The iOS of Sauron: How iOS Tracks Everything You Do

Sarah Edwards | oompa@csh.rit.edu | @iamevltwin | mac4n6.com

whoami

General Forensics Nerd & Mac Fan Girl

Government Contractor in Northern Virginia

- I'm hiring a Mobile Forensic Engineer! Contact me! http://bit.ly/1qGWAmT

Author & Instructor for SANS FOR518 – Mac Forensic Analysis

- www.sans.org/course/mac-forensic-analysis
- August/September – Virginia Beach, VA
- September – Las Vegas, NV
- October – Prague, CZ

Contact Info

- oompa@csh.rit.edu
- @iamevltwin
- mac4n6.com

PATTERN OF LIFE

- Application Usage
- Device State
- Health
- Location

INFO & CAVEATS

Jailbroken Device

- Files discussed are not available without root/physical access to the device.
  - Except Health databases if backup is encrypted.
- Capture files while screen unlocked. (Some are encrypted when device is locked)

Timestamps - Never Trust Implicitly

- Different Storage Formats
- Some differ from actual event time (Always, always, always test before you report wrong data!)

Data Retention

- Each database/file is different, each table in the database is different
- iOS versions may adjust these.
- Data Retentions in this presentation are what I see in my own data - yours may differ.

Work in Progress

- I reserve the right to change update the details of this presentation to reflect new research.
- Find updated copies of this presentation on mac4n6.com

Test Devices

- iPhone 6 (iOS 9.0.2), Apple Watch 1 (watchOS 2.0)

DATA FILES
FILE PATH & DETAILS

- **CoreDuet** - /private/var/mobile/Library/CoreDuet/
  - **coreduetd.db** (31 Tables)
  - coreduetdClassA.db (31 Tables)
  - **coreduetdClassD.db** (31 Tables)
  - Knowledge/knowledgeC.db (5 Tables)
  - People/interactionC.db (9 Tables)
- **Aggregate Dictionary** - /private/var/mobile/Library/AggregateDictionary/
  - ADDataStore.sqlitedb (4 Tables)
- **Battery Life (PowerLog)** - /private/var/mobile/Library/BatteryLife/
  - **CurrentPowerlog.PLSQL** (257 Tables)
  - Archives/powerlog_YYYY-MM-DD_XXXXXXXX.PLQSQL.gz (Previous ~5 Days)

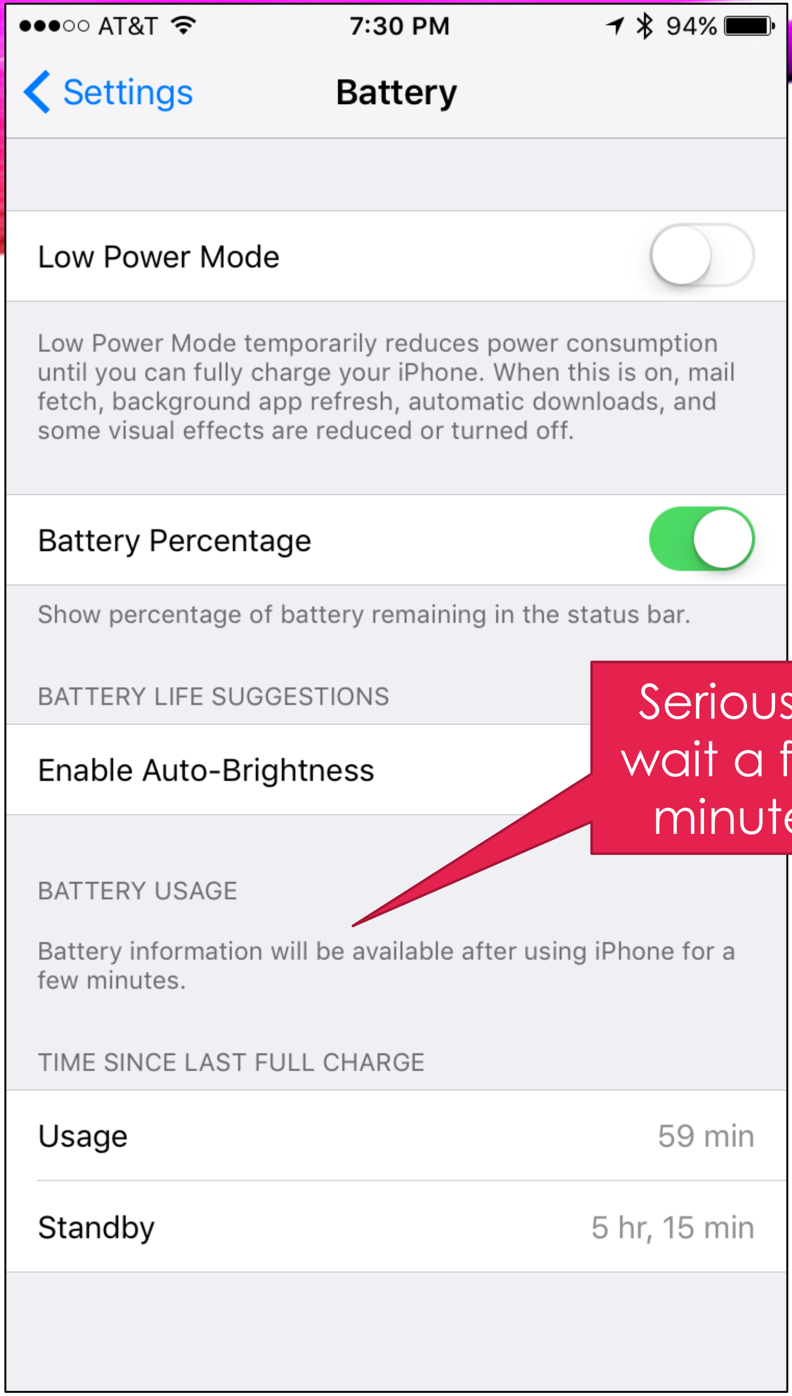
Note:
Files highlighted are discussed in this presentation.

DATA FILES
FILE PATH & DETAILS

- **networkd** - /private/var/networkd/
  - netusage.sqlite (13 Tables)
- **Health** - /private/var/mobile/Library/Health/
  - **healthdb.sqlite** (11 Tables)
  - **healthdb_secure.sqlite** (16 Tables)
- **routined** - /private/var/mobile/Library/Caches/com.apple.routined/
  - **cache_encryptedB.db** (5 Tables)
  - **StateModel1.archive**
  - **StateModel2.archive**
- **locationd** - /private/var/root/Library/Caches/locationd/
  - **cache_encryptedA.db** (79 Tables)
  - **lockCache_encryptedA.db** (51 Tables)
  - **cache_encryptedB.db** (167 Tables)
  - cache_encryptedC.db (9 Tables)

APPLICATION USAGE

APP BATTERY USAGE TIME



●●●○○ AT&T 7:30 PM 94%

< Settings **Battery**

Low Power Mode ○

Low Power Mode temporarily reduces power consumption until you can fully charge your iPhone. When this is on, mail fetch, background app refresh, automatic downloads, and some visual effects are reduced or turned off.

Battery Percentage ●

Show percentage of battery remaining in the status bar.

BATTERY LIFE SUGGESTIONS

Enable Auto-Brightness

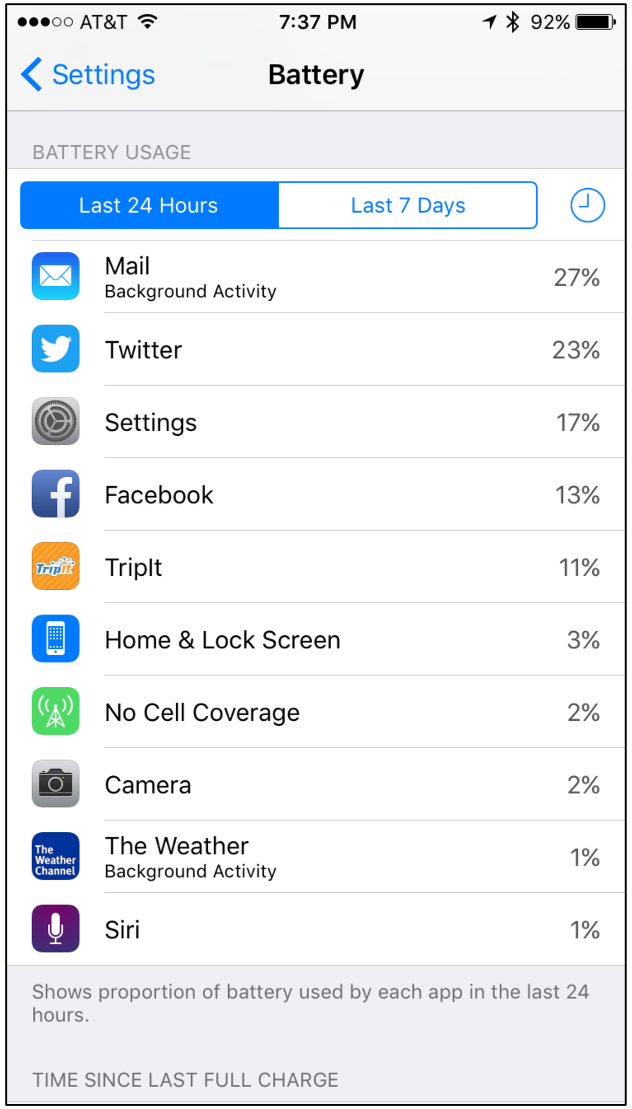
BATTERY USAGE

Battery information will be available after using iPhone for a few minutes.

TIME SINCE LAST FULL CHARGE

Usage	59 min
Standby	5 hr, 15 min

Seriously, wait a few minutes



●●●○○ AT&T 7:37 PM 92%

< Settings **Battery**

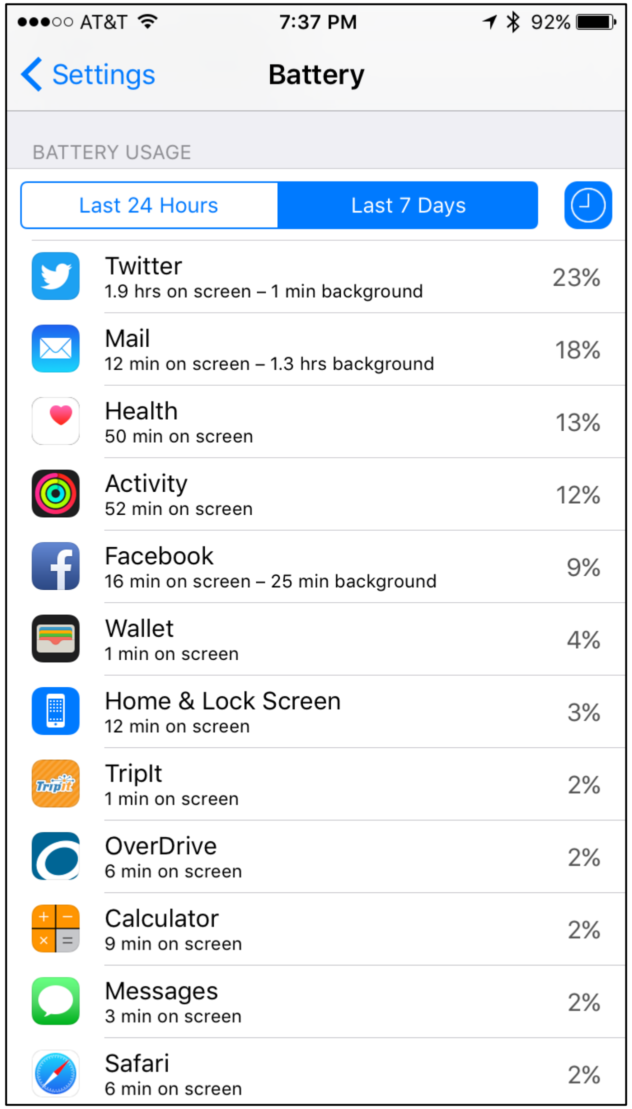
BATTERY USAGE

[Last 24 Hours] Last 7 Days

Mail Background Activity	27%
Twitter	23%
Settings	17%
Facebook	13%
TripIt	11%
Home & Lock Screen	3%
No Cell Coverage	2%
Camera	2%
The Weather Background Activity	1%
Siri	1%

Shows proportion of battery used by each app in the last 24 hours.

TIME SINCE LAST FULL CHARGE



●●●○○ AT&T 7:37 PM 92%

< Settings **Battery**

BATTERY USAGE

Last 24 Hours [Last 7 Days]

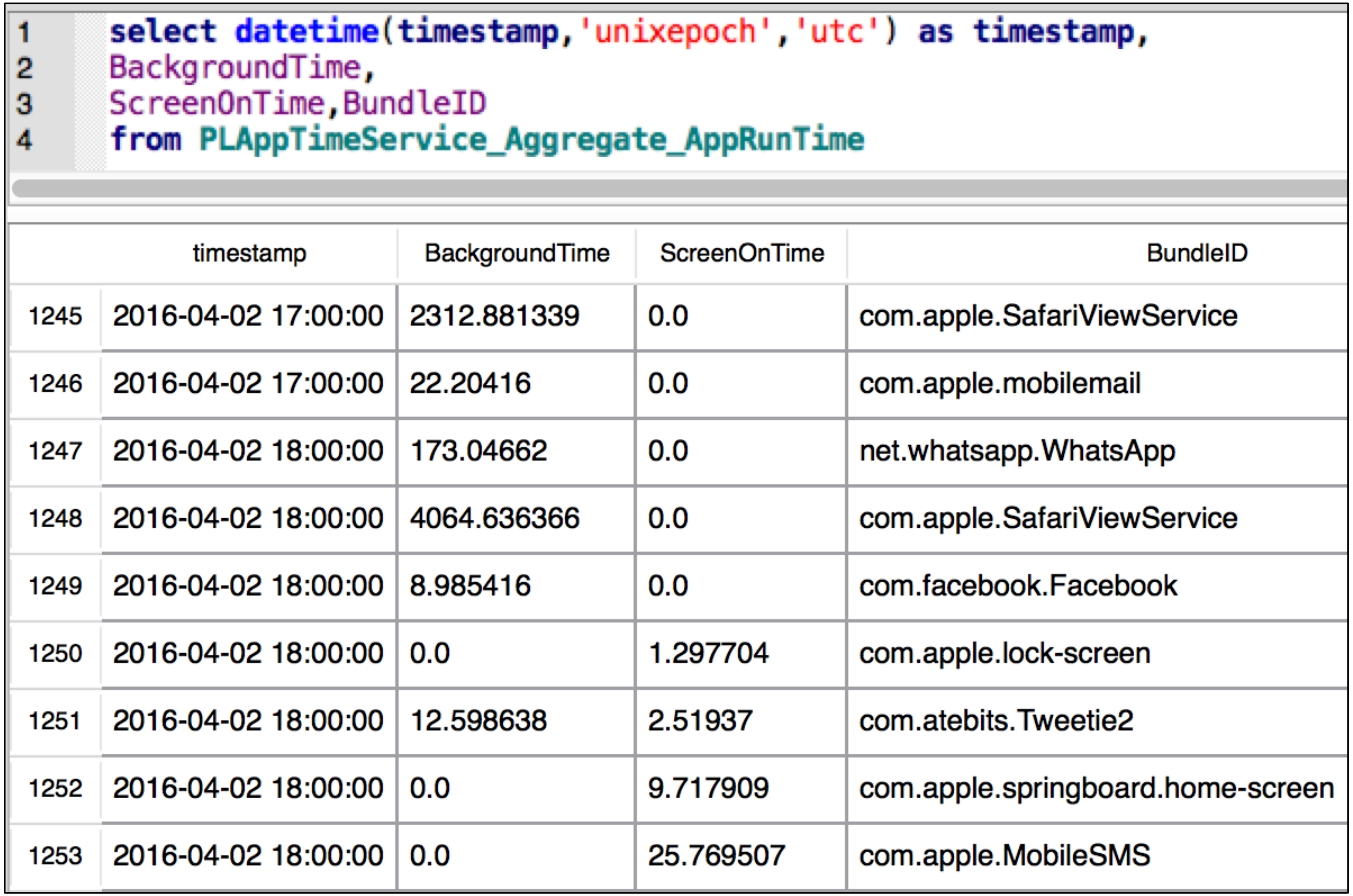
Twitter 1.9 hrs on screen – 1 min background	23%
Mail 12 min on screen – 1.3 hrs background	18%
Health 50 min on screen	13%
Activity 52 min on screen	12%
Facebook 16 min on screen – 25 min background	9%
Wallet 1 min on screen	4%
Home & Lock Screen 12 min on screen	3%
TripIt 1 min on screen	2%
OverDrive 6 min on screen	2%
Calculator 9 min on screen	2%
Messages 3 min on screen	2%
Safari 6 min on screen	2%

APP USAGE TIME
CurrentPowerlog.PLSQL

Data Retention:
~2 Weeks
(Don't Forget Powerlog Archives!)

Timestamps:
Accurate
Per Day, Per Hour

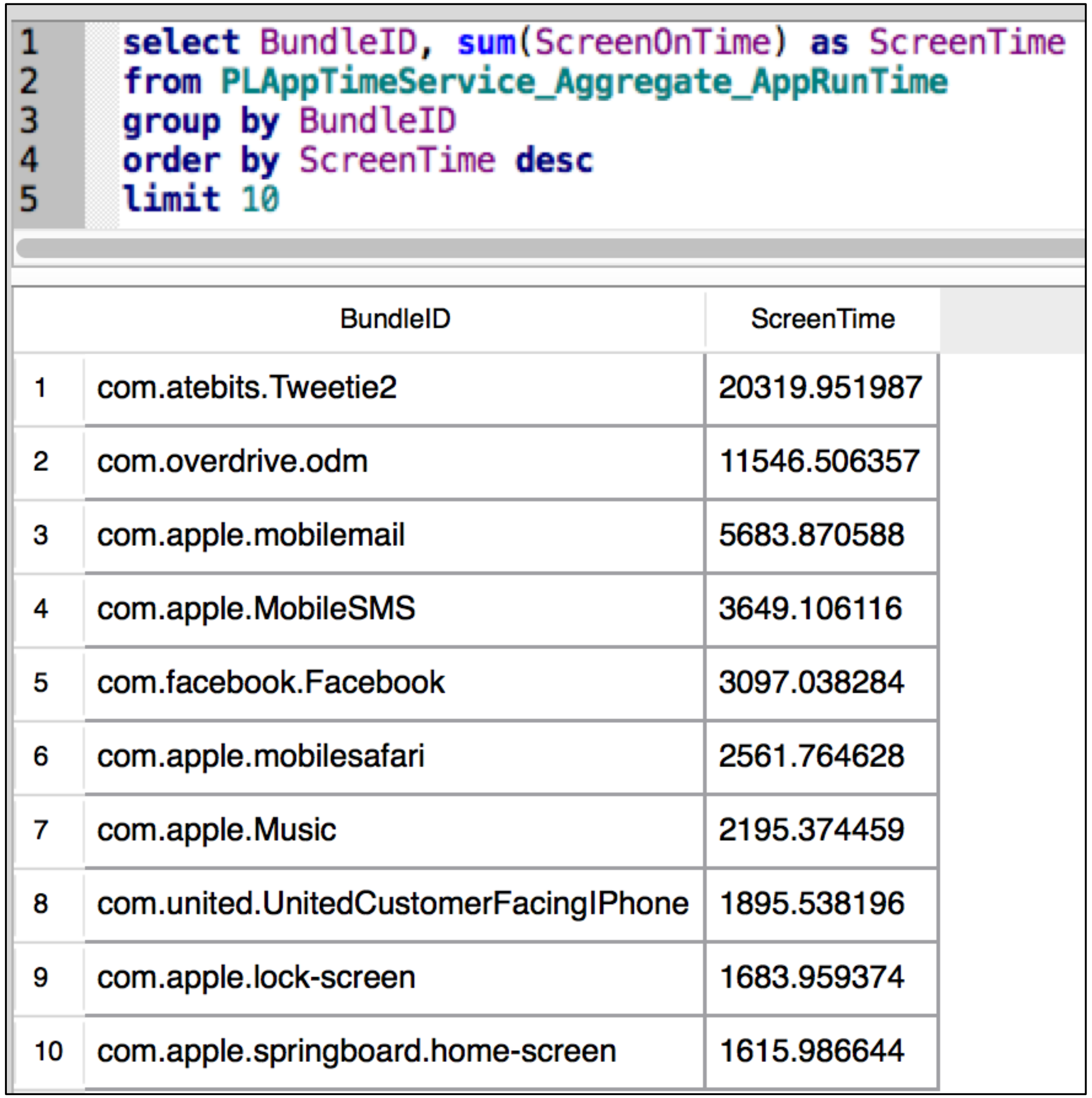
Timing:
In Seconds



```sql
select datetime(timestamp,'unixepoch','utc') as timestamp,
BackgroundTime,
ScreenOnTime,BundleID
from PLAppTimeService_Aggregate_AppRunTime
```

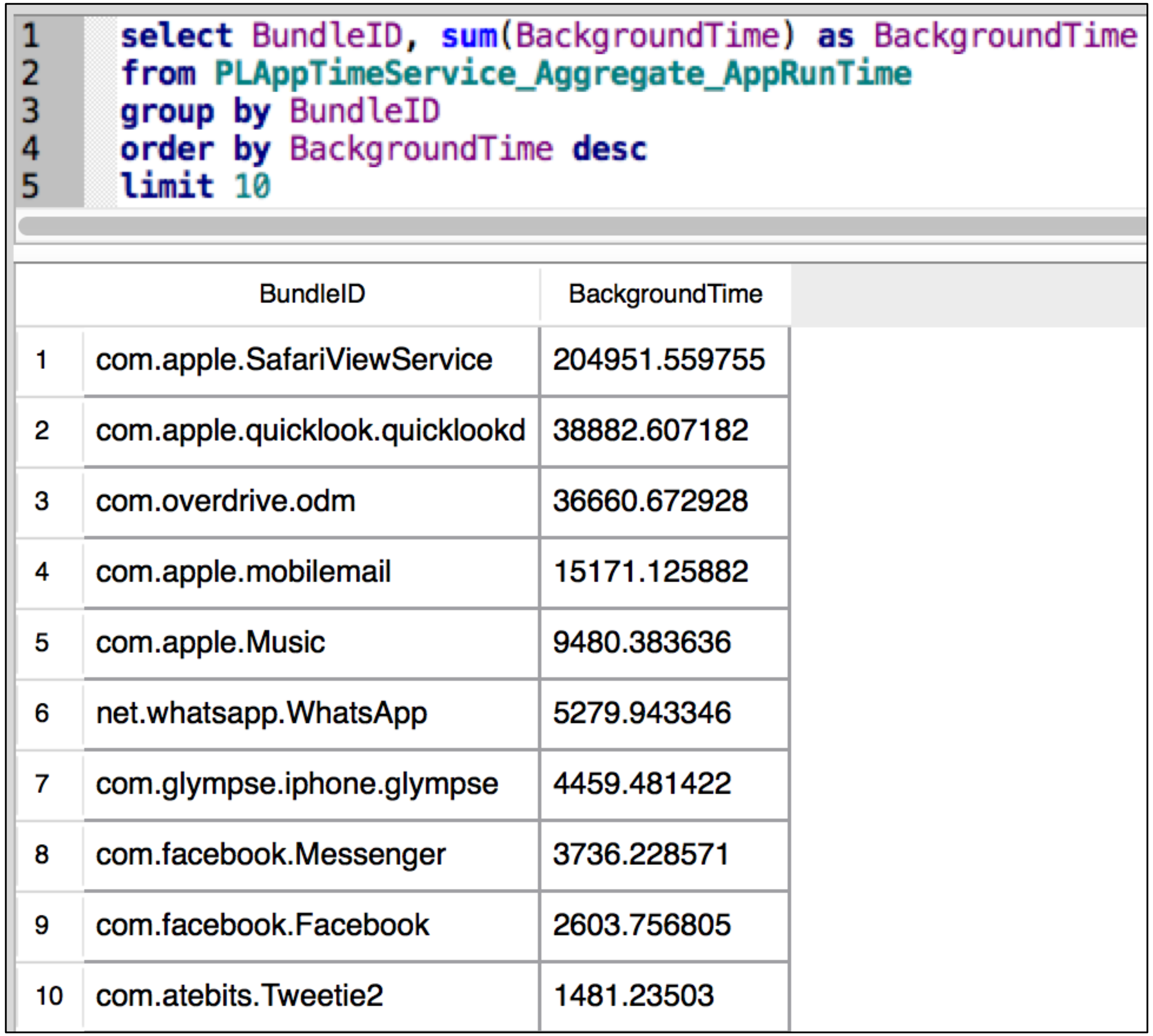
	timestamp	BackgroundTime	ScreenOnTime	BundleID
1245	2016-04-02 17:00:00	2312.881339	0.0	com.apple.SafariViewService
1246	2016-04-02 17:00:00	22.20416	0.0	com.apple.mobilemail
1247	2016-04-02 18:00:00	173.04662	0.0	net.whatsapp.WhatsApp
1248	2016-04-02 18:00:00	4064.636366	0.0	com.apple.SafariViewService
1249	2016-04-02 18:00:00	8.985416	0.0	com.facebook.Facebook
1250	2016-04-02 18:00:00	0.0	1.297704	com.apple.lock-screen
1251	2016-04-02 18:00:00	12.598638	2.51937	com.atebits.Tweetie2
1252	2016-04-02 18:00:00	0.0	9.717909	com.apple.springboard.home-screen
1253	2016-04-02 18:00:00	0.0	25.769507	com.apple.MobileSMS

