FROM APPLE SEEDS TO APPLE PIE

SARAH EDWARDS
@IAMEVLTWIN | MAC4N6.COM

THE REASON:
PATTERN OF LIFE ANALYSIS ON MACOS AND IOS DEVICES

Applications	Battery Level and Charging Habits	Network Consumption and Usage	CarPlay Activity
Audio Output/Input	Location Habits	Device Lock Status & Methods	Various Configuration Items
Heart Rate	Steps & Distance	Camera/Flashlight Usage	User Activities

THE PROBLEM – DATA ACCESS

iOS & macOS each have their own challenges

macOS FileVault Encryption

macOS File Level Encryption (routined Database)

iOS Physical Device Access via:

- Jailbreak – "Physical/Logical" Dump
- Cellebrite CAS
- GrayShift's GrayKey

THE PROBLEM - CORRELATION

knowledgeC – /private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db

routined – /private/var/mobile/Library/Caches/com.apple.routined/

- Cache.sqlite, Local.sqlite, Cloud.sqlite

locationd – /private/var/root/Library/Caches/locationd/

- cache_encryptedB.db
- cache_encryptedC.db

Powerlog – /private/var/containers/Shared/SystemGroup/<GUID>/Library/BatteryLife/CurrentPowerlog.PLSQL

- More in Archives/ (GZipped)

CoreDuet – /private/var/mobile/Library/CoreDuet/

- coreduetd.db
- coreduetdClassD.db
- /People/interactionC.db
- coreduetdClassA.db

Health – /private/var/mobile/Library/Health/

- healthdb.sqlite
- healthdb_secure.sqlite

Aggregate Dictionary – /private/var/mobile/Library/AggregateDictionary/ADDataStore.sqlitedb

NetUsage – /private/var/networkd/netusage.sqlite

DataUsage – /private/var//wireless/Library/Databases/DataUsage.sqlite

…and every other SQL database imaginable…

THE PROBLEM – SQL QUERY BUILDING & SHARING

Single Query for a single purpose may take hours of building and testing

Query Validation and Testing

- OS's Change
- Database Schemas Change
- Devices are not equal
- Platforms are not equal

Query Sharing

- Every self-respecting investigator (at least Mac/Mobile) has a text file with queries/partial/broken queries they have used for cases.
- Sharing is Caring – @AlexisBrignoni - https://github.com/abrignoni/DFIR-SQL-Query-Repo

THE PROBLEM – SINGLE USE SCRIPTS

- Parses a Single Database
- Schemas Changes
- SQL Query Updates
- Potentially difficult for others to update

THE PROBLEM – AIN'T GOT TIME FOR THIS

- Exigent Circumstances
- Analyst Time & Case Backlogs
- Analyst Expertise
- Triage

THE PROBLEM – TIMESTAMPS & STORAGE FORMATS

Timestamps

- Unix Epoch (1/1/1970 00:00:00 UTC)
- Mac Epoch (1/1/2001 00:00:00 UTC)
- Timestamps from "The Future" (Thanks, Powerlog)
- Timestamps for "Per Hour" or "Per Day"

Data Storage

- Embedded BLOBs
  - Locations mostly.
  - Unknown Structures
- Embedded Plists
- GZipped Database Files
- Aggregated Data

THE PROBLEM – THE UNKNOWN

Data Retention

- Sometimes a day, sometimes for years…

Unknown (and hard to test) Column Values

- 0 and 1 do not necessarily mean True/False, On/Off in the world of Apple

Units of Measure

- WTF - is this seconds, bytes, meters, miles, infinite loops?

What in the hell Apple is doing, and why?

- ❤️ you Apple!

LOCATION - GRANULAR LOCATION CACHE.SQLITE [~7 DAYS]

```
1  SELECT
2    DATETIME(ZTIMESTAMP + 978307200, 'unixepoch') AS "TIMESTAMP",
3    ZLATITUDE || ", " || ZLONGITUDE AS "COORDINATES",
4    ZALTITUDE AS "ALTITUDE",
5    ZCOURSE AS "COURSE",
6    ZSPEED AS "SPEED IN M/S",
7    ZHORIZONTALACCURACY AS "HORIZONTAL ACCURACY",
8    ZVERTICALACCURACY AS "VERTICAL ACCURACY",
9    ZLATITUDE AS "LATITUDE",
10   ZLONGITUDE AS "LONGITUDE",
11   ZRTCLLOCATIONMO.Z_PK AS "ZRTCLLOCATIONMO TABLE ID"
12 FROM
13   ZRTCLLOCATIONMO
```

