	2020-02-08 03:04:35	2508888.87773871
3	2020-03-06 14:09:24	0	2020-02-06 13:14:35	2020-02-08 03:04:35	2508888.87773871
4	2020-03-06 14:09:24	0	2020-02-06 13:14:35	2020-02-08 03:04:35	2508888.87773871
5	2020-03-07 03:25:05	1	2020-02-07 02:30:16	2020-02-08 03:04:35	2508888.87773871
6	2020-03-07 03:25:25	1	2020-02-07 02:30:36	2020-02-08 03:04:35	2508888.87773871
7	2020-03-07 17:42:16	1	2020-02-07 16:47:27	2020-02-08 03:04:35	2508888.87773871
8	2020-03-07 17:49:17	0	2020-02-07 16:54:28	2020-02-08 03:04:35	2508888.87773871
9	2020-03-07 17:49:17	0	2020-02-07 16:54:28	2020-02-08 03:04:35	2508888.87773871
10	2020-03-07 17:49:35	0	2020-02-07 16:54:46	2020-02-08 03:04:35	2508888.87773871
11	2020-03-07 17:49:35	0	2020-02-07 16:54:46	2020-02-08 03:04:35	2508888.87773871
12	2020-03-07 18:26:51	0	2020-02-07 17:32:02	2020-02-08 03:04:35	2508888.87773871
13	2020-03-08 03:58:49	1	2020-02-08 03:04:00	2020-02-08 03:04:35	2508888.87773871
14	2020-03-08 03:59:09	1	2020-02-08 03:04:20	2020-02-08 03:04:35	2508888.87773871
15	2020-03-08 14:08:49	0	2020-02-08 13:14:00	2020-02-08 03:04:35	2508888.87773871

CurrentPowerlog.PLSQL – Idle User?



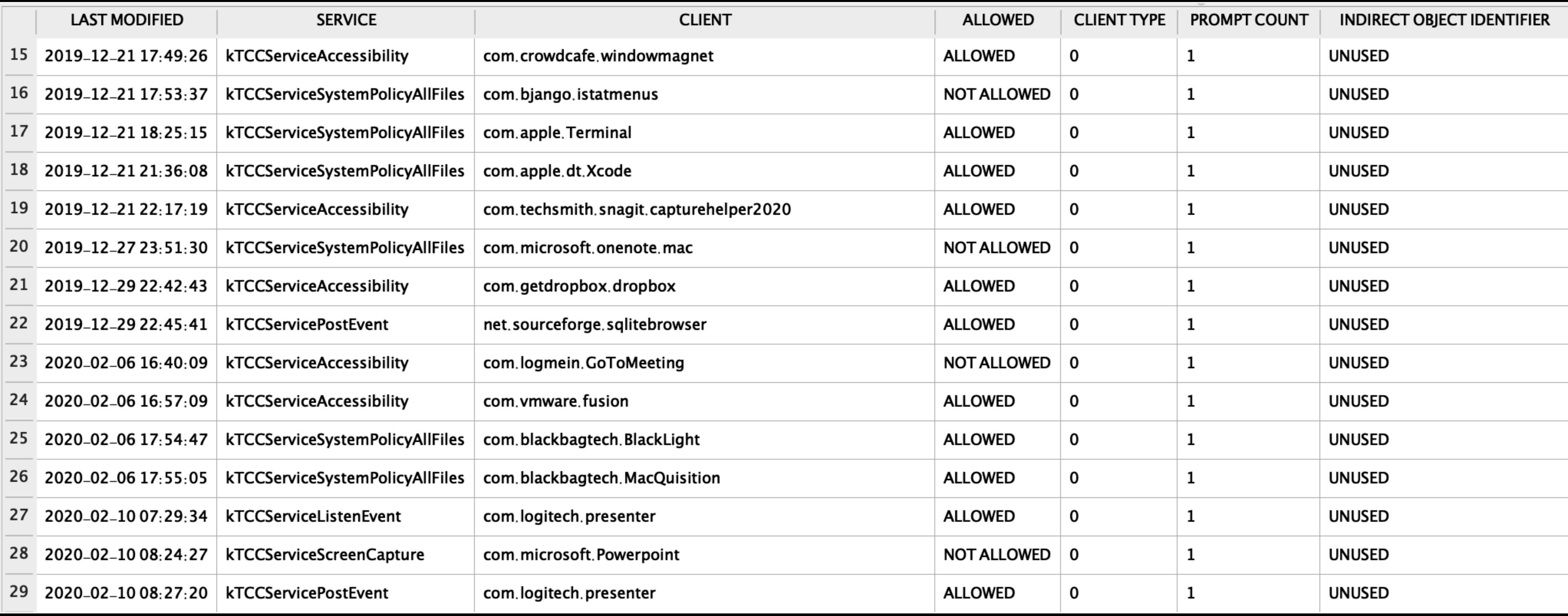
	ADJUSTED_TIMESTAMP	IDLE	ORIGINAL_TIMESTAMP	OFFSET_TIMESTAMP	TIME_OFFSET
52	2020-03-07 03:23:41	USER IS BACK	2020-02-07 02:28:52	2020-02-08 03:04:35	2508888.87773871
53	2020-03-07 03:25:05	USER IS IDLE	2020-02-07 02:30:16	2020-02-08 03:04:35	2508888.87773871
54	2020-03-07 17:49:17	USER IS BACK	2020-02-07 16:54:29	2020-02-08 03:04:35	2508888.87773871
55	2020-03-07 18:31:30	USER IS IDLE	2020-02-07 17:36:41	2020-02-08 03:04:35	2508888.87773871
56	2020-03-07 18:43:24	USER IS BACK	2020-02-07 17:48:35	2020-02-08 03:04:35	2508888.87773871
57	2020-03-07 20:17:45	USER IS IDLE	2020-02-07 19:22:56	2020-02-08 03:04:35	2508888.87773871
58	2020-03-07 20:43:20	USER IS BACK	2020-02-07 19:48:31	2020-02-08 03:04:35	2508888.87773871
59	2020-03-07 22:24:51	USER IS IDLE	2020-02-07 21:30:02	2020-02-08 03:04:35	2508888.87773871
60	2020-03-07 22:24:54	USER IS BACK	2020-02-07 21:30:05	2020-02-08 03:04:35	2508888.87773871
61	2020-03-07 23:12:56	USER IS IDLE	2020-02-07 22:18:07	2020-02-08 03:04:35	2508888.87773871
62	2020-03-07 23:14:52	USER IS BACK	2020-02-07 22:20:03	2020-02-08 03:04:35	2508888.87773871
63	2020-03-07 23:41:54	USER IS IDLE	2020-02-07 22:47:05	2020-02-08 03:04:35	2508888.87773871
64	2020-03-07 23:43:49	USER IS BACK	2020-02-07 22:49:00	2020-02-08 03:04:35	2508888.87773871
65	2020-03-07 23:48:53	USER IS IDLE	2020-02-07 22:54:04	2020-02-08 03:04:35	2508888.87773871
66	2020-03-07 23:59:45	USER IS BACK	2020-02-07 23:04:56	2020-02-08 03:04:35	2508888.87773871
67	2020-03-08 01:53:34	USER IS IDLE	2020-02-08 00:58:46	2020-02-08 03:04:35	2508888.87773871