APP USAGE - BY TIME
CurrentPowerlog.PLSQL



```
select BundleID, sum(ScreenOnTime) as ScreenTime
from PLAppTimeService_Aggregate_AppRunTime
group by BundleID
order by ScreenTime desc
limit 10
```

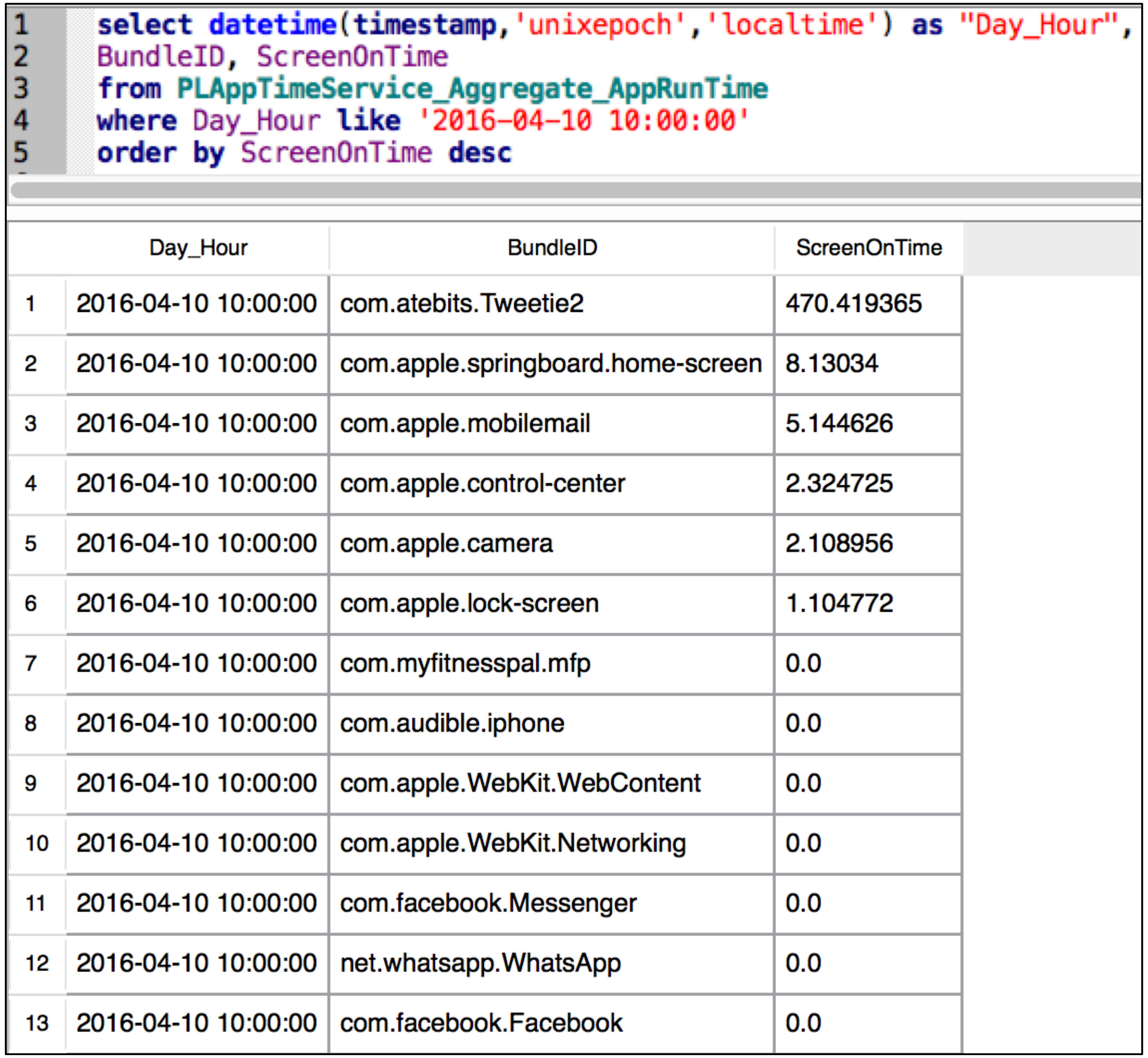
	BundleID	ScreenTime
1	com.atebits.Tweetie2	20319.951987
2	com.overdrive.odm	11546.506357
3	com.apple.mobilemail	5683.870588
4	com.apple.MobileSMS	3649.106116
5	com.facebook.Facebook	3097.038284
6	com.apple.mobilesafari	2561.764628
7	com.apple.Music	2195.374459
8	com.united.UnitedCustomerFacingIPhone	1895.538196
9	com.apple.lock-screen	1683.959374
10	com.apple.springboard.home-screen	1615.986644



```
select BundleID, sum(BackgroundTime) as BackgroundTime
from PLAppTimeService_Aggregate_AppRunTime
group by BundleID
order by BackgroundTime desc
limit 10
```

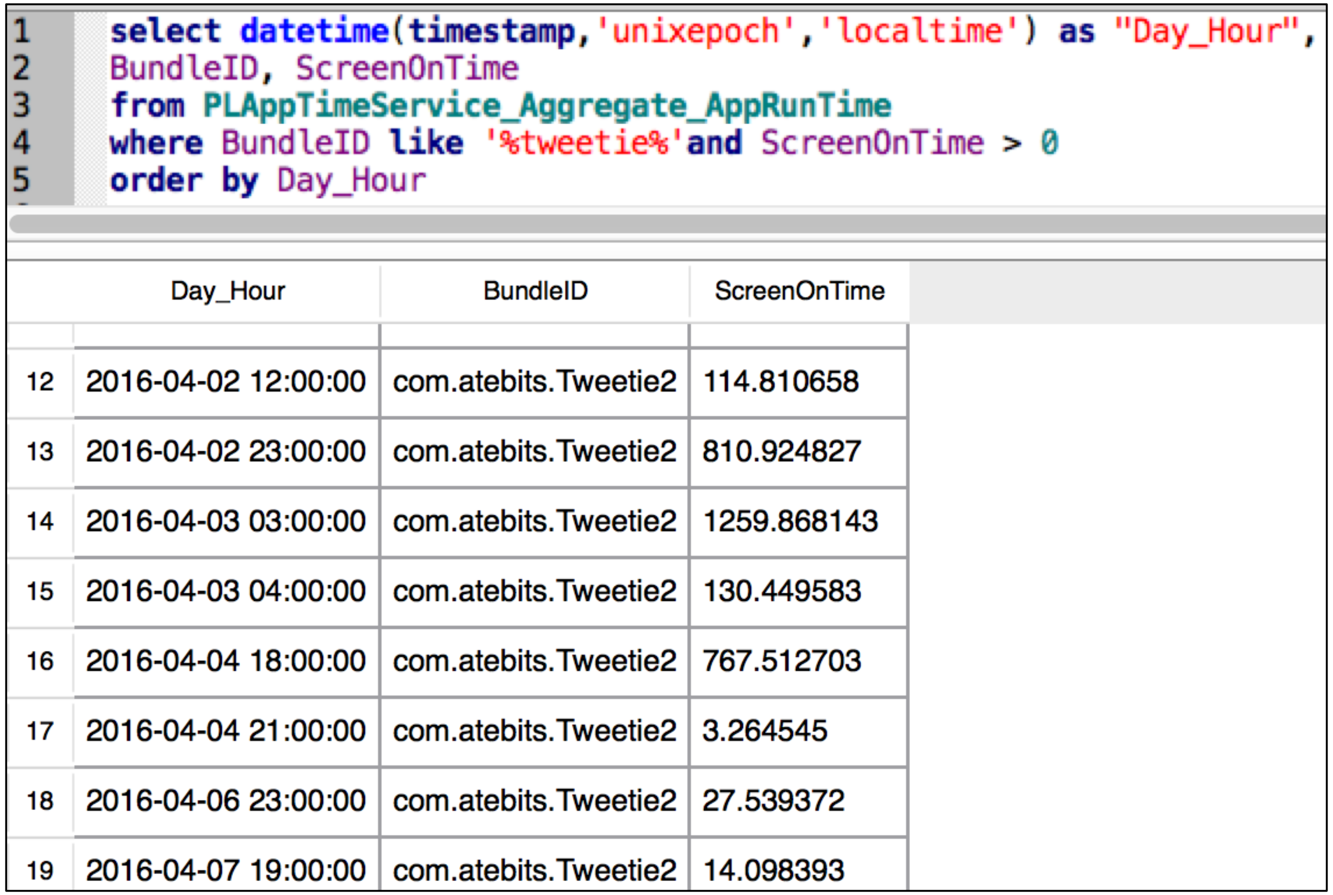
	BundleID	BackgroundTime
1	com.apple.SafariViewService	204951.559755
2	com.apple.quicklook.quicklookd	38882.607182
3	com.overdrive.odm	36660.672928
4	com.apple.mobilemail	15171.125882
5	com.apple.Music	9480.383636
6	net.whatsapp.WhatsApp	5279.943346
7	com.glympse.iphone.glympse	4459.481422
8	com.facebook.Messenger	3736.228571
9	com.facebook.Facebook	2603.756805
10	com.atebits.Tweetie2	1481.23503

APP USAGE - BY HOUR OR BY APP CurrentPowerlog.PLSQL



```
select datetime(timestamp,'unixepoch','localtime') as "Day_Hour",
BundleID, ScreenOnTime
from PLAppTimeService_Aggregate_AppRunTime
where Day_Hour like '2016-04-10 10:00:00'
order by ScreenOnTime desc
```

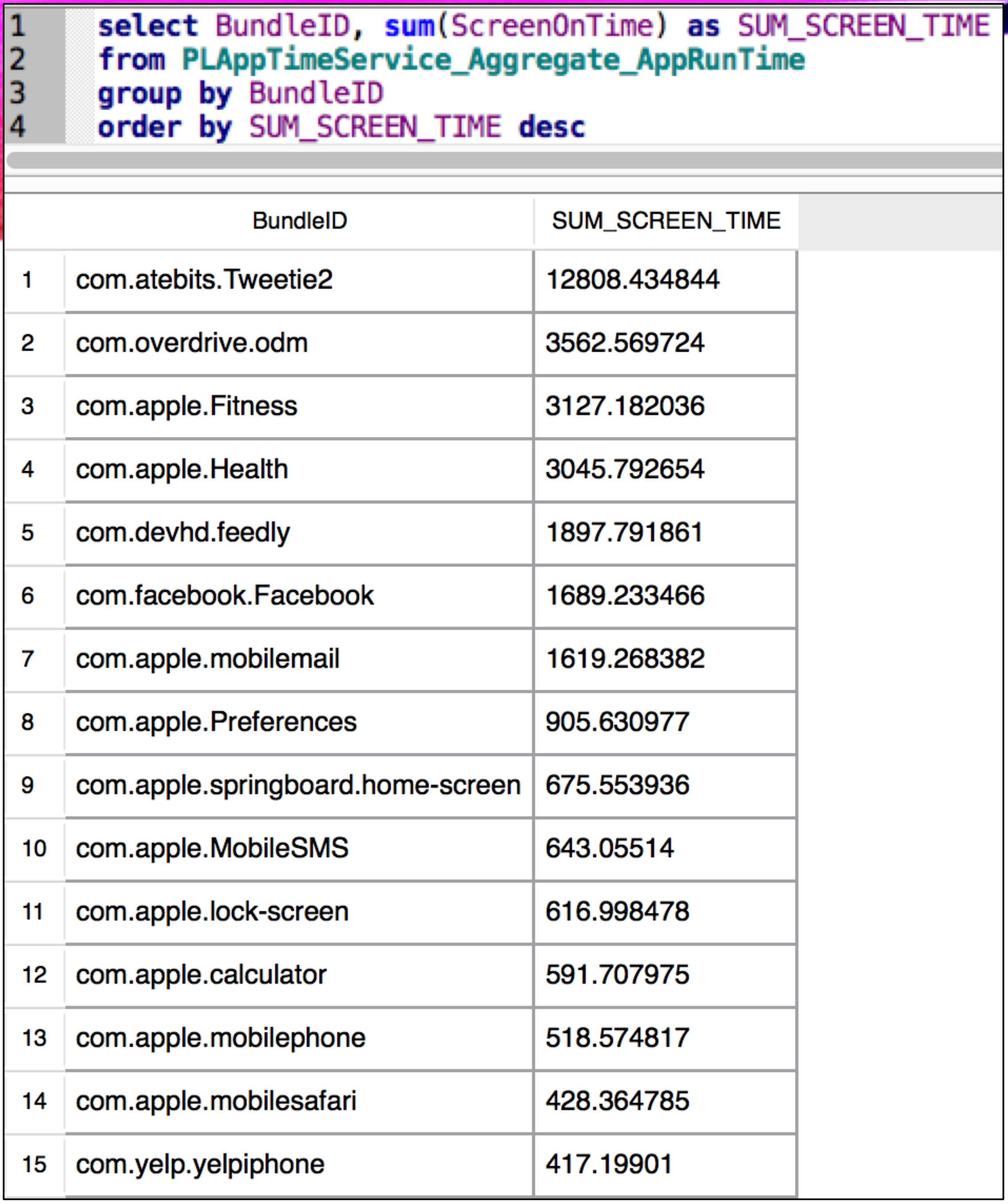
	Day_Hour	BundleID	ScreenOnTime
1	2016-04-10 10:00:00	com.atebits.Tweetie2	470.419365
2	2016-04-10 10:00:00	com.apple.springboard.home-screen	8.13034
3	2016-04-10 10:00:00	com.apple.mobilemail	5.144626
4	2016-04-10 10:00:00	com.apple.control-center	2.324725
5	2016-04-10 10:00:00	com.apple.camera	2.108956
6	2016-04-10 10:00:00	com.apple.lock-screen	1.104772
7	2016-04-10 10:00:00	com.myfitnesspal.mfp	0.0
8	2016-04-10 10:00:00	com.audible.iphone	0.0
9	2016-04-10 10:00:00	com.apple.WebKit.WebContent	0.0
10	2016-04-10 10:00:00	com.apple.WebKit.Networking	0.0
11	2016-04-10 10:00:00	com.facebook.Messenger	0.0
12	2016-04-10 10:00:00	net.whatsapp.WhatsApp	0.0
13	2016-04-10 10:00:00	com.facebook.Facebook	0.0



```
select datetime(timestamp,'unixepoch','localtime') as "Day_Hour",
BundleID, ScreenOnTime
from PLAppTimeService_Aggregate_AppRunTime
where BundleID like '%tweetie%'and ScreenOnTime > 0
order by Day_Hour
```

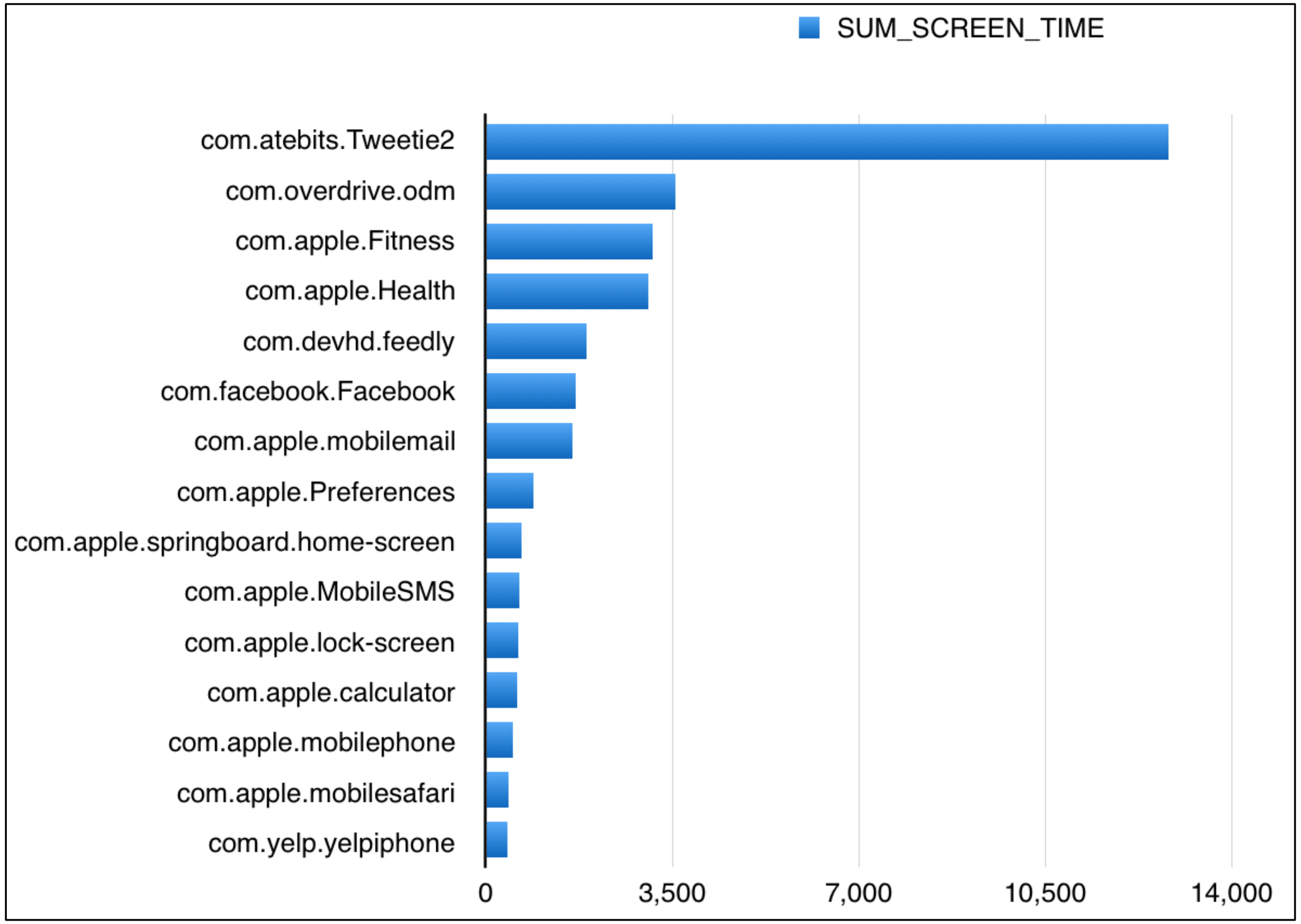
	Day_Hour	BundleID	ScreenOnTime
12	2016-04-02 12:00:00	com.atebits.Tweetie2	114.810658
13	2016-04-02 23:00:00	com.atebits.Tweetie2	810.924827
14	2016-04-03 03:00:00	com.atebits.Tweetie2	1259.868143
15	2016-04-03 04:00:00	com.atebits.Tweetie2	130.449583
16	2016-04-04 18:00:00	com.atebits.Tweetie2	767.512703
17	2016-04-04 21:00:00	com.atebits.Tweetie2	3.264545
18	2016-04-06 23:00:00	com.atebits.Tweetie2	27.539372
19	2016-04-07 19:00:00	com.atebits.Tweetie2	14.098393

OVERALL APP SCREEN TIME CurrentPowerlog.PLSQL

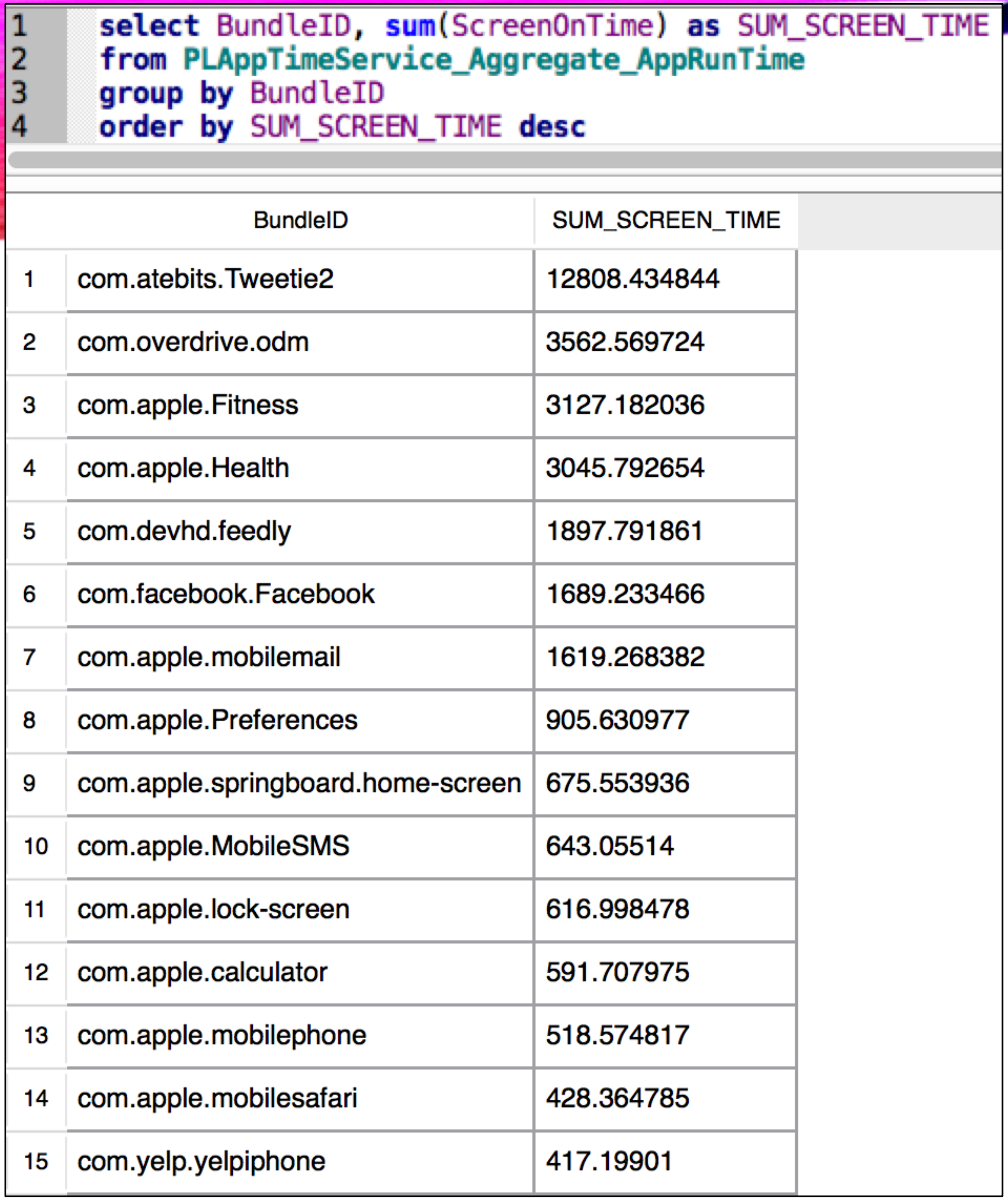


```
select BundleID, sum(ScreenOnTime) as SUM_SCREEN_TIME
from PLAppTimeService_Aggregate_AppRunTime
group by BundleID
order by SUM_SCREEN_TIME desc
```

	BundleID	SUM_SCREEN_TIME
1	com.atebits.Tweetie2	12808.434844
2	com.overdrive.odm	3562.569724
3	com.apple.Fitness	3127.182036
4	com.apple.Health	3045.792654
5	com.devhd.feedly	1897.791861
6	com.facebook.Facebook	1689.233466
7	com.apple.mobilemail	1619.268382
8	com.apple.Preferences	905.630977
9	com.apple.springboard.home-screen	675.553936
10	com.apple.MobileSMS	643.05514
11	com.apple.lock-screen	616.998478
12	com.apple.calculator	591.707975
13	com.apple.mobilephone	518.574817
14	com.apple.mobilesafari	428.364785
15	com.yelp.yelpiphone	417.19901