~7 Days of Granular Location Data = ~40k Data Points

	TIMESTAMP	COORDINATES	ALTITUDE	COURSE	SPEED IN M/S	HORIZONTAL ACCURACY	VERTICAL ACCURACY
37768	2018-09-17 21:35:35	38.8911858166667, -77.2098445333333	136.8	54.0	27.0597777777778	5.0	9.5
37769	2018-09-17 21:35:36	38.8913319166667, -77.2095898333333	136.9	53.5	27.5742222222222	5.0	9.5
37770	2018-09-17 21:35:37	38.8914809166667, -77.2093335333333	136.3	53.4	27.7285555555556	5.0	9.5
37771	2018-09-17 21:35:38	38.8916293166667, -77.2090776333333	136.3	53.5	27.6771111111111	5.0	9.5
37772	2018-09-17 21:35:39	38.8917772166667, -77.2088211166667	136.3	53.7	27.7285555555556	5.0	9.5
37773	2018-09-17 21:35:40	38.8919248166667, -77.20856395	136.3	53.7	27.78	5.0	9.5
37774	2018-09-17 21:35:41	38.89207385, -77.2083059666667	136.3	53.5	27.78	5.0	9.5
37775	2018-09-17 21:35:42	38.8922226833333, -77.2080493333333	136.1	53.5	27.78	5.0	9.5
37776	2018-09-17 21:35:43	38.8923720666667, -77.2077913833333	136.0	53.5	27.8828888888889	10.0	19.0
37777	2018-09-17 21:35:44	38.89252085, -77.2075343333333	135.7	53.5	27.8314444444444	5.0	9.5
37778	2018-09-17 21:35:45	38.8926699166667, -77.207277	135.5	53.5	27.8314444444444	5.0	9.5
37779	2018-09-17 21:35:46	38.89281995, -77.2070191166667	135.3	53.4	27.8828888888889	5.0	9.5

LOCATION – PARKING HISTORY LOCAL.SQLITE [~3 MONTHS]

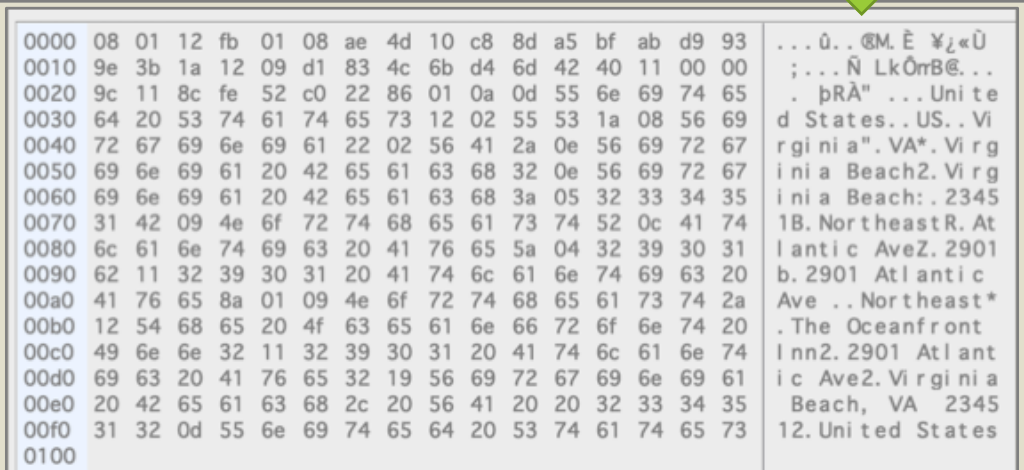
```
1  SELECT
2    DATETIME(ZRTVEHICLEEVENTHISTORYMO.ZDATE + 978307200, 'unixepoch') AS "DATE",
3    DATETIME(ZRTVEHICLEEVENTHISTORYMO.ZLOCDATE + 978307200, 'unixepoch') AS "LOCATION DATE",
4    ZLOCLATITUDE || ", " || ZLOCLONGITUDE AS "COORDINATES",
5    ZLOCUNCERTAINTY AS "LOCATION UNCERTAINTY",
6    ZIDENTIFIER AS "IDENTIFIER",
7    ZLOCLATITUDE AS "LATITUDE",
8    ZLOCLONGITUDE AS "LONGITUDE",
9    ZRTVEHICLEEVENTHISTORYMO.Z_PK AS "ZRTLEARNEDVISITMO TABLE ID"
10 FROM
11   ZRTVEHICLEEVENTHISTORYMO
```