TCC.db (Transparency, Consent, Control) - User



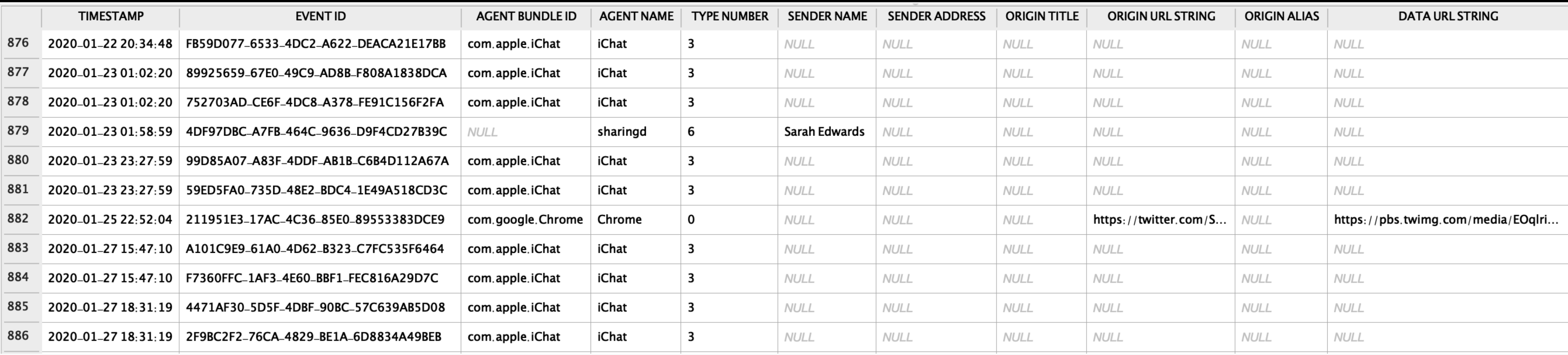
	LAST MODIFIED	SERVICE	CLIENT	ALLOWED	CLIENT TYPE	PROMPT COUNT	INDIRECT OBJECT IDENTIFIER
23	2019-12-11 16:30:49	kTCCServiceCamera	com.TechSmith.Snagit2020	ALLOWED	0	1	UNUSED
24	2019-12-19 20:53:57	kTCCServiceSystemPolicyDownloadsFolder	com.apple.Terminal	ALLOWED	0	1	UNUSED
25	2019-12-20 16:55:41	kTCCServiceMicrophone	com.tinyspeck.slackmacgap	ALLOWED	0	1	UNUSED
26	2019-12-22 00:07:14	kTCCServiceLiverpool	com.apple.Maps	ALLOWED	0	1	UNUSED
27	2019-12-26 13:58:36	kTCCServiceUbiquity	com.apple.iWork.Keynote	ALLOWED	0	1	UNUSED
28	2019-12-29 13:37:23	kTCCServiceAppleEvents	com.TechSmith.Snagit2020	ALLOWED	0	1	com.google.Chrome
29	2020-01-06 15:57:56	kTCCServiceMicrophone	com.logmein.GoToMeeting	ALLOWED	0	1	UNUSED
30	2020-01-31 18:02:35	kTCCServiceCamera	us.zoom.xos	NOT ALLOWED	0	1	UNUSED
31	2020-01-31 18:02:51	kTCCServiceMicrophone	us.zoom.xos	ALLOWED	0	1	UNUSED
32	2020-02-06 16:39:33	kTCCServiceAppleEvents	com.vmware.fusionApplicationsMenu	ALLOWED	0	1	com.apple.systemevents
33	2020-02-10 07:27:29	kTCCServiceAppleEvents	com.logitech.presenter	ALLOWED	0	1	com.apple.systempreferences
34	2020-02-10 07:30:49	kTCCServiceAppleEvents	com.logitech.presenter	ALLOWED	0	1	com.apple.Safari
35	2020-02-10 08:27:06	kTCCServiceMicrophone	com.microsoft.Powerpoint	NOT ALLOWED	0	1	UNUSED
36	2020-02-10 17:04:59	kTCCServiceCamera	com.apple.QuickTimePlayerX	ALLOWED	0	1	UNUSED
37	2020-02-10 17:05:01	kTCCServiceMicrophone	com.apple.QuickTimePlayerX	ALLOWED	0	1	UNUSED

TCC.db (Transparency, Consent, Control) - System



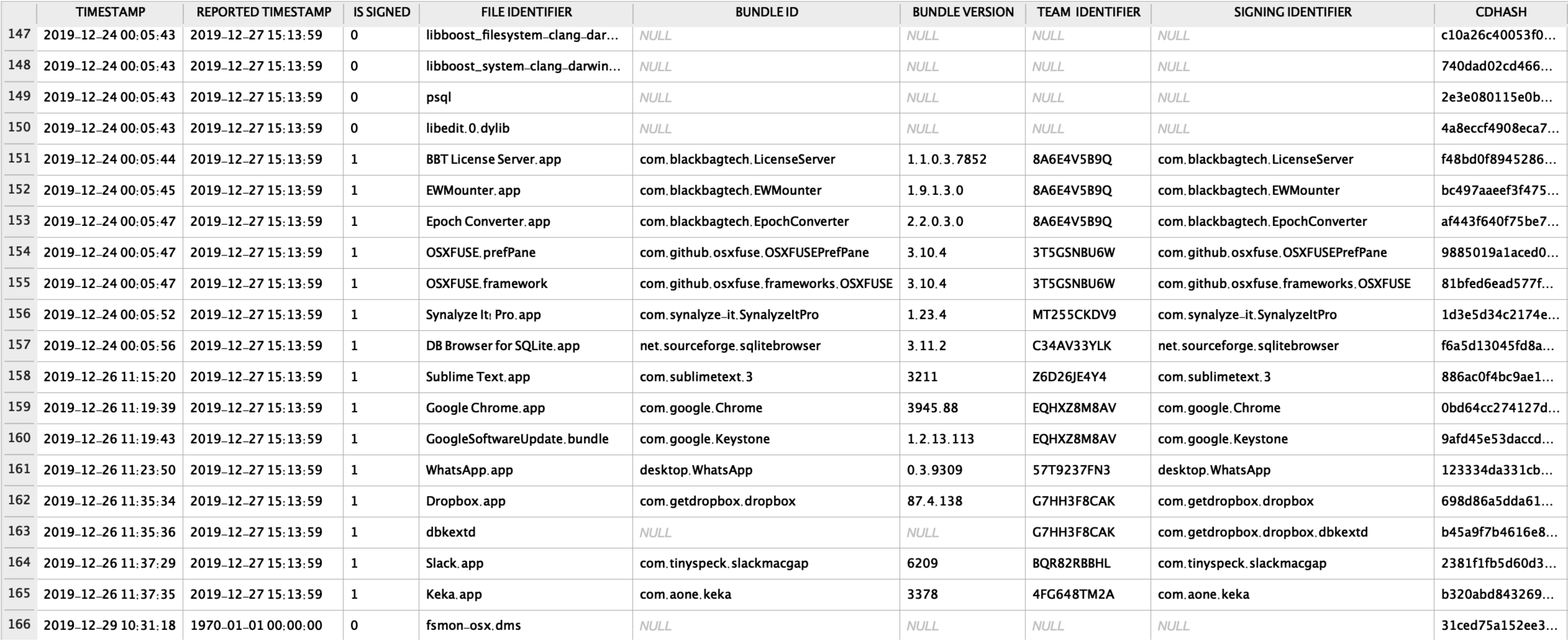
	LAST MODIFIED	SERVICE	CLIENT	ALLOWED	CLIENT TYPE	PROMPT COUNT	INDIRECT OBJECT IDENTIFIER
15	2019-12-21 17:49:26	kTCCServiceAccessibility	com.crowdcafe.windowmagnet	ALLOWED	0	1	UNUSED
16	2019-12-21 17:53:37	kTCCServiceSystemPolicyAllFiles	com.bjango.istatmenus	NOT ALLOWED	0	1	UNUSED
17	2019-12-21 18:25:15	kTCCServiceSystemPolicyAllFiles	com.apple.Terminal	ALLOWED	0	1	UNUSED
18	2019-12-21 21:36:08	kTCCServiceSystemPolicyAllFiles	com.apple.dt.Xcode	ALLOWED	0	1	UNUSED
19	2019-12-21 22:17:19	kTCCServiceAccessibility	com.techsmith.snagit.capturehelper2020	ALLOWED	0	1	UNUSED
20	2019-12-27 23:51:30	kTCCServiceSystemPolicyAllFiles	com.microsoft.onenote.mac	NOT ALLOWED	0	1	UNUSED
21	2019-12-29 22:42:43	kTCCServiceAccessibility	com.getdropbox.dropbox	ALLOWED	0	1	UNUSED
22	2019-12-29 22:45:41	kTCCServicePostEvent	net.sourceforge.sqlitebrowser	ALLOWED	0	1	UNUSED
23	2020-02-06 16:40:09	kTCCServiceAccessibility	com.logmein.GoToMeeting	NOT ALLOWED	0	1	UNUSED
24	2020-02-06 16:57:09	kTCCServiceAccessibility	com.vmware.fusion	ALLOWED	0	1	UNUSED
25	2020-02-06 17:54:47	kTCCServiceSystemPolicyAllFiles	com.blackbagtech.BlackLight	ALLOWED	0	1	UNUSED
26	2020-02-06 17:55:05	kTCCServiceSystemPolicyAllFiles	com.blackbagtech.MacQuisition	ALLOWED	0	1	UNUSED
27	2020-02-10 07:29:34	kTCCServiceListenEvent	com.logitech.presenter	ALLOWED	0	1	UNUSED
28	2020-02-10 08:24:27	kTCCServiceScreenCapture	com.microsoft.Powerpoint	NOT ALLOWED	0	1	UNUSED
29	2020-02-10 08:27:20	kTCCServicePostEvent	com.logitech.presenter	ALLOWED	0	1	UNUSED

Launch Services Quarantine (com.apple.LaunchServices.QuarantineEventsV2)