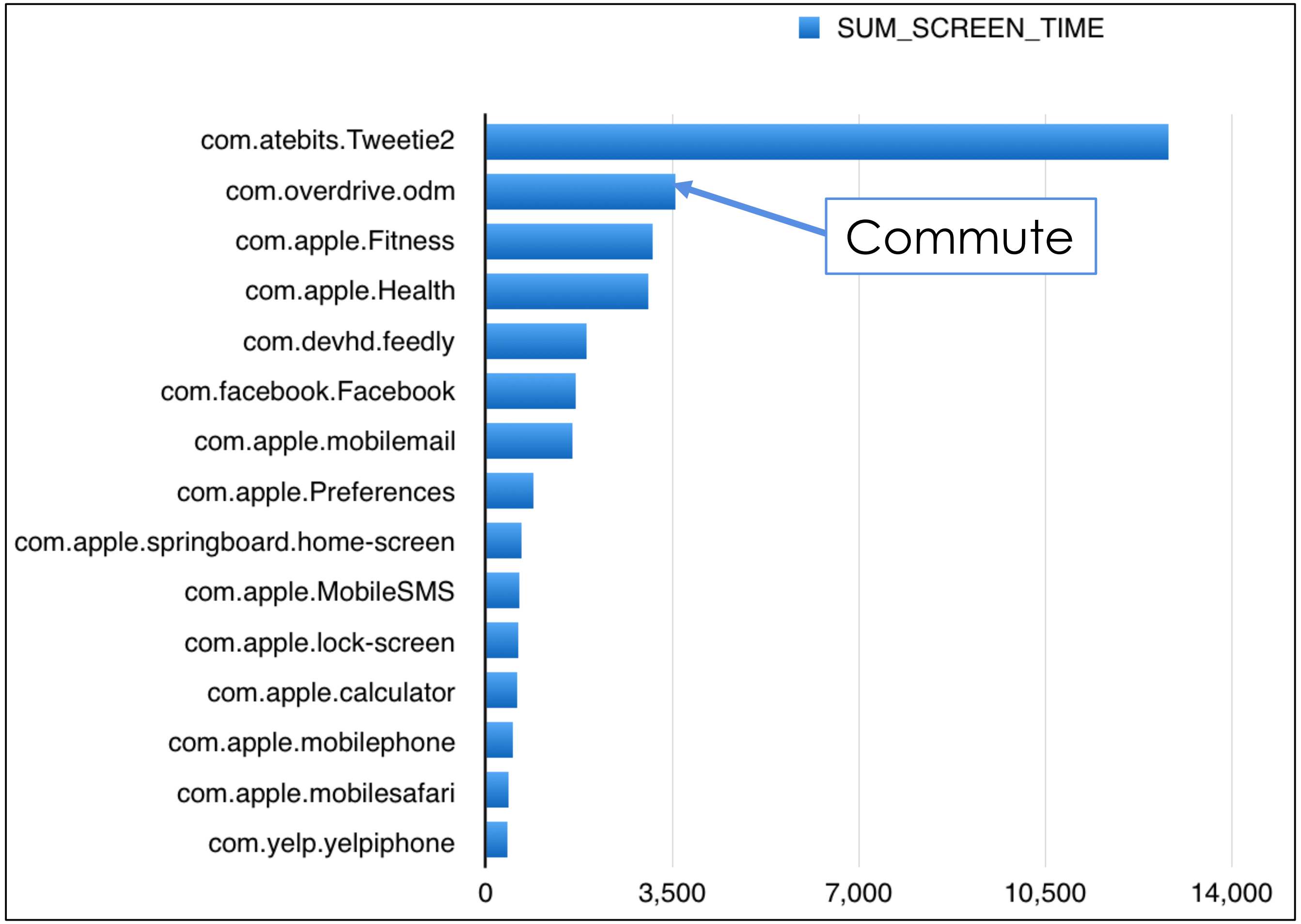


OVERALL APP SCREEN TIME CurrentPowerlog.PLSQL



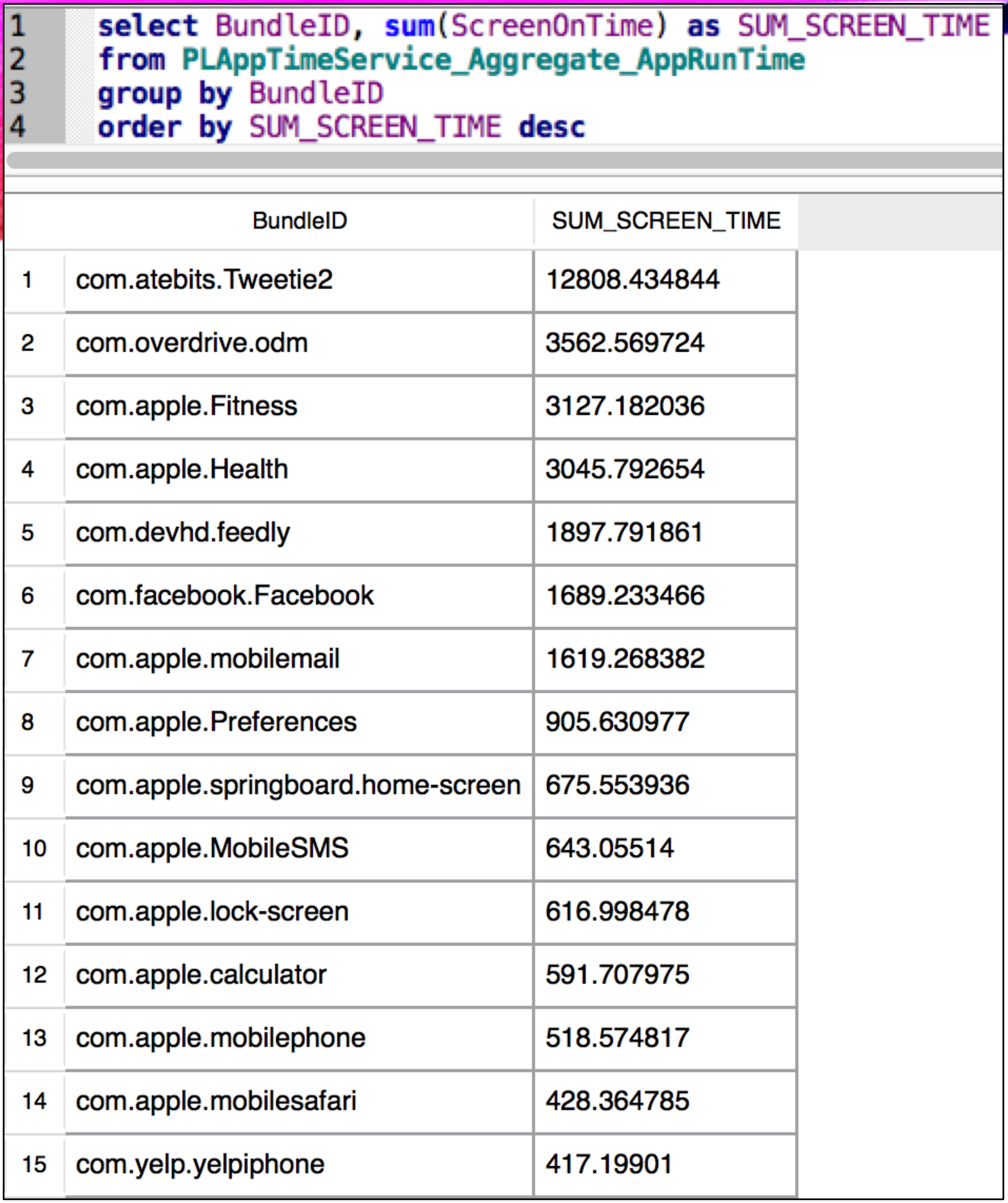
```
select BundleID, sum(ScreenOnTime) as SUM_SCREEN_TIME
from PLAppTimeService_Aggregate_AppRunTime
group by BundleID
order by SUM_SCREEN_TIME desc
```

	BundleID	SUM_SCREEN_TIME
1	com.atebits.Tweetie2	12808.434844
2	com.overdrive.odm	3562.569724
3	com.apple.Fitness	3127.182036
4	com.apple.Health	3045.792654
5	com.devhd.feedly	1897.791861
6	com.facebook.Facebook	1689.233466
7	com.apple.mobilemail	1619.268382
8	com.apple.Preferences	905.630977
9	com.apple.springboard.home-screen	675.553936
10	com.apple.MobileSMS	643.05514
11	com.apple.lock-screen	616.998478
12	com.apple.calculator	591.707975
13	com.apple.mobilephone	518.574817
14	com.apple.mobilesafari	428.364785
15	com.yelp.yelpiphone	417.19901



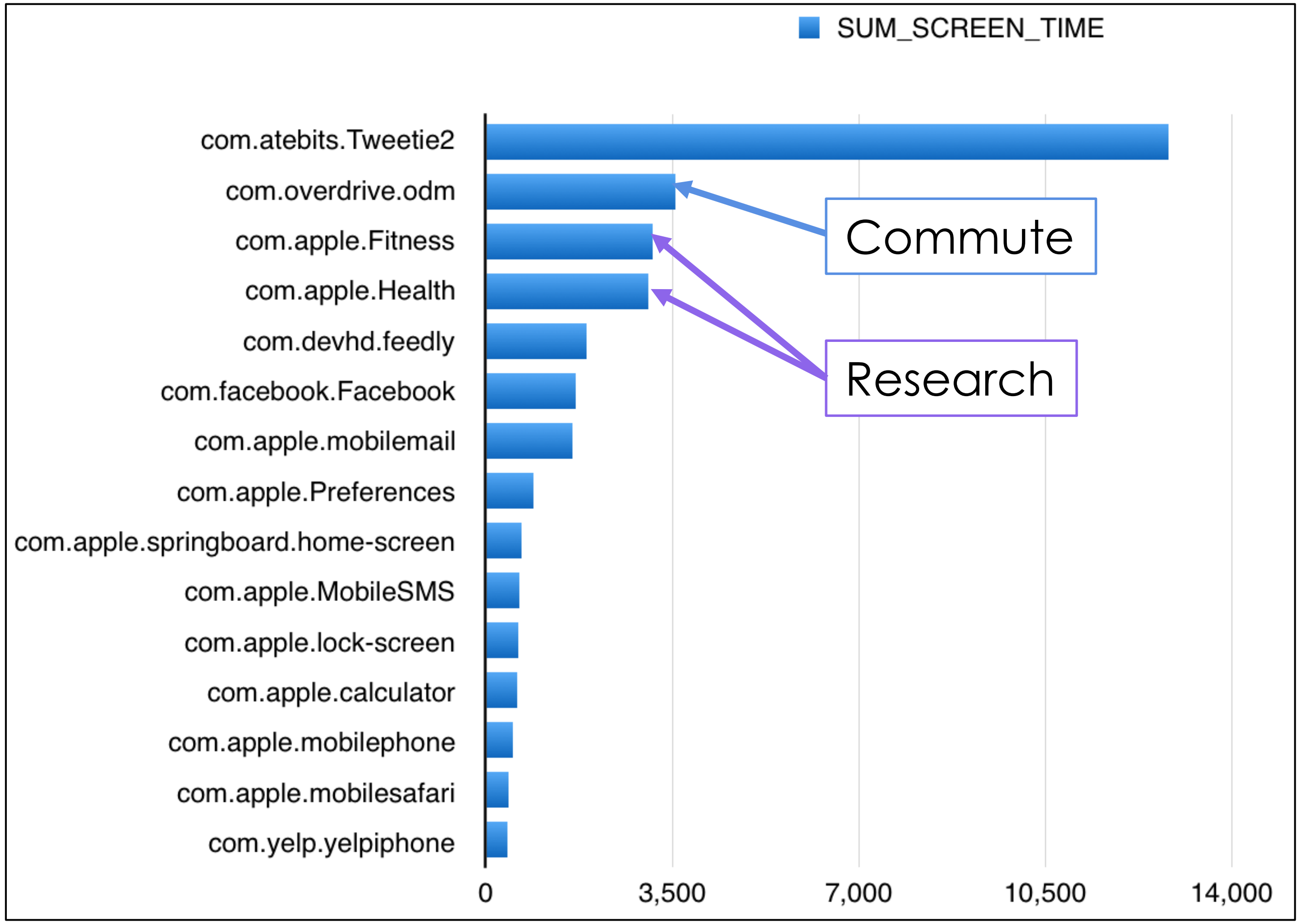
Commute

OVERALL APP SCREEN TIME CurrentPowerlog.PLSQL



```
select BundleID, sum(ScreenOnTime) as SUM_SCREEN_TIME
from PLAppTimeService_Aggregate_AppRunTime
group by BundleID
order by SUM_SCREEN_TIME desc
```

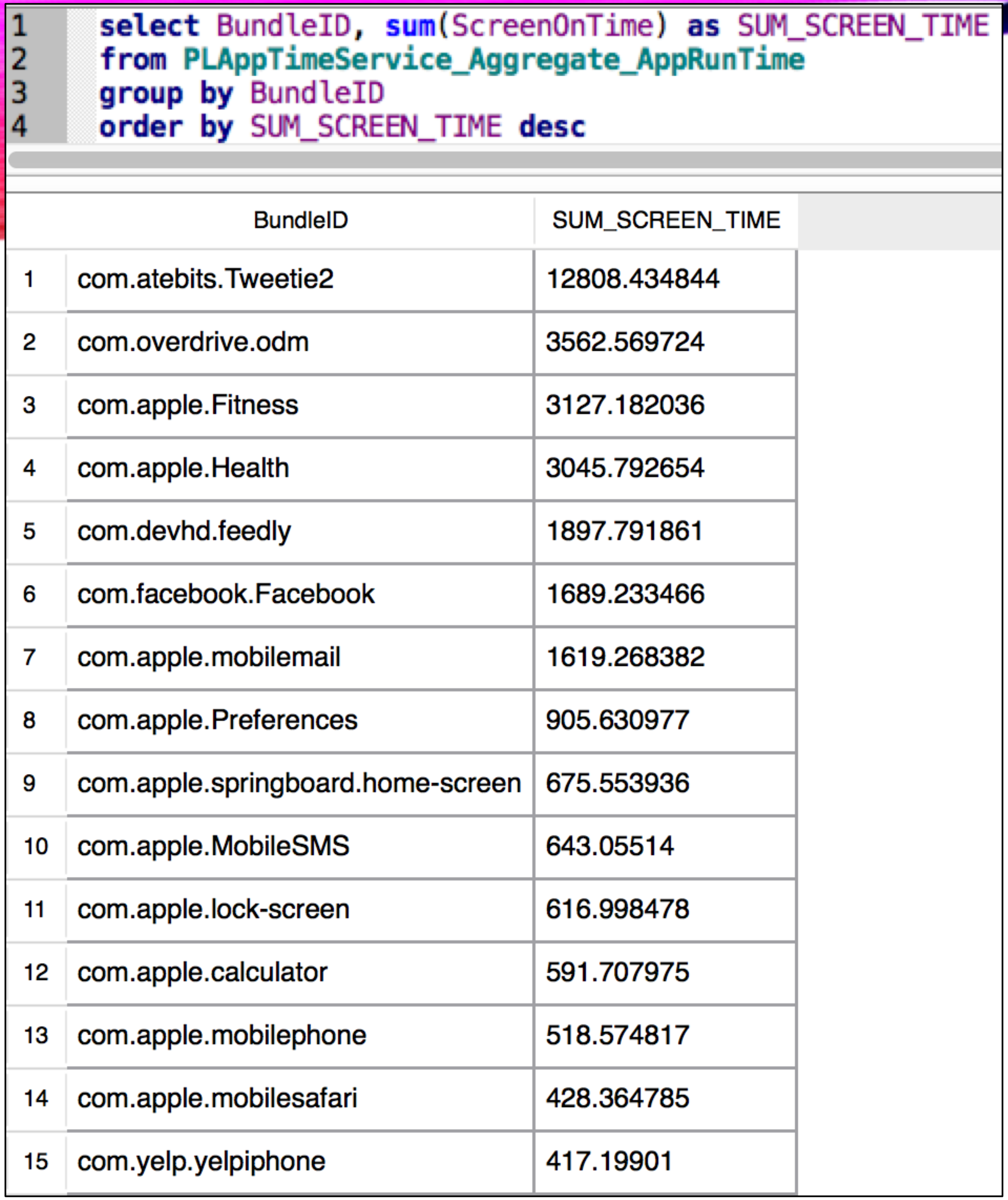
	BundleID	SUM_SCREEN_TIME
1	com.atebits.Tweetie2	12808.434844
2	com.overdrive.odm	3562.569724
3	com.apple.Fitness	3127.182036
4	com.apple.Health	3045.792654
5	com.devhd.feedly	1897.791861
6	com.facebook.Facebook	1689.233466
7	com.apple.mobilemail	1619.268382
8	com.apple.Preferences	905.630977
9	com.apple.springboard.home-screen	675.553936
10	com.apple.MobileSMS	643.05514
11	com.apple.lock-screen	616.998478
12	com.apple.calculator	591.707975
13	com.apple.mobilephone	518.574817
14	com.apple.mobilesafari	428.364785
15	com.yelp.yelpiphone	417.19901



Commute

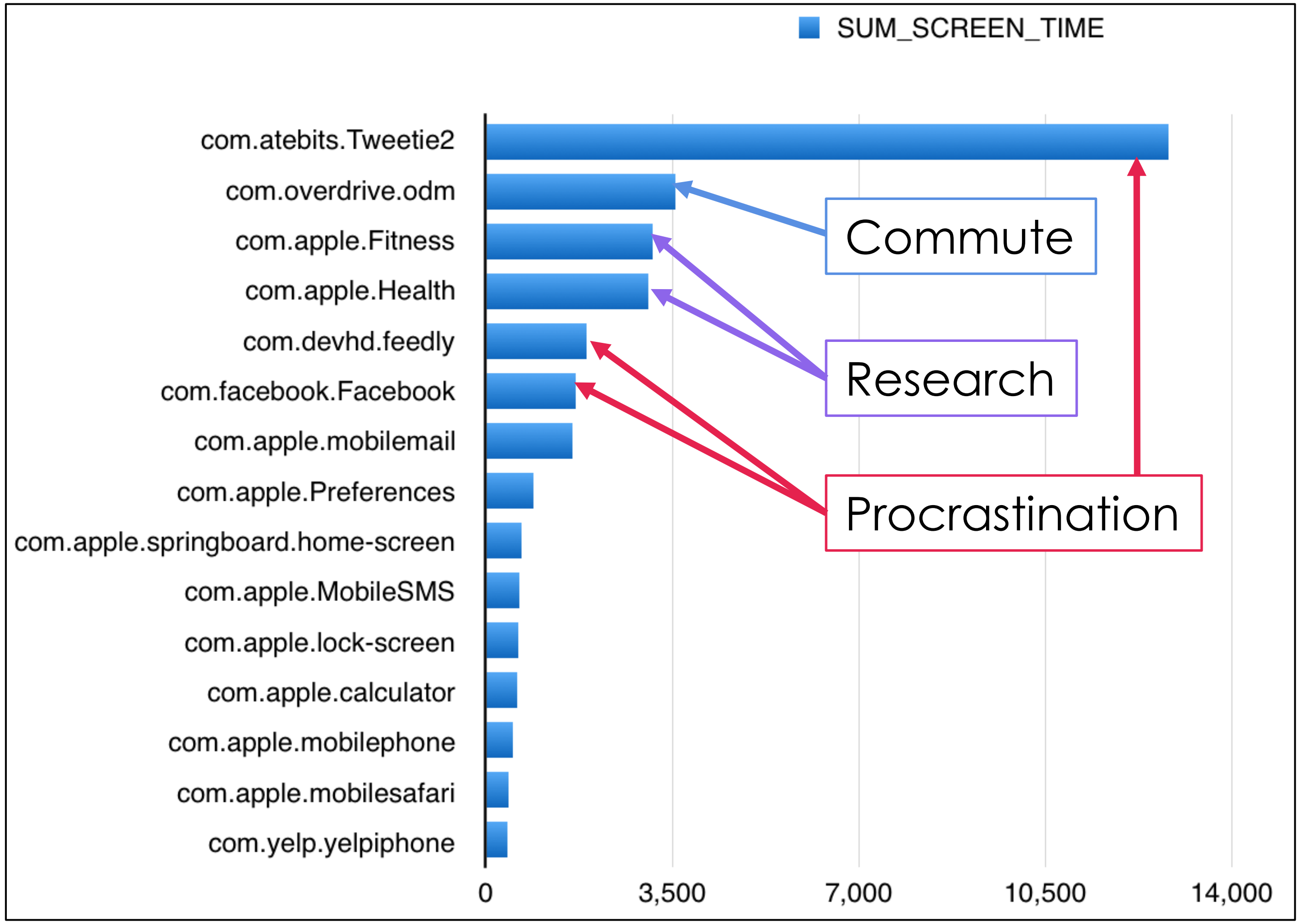
Research

OVERALL APP SCREEN TIME CurrentPowerlog.PLSQL



```
select BundleID, sum(ScreenOnTime) as SUM_SCREEN_TIME
from PLAppTimeService_Aggregate_AppRunTime
group by BundleID
order by SUM_SCREEN_TIME desc
```

	BundleID	SUM_SCREEN_TIME
1	com.atebits.Tweetie2	12808.434844
2	com.overdrive.odm	3562.569724
3	com.apple.Fitness	3127.182036
4	com.apple.Health	3045.792654
5	com.devhd.feedly	1897.791861
6	com.facebook.Facebook	1689.233466
7	com.apple.mobilemail	1619.268382
8	com.apple.Preferences	905.630977
9	com.apple.springboard.home-screen	675.553936
10	com.apple.MobileSMS	643.05514
11	com.apple.lock-screen	616.998478
12	com.apple.calculator	591.707975
13	com.apple.mobilephone	518.574817
14	com.apple.mobilesafari	428.364785
15	com.yelp.yelpiphone	417.19901

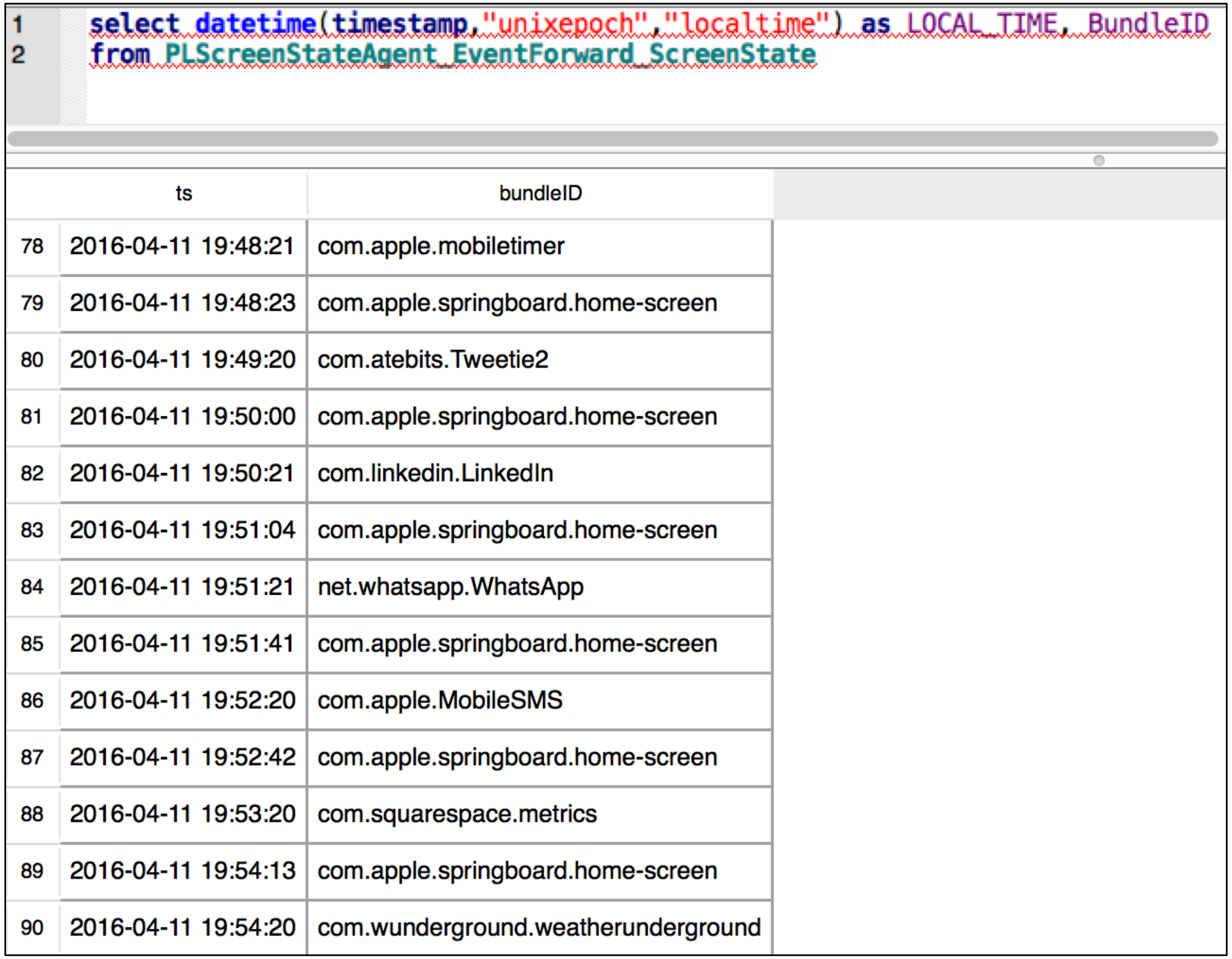


Commute

Research

Procrastination

APP USAGE PLAY-BY-PLAY
CurrentPowerlog.PLSQL



```
select datetime(timestamp,"unixepoch","localtime") as LOCAL_TIME, BundleID
from PLScreenStateAgent_EventForward_ScreenState
```

	ts	bundleID
78	2016-04-11 19:48:21	com.apple.mobiletimer
79	2016-04-11 19:48:23	com.apple.springboard.home-screen
80	2016-04-11 19:49:20	com.atebits.Tweetie2
81	2016-04-11 19:50:00	com.apple.springboard.home-screen
82	2016-04-11 19:50:21	com.linkedin.LinkedIn
83	2016-04-11 19:51:04	com.apple.springboard.home-screen
84	2016-04-11 19:51:21	net.whatsapp.WhatsApp
85	2016-04-11 19:51:41	com.apple.springboard.home-screen
86	2016-04-11 19:52:20	com.apple.MobileSMS
87	2016-04-11 19:52:42	com.apple.springboard.home-screen
88	2016-04-11 19:53:20	com.squarespace.metrics
89	2016-04-11 19:54:13	com.apple.springboard.home-screen
90	2016-04-11 19:54:20	com.wunderground.weatherunderground