	DATE	LOCATION DATE	COORDINATES	LOCATION UNCERTAINTY	IDENTIFIER
1	2018-07-30 12:43:18	2018-07-30 12:43:18	38.84 , -77.43	19.7281581163406	91438576-B81F-48F7-B16A-F3FDAEC1E52B
2	2018-07-30 12:43:18	2018-07-30 12:43:18	38.84 , -77.43	19.7281581163406	91438576-B81F-48F7-B16A-F3FDAEC1E52B
3	2018-07-30 23:21:43	2018-07-30 23:21:43	38.88 , -77.10	51.7145556211472	16076743-683D-47AC-8754-A3896A4BE746
4	2018-07-30 23:21:43	2018-07-30 23:21:43	38.88 , -77.10	51.7145556211472	16076743-683D-47AC-8754-A3896A4BE746
5	2018-07-30 23:21:43	2018-07-30 23:21:43	38.88 , -77.10	51.7145556211472	16076743-683D-47AC-8754-A3896A4BE746
6	2018-07-30 23:21:43	2018-07-30 23:21:43	38.88 , -77.10	51.7145556211472	16076743-683D-47AC-8754-A3896A4BE746
7	2018-07-30 23:21:43	2018-07-30 23:21:43	38.88 , -77.10	51.7145556211472	16076743-683D-47AC-8754-A3896A4BE746
8	2018-07-30 23:21:43	2018-07-30 23:21:43	38.88 , -77.10	51.7145556211472	16076743-683D-47AC-8754-A3896A4BE746
9	2018-07-31 13:25:38	2018-07-31 13:25:38	38.84 -77.43	19.1095933318138	0F92B57C-BE97-4455-945E-E4C1A4FF6ECD
10	2018-07-31 13:25:38	2018-07-31 13:25:38	38.84 -77.43	19.1095933318138	0F92B57C-BE97-4455-945E-E4C1A4FF6ECD
11	2018-07-31 20:41:34	2018-07-31 20:41:34	38.72 -77.200	19.6217827796936	680CCFF9-FB94-47F6-919C-7E618371B367
12	2018-08-01 13:28:04	2018-08-01 13:28:04	38.84 , -77.43	6.16909950971603	088B4785-29A9-49B5-BD41-630A2779EE98
13	2018-08-01 13:28:04	2018-08-01 13:28:04	38.84 , -77.43	6.16909950971603	088B4785-29A9-49B5-BD41-630A2779EE98
14	2018-08-01 13:28:04	2018-08-01 13:28:04	38.84 , -77.43	6.16909950971603	088B4785-29A9-49B5-BD41-630A2779EE98

LOCATION – SIGNIFICANT LOCATIONS CLOUD.SQLITE [VARIABLE RETENTION]

	INBOUND START DATE	INBOUND STOP DATE	COORDINATES	PLACE ID	DATA POINT COUNT	LOCATION UNCERTAINTY	CONFIDENCE	VISIT ENTRY	VISIT EXIT	VISIT CREATION
112	2018-08-28 07:49:23	2018-08-28 07:49:43	36.8584776161007, -75.9773382744851	256	1209	33.3465878342497	1.0	2018-08-28 07:49:43	2018-08-28 19:37:35	2018-08-31 02:05:24
113	2018-08-28 19:37:35	2018-08-28 19:38:03	36.8620089564409, -75.9783914610243	257	639	31.0881516698943	1.0	2018-08-28 19:38:03	2018-08-28 23:24:12	2018-08-31 02:05:24
114	2018-08-28 23:24:12	2018-08-28 23:24:20	36.864049006369, -75.9803518891189	258	143	56.9260913754098	1.0	2018-08-28 23:24:20	2018-08-29 00:03:24	2018-08-31 02:05:24
115	2018-08-29 00:03:24	2018-08-29 00:04:54	36.8619865697023, -75.9783645029448	257	688	23.2025883459664	1.0	2018-08-29 00:04:54	2018-08-29 04:01:08	2018-08-31 02:05:24