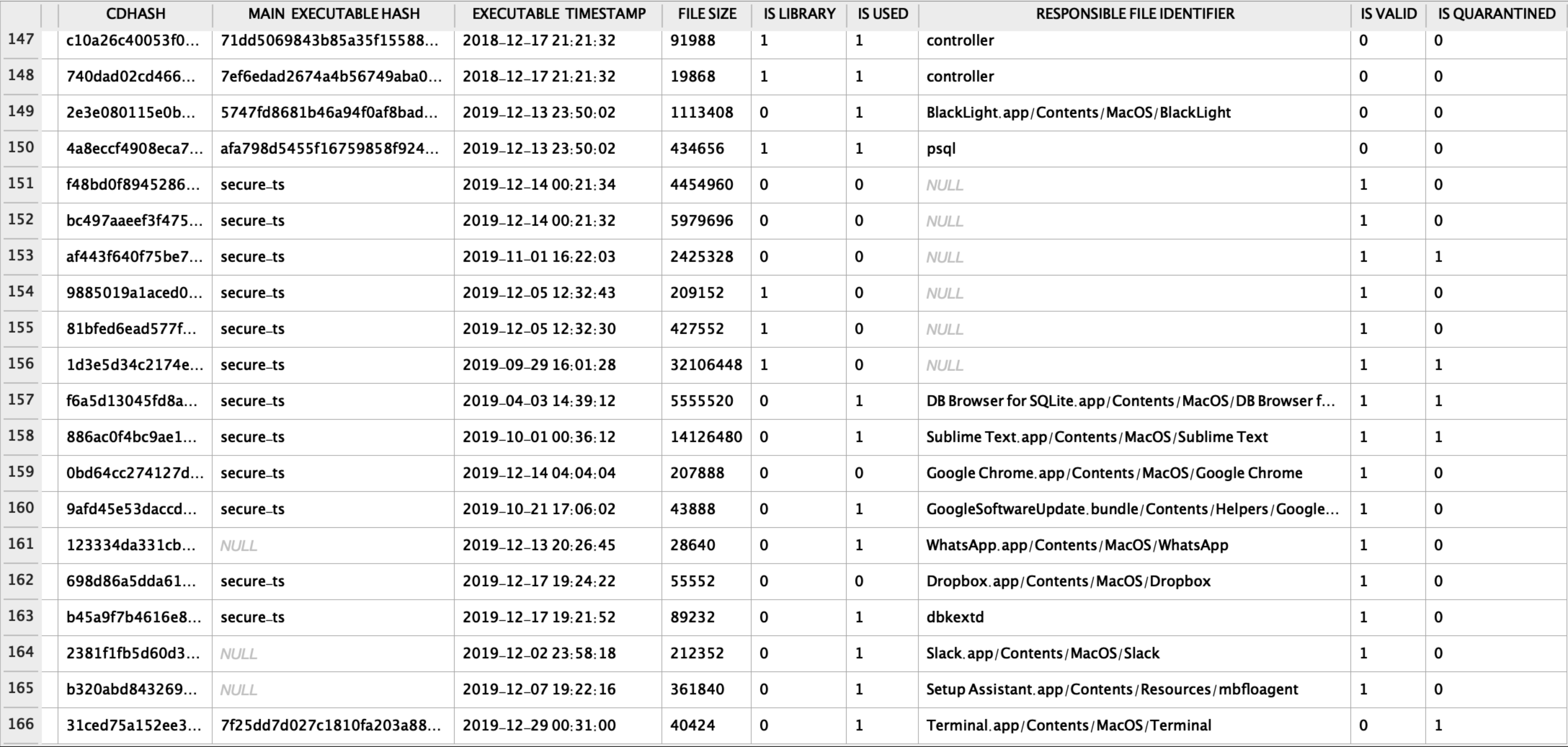
	TIMESTAMP	EVENT ID	AGENT BUNDLE ID	AGENT NAME	TYPE NUMBER	SENDER NAME	SENDER ADDRESS	ORIGIN TITLE	ORIGIN URL STRING	ORIGIN ALIAS	DATA URL STRING
876	2020-01-22 20:34:48	FB59D077-6533-4DC2-A622-DEACA21E17BB	com.apple.iChat	iChat	3	NULL	NULL	NULL	NULL	NULL	NULL
877	2020-01-23 01:02:20	89925659-67E0-49C9-AD8B-F808A1838DCA	com.apple.iChat	iChat	3	NULL	NULL	NULL	NULL	NULL	NULL
878	2020-01-23 01:02:20	752703AD-CE6F-4DC8-A378-FE91C156F2FA	com.apple.iChat	iChat	3	NULL	NULL	NULL	NULL	NULL	NULL
879	2020-01-23 01:58:59	4DF97DBC-A7FB-464C-9636-D9F4CD27B39C	NULL	sharingd	6	Sarah Edwards	NULL	NULL	NULL	NULL	NULL
880	2020-01-23 23:27:59	99D85A07-A83F-4DDF-AB1B-C6B4D112A67A	com.apple.iChat	iChat	3	NULL	NULL	NULL	NULL	NULL	NULL
881	2020-01-23 23:27:59	59ED5FA0-735D-48E2-BDC4-1E49A518CD3C	com.apple.iChat	iChat	3	NULL	NULL	NULL	NULL	NULL	NULL
882	2020-01-25 22:52:04	211951E3-17AC-4C36-85E0-89553383DCE9	com.google.Chrome	Chrome	0	NULL	NULL	NULL	https://twitter.com/S...	NULL	https://pbs.twimg.com/media/EOqlri...
883	2020-01-27 15:47:10	A101C9E9-61A0-4D62-B323-C7FC535F6464	com.apple.iChat	iChat	3	NULL	NULL	NULL	NULL	NULL	NULL
884	2020-01-27 15:47:10	F7360FFC-1AF3-4E60-BBF1-FEC816A29D7C	com.apple.iChat	iChat	3	NULL	NULL	NULL	NULL	NULL	NULL
885	2020-01-27 18:31:19	4471AF30-5D5F-4DBF-90BC-57C639AB5D08	com.apple.iChat	iChat	3	NULL	NULL	NULL	NULL	NULL	NULL
886	2020-01-27 18:31:19	2F9BC2F2-76CA-4829-BE1A-6D8834A49BEB	com.apple.iChat	iChat	3	NULL	NULL	NULL	NULL	NULL	NULL

ExecPolicy Exec Measurements (Part 1) –



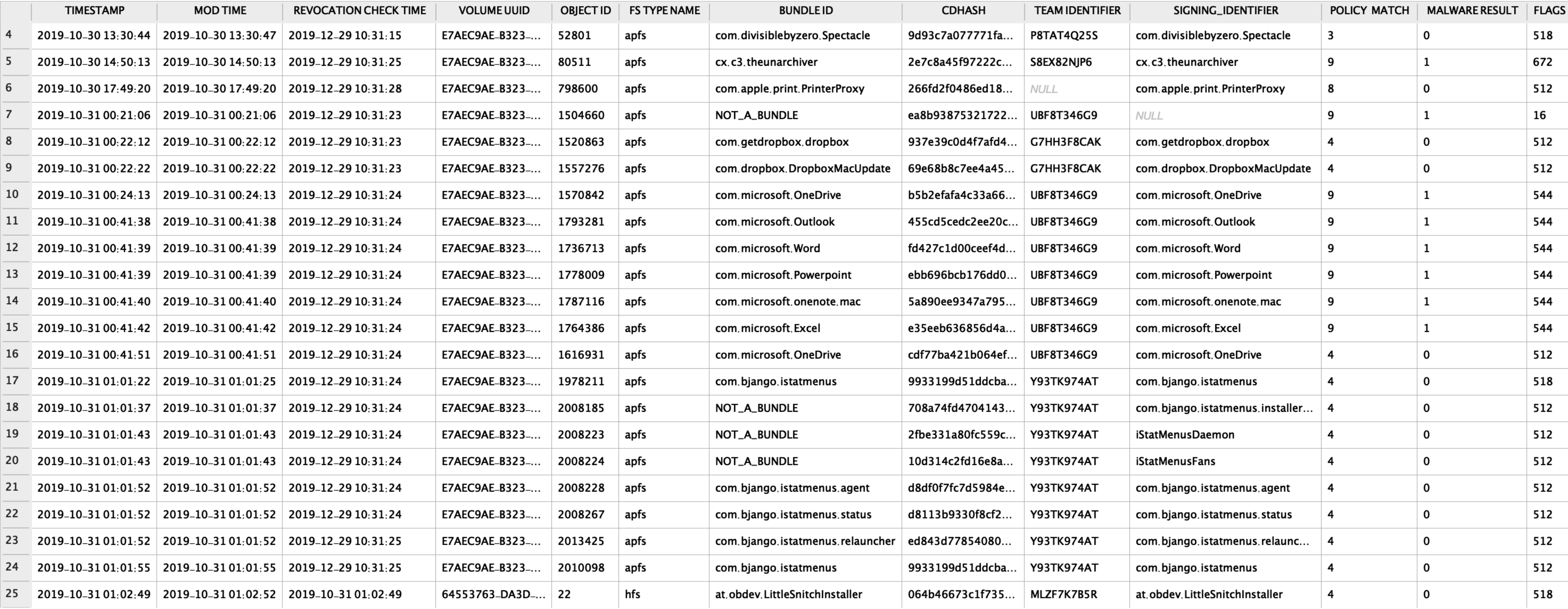
	TIMESTAMP	REPORTED TIMESTAMP	IS SIGNED	FILE IDENTIFIER	BUNDLE ID	BUNDLE VERSION	TEAM IDENTIFIER	SIGNING IDENTIFIER	CDHASH
147	2019-12-24 00:05:43	2019-12-27 15:13:59	0	libboost_filesystem-clang-dar...	NULL	NULL	NULL	NULL	c10a26c40053f0...
148	2019-12-24 00:05:43	2019-12-27 15:13:59	0	libboost_system-clang-darwin...	NULL	NULL	NULL	NULL	740dad02cd466...
149	2019-12-24 00:05:43	2019-12-27 15:13:59	0	psql	NULL	NULL	NULL	NULL	2e3e080115e0b...
150	2019-12-24 00:05:43	2019-12-27 15:13:59	0	libedit.0.dylib	NULL	NULL	NULL	NULL	4a8eccf4908eca7...
151	2019-12-24 00:05:44	2019-12-27 15:13:59	1	BBT License Server.app	com.blackbagtech.LicenseServer	1.1.0.3.7852	8A6E4V5B9Q	com.blackbagtech.LicenseServer	f48bd0f8945286...
152	2019-12-24 00:05:45	2019-12-27 15:13:59	1	EWMounter.app	com.blackbagtech.EWMounter	1.9.1.3.0	8A6E4V5B9Q	com.blackbagtech.EWMounter	bc497aaeef3f475...
153	2019-12-24 00:05:47	2019-12-27 15:13:59	1	Epoch Converter.app	com.blackbagtech.EpochConverter	2.2.0.3.0	8A6E4V5B9Q	com.blackbagtech.EpochConverter	af443f640f75be7...
154	2019-12-24 00:05:47	2019-12-27 15:13:59	1	OSXFUSE.prefPane	com.github.osxfuse.OSXFUSEPrefPane	3.10.4	3T5GSNBU6W	com.github.osxfuse.OSXFUSEPrefPane	9885019a1aced0...
155	2019-12-24 00:05:47	2019-12-27 15:13:59	1	OSXFUSE.framework	com.github.osxfuse.frameworks.OSXFUSE	3.10.4	3T5GSNBU6W	com.github.osxfuse.frameworks.OSXFUSE	81bfed6ead577f...
156	2019-12-24 00:05:52	2019-12-27 15:13:59	1	Synalyze It! Pro.app	com.synalyze-it.SynalyzeItPro	1.23.4	MT255CKDV9	com.synalyze-it.SynalyzeItPro	1d3e5d34c2174e...
157	2019-12-24 00:05:56	2019-12-27 15:13:59	1	DB Browser for SQLite.app	net.sourceforge.sqlitebrowser	3.11.2	C34AV33YLK	net.sourceforge.sqlitebrowser	f6a5d13045fd8a...
158	2019-12-26 11:15:20	2019-12-27 15:13:59	1	Sublime Text.app	com.sublimetext.3	3211	Z6D26JE4Y4	com.sublimetext.3	886ac0f4bc9ae1...
159	2019-12-26 11:19:39	2019-12-27 15:13:59	1	Google Chrome.app	com.google.Chrome	3945.88	EQHXZ8M8AV	com.google.Chrome	0bd64cc274127d...
160	2019-12-26 11:19:43	2019-12-27 15:13:59	1	GoogleSoftwareUpdate.bundle	com.google.Keystone	1.2.13.113	EQHXZ8M8AV	com.google.Keystone	9afd45e53daccd...
161	2019-12-26 11:23:50	2019-12-27 15:13:59	1	WhatsApp.app	desktop.WhatsApp	0.3.9309	57T9237FN3	desktop.WhatsApp	123334da331cb...
162	2019-12-26 11:35:34	2019-12-27 15:13:59	1	Dropbox.app	com.getdropbox.dropbox	87.4.138	G7HH3F8CAK	com.getdropbox.dropbox	698d86a5dda61...
163	2019-12-26 11:35:36	2019-12-27 15:13:59	1	dbkextd	NULL	NULL	G7HH3F8CAK	com.getdropbox.dropbox.dbkextd	b45a9f7b4616e8...
164	2019-12-26 11:37:29	2019-12-27 15:13:59	1	Slack.app	com.tinyspeck.slackmacgap	6209	BQR82RBBHL	com.tinyspeck.slackmacgap	2381f1fb5d60d3...
165	2019-12-26 11:37:35	2019-12-27 15:13:59	1	Keka.app	com.aone.keka	3378	4FG648TM2A	com.aone.keka	b320abd843269...
166	2019-12-29 10:31:18	1970-01-01 00:00:00	0	fsmon-osx.dms	NULL	NULL	NULL	NULL	31ced75a152ee3...