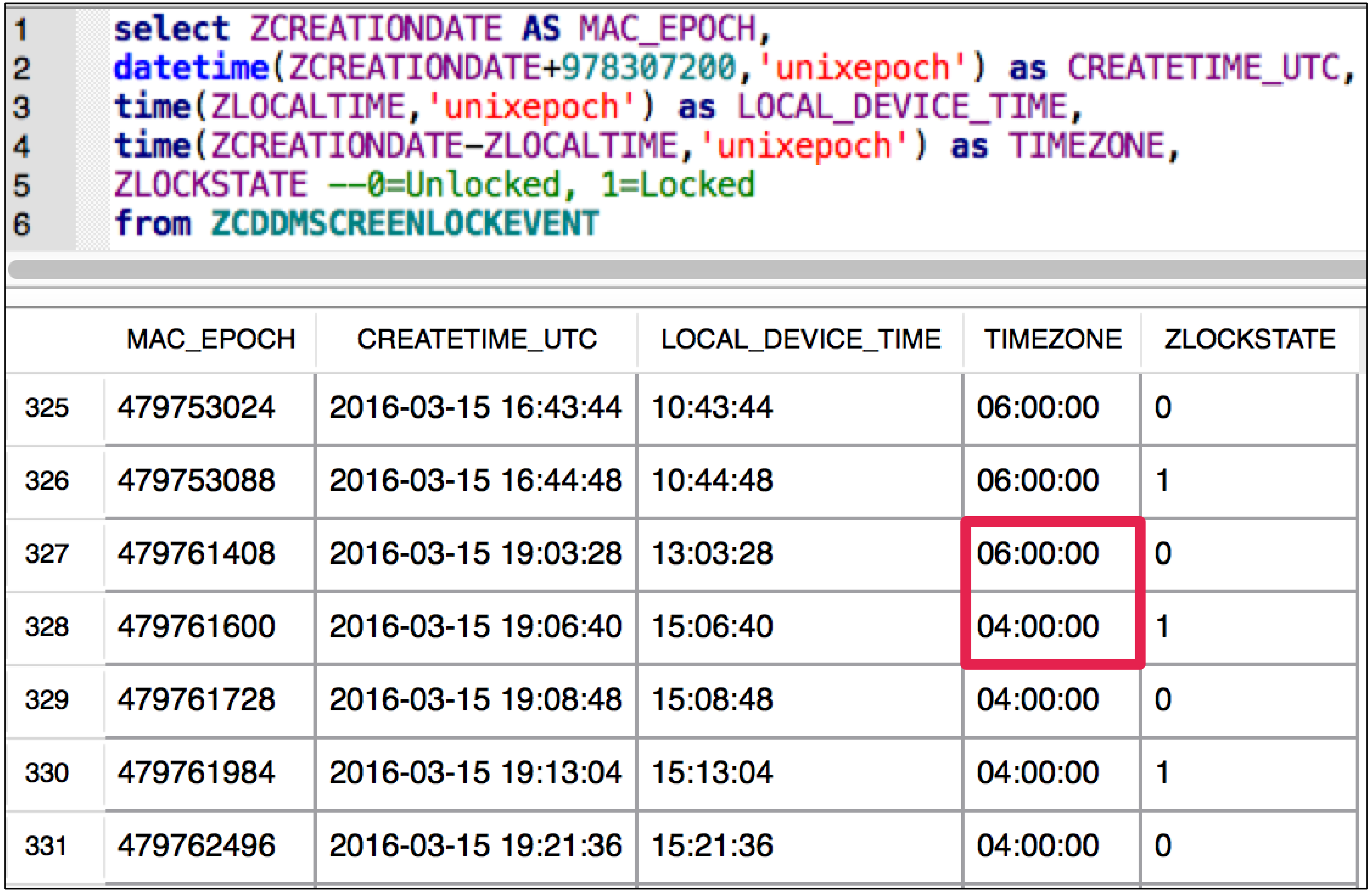
Data Retention:
~1 Day

Timestamp Warning:
My timestamps were off by +9:20
¯_(ツ)_/¯

Timing:
In Seconds

DEVICE STATE

DEVICE LOCK STATE
coreduetd.db



```
select ZCREATIONDATE AS MAC_EPOCH,
datetime(ZCREATIONDATE+978307200,'unixepoch') as CREATETIME_UTC,
time(ZLOCALTIME,'unixepoch') as LOCAL_DEVICE_TIME,
time(ZCREATIONDATE-ZLOCALTIME,'unixepoch') as TIMEZONE,
ZLOCKSTATE --0=Unlocked, 1=Locked
from ZCDDMSCREENLOCKEVENT
```

	MAC_EPOCH	CREATETIME_UTC	LOCAL_DEVICE_TIME	TIMEZONE	ZLOCKSTATE
325	479753024	2016-03-15 16:43:44	10:43:44	06:00:00	0
326	479753088	2016-03-15 16:44:48	10:44:48	06:00:00	1
327	479761408	2016-03-15 19:03:28	13:03:28	06:00:00	0
328	479761600	2016-03-15 19:06:40	15:06:40	04:00:00	1
329	479761728	2016-03-15 19:08:48	15:08:48	04:00:00	0
330	479761984	2016-03-15 19:13:04	15:13:04	04:00:00	1
331	479762496	2016-03-15 19:21:36	15:21:36	04:00:00	0

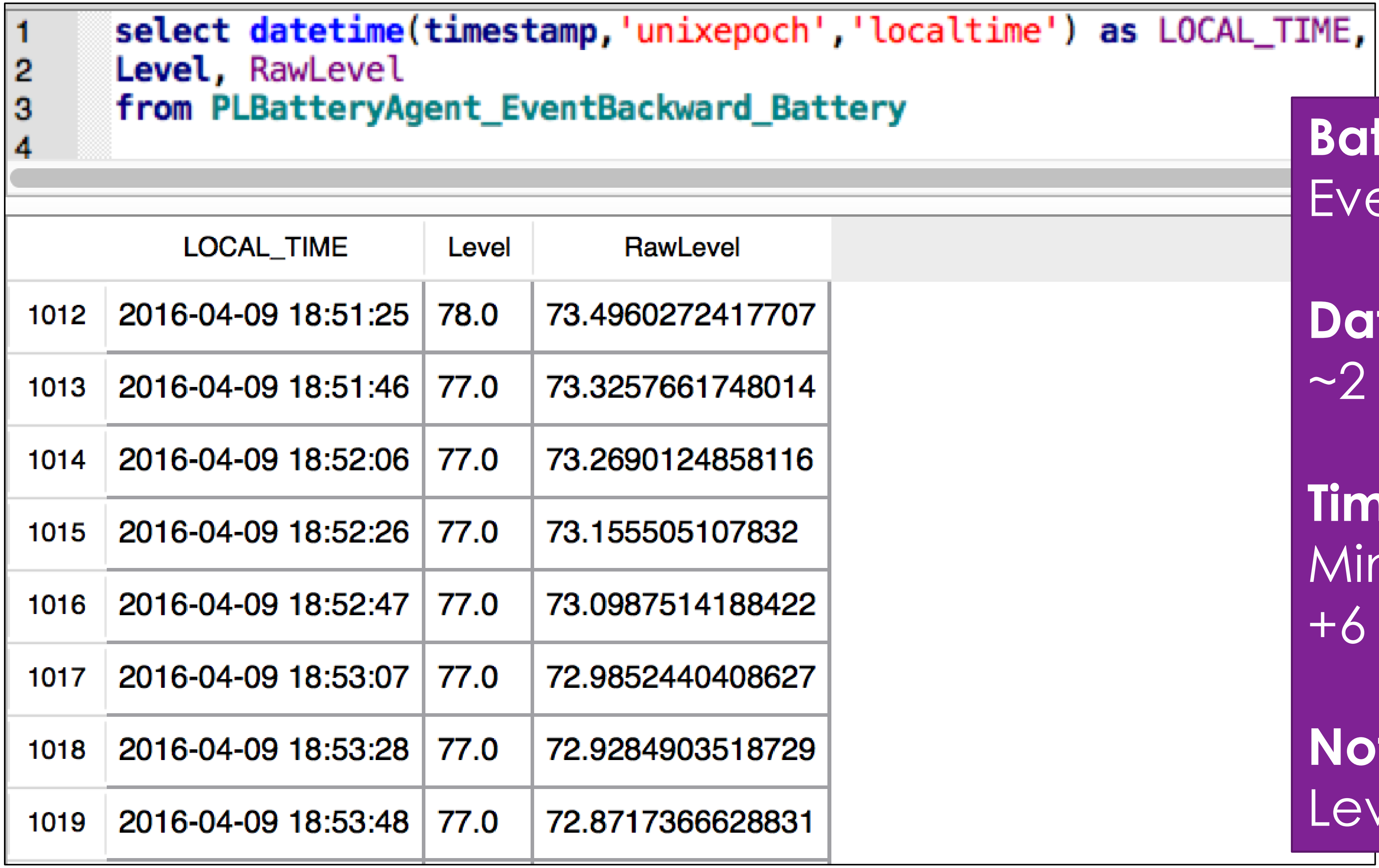
Data Retention:
~1 Month

Time Zone:
"ZCREATIONDATE" - "ZLOCALTIME"

Timestamp Warning:
Timestamps seem to be off ever so slightly. (~1m or so)
¯_(ツ)_/¯

State:
0 = Unlocked
1 = Locked

DEVICE BATTERY LEVEL CurrentPowerlog.PLSQL



```sql
select datetime(timestamp,'unixepoch','localtime') as LOCAL_TIME,
Level, RawLevel
from PLBatteryAgent_EventBackward_Battery
```

	LOCAL_TIME	Level	RawLevel
1012	2016-04-09 18:51:25	78.0	73.4960272417707
1013	2016-04-09 18:51:46	77.0	73.3257661748014
1014	2016-04-09 18:52:06	77.0	73.2690124858116
1015	2016-04-09 18:52:26	77.0	73.155505107832
1016	2016-04-09 18:52:47	77.0	73.0987514188422
1017	2016-04-09 18:53:07	77.0	72.9852440408627
1018	2016-04-09 18:53:28	77.0	72.9284903518729
1019	2016-04-09 18:53:48	77.0	72.8717366628831

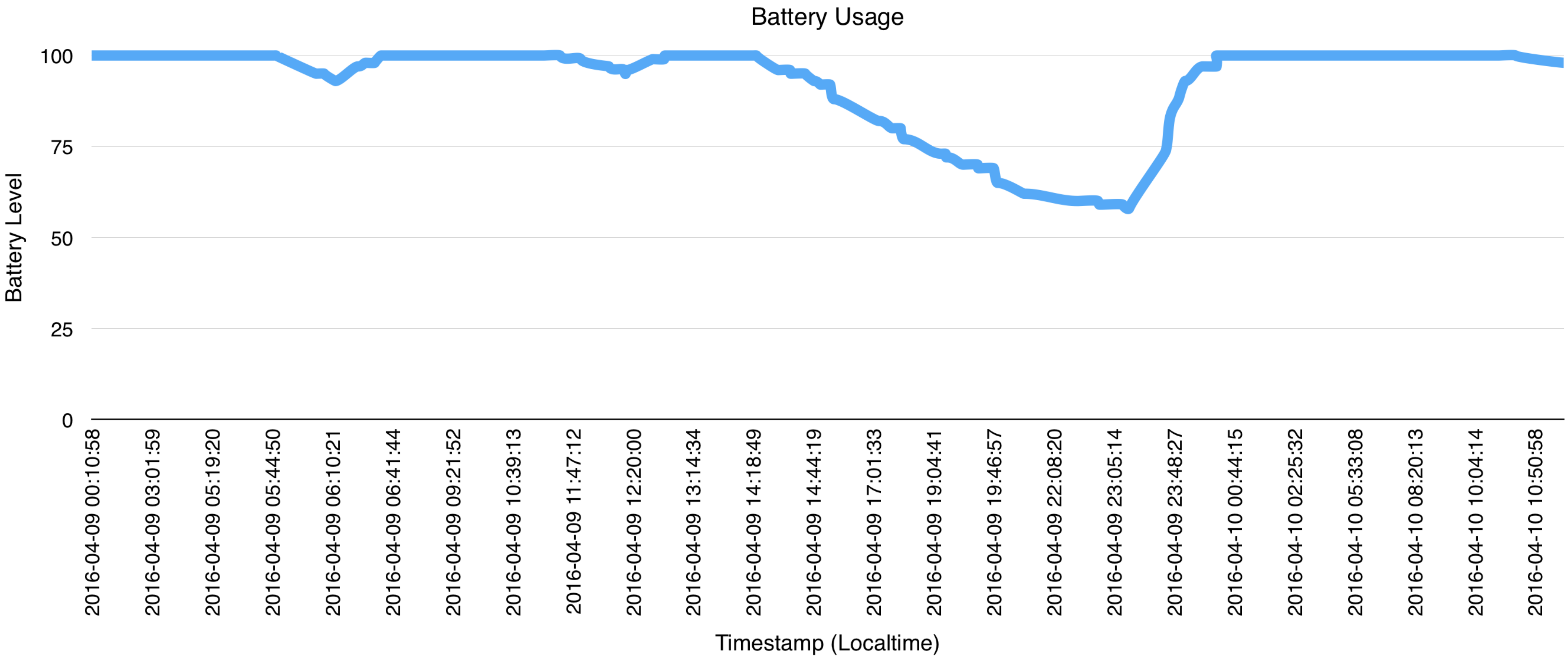
Battery Level:
Every ~20 Seconds

Data Retention:
~2 Days

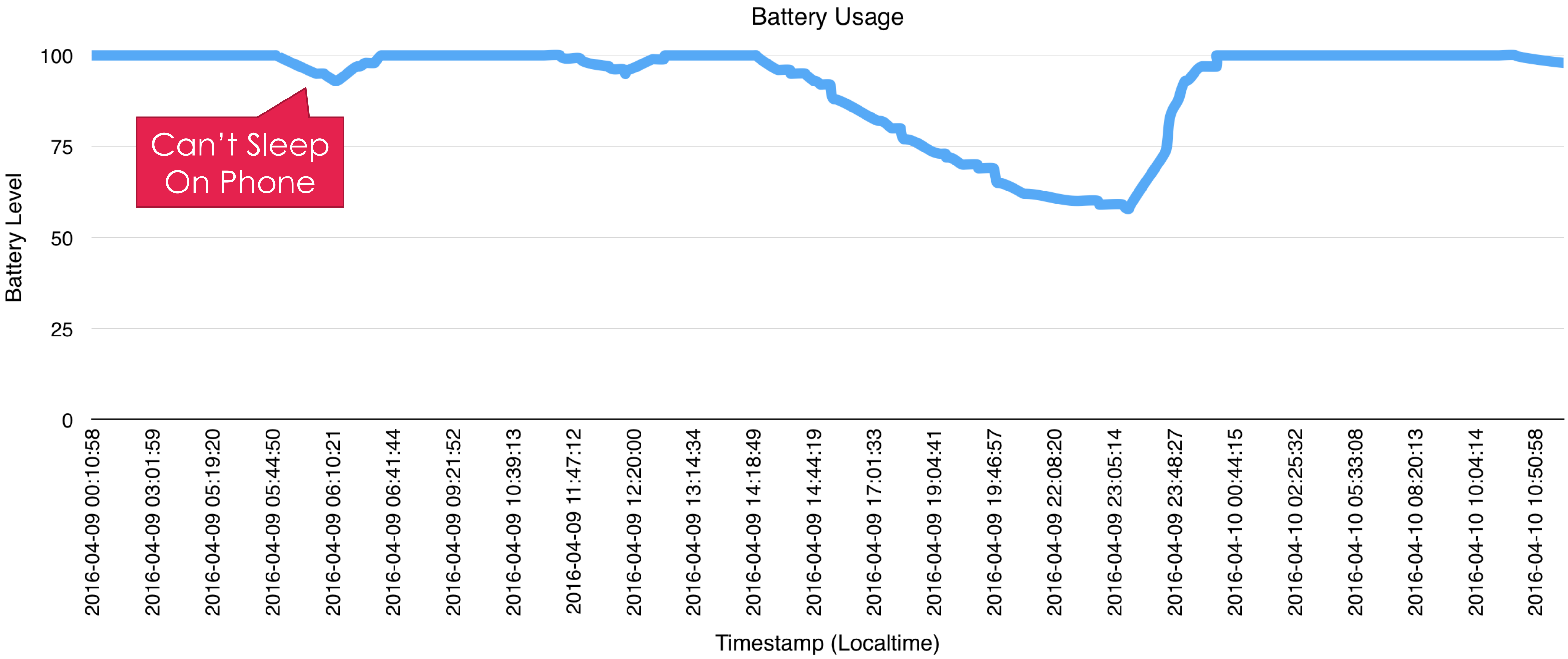
Timestamp Warning:
Mine were off by about +6 minutes

Note:
Level Vs. RawLevel

DEVICE BATTERY LEVEL CurrentPowerlog.PLSQL

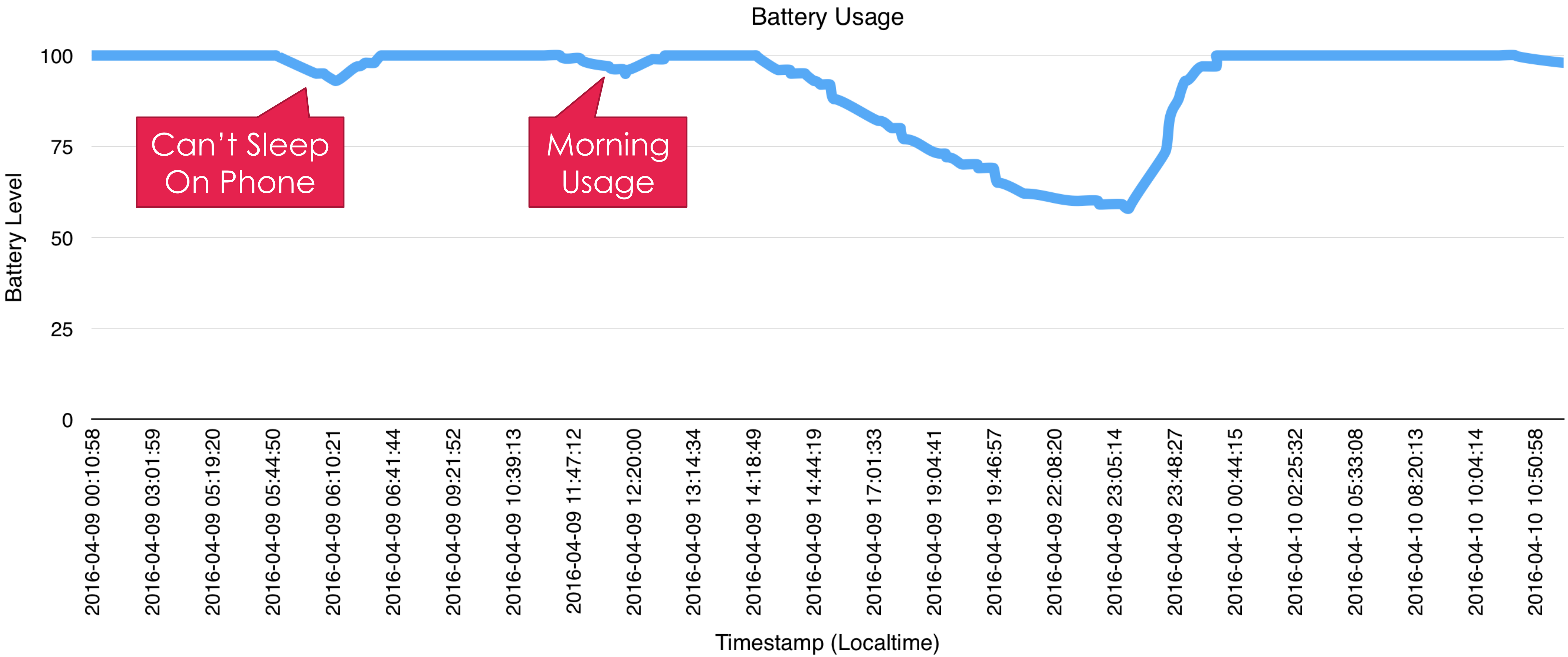


DEVICE BATTERY LEVEL CurrentPowerlog.PLSQL



Can't Sleep On Phone

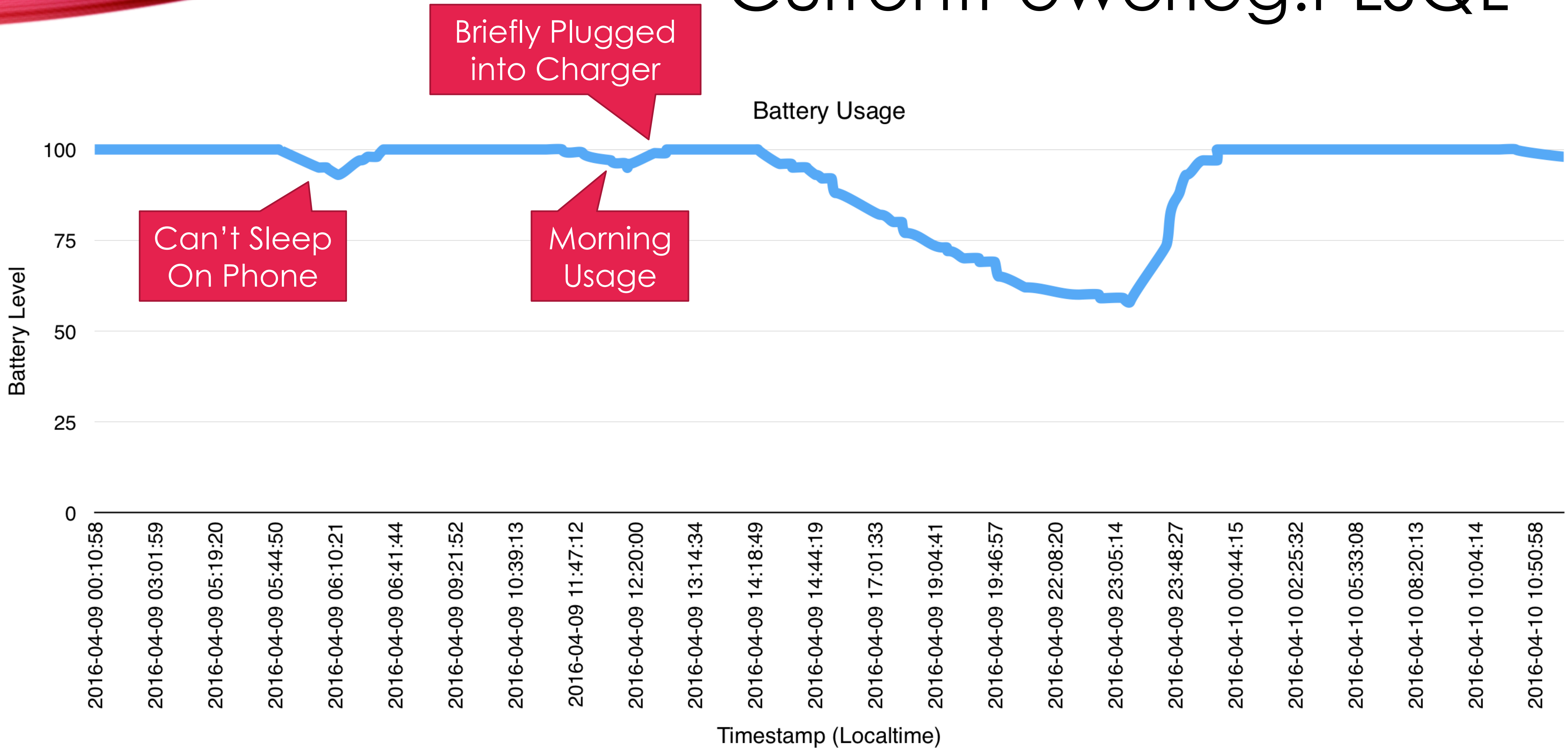
DEVICE BATTERY LEVEL
CurrentPowerlog.PLSQL