	DEVICE CLASS	DEVICE MODEL	LEARNED PLACE CREATION	LEARNED PLACE EXPIRATION	MAP ITEM CREATION	PLACE NAME BLOB	PLACE GEO BLOB	LATITUDE	LONGITUDE
112	iPhone	D221AP	2018-08-31 02:06:21	2018-11-03 01:47:03	2018-08-31 02:06:09	*BLOB*	*BLOB*	36.8584776161007	-75.9773382744851
113	iPhone	D221AP	2018-08-31 02:06:49	2018-11-03 01:47:03	2018-08-31 02:06:46	*BLOB*	*BLOB*	36.8620089564409	-75.9783914610243
114	iPhone	D221AP	2018-08-31 02:07:16	2018-11-03 01:47:03	2018-08-31 02:07:14	*BLOB*	*BLOB*	36.864049006369	-75.9803518891189
115	iPhone	D221AP	2018-08-31 02:06:49	2018-11-03 01:47:03	2018-08-31 02:06:46	*BLOB*	*BLOB*	36.8619865697023	-75.9783645029448



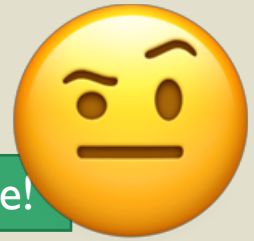
```
0000  08 01 12 fb 01 08 ae  4d 10 c8 8d a5 bf  ab d9 93   ...û..®M.È ¥¿«Ù
0010  9e 3b 1a 12 09 d1 83  4c 6b d4 6d 42 40  11 00 00   ;...Ñ LkÔmB@...
0020  9c 11 8c fe 52 c0 22  86 01 0a 0d 55 6e  69 74 65   . þRÀ" ...Unite
0030  64 20 53 74 61 74 65  73 12 02 55 53 1a  08 56 69   d States..US..Vi
0040  72 67 69 6e 69 61 22  02 56 41 2a 0e 56  69 72 67   rginia".VA*.Virg
0050  69 6e 69 61 20 42 65  61 63 68 32 0e 56  69 72 67   inia Beach2.Virg
0060  69 6e 69 61 20 42 65  61 63 68 3a 05 32  33 34 35   inia Beach:.2345
0070  31 42 09 4e 6f 72 74  68 65 61 73 74 52  0c 41 74   1B.NortheastR.At
0080  6c 61 6e 74 69 63 20  41 76 65 5a 04 32  39 30 31   lantic AveZ.2901
0090  62 11 32 39 30 31 20  41 74 6c 61 6e 74  69 63 20   b.2901 Atlantic
00a0  41 76 65 8a 01 09 4e  6f 72 74 68 65 61  73 74 2a   Ave ..Northeast*
00b0  12 54 68 65 20 4f 63  65 61 6e 66 72 6f  6e 74 20   .The Oceanfront
00c0  49 6e 6e 32 11 32 39  30 31 20 41 74 6c  61 6e 74   Inn2.2901 Atlant
00d0  69 63 20 41 76 65 32  19 56 69 72 67 69  6e 69 61   ic Ave2.Virginia
00e0  20 42 65 61 63 68 2c  20 56 41 20 20 32  33 34 35    Beach, VA  2345
00f0  31 32 0d 55 6e 69 74  65 64 20 53 74 61  74 65 73   12.United States
0100
```

APPLICATION USAGE – APPS USED KNOWLEDGEC.DB [~4 WEEKS]

```
1  SELECT
2  datetime(ZOBJECT.ZCREATIONDATE+978307200,'UNIXEPOCH') as "ENTRY CREATION",
3  ZOBJECT.ZVALUESTRING AS "BUNDLE ID",
4  CASE ZOBJECT.ZSTARTDAYOFWEEK
5     WHEN "1" THEN "Sunday"
6     WHEN "2" THEN "Monday"
7     WHEN "3" THEN "Tuesday"
8     WHEN "4" THEN "Wednesday"
9     WHEN "5" THEN "Thursday"
10    WHEN "6" THEN "Friday"
11    WHEN "7" THEN "Saturday"
12 END "DAY OF WEEK",
13 ZOBJECT.ZSECONDSFROMGMT/3600 AS "GMT OFFSET",
14 datetime(ZOBJECT.ZSTARTDATE+978307200,'UNIXEPOCH') as "START",
15 datetime(ZOBJECT.ZENDDATE+978307200,'UNIXEPOCH') as "END",
16 (ZOBJECT.ZENDDATE-ZOBJECT.ZSTARTDATE) as "USAGE IN SECONDS"
17 FROM ZOBJECT
```