ExecPolicy – Exec Measurements (Part 2)



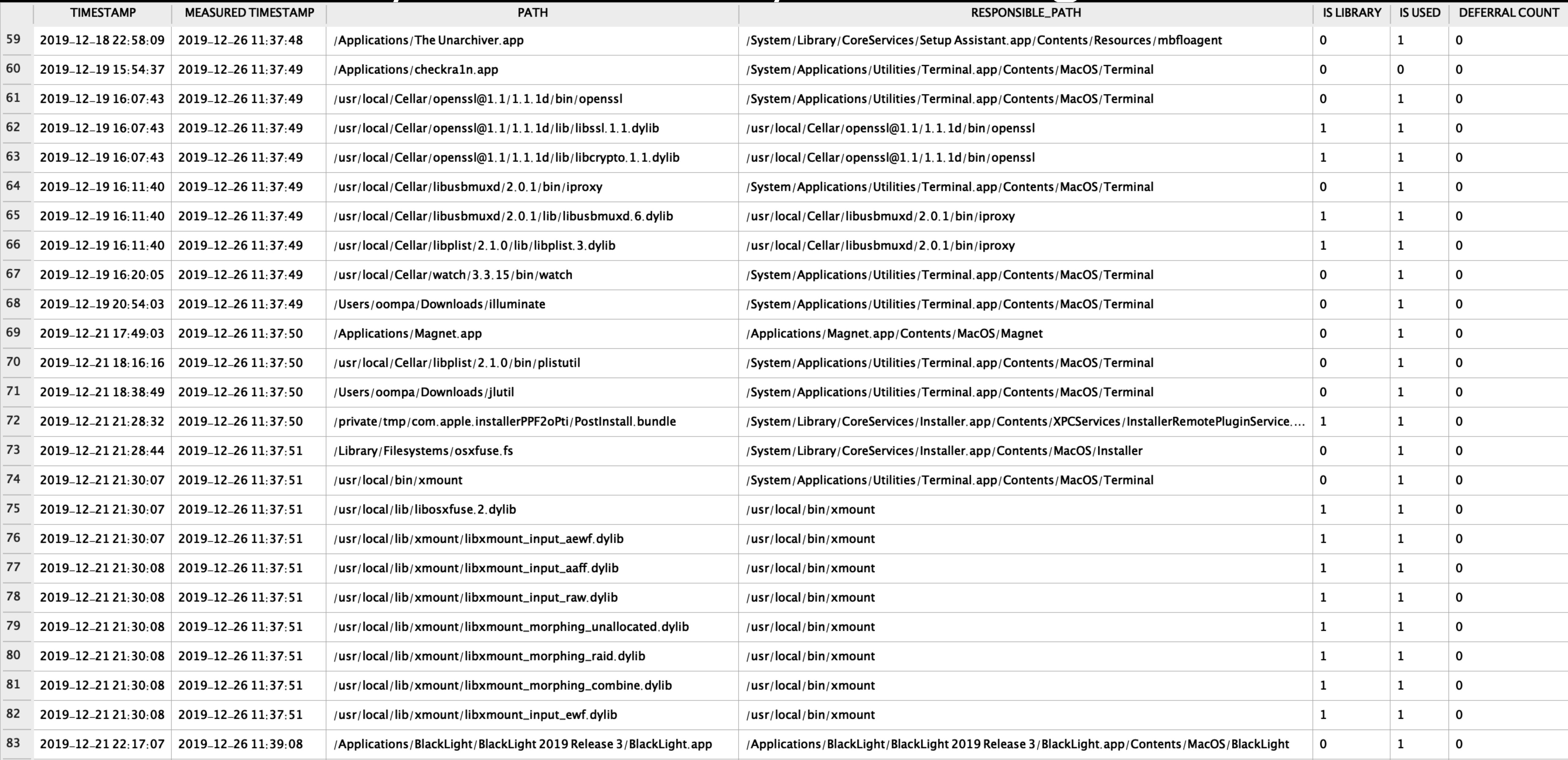
		CDHASH	MAIN EXECUTABLE HASH	EXECUTABLE TIMESTAMP	FILE SIZE	IS LIBRARY	IS USED	RESPONSIBLE FILE IDENTIFIER	IS VALID	IS QUARANTINED
147		c10a26c40053f0…	71dd5069843b85a35f15588…	2018-12-17 21:21:32	91988	1	1	controller	0	0
148		740dad02cd466…	7ef6edad2674a4b56749aba0…	2018-12-17 21:21:32	19868	1	1	controller	0	0
149		2e3e080115e0b…	5747fd8681b46a94f0af8bad…	2019-12-13 23:50:02	1113408	0	1	BlackLight.app/Contents/MacOS/BlackLight	0	0
150		4a8eccf4908eca7…	afa798d5455f16759858f924…	2019-12-13 23:50:02	434656	1	1	psql	0	0
151		f48bd0f8945286…	secure_ts	2019-12-14 00:21:34	4454960	0	0	NULL	1	0
152		bc497aaeef3f475…	secure_ts	2019-12-14 00:21:32	5979696	0	0	NULL	1	0
153		af443f640f75be7…	secure_ts	2019-11-01 16:22:03	2425328	0	0	NULL	1	1
154		9885019a1aced0…	secure_ts	2019-12-05 12:32:43	209152	1	0	NULL	1	0
155		81bfed6ead577f…	secure_ts	2019-12-05 12:32:30	427552	1	0	NULL	1	0
156		1d3e5d34c2174e…	secure_ts	2019-09-29 16:01:28	32106448	1	0	NULL	1	1
157		f6a5d13045fd8a…	secure_ts	2019-04-03 14:39:12	5555520	0	1	DB Browser for SQLite.app/Contents/MacOS/DB Browser f…	1	1
158		886ac0f4bc9ae1…	secure_ts	2019-10-01 00:36:12	14126480	0	1	Sublime Text.app/Contents/MacOS/Sublime Text	1	1
159		0bd64cc274127d…	secure_ts	2019-12-14 04:04:04	207888	0	0	Google Chrome.app/Contents/MacOS/Google Chrome	1	0
160		9afd45e53daccd…	secure_ts	2019-10-21 17:06:02	43888	0	1	GoogleSoftwareUpdate.bundle/Contents/Helpers/Google…	1	0
161		123334da331cb…	NULL	2019-12-13 20:26:45	28640	0	1	WhatsApp.app/Contents/MacOS/WhatsApp	1	0
162		698d86a5dda61…	secure_ts	2019-12-17 19:24:22	55552	0	0	Dropbox.app/Contents/MacOS/Dropbox	1	0
163		b45a9f7b4616e8…	secure_ts	2019-12-17 19:21:52	89232	0	1	dbkextd	1	0
164		2381f1fb5d60d3…	NULL	2019-12-02 23:58:18	212352	0	1	Slack.app/Contents/MacOS/Slack	1	0
165		b320abd843269…	NULL	2019-12-07 19:22:16	361840	0	1	Setup Assistant.app/Contents/Resources/mbfloagent	1	0
166		31ced75a152ee3…	7f25dd7d027c1810fa203a88…	2019-12-29 00:31:00	40424	0	1	Terminal.app/Contents/MacOS/Terminal	0	1