Can’t Sleep On Phone

Morning Usage

DEVICE BATTERY LEVEL
CurrentPowerlog.PLSQL

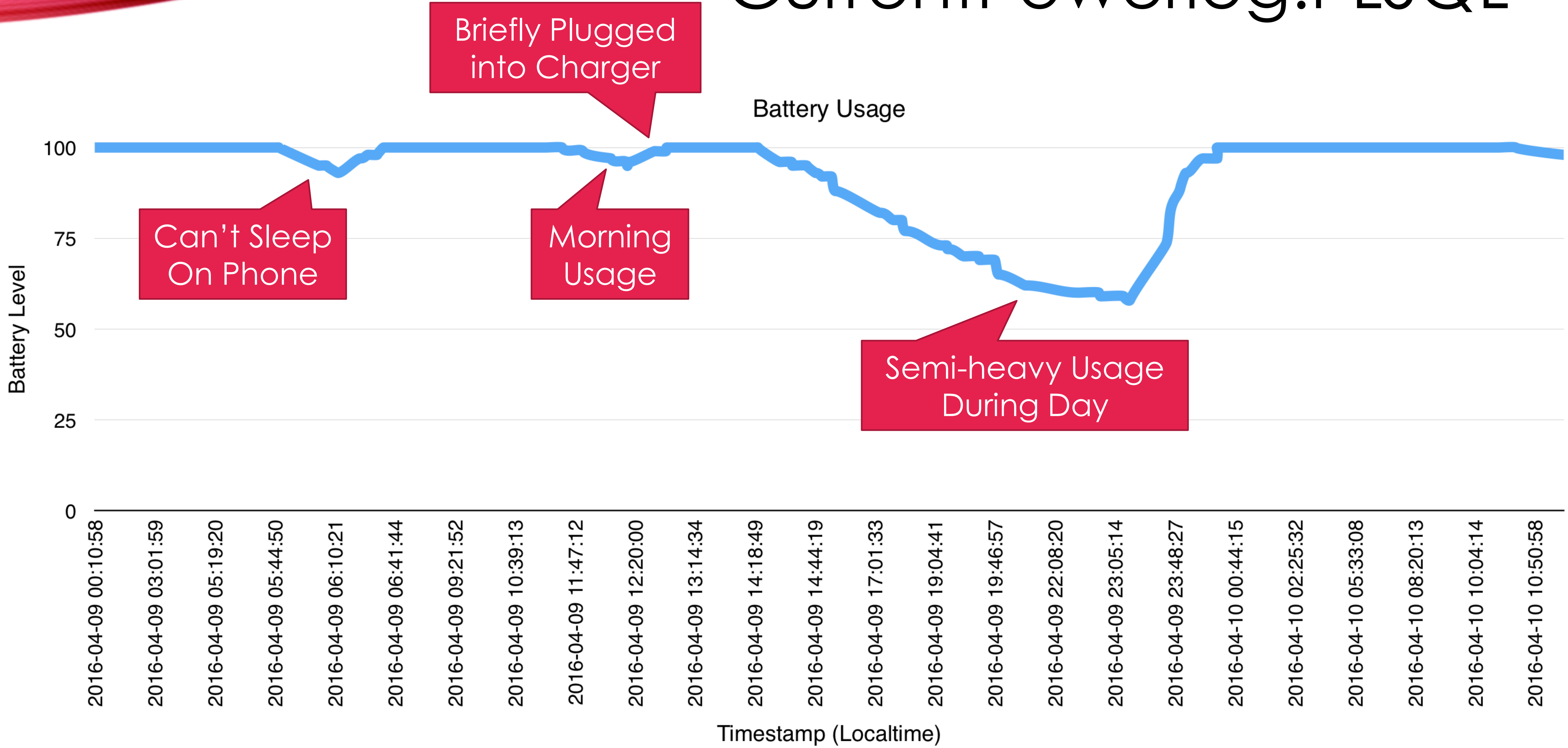


Briefly Plugged into Charger

Can't Sleep On Phone

Morning Usage

DEVICE BATTERY LEVEL CurrentPowerlog.PLSQL



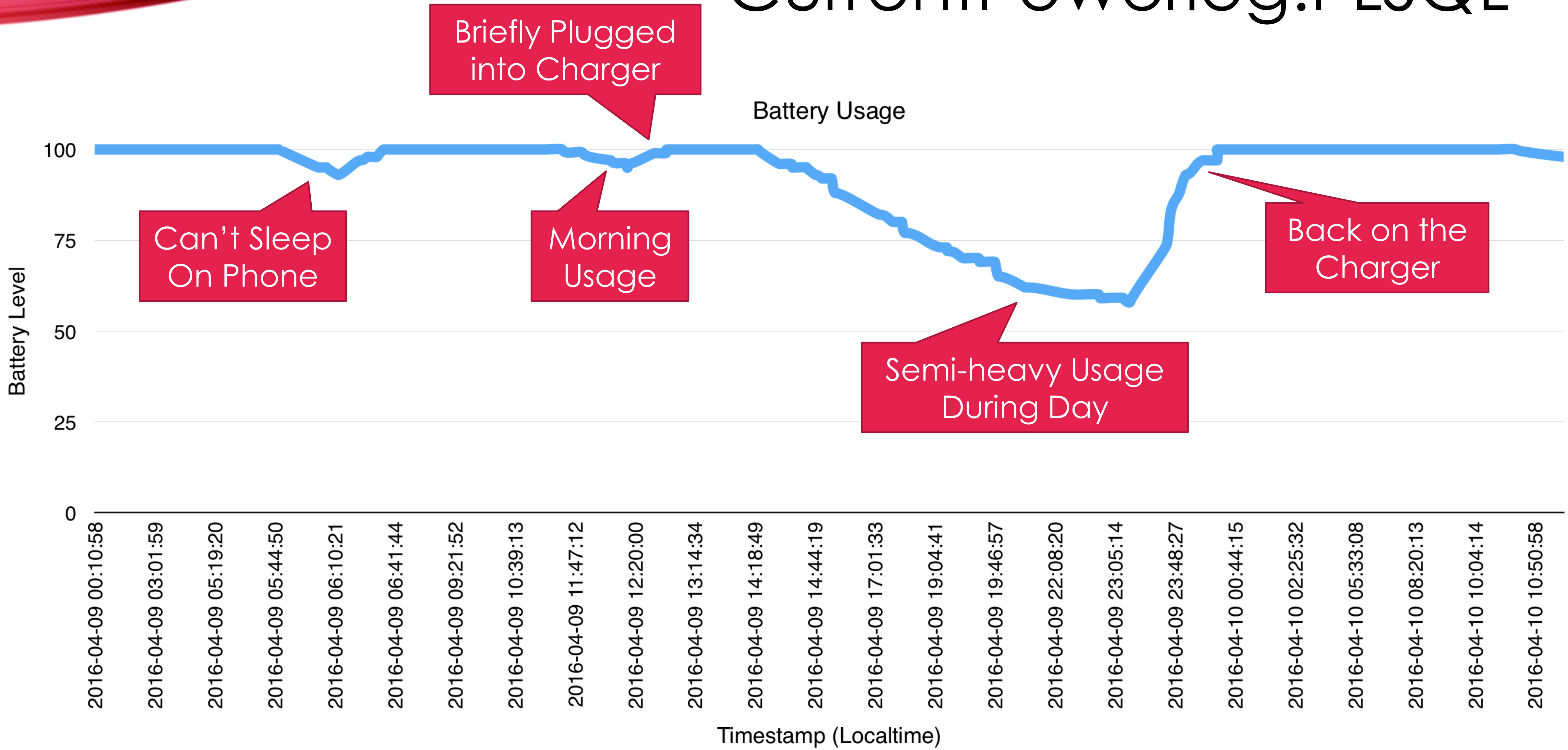
Briefly Plugged into Charger

Can’t Sleep On Phone

Morning Usage

Semi-heavy Usage During Day

DEVICE BATTERY LEVEL
CurrentPowerlog.PLSQL



Briefly Plugged into Charger

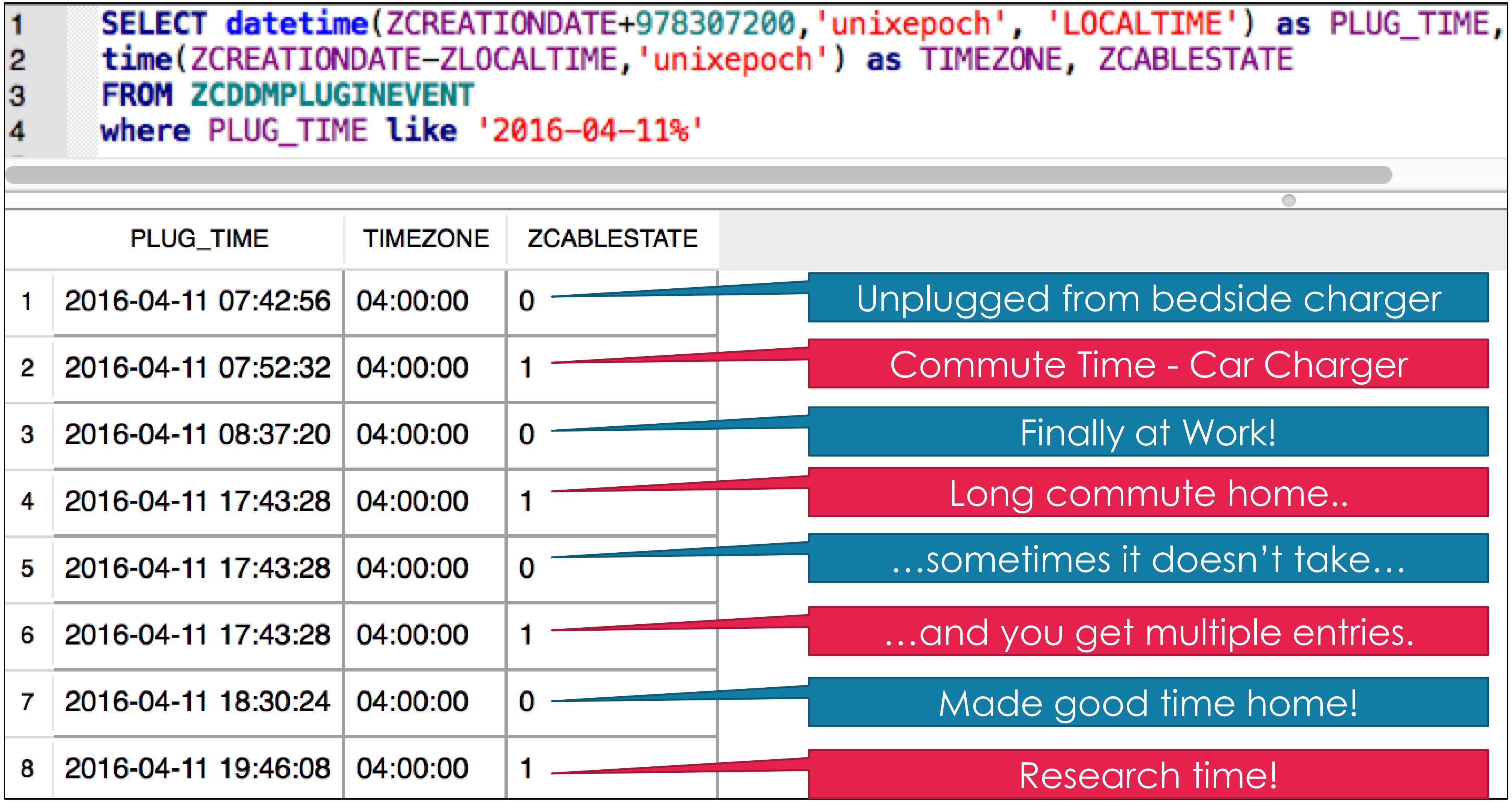
Can't Sleep On Phone

Morning Usage

Semi-heavy Usage During Day

Back on the Charger

DEVICE PLUGIN STATE
coreduetdClassD.db



```
SELECT datetime(ZCREATIONDATE+978307200,'unixepoch', 'LOCALTIME') as PLUG_TIME,
time(ZCREATIONDATE-ZLOCALTIME,'unixepoch') as TIMEZONE, ZCABLESTATE
FROM ZCDDMPLUGINEVENT
where PLUG_TIME like '2016-04-11%'
```

	PLUG_TIME	TIMEZONE	ZCABLESTATE
1	2016-04-11 07:42:56	04:00:00	0
2	2016-04-11 07:52:32	04:00:00	1
3	2016-04-11 08:37:20	04:00:00	0
4	2016-04-11 17:43:28	04:00:00	1
5	2016-04-11 17:43:28	04:00:00	0
6	2016-04-11 17:43:28	04:00:00	1
7	2016-04-11 18:30:24	04:00:00	0
8	2016-04-11 19:46:08	04:00:00	1

Unplugged from bedside charger

Commute Time - Car Charger

Finally at Work!

Long commute home..

…sometimes it doesn't take…

…and you get multiple entries.

Made good time home!

Research time!

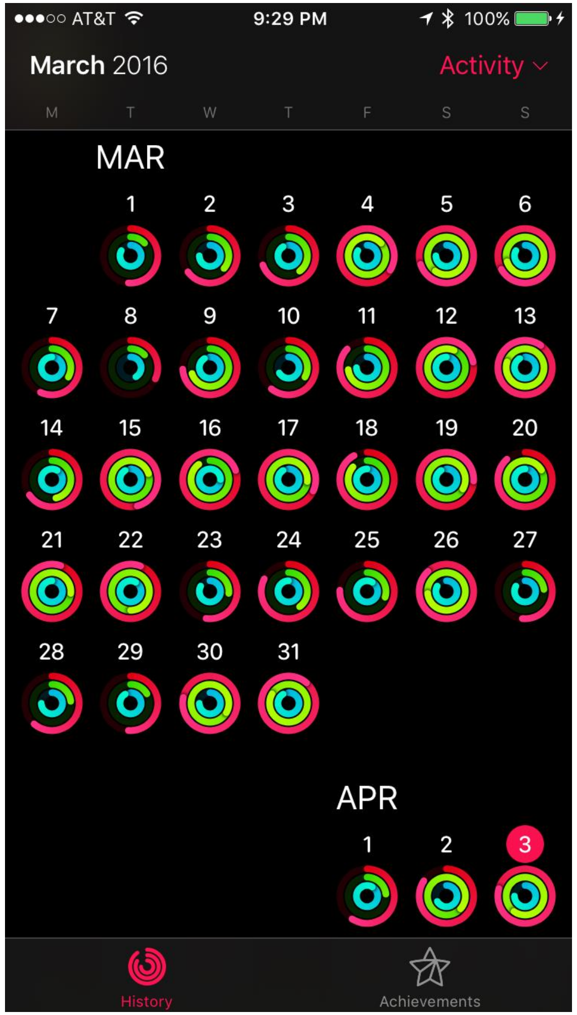
Data Retention:
~1 Month

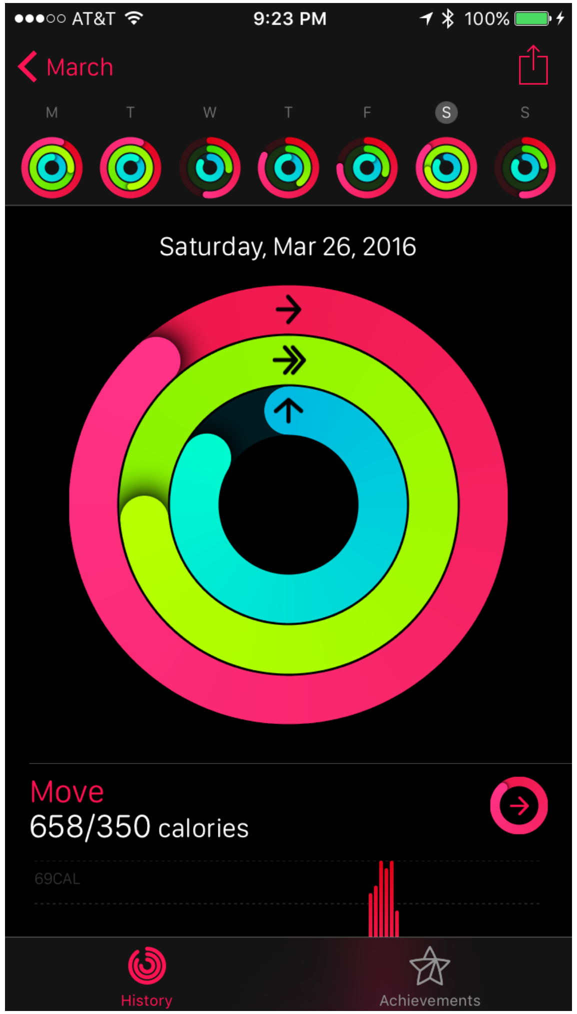
Timestamps:
Accurate

State:
0 = Unplugged
1 = Plugged In

HEALTH

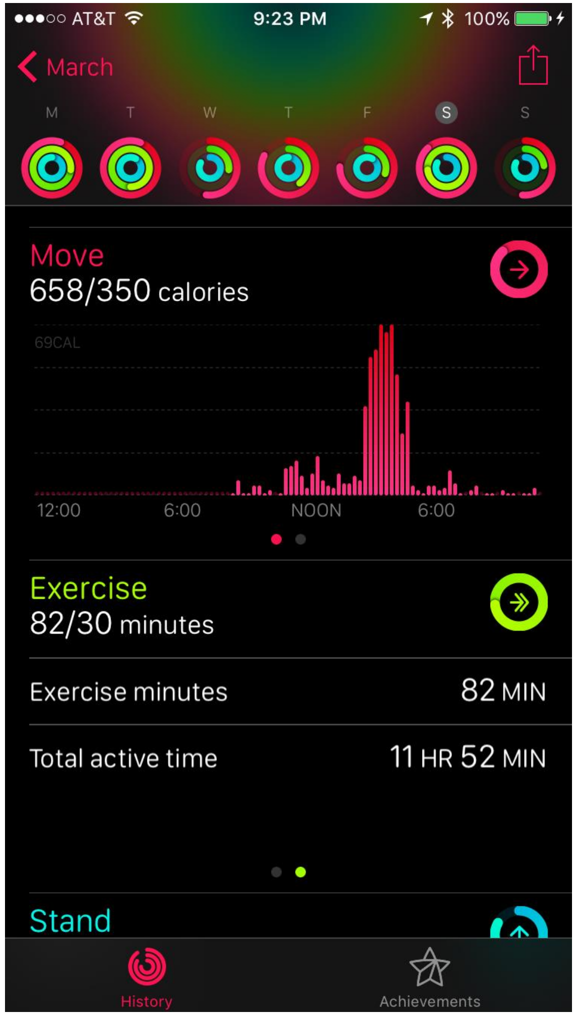
ACTIVITY CACHE
healthdb_secure.sqlite





Saturday, Mar 26, 2016

Move
658/350 calories



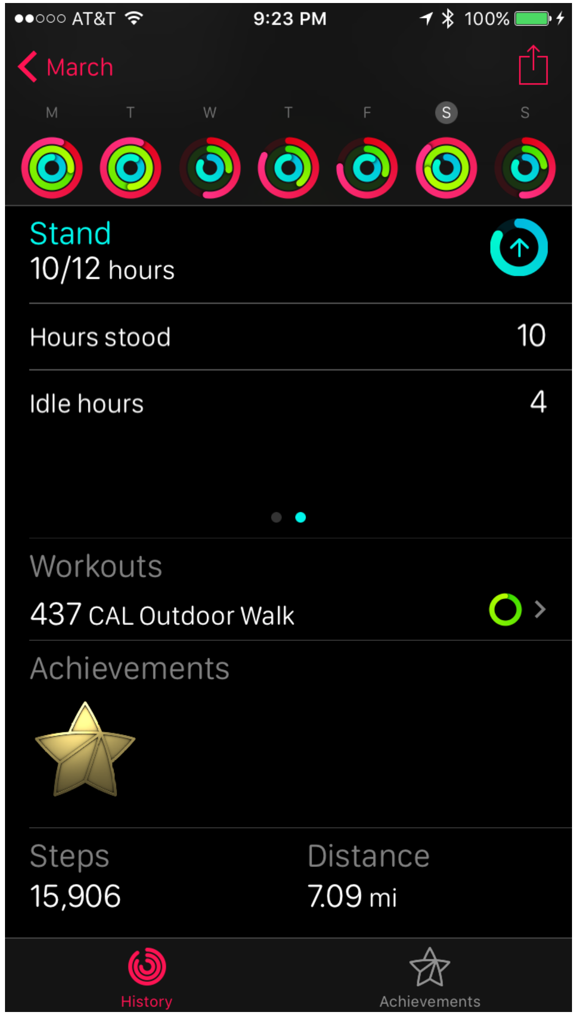
Move
658/350 calories

Exercise
82/30 minutes

Exercise minutes 82 MIN

Total active time 11 HR 52 MIN

Stand



Stand
10/12 hours

Hours stood 10

Idle hours 4

Workouts

437 CAL Outdoor Walk

Achievements

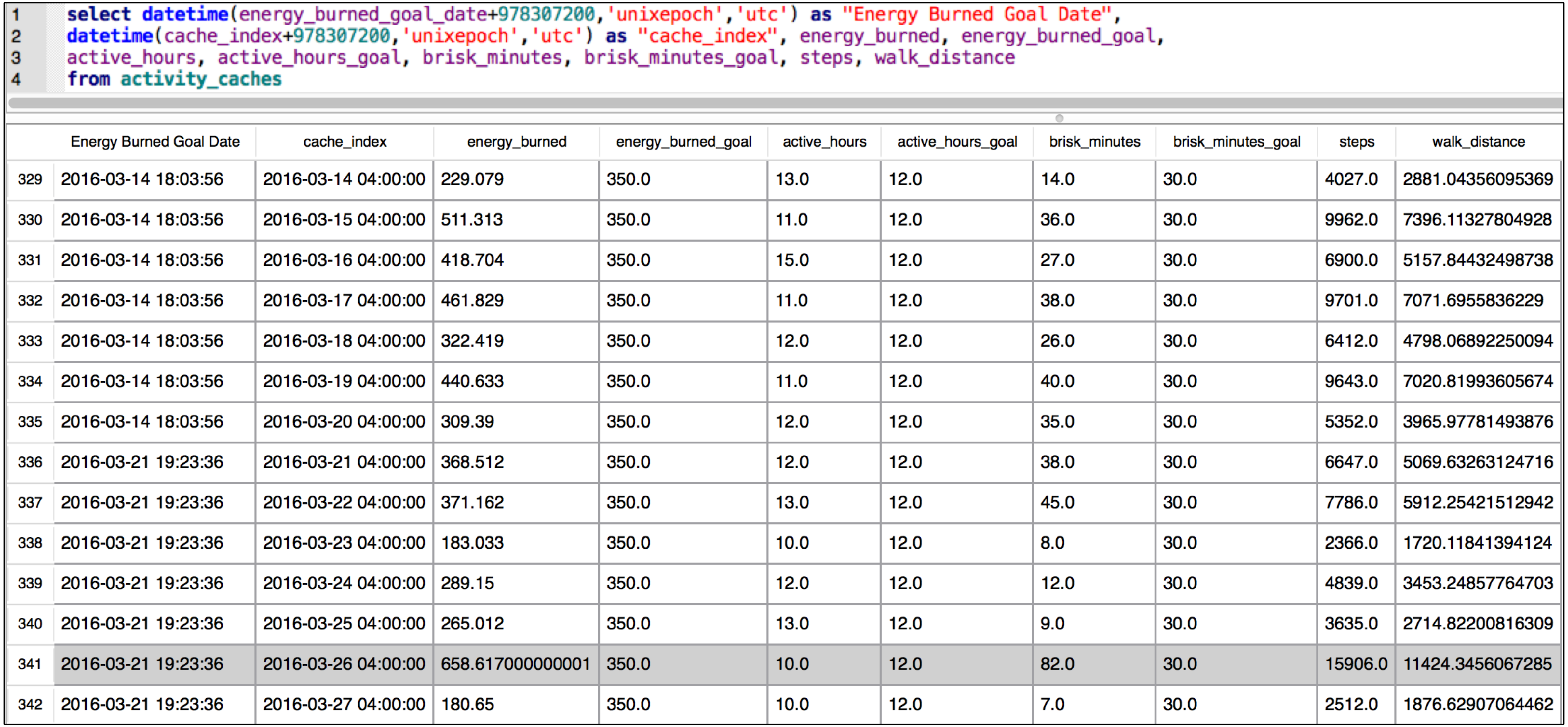
Steps
15,906

Distance
7.09 mi

Data Retention:
For All Time

Timestamps:
Accurate

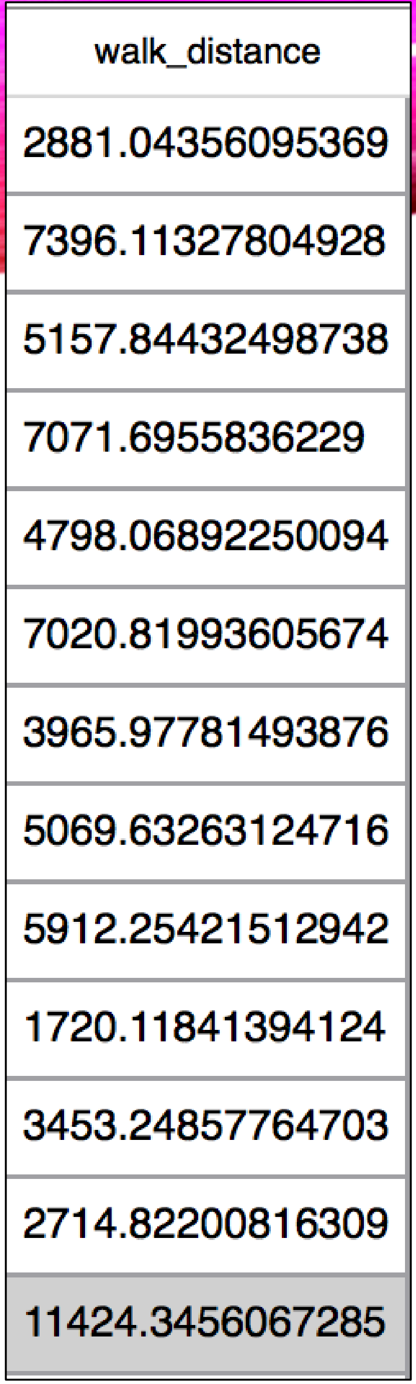
ACTIVITY CACHE
healthdb_secure.sqlite



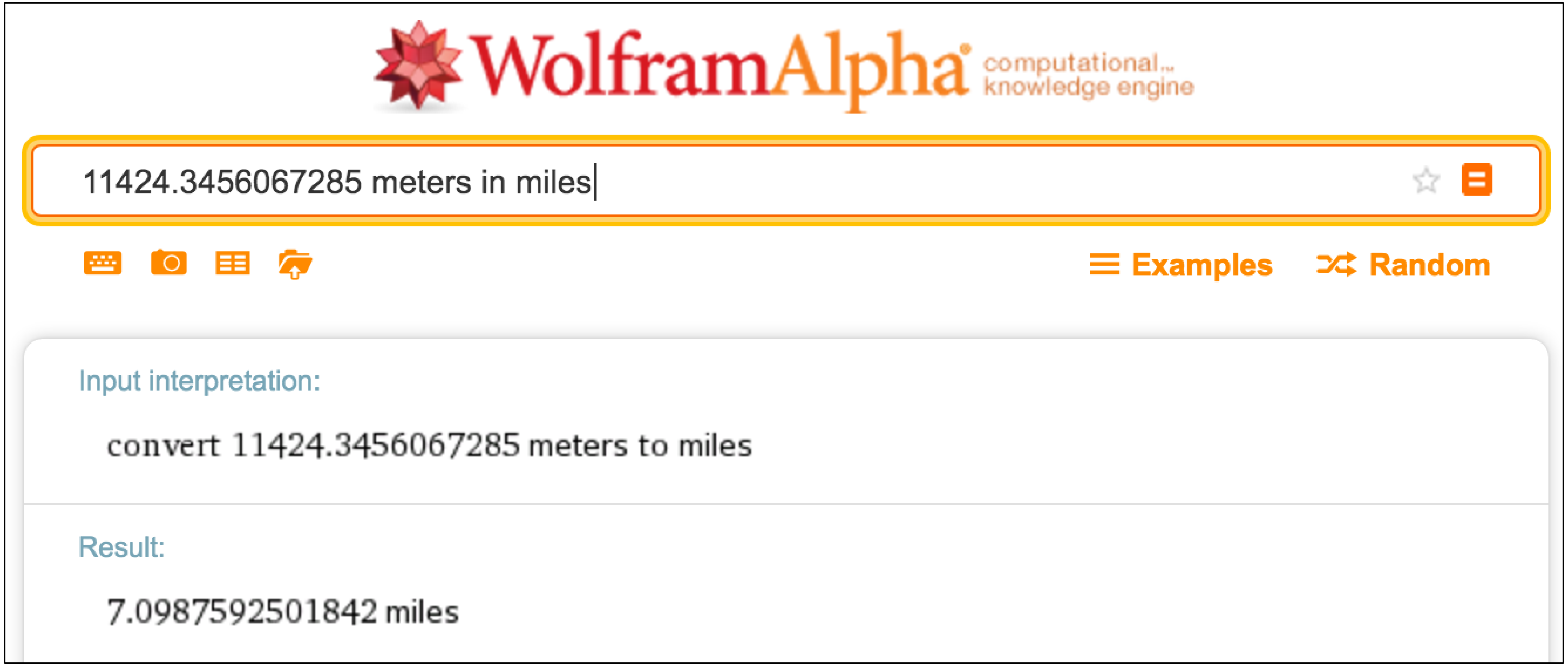
```
select datetime(energy_burned_goal_date+978307200,'unixepoch','utc') as "Energy Burned Goal Date",
datetime(cache_index+978307200,'unixepoch','utc') as "cache_index", energy_burned, energy_burned_goal,
active_hours, active_hours_goal, brisk_minutes, brisk_minutes_goal, steps, walk_distance
from activity_caches
```