	ENTRY CREATION	BUNDLE ID	DAY OF WEEK	GMT OFFSET	START	END	USAGE IN SECONDS
211	2018-08-21 21:59:33	com.contextoptional.OpenTable	Tuesday	-4	2018-08-21 21:58:04	2018-08-21 21:59:33	89
212	2018-08-21 21:59:50	com.apple.MobileSMS	Tuesday	-4	2018-08-21 21:59:35	2018-08-21 21:59:49	14
213	2018-08-21 22:02:03	com.atebits.Tweetie2	Tuesday	-4	2018-08-21 21:59:50	2018-08-21 22:02:03	133
214	2018-08-21 22:03:23	com.contextoptional.OpenTable	Tuesday	-4	2018-08-21 22:02:05	2018-08-21 22:03:23	78
215	2018-08-21 22:05:09	com.apple.Fitness.activity-widget	Tuesday	-4	2018-08-21 22:05:07	2018-08-21 22:05:09	2
216	2018-08-21 22:05:09	com.waze.iphone.today	Tuesday	-4	2018-08-21 22:05:07	2018-08-21 22:05:09	2
217	2018-08-21 22:05:10	com.wunderground.weatherunderground.weatherwidget	Tuesday	-4	2018-08-21 22:05:07	2018-08-21 22:05:10	3
218	2018-08-21 22:05:11	com.apple.news.widget	Tuesday	-4	2018-08-21 22:05:07	2018-08-21 22:05:11	4
219	2018-08-21 22:11:33	com.atebits.Tweetie2	Tuesday	-4	2018-08-21 22:03:24	2018-08-21 22:11:33	489
220	2018-08-21 22:16:45	com.atebits.Tweetie2	Tuesday	-4	2018-08-21 22:13:13	2018-08-21 22:16:45	212

APPLICATION USAGE – APPS USED [1] CURRENTPOWERLOG.PLSQL [~3 DAYS]



WARNING: Time offsets anywhere from 13 seconds in the past to 12 minutes into the future!

	ADJUSTED_TIMESTAMP	BUNDLE_ID	APPROLE	DISPLAY	LEVEL	ORIENTATION	SCREENWEIGHT	ORIGINAL_SCREEN_STATE_TIMESTAMP	OFFSET_TIMESTAMP	TIME_OFFSET
624	2018-09-17 03:01:44	com.apple.lock-screen	3	0	1050.0	1	1.0	2018-09-17 03:01:31	2018-09-16 18:47:35	13.1328829526901
625	2018-09-17 03:01:46	net.whatsapp.WhatsApp	1	0	1.0	1	1.0	2018-09-17 03:01:32	2018-09-16 18:47:35	13.1328829526901
626	2018-09-17 03:01:54	com.apple.springboard.home-screen	1	0	0.0	1	1.0	2018-09-17 03:01:41	2018-09-16 18:47:35	13.1328829526901
627	2018-09-17 03:01:57	com.atebits.Tweetie2	1	0	1.0	1	1.0	2018-09-17 03:01:44	2018-09-16 18:47:35	13.1328829526901
628	2018-09-17 03:02:06	com.apple.springboard.home-screen	1	0	0.0	1	1.0	2018-09-17 03:01:53	2018-09-16 18:47:35	13.1328829526901
629	2018-09-17 03:02:08	com.apple.MobileSMS	1	0	1.0	1	1.0	2018-09-17 03:01:55	2018-09-16 18:47:35	13.1328829526901
630	2018-09-17 03:02:09	com.apple.MobileSMS	1	0	1.0	1	1.0	2018-09-17 03:01:56	2018-09-16 18:47:35	13.1328829526901
631	2018-09-17 03:05:39	com.apple.lock-screen	3	0	1050.0	1	1.0	2018-09-17 03:05:26	2018-09-16 18:47:35	13.1328829526901
632	2018-09-17 03:05:40	com.apple.MobileSMS	1	0	1.0	1	1.0	2018-09-17 03:05:27	2018-09-16 18:47:35	13.1328829526901
633	2018-09-17 03:05:43	com.apple.MobileSMS	1	0	1.0	4	1.0	2018-09-17 03:05:30	2018-09-16 18:47:35	13.1328829526901
634	2018-09-17 03:05:45	com.apple.MobileSMS	1	0	1.0	1	1.0	2018-09-17 03:05:31	2018-09-16 18:47:35	13.1328829526901
635	2018-09-17 03:05:46	com.apple.springboard.home-screen	1	0	0.0	1	1.0	2018-09-17 03:05:33	2018-09-16 18:47:35	13.1328829526901
636	2018-09-17 03:05:48	com.apple.springboard.spotlight	6	0	0.0	1	1.0	2018-09-17 03:05:34	2018-09-16 18:47:35	13.1328829526901
637	2018-09-17 03:05:48	com.espn.fantasyFootball	1	0	1.0	1	1.0	2018-09-17 03:05:35	2018-09-16 18:47:35	13.1328829526901
638	2018-09-17 03:05:49	com.espn.fantasyFootball	1	0	1.0	1	1.0	2018-09-17 03:05:35	2018-09-16 18:47:35	13.1328829526901
639	2018-09-17 03:10:16	com.apple.lock-screen	3	0	1050.0	1	1.0	2018-09-17 03:10:03	2018-09-16 18:47:35	13.1328829526901