ExecPolicy – Exec Policy Scan



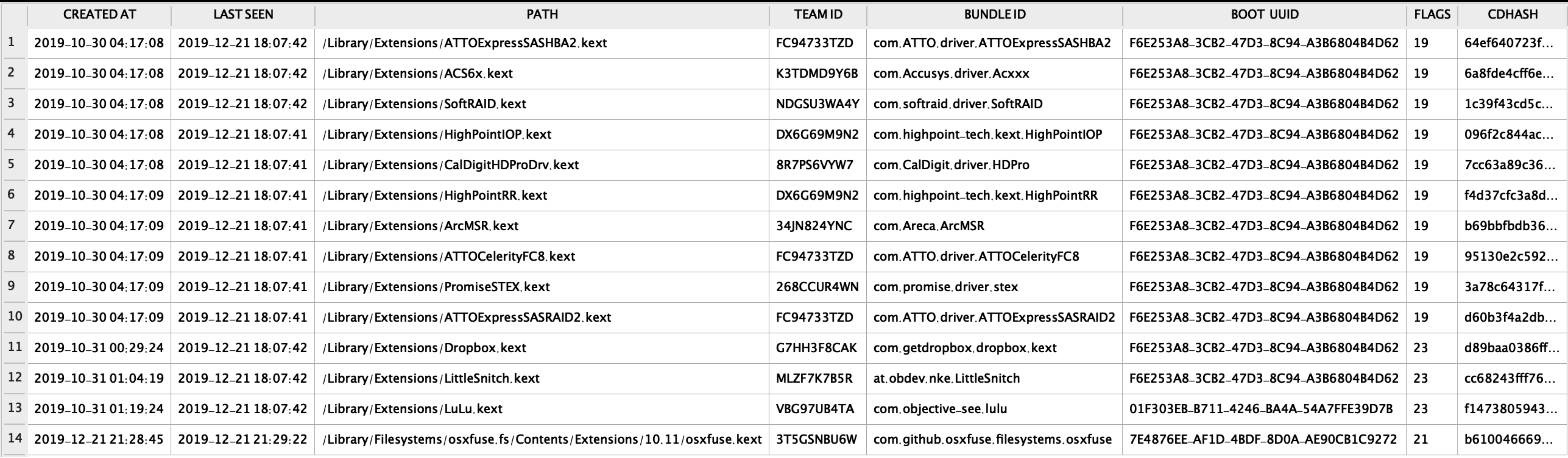
	TIMESTAMP	MOD TIME	REVOCATION CHECK TIME	VOLUME UUID	OBJECT ID	FS TYPE NAME	BUNDLE ID	CDHASH	TEAM IDENTIFIER	SIGNING_IDENTIFIER	POLICY MATCH	MALWARE RESULT	FLAGS
4	2019-10-30 13:30:44	2019-10-30 13:30:47	2019-12-29 10:31:15	E7AEC9AE-B323-…	52801	apfs	com.divisiblebyzero.Spectacle	9d93c7a077771fa…	P8TAT4Q25S	com.divisiblebyzero.Spectacle	3	0	518
5	2019-10-30 14:50:13	2019-10-30 14:50:13	2019-12-29 10:31:25	E7AEC9AE-B323-…	80511	apfs	cx.c3.theunarchiver	2e7c8a45f97222c…	S8EX82NJP6	cx.c3.theunarchiver	9	1	672
6	2019-10-30 17:49:20	2019-10-30 17:49:20	2019-12-29 10:31:28	E7AEC9AE-B323-…	798600	apfs	com.apple.print.PrinterProxy	266fd2f0486ed18…	NULL	com.apple.print.PrinterProxy	8	0	512
7	2019-10-31 00:21:06	2019-10-31 00:21:06	2019-12-29 10:31:23	E7AEC9AE-B323-…	1504660	apfs	NOT_A_BUNDLE	ea8b93875321722…	UBF8T346G9	NULL	9	1	16
8	2019-10-31 00:22:12	2019-10-31 00:22:12	2019-12-29 10:31:23	E7AEC9AE-B323-…	1520863	apfs	com.getdropbox.dropbox	937e39c0d4f7afd4…	G7HH3F8CAK	com.getdropbox.dropbox	4	0	512
9	2019-10-31 00:22:22	2019-10-31 00:22:22	2019-12-29 10:31:23	E7AEC9AE-B323-…	1557276	apfs	com.dropbox.DropboxMacUpdate	69e68b8c7ee4a45…	G7HH3F8CAK	com.dropbox.DropboxMacUpdate	4	0	512
10	2019-10-31 00:24:13	2019-10-31 00:24:13	2019-12-29 10:31:24	E7AEC9AE-B323-…	1570842	apfs	com.microsoft.OneDrive	b5b2efafa4c33a66…	UBF8T346G9	com.microsoft.OneDrive	9	1	544
11	2019-10-31 00:41:38	2019-10-31 00:41:38	2019-12-29 10:31:24	E7AEC9AE-B323-…	1793281	apfs	com.microsoft.Outlook	455cd5cedc2ee20c…	UBF8T346G9	com.microsoft.Outlook	9	1	544
12	2019-10-31 00:41:39	2019-10-31 00:41:39	2019-12-29 10:31:24	E7AEC9AE-B323-…	1736713	apfs	com.microsoft.Word	fd427c1d00ceef4d…	UBF8T346G9	com.microsoft.Word	9	1	544
13	2019-10-31 00:41:39	2019-10-31 00:41:39	2019-12-29 10:31:24	E7AEC9AE-B323-…	1778009	apfs	com.microsoft.Powerpoint	ebb696bcb176dd0…	UBF8T346G9	com.microsoft.Powerpoint	9	1	544
14	2019-10-31 00:41:40	2019-10-31 00:41:40	2019-12-29 10:31:24	E7AEC9AE-B323-…	1787116	apfs	com.microsoft.onenote.mac	5a890ee9347a795…	UBF8T346G9	com.microsoft.onenote.mac	9	1	544
15	2019-10-31 00:41:42	2019-10-31 00:41:42	2019-12-29 10:31:24	E7AEC9AE-B323-…	1764386	apfs	com.microsoft.Excel	e35eeb636856d4a…	UBF8T346G9	com.microsoft.Excel	9	1	544
16	2019-10-31 00:41:51	2019-10-31 00:41:51	2019-12-29 10:31:24	E7AEC9AE-B323-…	1616931	apfs	com.microsoft.OneDrive	cdf77ba421b064ef…	UBF8T346G9	com.microsoft.OneDrive	4	0	512
17	2019-10-31 01:01:22	2019-10-31 01:01:25	2019-12-29 10:31:24	E7AEC9AE-B323-…	1978211	apfs	com.bjango.istatmenus	9933199d51ddcba…	Y93TK974AT	com.bjango.istatmenus	4	0	518
18	2019-10-31 01:01:37	2019-10-31 01:01:37	2019-12-29 10:31:24	E7AEC9AE-B323-…	2008185	apfs	NOT_A_BUNDLE	708a74fd4704143…	Y93TK974AT	com.bjango.istatmenus.installer…	4	0	512
19	2019-10-31 01:01:43	2019-10-31 01:01:43	2019-12-29 10:31:24	E7AEC9AE-B323-…	2008223	apfs	NOT_A_BUNDLE	2fbe331a80fc559c…	Y93TK974AT	iStatMenusDaemon	4	0	512
20	2019-10-31 01:01:43	2019-10-31 01:01:43	2019-12-29 10:31:24	E7AEC9AE-B323-…	2008224	apfs	NOT_A_BUNDLE	10d314c2fd16e8a…	Y93TK974AT	iStatMenusFans	4	0	512
21	2019-10-31 01:01:52	2019-10-31 01:01:52	2019-12-29 10:31:24	E7AEC9AE-B323-…	2008228	apfs	com.bjango.istatmenus.agent	d8df0f7fc7d5984e…	Y93TK974AT	com.bjango.istatmenus.agent	4	0	512
22	2019-10-31 01:01:52	2019-10-31 01:01:52	2019-12-29 10:31:24	E7AEC9AE-B323-…	2008267	apfs	com.bjango.istatmenus.status	d8113b9330f8cf2…	Y93TK974AT	com.bjango.istatmenus.status	4	0	512
23	2019-10-31 01:01:52	2019-10-31 01:01:52	2019-12-29 10:31:25	E7AEC9AE-B323-…	2013425	apfs	com.bjango.istatmenus.relauncher	ed843d77854080…	Y93TK974AT	com.bjango.istatmenus.relaunc…	4	0	512
24	2019-10-31 01:01:55	2019-10-31 01:01:55	2019-12-29 10:31:25	E7AEC9AE-B323-…	2010098	apfs	com.bjango.istatmenus	9933199d51ddcba…	Y93TK974AT	com.bjango.istatmenus	4	0	512
25	2019-10-31 01:02:49	2019-10-31 01:02:52	2019-10-31 01:02:49	64553763-DA3D-…	22	hfs	at.obdev.LittleSnitchInstaller	064b46673c1f735…	MLZF7K7B5R	at.obdev.LittleSnitchInstaller	4	0	518