	Energy Burned Goal Date	cache_index	energy_burned	energy_burned_goal	active_hours	active_hours_goal	brisk_minutes	brisk_minutes_goal	steps	walk_distance
329	2016-03-14 18:03:56	2016-03-14 04:00:00	229.079	350.0	13.0	12.0	14.0	30.0	4027.0	2881.04356095369
330	2016-03-14 18:03:56	2016-03-15 04:00:00	511.313	350.0	11.0	12.0	36.0	30.0	9962.0	7396.11327804928
331	2016-03-14 18:03:56	2016-03-16 04:00:00	418.704	350.0	15.0	12.0	27.0	30.0	6900.0	5157.84432498738
332	2016-03-14 18:03:56	2016-03-17 04:00:00	461.829	350.0	11.0	12.0	38.0	30.0	9701.0	7071.6955836229
333	2016-03-14 18:03:56	2016-03-18 04:00:00	322.419	350.0	12.0	12.0	26.0	30.0	6412.0	4798.0692250094
334	2016-03-14 18:03:56	2016-03-19 04:00:00	440.633	350.0	11.0	12.0	40.0	30.0	9643.0	7020.81993605674
335	2016-03-14 18:03:56	2016-03-20 04:00:00	309.39	350.0	12.0	12.0	35.0	30.0	5352.0	3965.97781493876
336	2016-03-21 19:23:36	2016-03-21 04:00:00	368.512	350.0	12.0	12.0	38.0	30.0	6647.0	5069.63263124716
337	2016-03-21 19:23:36	2016-03-22 04:00:00	371.162	350.0	13.0	12.0	45.0	30.0	7786.0	5912.25421512942
338	2016-03-21 19:23:36	2016-03-23 04:00:00	183.033	350.0	10.0	12.0	8.0	30.0	2366.0	1720.11841394124
339	2016-03-21 19:23:36	2016-03-24 04:00:00	289.15	350.0	12.0	12.0	12.0	30.0	4839.0	3453.24857764703
340	2016-03-21 19:23:36	2016-03-25 04:00:00	265.012	350.0	13.0	12.0	9.0	30.0	3635.0	2714.82200816309
341	2016-03-21 19:23:36	2016-03-26 04:00:00	658.617000000001	350.0	10.0	12.0	82.0	30.0	15906.0	11424.3456067285
342	2016-03-21 19:23:36	2016-03-27 04:00:00	180.65	350.0	10.0	12.0	7.0	30.0	2512.0	1876.62907064462

ACTIVITY CACHE
healthdb_secure.sqlite



walk_distance
2881.04356095369
7396.11327804928
5157.84432498738
7071.6955836229
4798.06892250094
7020.81993605674
3965.97781493876
5069.63263124716
5912.25421512942
1720.11841394124
3453.24857764703
2714.82200816309
11424.3456067285



11424.3456067285 meters in miles

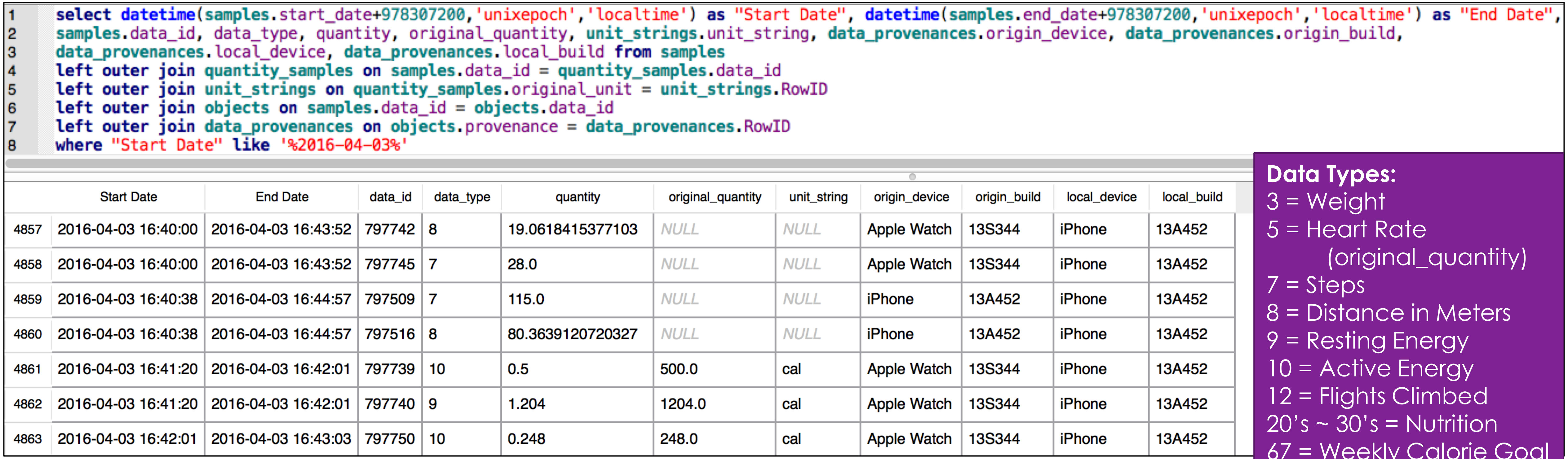
Input interpretation:

convert 11424.3456067285 meters to miles

Result:

7.0987592501842 miles

ACTIVITY "SAMPLES"
healthdb_secure.sqlite



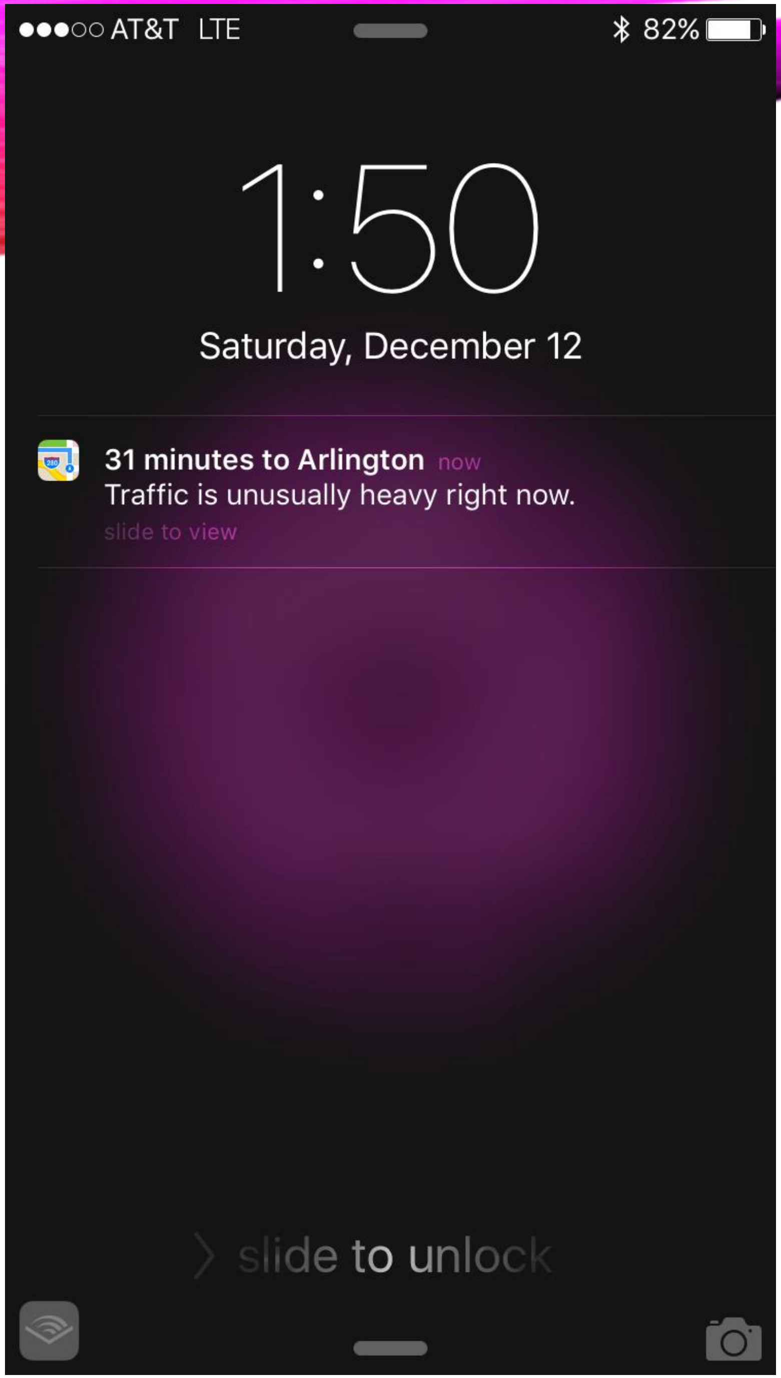
```
select datetime(samples.start_date+978307200,'unixepoch','localtime') as "Start Date", datetime(samples.end_date+978307200,'unixepoch','localtime') as "End Date",
samples.data_id, data_type, quantity, original_quantity, unit_strings.unit_string, data_provenances.origin_device, data_provenances.origin_build,
data_provenances.local_device, data_provenances.local_build from samples
left outer join quantity_samples on samples.data_id = quantity_samples.data_id
left outer join unit_strings on quantity_samples.original_unit = unit_strings.RowID
left outer join objects on samples.data_id = objects.data_id
left outer join data_provenances on objects.provenance = data_provenances.RowID
where "Start Date" like '%2016-04-03%'
```

	Start Date	End Date	data_id	data_type	quantity	original_quantity	unit_string	origin_device	origin_build	local_device	local_build
4857	2016-04-03 16:40:00	2016-04-03 16:43:52	797742	8	19.0618415377103	NULL	NULL	Apple Watch	13S344	iPhone	13A452
4858	2016-04-03 16:40:00	2016-04-03 16:43:52	797745	7	28.0	NULL	NULL	Apple Watch	13S344	iPhone	13A452
4859	2016-04-03 16:40:38	2016-04-03 16:44:57	797509	7	115.0	NULL	NULL	iPhone	13A452	iPhone	13A452
4860	2016-04-03 16:40:38	2016-04-03 16:44:57	797516	8	80.3639120720327	NULL	NULL	iPhone	13A452	iPhone	13A452
4861	2016-04-03 16:41:20	2016-04-03 16:42:01	797739	10	0.5	500.0	cal	Apple Watch	13S344	iPhone	13A452
4862	2016-04-03 16:41:20	2016-04-03 16:42:01	797740	9	1.204	1204.0	cal	Apple Watch	13S344	iPhone	13A452
4863	2016-04-03 16:42:01	2016-04-03 16:43:03	797750	10	0.248	248.0	cal	Apple Watch	13S344	iPhone	13A452

Data Types:

3 = Weight
5 = Heart Rate
(original_quantity)
7 = Steps
8 = Distance in Meters
9 = Resting Energy
10 = Active Energy
12 = Flights Climbed
20's ~ 30's = Nutrition
67 = Weekly Calorie Goal
70= Watch On
75 = Stand (Stood)
76 = Activity
79 = Workout
83 = Some Workouts

LOCATION



●●●○○ AT&T LTE 82%

1:50

Saturday, December 12

31 minutes to Arlington now

Traffic is unusually heavy right now.

slide to view

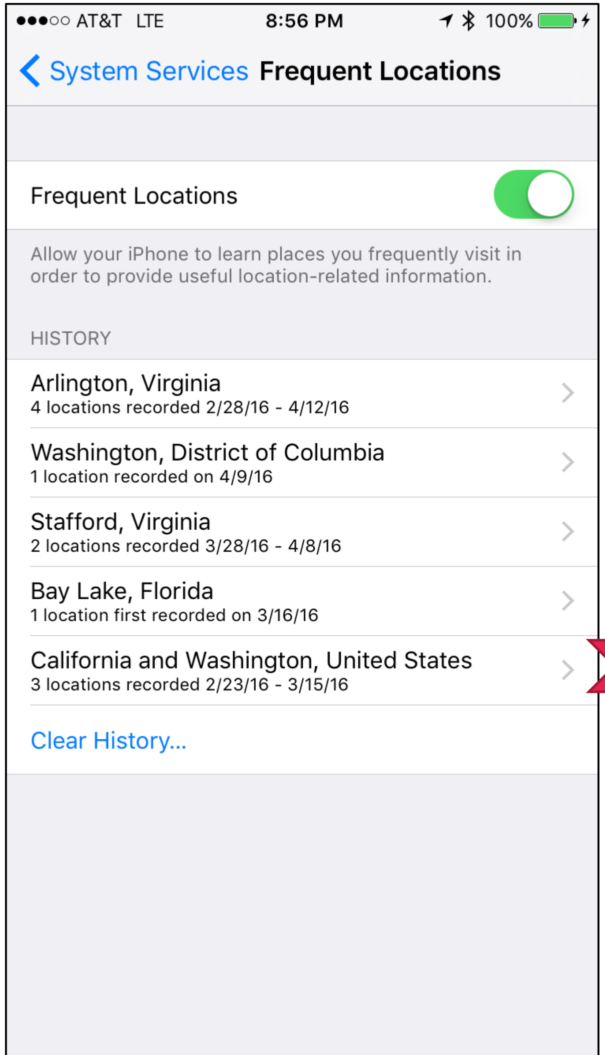
slide to unlock

FREQUENT LOCATIONS (ROUTINED)

- User Viewable (View Yours!):
  - Settings ->
  - Privacy ->
  - Location Services ->
  - System Services ->
  - Frequent Locations
- Uses Location Services
- More like “Frequent” and “Recent” Locations
- “Frequent” algorithm is unknown

FREQUENT LOCATIONS (ROUTINED)

Settings -> Privacy -> Location Services -> System Services -> Frequent Locations



●●●○○ AT&T LTE 8:56 PM 100%

‹ System Services **Frequent Locations**

Frequent Locations

Allow your iPhone to learn places you frequently visit in order to provide useful location-related information.

HISTORY

Arlington, Virginia
4 locations recorded 2/28/16 - 4/12/16

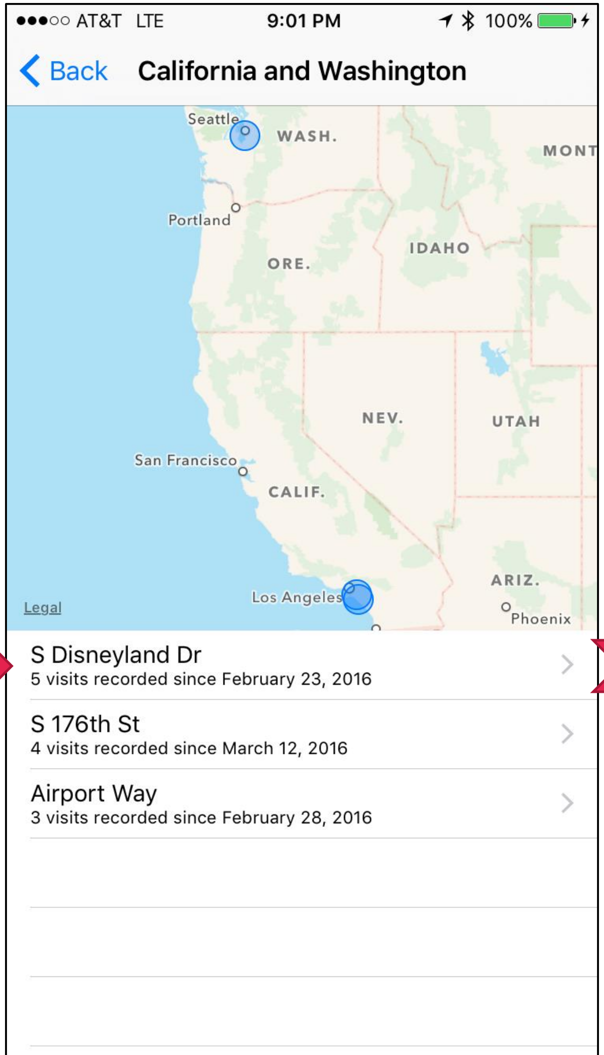
Washington, District of Columbia
1 location recorded on 4/9/16

Stafford, Virginia
2 locations recorded 3/28/16 - 4/8/16

Bay Lake, Florida
1 location first recorded on 3/16/16

California and Washington, United States
3 locations recorded 2/23/16 - 3/15/16

Clear History...



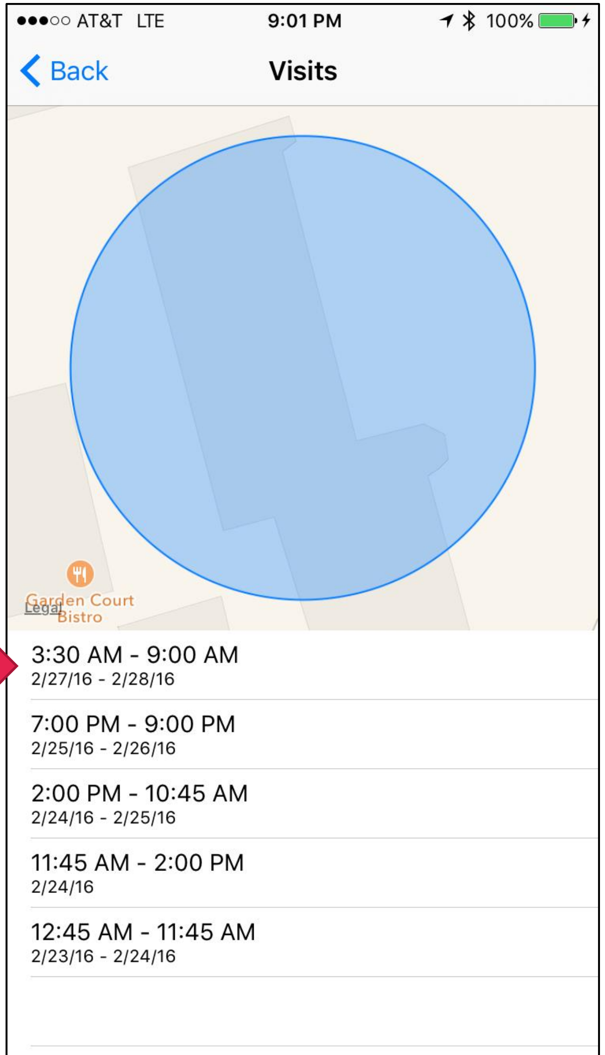
●●●○○ AT&T LTE 9:01 PM 100%

‹ Back **California and Washington**

S Disneyland Dr
5 visits recorded since February 23, 2016

S 176th St
4 visits recorded since March 12, 2016

Airport Way
3 visits recorded since February 28, 2016



●●●○○ AT&T LTE 9:01 PM 100%

‹ Back **Visits**

3:30 AM - 9:00 AM
2/27/16 - 2/28/16

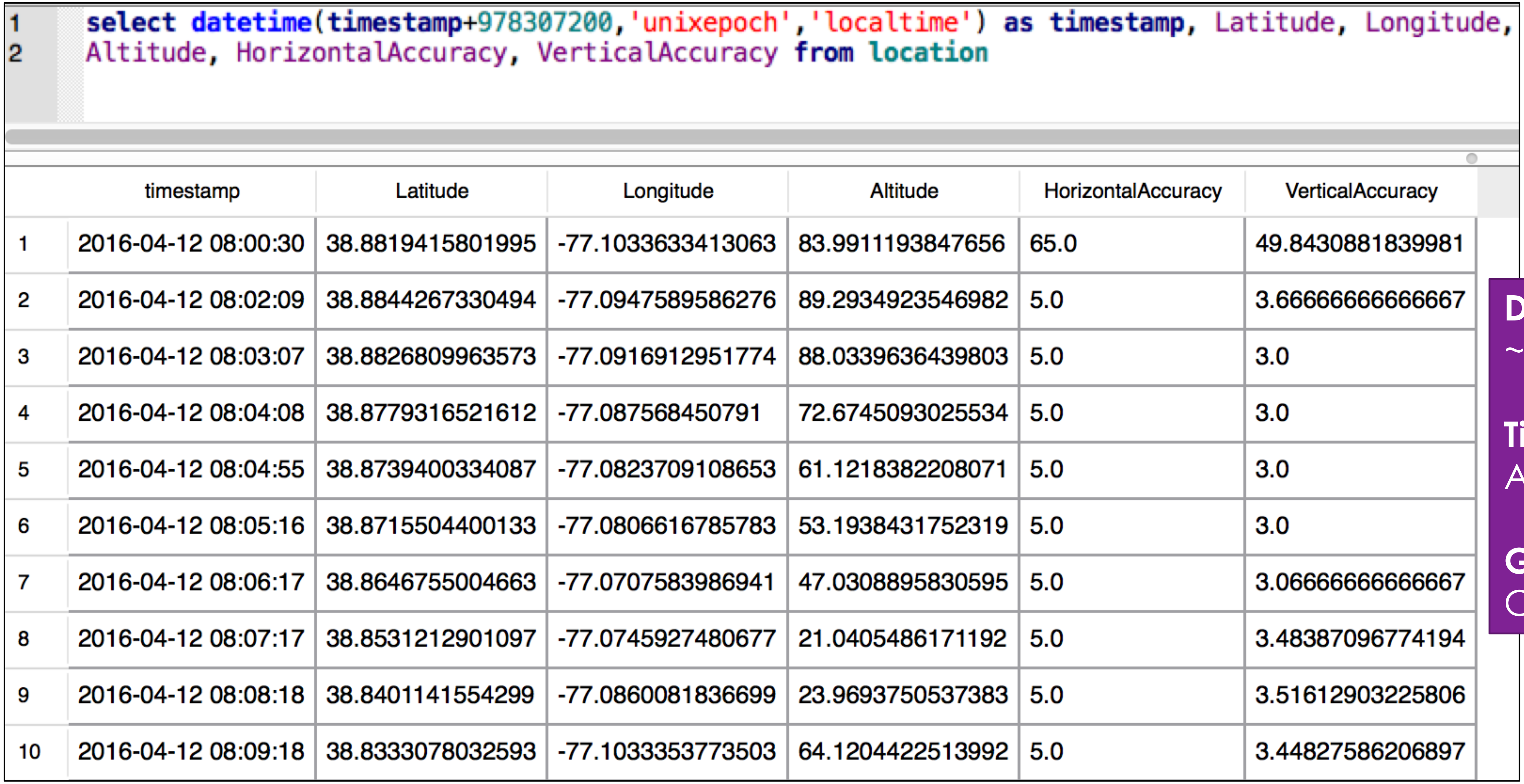
7:00 PM - 9:00 PM
2/25/16 - 2/26/16

2:00 PM - 10:45 AM
2/24/16 - 2/25/16

11:45 AM - 2:00 PM
2/24/16

12:45 AM - 11:45 AM
2/23/16 - 2/24/16

LOCATIONS (ROUTINED) cache_encryptedB.db



```
select datetime(timestamp+978307200,'unixepoch','localtime') as timestamp, Latitude, Longitude,
Altitude, HorizontalAccuracy, VerticalAccuracy from location
```