APPLICATION USAGE – APPS USED [2] CURRENTPOWERLOG.PLSQL [~3 DAYS]

	ADJUSTED_TIMESTAMP	BUNDLE_ID	APPROLE	DISPLAY	LEVEL	ORIENTATION	SCREENWEIGHT	ORIGINAL_SCREEN_STATE_TIMESTAMP	OFFSET_TIMESTAMP	TIME_OFFSET
846	2018-09-17 19:30:52	com.apple.lock-screen	3	0	1050.0	1	1.0	2018-09-17 19:30:39	2018-09-17 16:02:01	13.1328829526901
847	2018-09-17 19:30:52	com.apple.springboard.home-screen	1	3	0.0	NULL	1.0	2018-09-17 19:30:39	2018-09-17 16:02:01	13.1328829526901
848	2018-09-17 19:30:52	com.apple.Music	1	3	1.0	NULL	0.89	2018-09-17 19:30:39	2018-09-17 16:02:01	13.1328829526901
849	2018-09-17 19:31:03	com.apple.Music	1	3	1.0	NULL	0.89	2018-09-17 19:30:50	2018-09-17 16:02:01	13.1328829526901
850	2018-09-17 19:31:03	com.apple.carplay.oem	3	3	8.0	NULL	1.0	2018-09-17 19:30:50	2018-09-17 16:02:01	13.1328829526901
851	2018-09-17 19:31:03	com.apple.Music	1	3	1.0	NULL	0.89	2018-09-17 19:30:50	2018-09-17 16:02:01	13.1328829526901
852	2018-09-17 19:31:03	com.apple.Music	1	3	1.0	NULL	0.89	2018-09-17 19:30:50	2018-09-17 16:02:01	13.1328829526901
853	2018-09-17 19:31:03	com.apple.carplay.oem	3	3	8.0	NULL	1.0	2018-09-17 19:30:50	2018-09-17 16:02:01	13.1328829526901
854	2018-09-17 19:31:14	com.apple.Music	1	3	1.0	NULL	0.89	2018-09-17 19:31:01	2018-09-17 16:02:01	13.1328829526901
855	2018-09-17 19:31:32	com.apple.Music	1	3	1.0	NULL	0.89	2018-09-17 19:31:19	2018-09-17 16:02:01	13.1328829526901
856	2018-09-17 19:31:32	com.apple.carplay.oem	3	3	8.0	NULL	1.0	2018-09-17 19:31:19	2018-09-17 16:02:01	13.1328829526901
857	2018-09-17 19:31:33	com.apple.Music	1	3	1.0	NULL	0.89	2018-09-17 19:31:20	2018-09-17 16:02:01	13.1328829526901
858	2018-09-17 19:34:53	com.apple.springboard.home-screen	1	3	0.0	NULL	1.0	2018-09-17 19:34:40	2018-09-17 16:02:01	13.1328829526901
859	2018-09-17 19:34:56	com.audible.iphone	1	3	1.0	NULL	1.0	2018-09-17 19:34:43	2018-09-17 16:02:01	13.1328829526901
860	2018-09-17 19:48:58	com.audible.iphone	1	3	1.0	NULL	1.0	2018-09-17 19:48:45	2018-09-17 16:02:01	13.1328829526901
861	2018-09-17 19:48:58	com.apple.Siri	4	3	3.0	NULL	1.0	2018-09-17 19:48:45	2018-09-17 16:02:01	13.1328829526901