ExecPolicy – Exec Policy Scan Targets



	TIMESTAMP	MEASURED TIMESTAMP	PATH	RESPONSIBLE_PATH	IS LIBRARY	IS USED	DEFERRAL COUNT
59	2019-12-18 22:58:09	2019-12-26 11:37:48	/Applications/The Unarchiver.app	/System/Library/CoreServices/Setup Assistant.app/Contents/Resources/mbfloagent	0	1	0
60	2019-12-19 15:54:37	2019-12-26 11:37:49	/Applications/checkra1n.app	/System/Applications/Utilities/Terminal.app/Contents/MacOS/Terminal	0	0	0
61	2019-12-19 16:07:43	2019-12-26 11:37:49	/usr/local/Cellar/openssl@1.1/1.1.1d/bin/openssl	/System/Applications/Utilities/Terminal.app/Contents/MacOS/Terminal	0	1	0
62	2019-12-19 16:07:43	2019-12-26 11:37:49	/usr/local/Cellar/openssl@1.1/1.1.1d/lib/libssl.1.1.dylib	/usr/local/Cellar/openssl@1.1/1.1.1d/bin/openssl	1	1	0
63	2019-12-19 16:07:43	2019-12-26 11:37:49	/usr/local/Cellar/openssl@1.1/1.1.1d/lib/libcrypto.1.1.dylib	/usr/local/Cellar/openssl@1.1/1.1.1d/bin/openssl	1	1	0
64	2019-12-19 16:11:40	2019-12-26 11:37:49	/usr/local/Cellar/libusbmuxd/2.0.1/bin/iproxy	/System/Applications/Utilities/Terminal.app/Contents/MacOS/Terminal	0	1	0
65	2019-12-19 16:11:40	2019-12-26 11:37:49	/usr/local/Cellar/libusbmuxd/2.0.1/lib/libusbmuxd.6.dylib	/usr/local/Cellar/libusbmuxd/2.0.1/bin/iproxy	1	1	0
66	2019-12-19 16:11:40	2019-12-26 11:37:49	/usr/local/Cellar/libplist/2.1.0/lib/libplist.3.dylib	/usr/local/Cellar/libusbmuxd/2.0.1/bin/iproxy	1	1	0
67	2019-12-19 16:20:05	2019-12-26 11:37:49	/usr/local/Cellar/watch/3.3.15/bin/watch	/System/Applications/Utilities/Terminal.app/Contents/MacOS/Terminal	0	1	0
68	2019-12-19 20:54:03	2019-12-26 11:37:49	/Users/oompa/Downloads/illuminate	/System/Applications/Utilities/Terminal.app/Contents/MacOS/Terminal	0	1	0
69	2019-12-21 17:49:03	2019-12-26 11:37:50	/Applications/Magnet.app	/Applications/Magnet.app/Contents/MacOS/Magnet	0	1	0
70	2019-12-21 18:16:16	2019-12-26 11:37:50	/usr/local/Cellar/libplist/2.1.0/bin/plistutil	/System/Applications/Utilities/Terminal.app/Contents/MacOS/Terminal	0	1	0
71	2019-12-21 18:38:49	2019-12-26 11:37:50	/Users/oompa/Downloads/jlutil	/System/Applications/Utilities/Terminal.app/Contents/MacOS/Terminal	0	1	0
72	2019-12-21 21:28:32	2019-12-26 11:37:50	/private/tmp/com.apple.installerPPF2oPti/PostInstall.bundle	/System/Library/CoreServices/Installer.app/Contents/XPCServices/InstallerRemotePluginService.…	1	1	0
73	2019-12-21 21:28:44	2019-12-26 11:37:51	/Library/Filesystems/osxfuse.fs	/System/Library/CoreServices/Installer.app/Contents/MacOS/Installer	0	1	0
74	2019-12-21 21:30:07	2019-12-26 11:37:51	/usr/local/bin/xmount	/System/Applications/Utilities/Terminal.app/Contents/MacOS/Terminal	0	1	0
75	2019-12-21 21:30:07	2019-12-26 11:37:51	/usr/local/lib/libosxfuse.2.dylib	/usr/local/bin/xmount	1	1	0
76	2019-12-21 21:30:07	2019-12-26 11:37:51	/usr/local/lib/xmount/libxmount_input_aewf.dylib	/usr/local/bin/xmount	1	1	0
77	2019-12-21 21:30:08	2019-12-26 11:37:51	/usr/local/lib/xmount/libxmount_input_aaff.dylib	/usr/local/bin/xmount	1	1	0
78	2019-12-21 21:30:08	2019-12-26 11:37:51	/usr/local/lib/xmount/libxmount_input_raw.dylib	/usr/local/bin/xmount	1	1	0
79	2019-12-21 21:30:08	2019-12-26 11:37:51	/usr/local/lib/xmount/libxmount_morphing_unallocated.dylib	/usr/local/bin/xmount	1	1	0
80	2019-12-21 21:30:08	2019-12-26 11:37:51	/usr/local/lib/xmount/libxmount_morphing_raid.dylib	/usr/local/bin/xmount	1	1	0
81	2019-12-21 21:30:08	2019-12-26 11:37:51	/usr/local/lib/xmount/libxmount_morphing_combine.dylib	/usr/local/bin/xmount	1	1	0
82	2019-12-21 21:30:08	2019-12-26 11:37:51	/usr/local/lib/xmount/libxmount_input_ewf.dylib	/usr/local/bin/xmount	1	1	0
83	2019-12-21 22:17:07	2019-12-26 11:39:08	/Applications/BlackLight/BlackLight 2019 Release 3/BlackLight.app	/Applications/BlackLight/BlackLight 2019 Release 3/BlackLight.app/Contents/MacOS/BlackLight	0	1	0