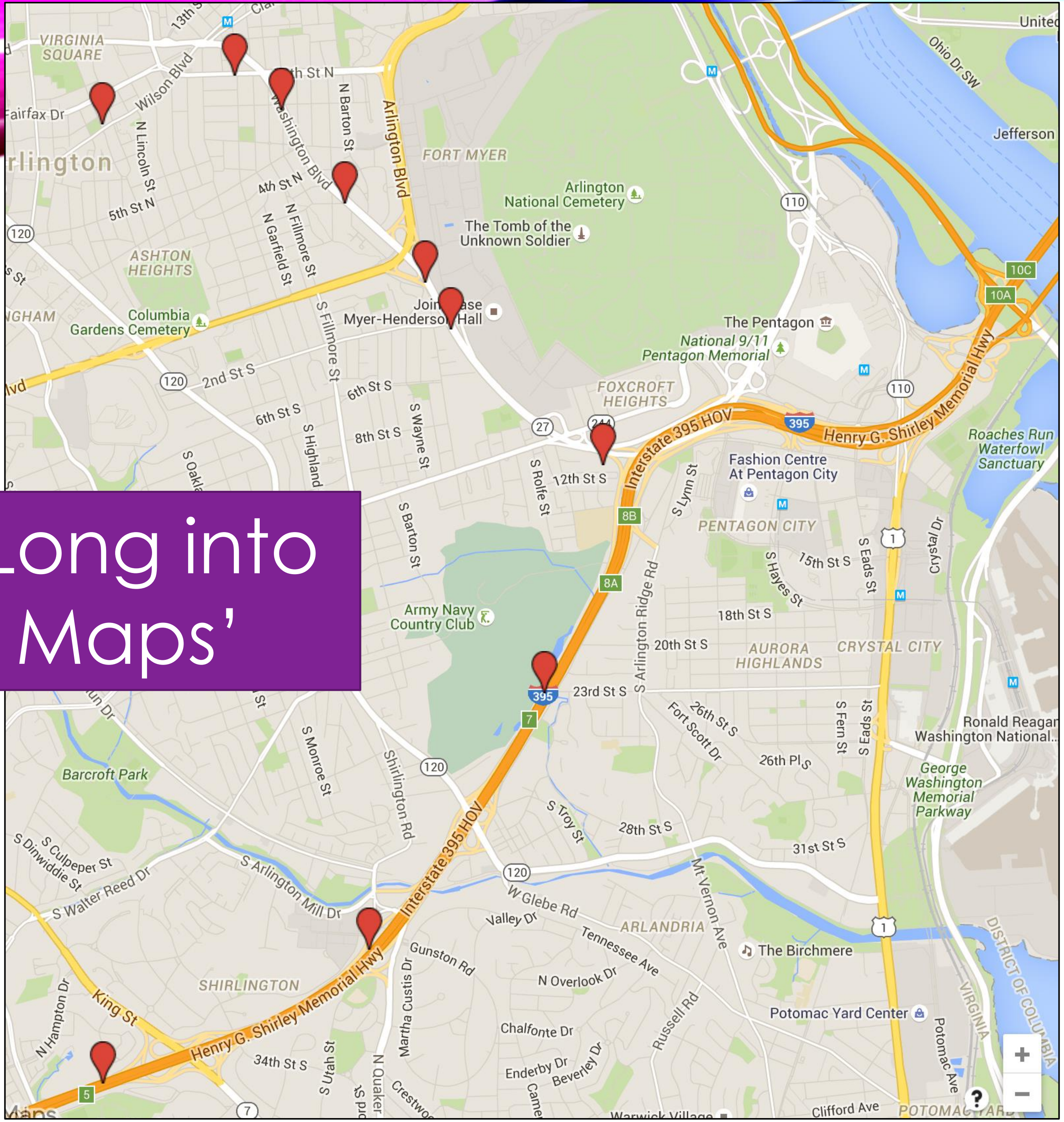
	timestamp	Latitude	Longitude	Altitude	HorizontalAccuracy	VerticalAccuracy
1	2016-04-12 08:00:30	38.8819415801995	-77.1033633413063	83.9911193847656	65.0	49.8430881839981
2	2016-04-12 08:02:09	38.8844267330494	-77.0947589586276	89.2934923546982	5.0	3.66666666666667
3	2016-04-12 08:03:07	38.8826809963573	-77.0916912951774	88.0339636439803	5.0	3.0
4	2016-04-12 08:04:08	38.8779316521612	-77.087568450791	72.6745093025534	5.0	3.0
5	2016-04-12 08:04:55	38.8739400334087	-77.0823709108653	61.1218382208071	5.0	3.0
6	2016-04-12 08:05:16	38.8715504400133	-77.0806616785783	53.1938431752319	5.0	3.0
7	2016-04-12 08:06:17	38.8646755004663	-77.0707583986941	47.0308895830595	5.0	3.06666666666667
8	2016-04-12 08:07:17	38.8531212901097	-77.0745927480677	21.0405486171192	5.0	3.48387096774194
9	2016-04-12 08:08:18	38.8401141554299	-77.0860081836699	23.9693750537383	5.0	3.51612903225806
10	2016-04-12 08:09:18	38.8333078032593	-77.1033353773503	64.1204422513992	5.0	3.44827586206897

Data Retention:
~1 Days

Timestamps:
Accurate*

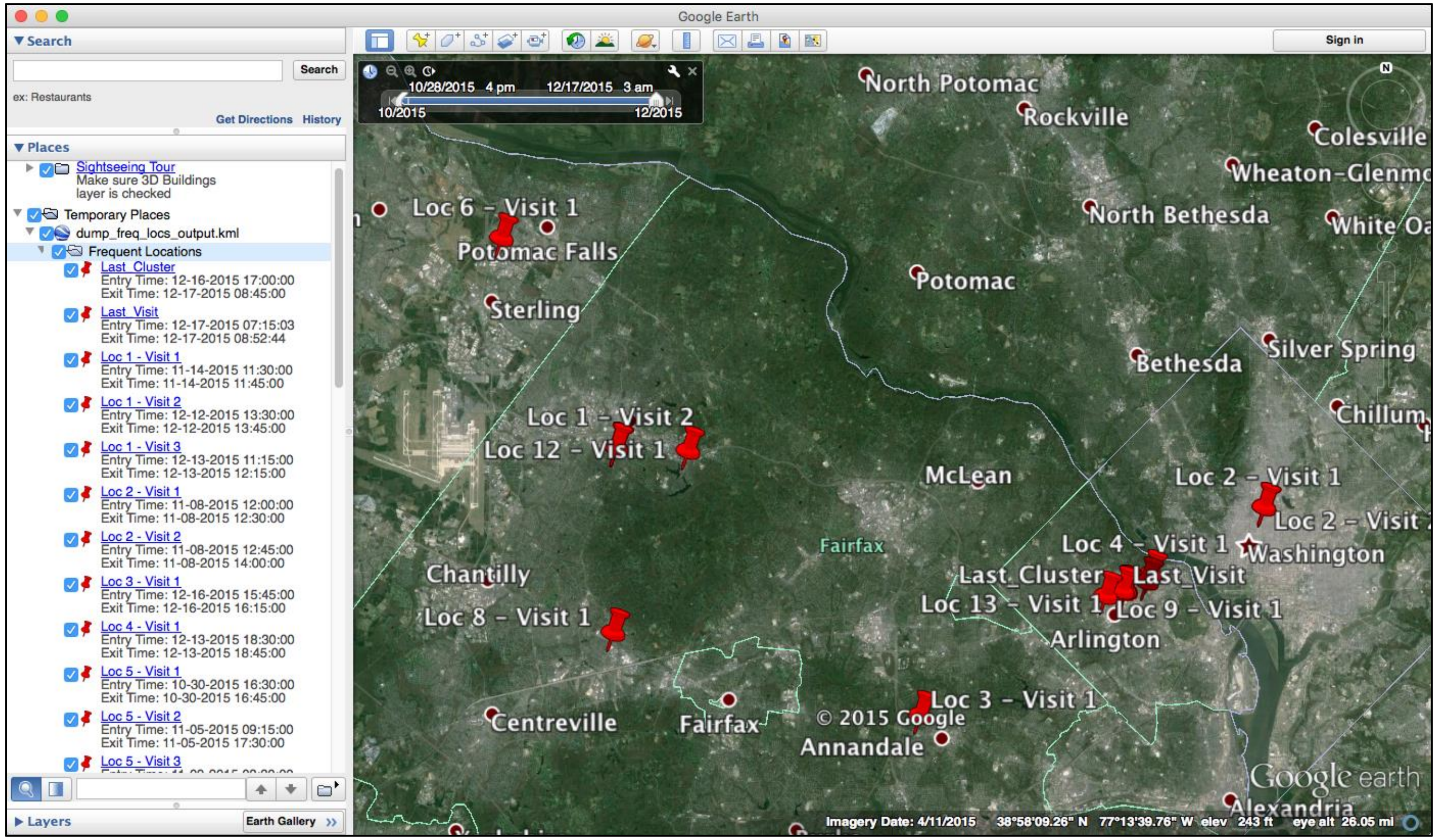
GPS Accuracy:
Close, but YMMV

Import Lat/Long into Google‘My Maps’



FREQUENT LOCATIONS
StateModel#.archive (1 or 2)

- Contains Historical Data
  - Not every location for all time
  - Uses algorithm to decide
- NSKeyedArchiver Property List Files
  - No immediate context to keys/values
  - Very manual analysis process. ☹
- Python Script!
  - https://github.com/mac4n6/iOS-Frequent-Locations-Dumper
- Outputs
  - KML
  - CSV
  - Textual (Example Next Slide)



☑ Sightseeing Tour
Make sure 3D Buildings
layer is checked

☑ Temporary Places

☑ dump_freq_locs_output.kml

☑ Frequent Locations

☑ Last_Cluster
Entry Time: 12-16-2015 17:00:00
Exit Time: 12-17-2015 08:45:00

☑ Last_Visit
Entry Time: 12-17-2015 07:15:03
Exit Time: 12-17-2015 08:52:44

☑ Loc 1 - Visit 1
Entry Time: 11-14-2015 11:30:00
Exit Time: 11-14-2015 11:45:00

☑ Loc 1 - Visit 2
Entry Time: 12-12-2015 13:30:00
Exit Time: 12-12-2015 13:45:00

☑ Loc 1 - Visit 3
Entry Time: 12-13-2015 11:15:00
Exit Time: 12-13-2015 12:15:00

☑ Loc 2 - Visit 1
Entry Time: 11-08-2015 12:00:00
Exit Time: 11-08-2015 12:30:00

☑ Loc 2 - Visit 2
Entry Time: 11-08-2015 12:45:00
Exit Time: 11-08-2015 14:00:00

☑ Loc 3 - Visit 1
Entry Time: 12-16-2015 15:45:00
Exit Time: 12-16-2015 16:15:00

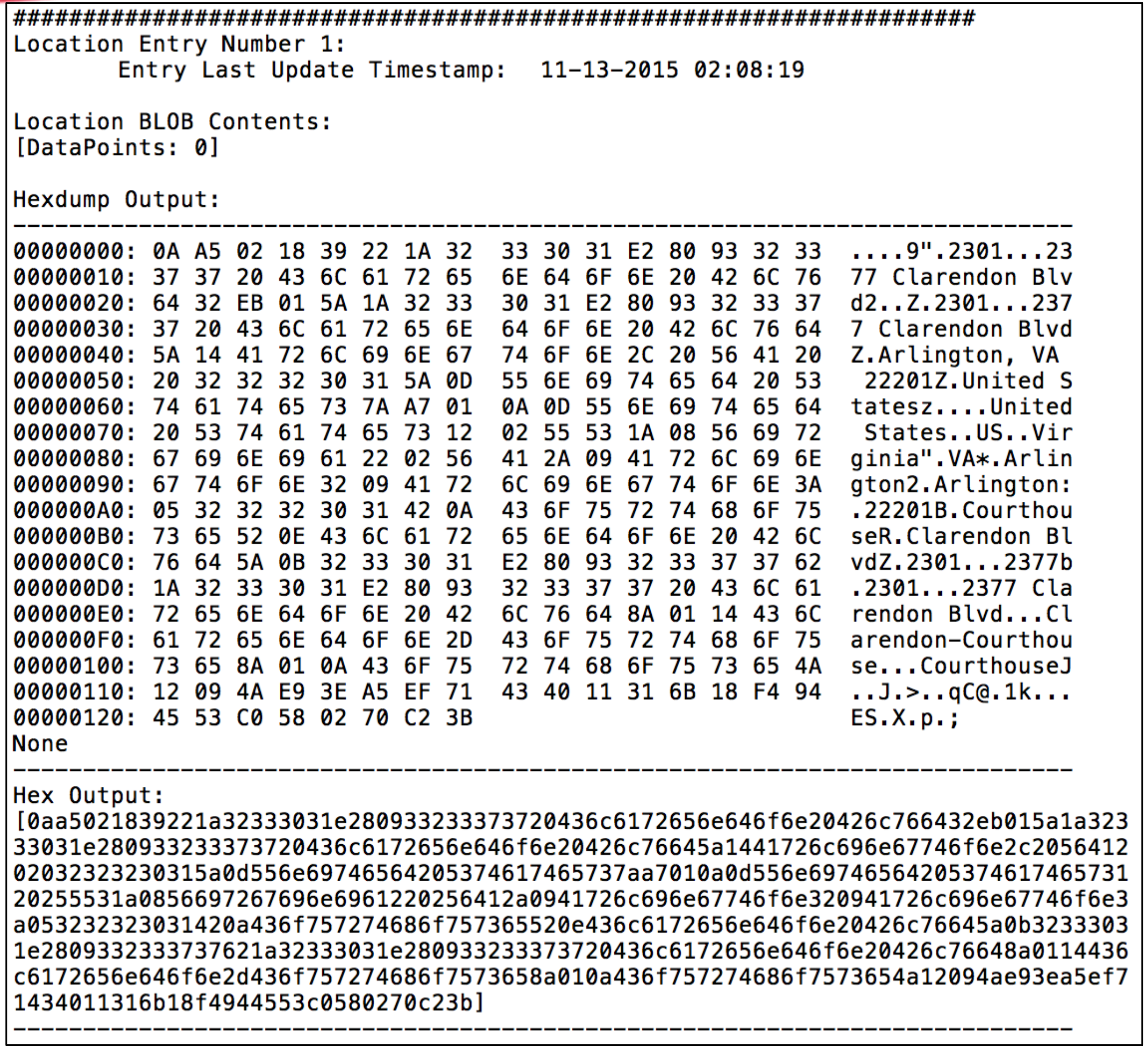
☑ Loc 4 - Visit 1
Entry Time: 12-13-2015 18:30:00
Exit Time: 12-13-2015 18:45:00

☑ Loc 5 - Visit 1
Entry Time: 10-30-2015 16:30:00
Exit Time: 10-30-2015 16:45:00

☑ Loc 5 - Visit 2
Entry Time: 11-05-2015 09:15:00
Exit Time: 11-05-2015 17:30:00

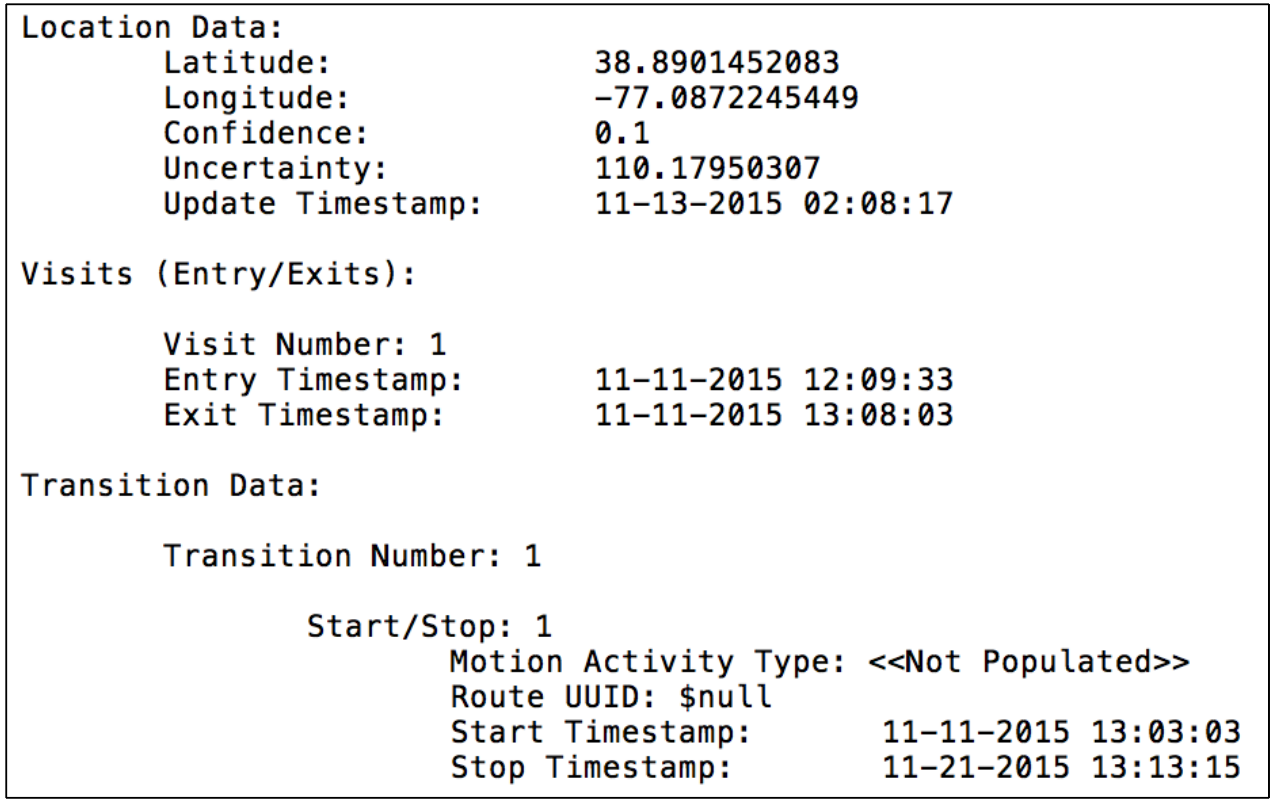
☑ Loc 5 - Visit 3

FREQUENT LOCATIONS
StateModel#.archive (1 or 2)



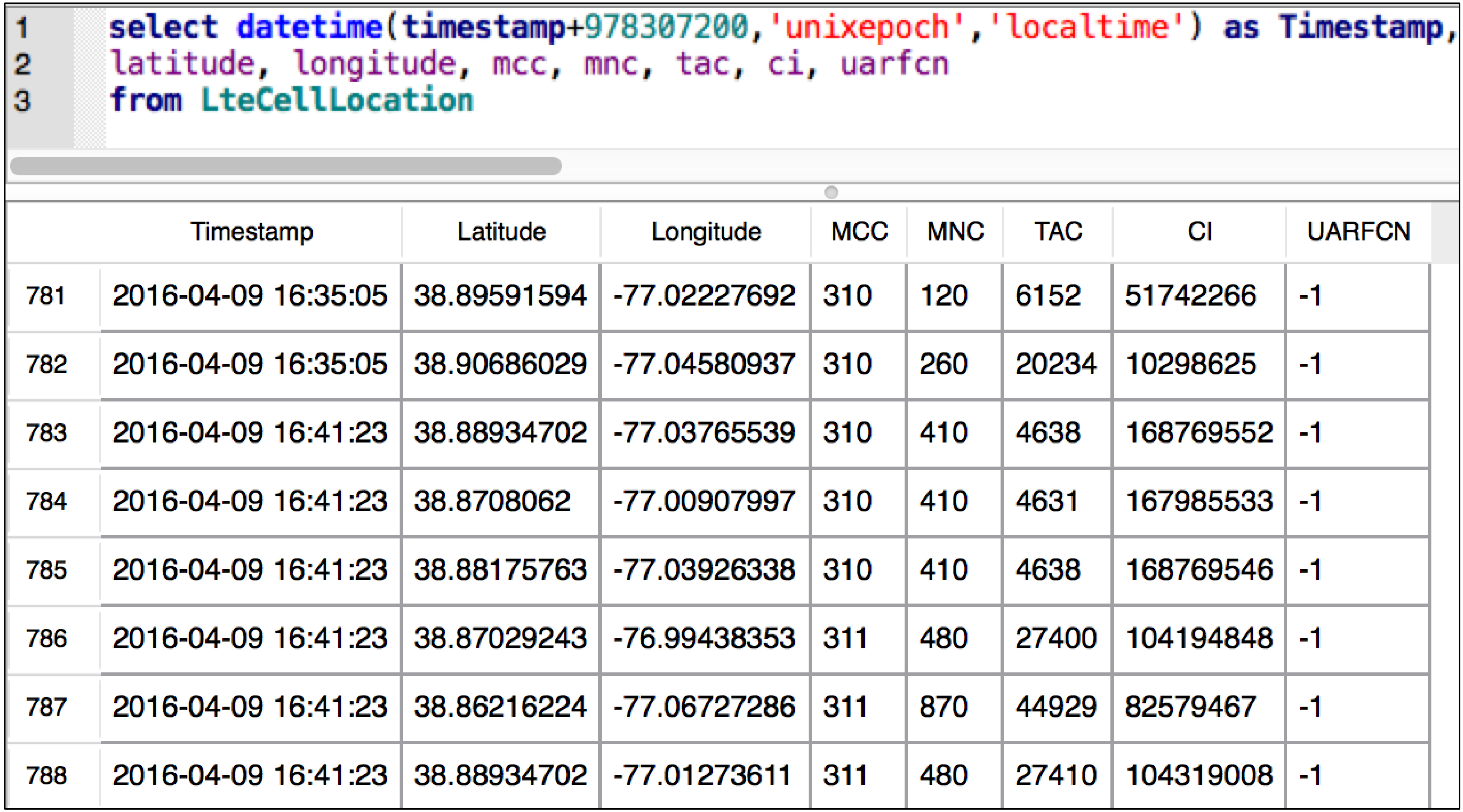
```
#####################################################################
Location Entry Number 1:
        Entry Last Update Timestamp:  11-13-2015 02:08:19

Location BLOB Contents:
[DataPoints: 0]

Hexdump Output:
----------------------------------------------------------------------------
00000000: 0A A5 02 18 39 22 1A 32  33 30 31 E2 80 93 32 33  ....9".2301...23
00000010: 37 37 20 43 6C 61 72 65  6E 64 6F 6E 20 42 6C 76  77 Clarendon Blv
00000020: 64 32 EB 01 5A 1A 32 33  30 31 E2 80 93 32 33 37  d2..Z.2301...237
00000030: 37 20 43 6C 61 72 65 6E  64 6F 6E 20 42 6C 76 64  7 Clarendon Blvd
00000040: 5A 14 41 72 6C 69 6E 67  74 6F 6E 2C 20 56 41 20  Z.Arlington, VA
00000050: 20 32 32 32 30 31 5A 0D  55 6E 69 74 65 64 20 53   22201Z.United S
00000060: 74 61 74 65 73 7A A7 01  0A 0D 55 6E 69 74 65 64  tatesz....United
00000070: 20 53 74 61 74 65 73 12  02 55 53 1A 08 56 69 72   States..US..Vir
00000080: 67 69 6E 69 61 22 02 56  41 2A 09 41 72 6C 69 6E  ginia".VA*.Arlin
00000090: 67 74 6F 6E 32 09 41 72  6C 69 6E 67 74 6F 6E 3A  gton2.Arlington:
000000A0: 05 32 32 32 30 31 42 0A  43 6F 75 72 74 68 6F 75  .22201B.Courthou
000000B0: 73 65 52 0E 43 6C 61 72  65 6E 64 6F 6E 20 42 6C  seR.Clarendon Bl
000000C0: 76 64 5A 0B 32 33 30 31  E2 80 93 32 33 37 37 62  vdZ.2301...2377b
000000D0: 1A 32 33 30 31 E2 80 93  32 33 37 37 20 43 6C 61  .2301...2377 Cla
000000E0: 72 65 6E 64 6F 6E 20 42  6C 76 64 8A 01 14 43 6C  rendon Blvd...Cl
000000F0: 61 72 65 6E 64 6F 6E 2D  43 6F 75 72 74 68 6F 75  arendon-Courthou
00000100: 73 65 8A 01 0A 43 6F 75  72 74 68 6F 75 73 65 4A  se...CourthouseJ
00000110: 12 09 4A E9 3E A5 EF 71  43 40 11 31 6B 18 F4 94  ..J.>..qC@.1k...
00000120: 45 53 C0 58 02 70 C2 3B                           ES.X.p.;
None
----------------------------------------------------------------------------
Hex Output:
[0aa5021839221a32333031e2809332333737720436c6172656e646f6e20426c766432eb015a1a323
33031e2809332333737720436c6172656e646f6e20426c76645a1441726c696e67746f6e2c2056412
02032323230315a0d556e6974656420537461746573 7aa7010a0d556e69746564205374617465731
```

```
a05323232303142 0a436f757274686f757365520e436c6172656e646f6e20426c76645a0b3233303
```



```
Location Data:
        Latitude:               38.8901452083
        Longitude:              -77.0872245449
        Confidence:             0.1
        Uncertainty:            110.17950307
        Update Timestamp:       11-13-2015 02:08:17

Visits (Entry/Exits):

        Visit Number: 1
        Entry Timestamp:        11-11-2015 12:09:33
        Exit Timestamp:         11-11-2015 13:08:03

Transition Data:

        Transition Number: 1

                Start/Stop: 1
                        Motion Activity Type: <<Not Populated>>
                        Route UUID: $null
                        Start Timestamp:        11-11-2015 13:03:03
                        Stop Timestamp:         11-21-2015 13:13:15
```