KextPolicy – Kext Load History



	CREATED AT	LAST SEEN	PATH	TEAM ID	BUNDLE ID	BOOT UUID	FLAGS	CDHASH
1	2019-10-30 04:17:08	2019-12-21 18:07:42	/Library/Extensions/ATTOExpressSASHBA2.kext	FC94733TZD	com.ATTO.driver.ATTOExpressSASHBA2	F6E253A8-3CB2-47D3-8C94-A3B6804B4D62	19	64ef640723f...
2	2019-10-30 04:17:08	2019-12-21 18:07:42	/Library/Extensions/ACS6x.kext	K3TDMD9Y6B	com.Accusys.driver.Acxxx	F6E253A8-3CB2-47D3-8C94-A3B6804B4D62	19	6a8fde4cff6e...
3	2019-10-30 04:17:08	2019-12-21 18:07:42	/Library/Extensions/SoftRAID.kext	NDGSU3WA4Y	com.softraid.driver.SoftRAID	F6E253A8-3CB2-47D3-8C94-A3B6804B4D62	19	1c39f43cd5c...
4	2019-10-30 04:17:08	2019-12-21 18:07:41	/Library/Extensions/HighPointIOP.kext	DX6G69M9N2	com.highpoint-tech.kext.HighPointIOP	F6E253A8-3CB2-47D3-8C94-A3B6804B4D62	19	096f2c844ac...
5	2019-10-30 04:17:08	2019-12-21 18:07:41	/Library/Extensions/CalDigitHDProDrv.kext	8R7PS6VYW7	com.CalDigit.driver.HDPro	F6E253A8-3CB2-47D3-8C94-A3B6804B4D62	19	7cc63a89c36...
6	2019-10-30 04:17:09	2019-12-21 18:07:41	/Library/Extensions/HighPointRR.kext	DX6G69M9N2	com.highpoint-tech.kext.HighPointRR	F6E253A8-3CB2-47D3-8C94-A3B6804B4D62	19	f4d37cfc3a8d...
7	2019-10-30 04:17:09	2019-12-21 18:07:41	/Library/Extensions/ArcMSR.kext	34JN824YNC	com.Areca.ArcMSR	F6E253A8-3CB2-47D3-8C94-A3B6804B4D62	19	b69bbfbdb36...
8	2019-10-30 04:17:09	2019-12-21 18:07:41	/Library/Extensions/ATTOCelerityFC8.kext	FC94733TZD	com.ATTO.driver.ATTOCelerityFC8	F6E253A8-3CB2-47D3-8C94-A3B6804B4D62	19	95130e2c592...
9	2019-10-30 04:17:09	2019-12-21 18:07:41	/Library/Extensions/PromiseSTEX.kext	268CCUR4WN	com.promise.driver.stex	F6E253A8-3CB2-47D3-8C94-A3B6804B4D62	19	3a78c64317f...
10	2019-10-30 04:17:09	2019-12-21 18:07:41	/Library/Extensions/ATTOExpressSASRAID2.kext	FC94733TZD	com.ATTO.driver.ATTOExpressSASRAID2	F6E253A8-3CB2-47D3-8C94-A3B6804B4D62	19	d60b3f4a2db...
11	2019-10-31 00:29:24	2019-12-21 18:07:42	/Library/Extensions/Dropbox.kext	G7HH3F8CAK	com.getdropbox.dropbox.kext	F6E253A8-3CB2-47D3-8C94-A3B6804B4D62	23	d89baa0386ff...
12	2019-10-31 01:04:19	2019-12-21 18:07:42	/Library/Extensions/LittleSnitch.kext	MLZF7K7B5R	at.obdev.nke.LittleSnitch	F6E253A8-3CB2-47D3-8C94-A3B6804B4D62	23	cc68243fff76...
13	2019-10-31 01:19:24	2019-12-21 18:07:42	/Library/Extensions/LuLu.kext	VBG97UB4TA	com.objective-see.lulu	01F303EB-B711-4246-BA4A-54A7FFE39D7B	23	f1473805943...
14	2019-12-21 21:28:45	2019-12-21 21:29:22	/Library/Filesystems/osxfuse.fs/Contents/Extensions/10.11/osxfuse.kext	3T5GSNBU6W	com.github.osxfuse.filesystems.osxfuse	7E4876EE-AF1D-4BDF-8D0A-AE90CB1C9272	21	b610046669...

Why APOLLO? Put the puzzle together!

Scenario:

Doing quality assurance research about sinks (no, not really)

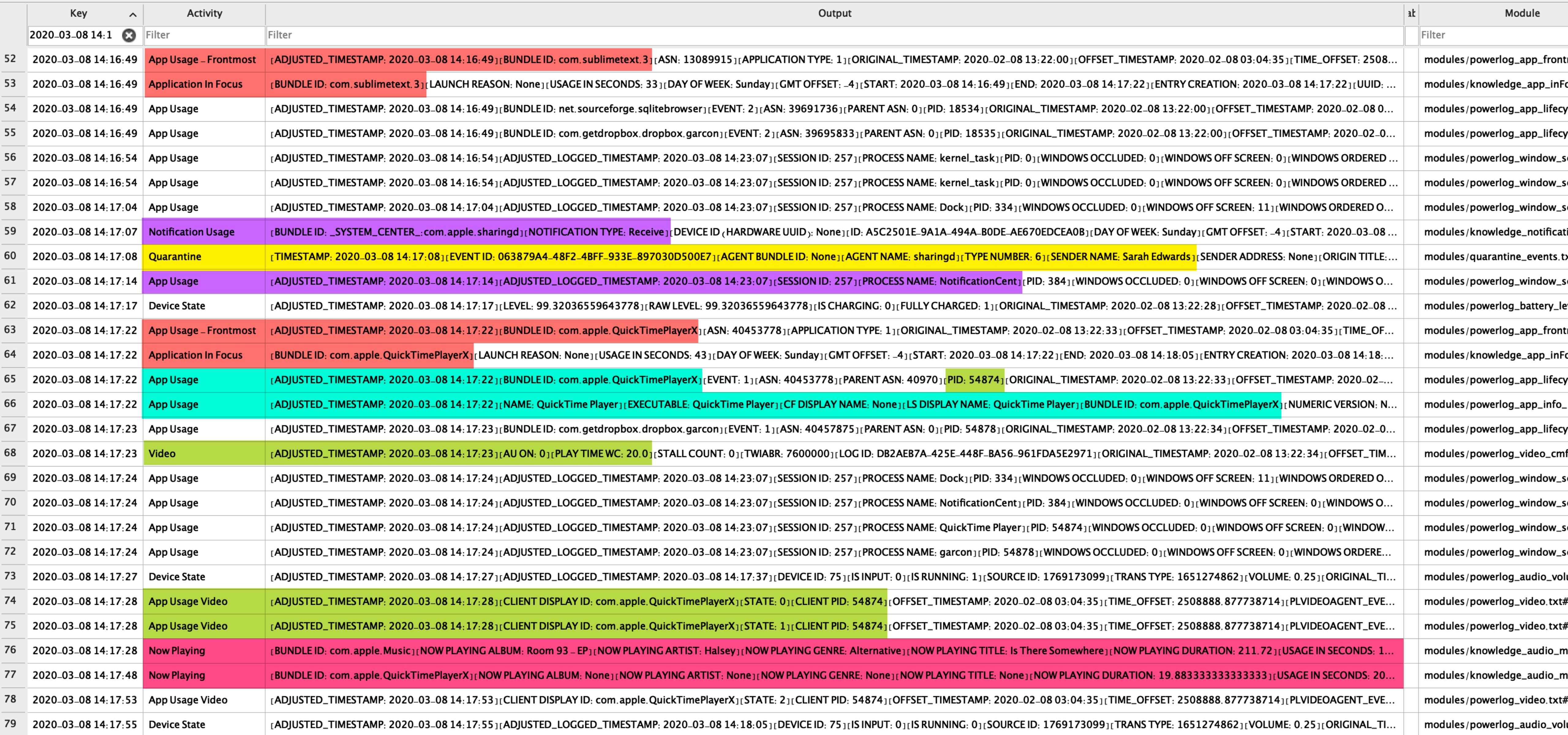
Need a video for a presentation

Got a great one on my iPhone!

Send to my laptop via AirDrop (sharingd)

Open and watch video before putting it into my super exciting Sink QA presentation

Why APOLLO? Put the puzzle together!



	Key ^	Activity	Output	ak	Module
	2020-03-08 14:1 ⊗	Filter	Filter		Filter
52	2020-03-08 14:16:49	App Usage - Frontmost	[ADJUSTED_TIMESTAMP: 2020-03-08 14:16:49][BUNDLE ID: com.sublimetext.3][ASN: 13089915][APPLICATION TYPE: 1][ORIGINAL_TIMESTAMP: 2020-02-08 13:22:00][OFFSET_TIMESTAMP: 2020-02-08 03:04:35][TIME_OFFSET: 2508…		modules/powerlog_app_front
53	2020-03-08 14:16:49	Application In Focus	[BUNDLE ID: com.sublimetext.3][LAUNCH REASON: None][USAGE IN SECONDS: 33][DAY OF WEEK: Sunday][GMT OFFSET: -4][START: 2020-03-08 14:16:49][END: 2020-03-08 14:17:22][ENTRY CREATION: 2020-03-08 14:17:22][UUID: …		modules/knowledge_app_inFo
54	2020-03-08 14:16:49	App Usage	[ADJUSTED_TIMESTAMP: 2020-03-08 14:16:49][BUNDLE ID: net.sourceforge.sqlitebrowser][EVENT: 2][ASN: 39691736][PARENT ASN: 0][PID: 18534][ORIGINAL_TIMESTAMP: 2020-02-08 13:22:00][OFFSET_TIMESTAMP: 2020-02-08 0…		modules/powerlog_app_lifecy
55	2020-03-08 14:16:49	App Usage	[ADJUSTED_TIMESTAMP: 2020-03-08 14:16:49][BUNDLE ID: com.getdropbox.dropbox.garcon][EVENT: 2][ASN: 39695833][PARENT ASN: 0][PID: 18535][ORIGINAL_TIMESTAMP: 2020-02-08 13:22:00][OFFSET_TIMESTAMP: 2020-02-0…		modules/powerlog_app_lifecy
56	2020-03-08 14:16:54	App Usage	[ADJUSTED_TIMESTAMP: 2020-03-08 14:16:54][ADJUSTED_LOGGED_TIMESTAMP: 2020-03-08 14:23:07][SESSION ID: 257][PROCESS NAME: kernel_task][PID: 0][WINDOWS OCCLUDED: 0][WINDOWS OFF SCREEN: 0][WINDOWS ORDERED …		modules/powerlog_window_s
57	2020-03-08 14:16:54	App Usage	[ADJUSTED_TIMESTAMP: 2020-03-08 14:16:54][ADJUSTED_LOGGED_TIMESTAMP: 2020-03-08 14:23:07][SESSION ID: 257][PROCESS NAME: kernel_task][PID: 0][WINDOWS OCCLUDED: 0][WINDOWS OFF SCREEN: 0][WINDOWS ORDERED …		modules/powerlog_window_s
58	2020-03-08 14:17:04	App Usage	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:04][ADJUSTED_LOGGED_TIMESTAMP: 2020-03-08 14:23:07][SESSION ID: 257][PROCESS NAME: Dock][PID: 334][WINDOWS OCCLUDED: 0][WINDOWS OFF SCREEN: 11][WINDOWS ORDERED O…		modules/powerlog_window_s
59	2020-03-08 14:17:07	Notification Usage	[BUNDLE ID: _SYSTEM_CENTER_:com.apple.sharingd][NOTIFICATION TYPE: Receive][DEVICE ID (HARDWARE UUID): None][ID: A5C2501E-9A1A-494A-B0DE-AE670EDCEA0B][DAY OF WEEK: Sunday][GMT OFFSET: -4][START: 2020-03-08 …		modules/knowledge_notificati
60	2020-03-08 14:17:08	Quarantine	[TIMESTAMP: 2020-03-08 14:17:08][EVENT ID: 063879A4-48F2-4BFF-933E-897030D500E7][AGENT BUNDLE ID: None][AGENT NAME: sharingd][TYPE NUMBER: 6][SENDER NAME: Sarah Edwards][SENDER ADDRESS: None][ORIGIN TITLE:…		modules/quarantine_events.tx
61	2020-03-08 14:17:14	App Usage	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:14][ADJUSTED_LOGGED_TIMESTAMP: 2020-03-08 14:23:07][SESSION ID: 257][PROCESS NAME: NotificationCent][PID: 384][WINDOWS OCCLUDED: 0][WINDOWS OFF SCREEN: 0][WINDOWS O…		modules/powerlog_window_s
62	2020-03-08 14:17:17	Device State	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:17][LEVEL: 99.32036559643778][RAW LEVEL: 99.32036559643778][IS CHARGING: 0][FULLY CHARGED: 1][ORIGINAL_TIMESTAMP: 2020-02-08 13:22:28][OFFSET_TIMESTAMP: 2020-02-08 …		modules/powerlog_battery_le
63	2020-03-08 14:17:22	App Usage - Frontmost	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:22][BUNDLE ID: com.apple.QuickTimePlayerX][ASN: 40453778][APPLICATION TYPE: 1][ORIGINAL_TIMESTAMP: 2020-02-08 13:22:33][OFFSET_TIMESTAMP: 2020-02-08 03:04:35][TIME_OF…		modules/powerlog_app_front
64	2020-03-08 14:17:22	Application In Focus	[BUNDLE ID: com.apple.QuickTimePlayerX][LAUNCH REASON: None][USAGE IN SECONDS: 43][DAY OF WEEK: Sunday][GMT OFFSET: -4][START: 2020-03-08 14:17:22][END: 2020-03-08 14:18:05][ENTRY CREATION: 2020-03-08 14:18:…		modules/knowledge_app_inFo
65	2020-03-08 14:17:22	App Usage	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:22][BUNDLE ID: com.apple.QuickTimePlayerX][EVENT: 1][ASN: 40453778][PARENT ASN: 40970][PID: 54874][ORIGINAL_TIMESTAMP: 2020-02-08 13:22:33][OFFSET_TIMESTAMP: 2020-02-…		modules/powerlog_app_lifecy
66	2020-03-08 14:17:22	App Usage	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:22][NAME: QuickTime Player][EXECUTABLE: QuickTime Player][CF DISPLAY NAME: None][LS DISPLAY NAME: QuickTime Player][BUNDLE ID: com.apple.QuickTimePlayerX][NUMERIC VERSION: N…		modules/powerlog_app_info_
67	2020-03-08 14:17:23	App Usage	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:23][BUNDLE ID: com.getdropbox.dropbox.garcon][EVENT: 1][ASN: 40457875][PARENT ASN: 0][PID: 54878][ORIGINAL_TIMESTAMP: 2020-02-08 13:22:34][OFFSET_TIMESTAMP: 2020-02-0…		modules/powerlog_app_lifecy
68	2020-03-08 14:17:23	Video	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:23][AU ON: 0][PLAY TIME WC: 20.0][STALL COUNT: 0][TWIABR: 7600000][LOG ID: DB2AEB7A-425E-448F-BA56-961FDA5E2971][ORIGINAL_TIMESTAMP: 2020-02-08 13:22:34][OFFSET_TIM…		modules/powerlog_video_cmf
69	2020-03-08 14:17:24	App Usage	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:24][ADJUSTED_LOGGED_TIMESTAMP: 2020-03-08 14:23:07][SESSION ID: 257][PROCESS NAME: Dock][PID: 334][WINDOWS OCCLUDED: 0][WINDOWS OFF SCREEN: 11][WINDOWS ORDERED O…		modules/powerlog_window_s
70	2020-03-08 14:17:24	App Usage	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:24][ADJUSTED_LOGGED_TIMESTAMP: 2020-03-08 14:23:07][SESSION ID: 257][PROCESS NAME: NotificationCent][PID: 384][WINDOWS OCCLUDED: 0][WINDOWS OFF SCREEN: 0][WINDOWS O…		modules/powerlog_window_s
71	2020-03-08 14:17:24	App Usage	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:24][ADJUSTED_LOGGED_TIMESTAMP: 2020-03-08 14:23:07][SESSION ID: 257][PROCESS NAME: QuickTime Player][PID: 54874][WINDOWS OCCLUDED: 0][WINDOWS OFF SCREEN: 0][WINDOW…		modules/powerlog_window_s
72	2020-03-08 14:17:24	App Usage	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:24][ADJUSTED_LOGGED_TIMESTAMP: 2020-03-08 14:23:07][SESSION ID: 257][PROCESS NAME: garcon][PID: 54878][WINDOWS OCCLUDED: 0][WINDOWS OFF SCREEN: 0][WINDOWS ORDERE…		modules/powerlog_window_s
73	2020-03-08 14:17:27	Device State	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:27][ADJUSTED_LOGGED_TIMESTAMP: 2020-03-08 14:17:37][DEVICE ID: 75][IS INPUT: 0][IS RUNNING: 1][SOURCE ID: 1769173099][TRANS TYPE: 1651274862][VOLUME: 0.25][ORIGINAL_TI…		modules/powerlog_audio_volu
74	2020-03-08 14:17:28	App Usage Video	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:28][CLIENT DISPLAY ID: com.apple.QuickTimePlayerX][STATE: 0][CLIENT PID: 54874][OFFSET_TIMESTAMP: 2020-02-08 03:04:35][TIME_OFFSET: 2508888.877738714][PLVIDEOAGENT_EVE…		modules/powerlog_video.txt#
75	2020-03-08 14:17:28	App Usage Video	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:28][CLIENT DISPLAY ID: com.apple.QuickTimePlayerX][STATE: 1][CLIENT PID: 54874][OFFSET_TIMESTAMP: 2020-02-08 03:04:35][TIME_OFFSET: 2508888.877738714][PLVIDEOAGENT_EVE…		modules/powerlog_video.txt#
76	2020-03-08 14:17:28	Now Playing	[BUNDLE ID: com.apple.Music][NOW PLAYING ALBUM: Room 93 - EP][NOW PLAYING ARTIST: Halsey][NOW PLAYING GENRE: Alternative][NOW PLAYING TITLE: Is There Somewhere][NOW PLAYING DURATION: 211.72][USAGE IN SECONDS: 1…		modules/knowledge_audio_m
77	2020-03-08 14:17:48	Now Playing	[BUNDLE ID: com.apple.QuickTimePlayerX][NOW PLAYING ALBUM: None][NOW PLAYING ARTIST: None][NOW PLAYING GENRE: None][NOW PLAYING TITLE: None][NOW PLAYING DURATION: 19.883333333333333][USAGE IN SECONDS: 20…		modules/knowledge_audio_m
78	2020-03-08 14:17:53	App Usage Video	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:53][CLIENT DISPLAY ID: com.apple.QuickTimePlayerX][STATE: 2][CLIENT PID: 54874][OFFSET_TIMESTAMP: 2020-02-08 03:04:35][TIME_OFFSET: 2508888.877738714][PLVIDEOAGENT_EVE…		modules/powerlog_video.txt#
79	2020-03-08 14:17:55	Device State	[ADJUSTED_TIMESTAMP: 2020-03-08 14:17:55][ADJUSTED_LOGGED_TIMESTAMP: 2020-03-08 14:18:05][DEVICE ID: 75][IS INPUT: 0][IS RUNNING: 0][SOURCE ID: 1769173099][TRANS TYPE: 1651274862][VOLUME: 0.25][ORIGINAL_TI…		modules/powerlog_audio_volu

So…What’s Next?

These modules – Will Release Soon!

github.com/mac4n6/APOLLO

Support for older macOS (back to 10.13 at least)

Who wants to write Android/Windows/etc modules?

- Current support with `[-p other -v yolo]`
- Happy to build in ‘official’ `-v` versions when modules created.

Powerlog Gzip’ed Log Files

More Mac & iOS modules!

- Native Application Specific
- Output Options - Improved CSV/Separate CSV, JSON

Contact Me!

@iamevltwin | mac4n6.com | for518.com | sarah@blackbagtech.com