CELL LOCATIONS cache_encryptedA.db lockCache_encryptedA.db



```
select datetime(timestamp+978307200,'unixepoch','localtime') as Timestamp,
latitude, longitude, mcc, mnc, tac, ci, uarfcn
from LteCellLocation
```

	Timestamp	Latitude	Longitude	MCC	MNC	TAC	CI	UARFCN
781	2016-04-09 16:35:05	38.89591594	-77.02227692	310	120	6152	51742266	-1
782	2016-04-09 16:35:05	38.90686029	-77.04580937	310	260	20234	10298625	-1
783	2016-04-09 16:41:23	38.88934702	-77.03765539	310	410	4638	168769552	-1
784	2016-04-09 16:41:23	38.8708062	-77.00907997	310	410	4631	167985533	-1
785	2016-04-09 16:41:23	38.88175763	-77.03926338	310	410	4638	168769546	-1
786	2016-04-09 16:41:23	38.87029243	-76.99438353	311	480	27400	104194848	-1
787	2016-04-09 16:41:23	38.86216224	-77.06727286	311	870	44929	82579467	-1
788	2016-04-09 16:41:23	38.88934702	-77.01273611	311	480	27410	104319008	-1

Data Retention:
~1 Week
(Varies Per Table)

Timestamps:
Accurate*

GPS Accuracy:
Within General Area
(See Next Slide)

Many Other Tables:

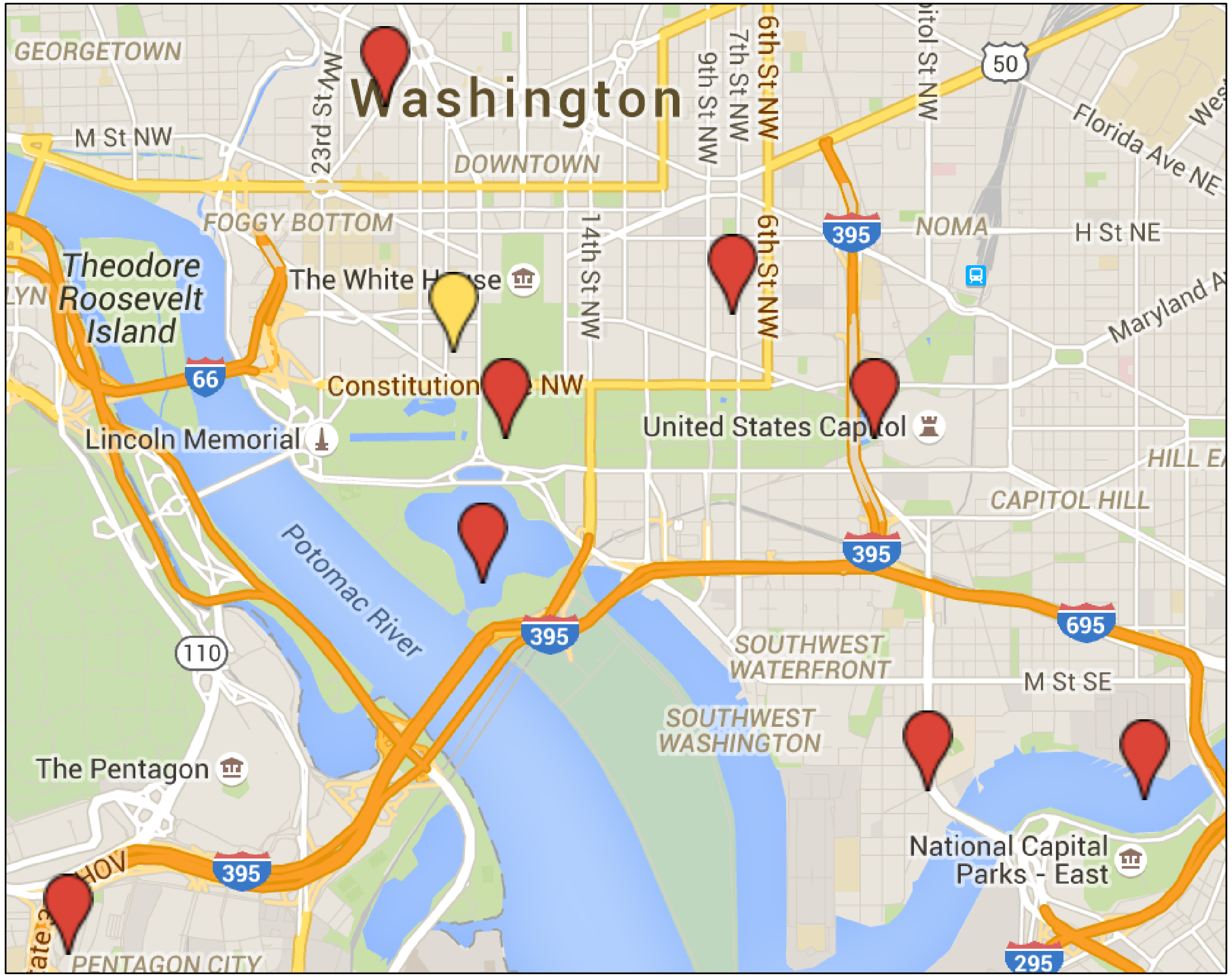
- CDMA
- SCDMA
- LTE
- WIFI
- “Indoor”
- Application/“WTW”

CELL LOCATIONS
cache_encryptedA.db

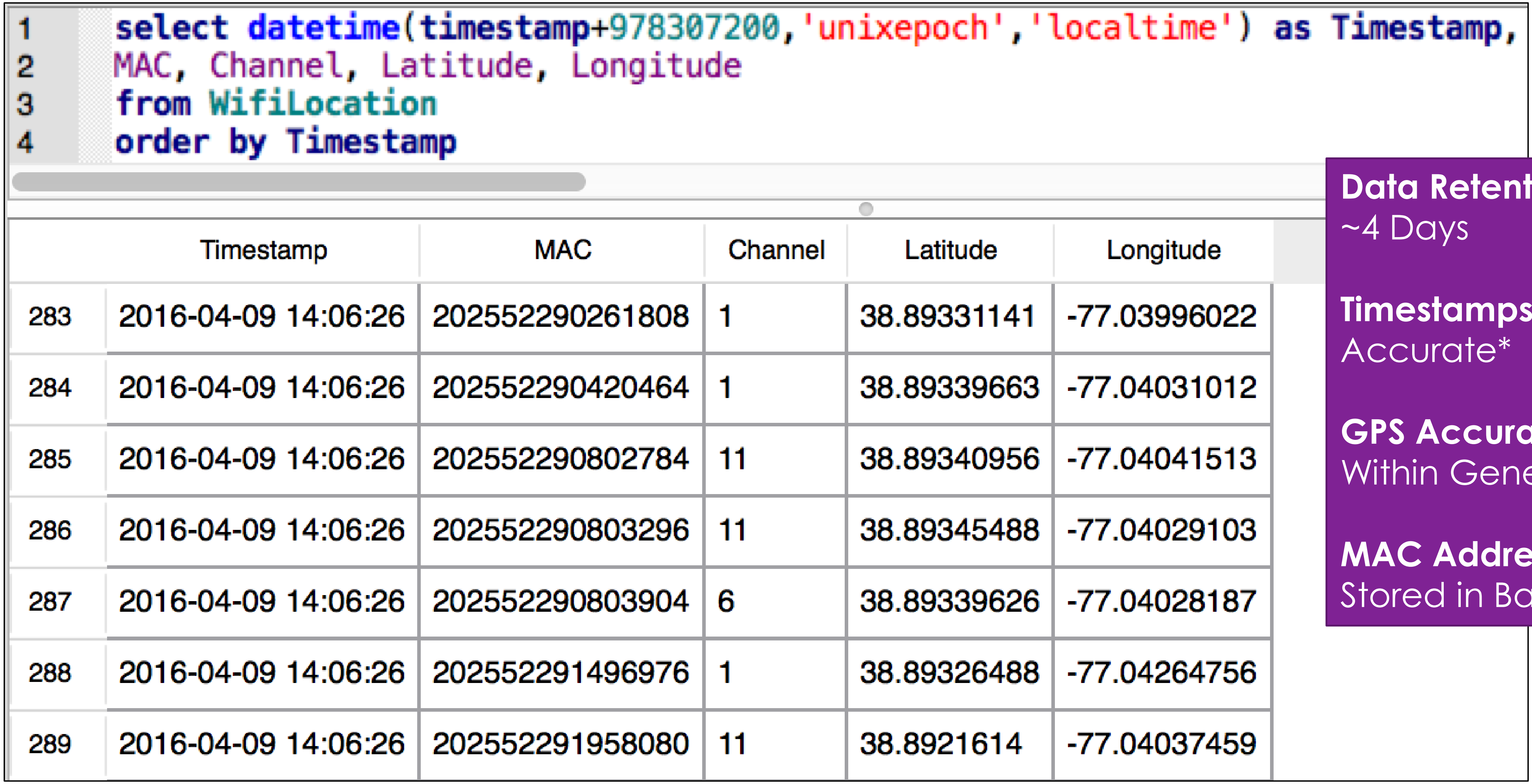
Yellow Point:
My Actual Location

Red Points:
"LTE Cell Locations"

Warning:
Locations are in general area, NOT exact area



WIFI LOCATIONS
cache_encryptedB.db



```
select datetime(timestamp+978307200,'unixepoch','localtime') as Timestamp,
MAC, Channel, Latitude, Longitude
from WifiLocation
order by Timestamp
```

	Timestamp	MAC	Channel	Latitude	Longitude
283	2016-04-09 14:06:26	202552290261808	1	38.89331141	-77.03996022
284	2016-04-09 14:06:26	202552290420464	1	38.89339663	-77.04031012
285	2016-04-09 14:06:26	202552290802784	11	38.89340956	-77.04041513
286	2016-04-09 14:06:26	202552290803296	11	38.89345488	-77.04029103
287	2016-04-09 14:06:26	202552290803904	6	38.89339626	-77.04028187
288	2016-04-09 14:06:26	202552291496976	1	38.89326488	-77.04264756
289	2016-04-09 14:06:26	202552291958080	11	38.8921614	-77.04037459

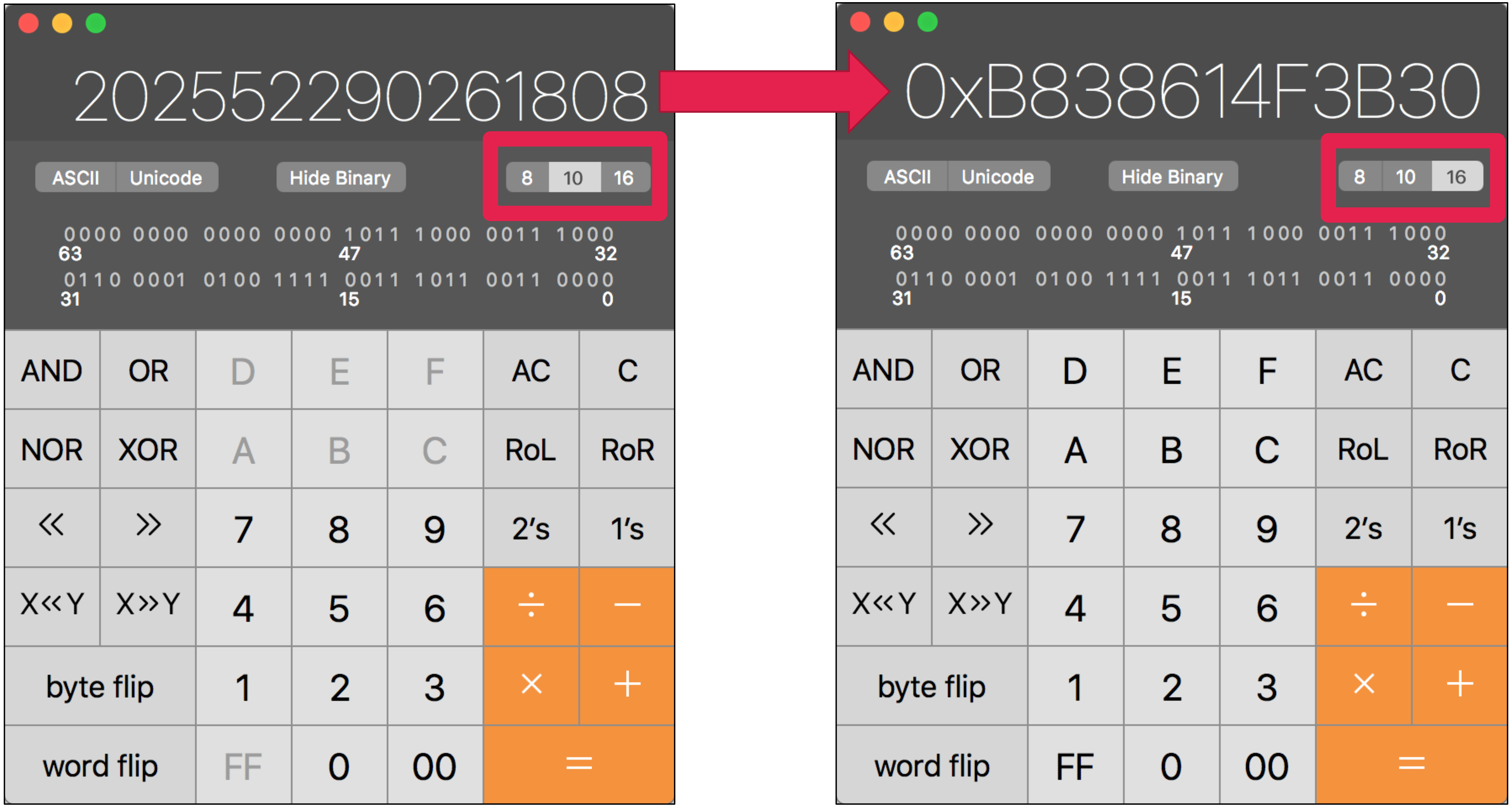
Data Retention:
~4 Days

Timestamps:
Accurate*

GPS Accuracy:
Within General Area

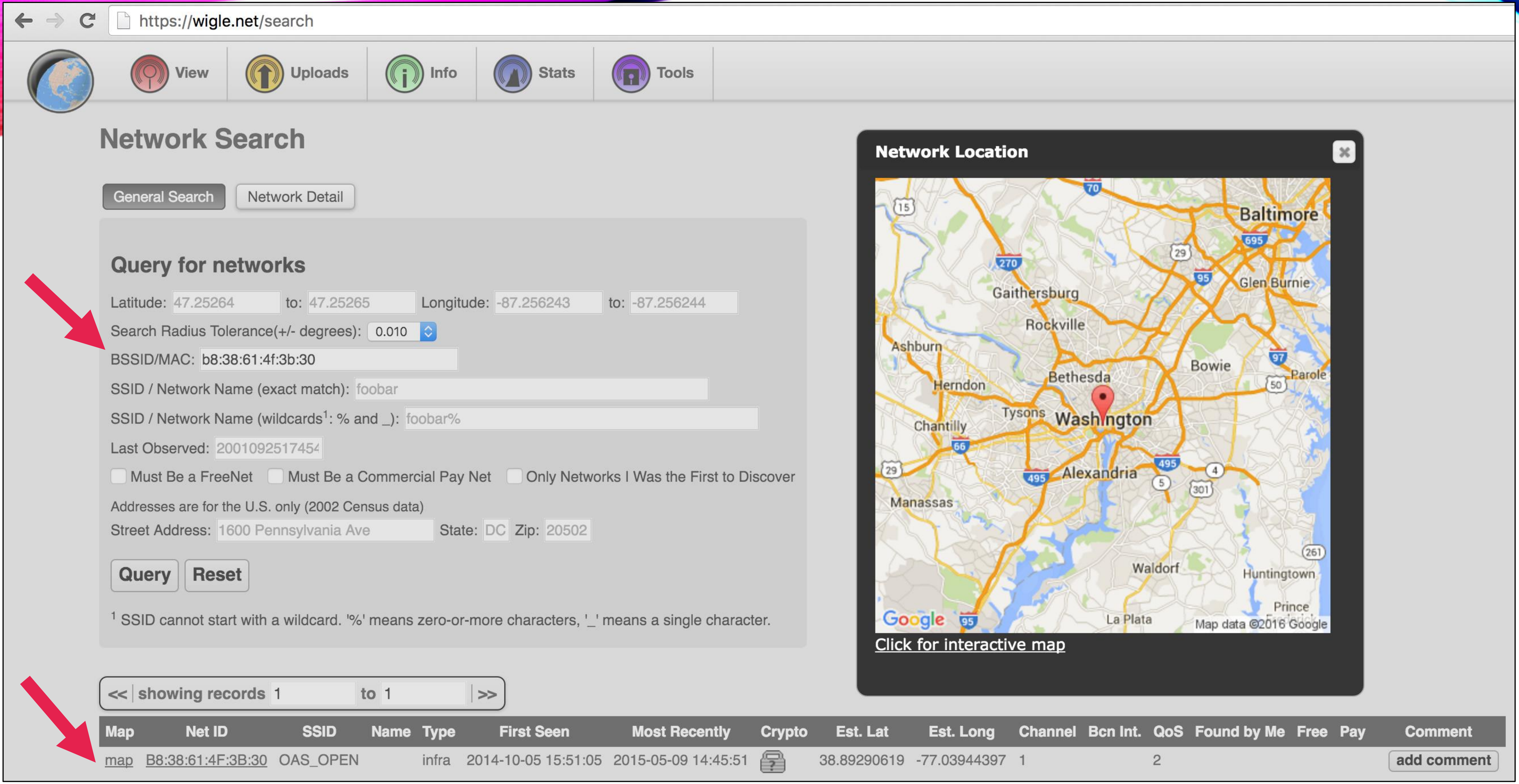
MAC Address:
Stored in Base10

WIFI LOCATIONS
cache_encryptedB.db



```
202552290261808
0000 0000 0000 0000 1011 1000 0011 1000
63                 47                 32
0110 0001 0100 1111 0011 1011 0011 0000
31                 15                  0
```

```
0xB838614F3B30
0000 0000 0000 0000 1011 1000 0011 1000
63                 47                 32
0110 0001 0100 1111 0011 1011 0011 0000
31                 15                  0
```



Network Search

General Search | Network Detail

Query for networks

Latitude: 47.25264 to: 47.25265 Longitude: -87.256243 to: -87.256244

Search Radius Tolerance(+/- degrees): 0.010

BSSID/MAC: b8:38:61:4f:3b:30

SSID / Network Name (exact match): foobar

SSID / Network Name (wildcards[1]: % and _): foobar%

Last Observed: 2001092517454

□ Must Be a FreeNet □ Must Be a Commercial Pay Net □ Only Networks I Was the First to Discover

Addresses are for the U.S. only (2002 Census data)

Street Address: 1600 Pennsylvania Ave State: DC Zip: 20502

Query Reset

[1] SSID cannot start with a wildcard. '%' means zero-or-more characters, '_' means a single character.

Network Location

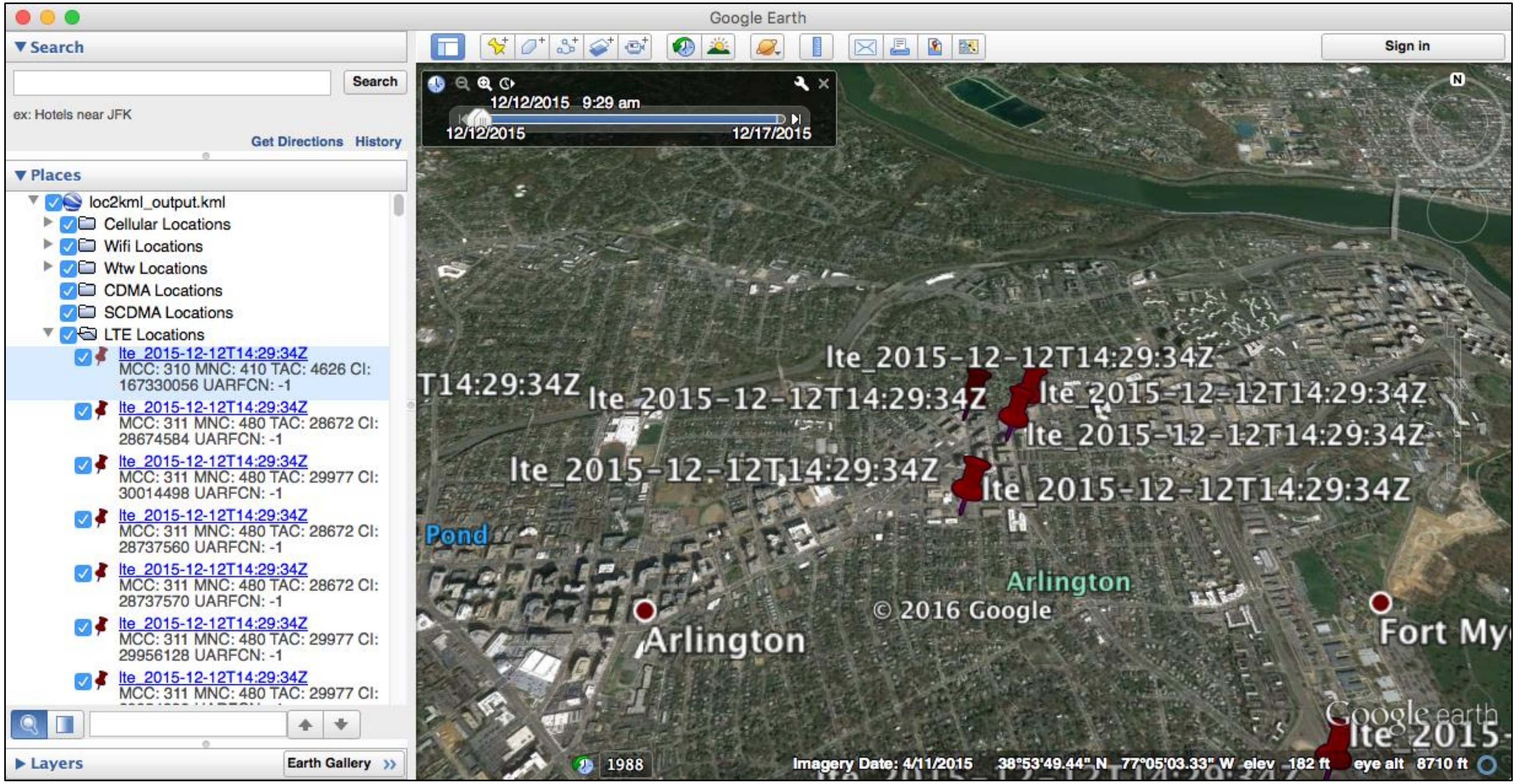
Click for interactive map

<< showing records 1 to 1 >>

Map	Net ID	SSID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long	Channel	Bcn Int.	QoS	Found by Me	Free	Pay	Comment
map	B8:38:61:4F:3B:30	OAS_OPEN		infra	2014-10-05 15:51:05	2015-05-09 14:45:51	?	38.89290619	-77.03944397	1		2				add comment

LOCATIONS SCRAPER PYTHON SCRIPT

- Gimme All the Locations!
  - Routined
  - Locationd
- Python Script!
  - Will Release Soon!
  - Making code less redundant
  - Need it NOW? Just ask, politely.
- Outputs
  - KML
  - CSV



Google Earth

▼ Search

ex: Hotels near JFK

Get Directions History

▼ Places

- ☑ loc2kml_output.kml
  - ☑ Cellular Locations
  - ☑ Wifi Locations
  - ☑ Wtw Locations
  - ☑ CDMA Locations
  - ☑ SCDMA Locations
  - ☑ LTE Locations
    - ☑ lte_2015-12-12T14:29:34Z
      MCC: 310 MNC: 410 TAC: 4626 CI: 167330056 UARFCN: -1
    - ☑ lte_2015-12-12T14:29:34Z
      MCC: 311 MNC: 480 TAC: 28672 CI: 28674584 UARFCN: -1
    - ☑ lte_2015-12-12T14:29:34Z
      MCC: 311 MNC: 480 TAC: 29977 CI: 30014498 UARFCN: -1
    - ☑ lte_2015-12-12T14:29:34Z
      MCC: 311 MNC: 480 TAC: 28672 CI: 28737560 UARFCN: -1
    - ☑ lte_2015-12-12T14:29:34Z
      MCC: 311 MNC: 480 TAC: 28672 CI: 28737570 UARFCN: -1
    - ☑ lte_2015-12-12T14:29:34Z
      MCC: 311 MNC: 480 TAC: 29977 CI: 29956128 UARFCN: -1
    - ☑ lte_2015-12-12T14:29:34Z
      MCC: 311 MNC: 480 TAC: 29977 CI:

▶ Layers

Imagery Date: 4/11/2015 38°53'49.44" N 77°05'03.33" W elev 182 ft eye alt 8710 ft

Work With Me!

- http://bit.ly/1qGWAmT

Attend SANS FOR518 – Mac Forensic Analysis!

- August/September – Virginia Beach, VA
- September – Las Vegas, NV
- October – Prague, CZ

Contact Info

- oompa@csh.rit.edu, @iamevltwin, mac4n6.com

Scripts & Presentations

- github.com/mac4n6

Questions?