HEALTH – HEART RATE
HEALTHDB_SECURE.SQLITE [FOREVER]

```
1  select datetime(samples.start_date+978307200,'unixepoch') as "Start Date",
2  datetime(samples.end_date+978307200,'unixepoch') as "End Date", samples.
3  data_type as "Data Type",
4  quantity,
5  original_quantity,
6  unit_strings.unit_string,
7  metadata_keys.key,
8  samples.data_id as "Samples Table ID"
9  from samples
10 left outer join quantity_samples on samples.data_id = quantity_samples.data_id
11 left outer join unit_strings on quantity_samples.original_unit = unit_strings.RowID
12 left outer join correlations on samples.data_id = correlations.object
13 left outer join metadata_values on metadata_values.object_id = samples.data_id
14 left outer join metadata_keys on metadata_keys.ROWID = metadata_values.key_id
15 where samples.data_type = 5
```

	Start Date	End Date	Data Type	quantity	original_quantity	unit_string	key	Samples Table ID
479576	2018-09-16 16:24:46	2018-09-16 16:24:46	5	3.01666666666667	181.0	count/min	_HKPrivateHeartRateContext	3637289
479577	2018-09-16 16:24:50	2018-09-16 16:24:50	5	3.03333333333333	182.0	count/min	HKMetadataKeyHeartRateMotionContext	3637294
479578	2018-09-16 16:24:50	2018-09-16 16:24:50	5	3.03333333333333	182.0	count/min	_HKPrivateHeartRateContext	3637294
479579	2018-09-16 16:24:53	2018-09-16 16:24:53	5	3.06666666666667	184.0	count/min	HKMetadataKeyHeartRateMotionContext	3637301
479580	2018-09-16 16:24:53	2018-09-16 16:24:53	5	3.06666666666667	184.0	count/min	_HKPrivateHeartRateContext	3637301
479581	2018-09-16 16:25:03	2018-09-16 16:25:03	5	3.11666666666667	187.0	count/min	HKMetadataKeyHeartRateMotionContext	3637310
479582	2018-09-16 16:25:03	2018-09-16 16:25:03	5	3.11666666666667	187.0	count/min	_HKPrivateHeartRateContext	3637310
479583	2018-09-16 16:25:07	2018-09-16 16:25:07	5	3.1	186.0	count/min	HKMetadataKeyHeartRateMotionContext	3637318
479584	2018-09-16 16:25:07	2018-09-16 16:25:07	5	3.1	186.0	count/min	_HKPrivateHeartRateContext	3637318
479585	2018-09-16 16:25:09	2018-09-16 16:25:09	5	3.08333333333333	185.0	count/min	HKMetadataKeyHeartRateMotionContext	3637335
479586	2018-09-16 16:25:09	2018-09-16 16:25:09	5	3.08333333333333	185.0	count/min	_HKPrivateHeartRateContext	3637335

HEALTH – STEPS & DISTANCE
HEALTHDB_SECURE.SQLITE [FOREVER]

```
1  select datetime(samples.start_date+978307200,'unixepoch','utc') as "Start Date",
2  datetime(samples.end_date+978307200,'unixepoch','utc') as "End Date",
3  samples.
4  data_type as "Data Type",
5  quantity as "Steps",
6  samples.data_id as "Samples Table ID"
7  from samples
8  left outer join quantity_samples on samples.data_id = quantity_samples.data_id
9  left outer join unit_strings on quantity_samples.original_unit = unit_strings.RowID
10 left outer join correlations on samples.data_id = correlations.object
11 left outer join metadata_values on metadata_values.object_id = samples.data_id
12 left outer join metadata_keys on metadata_keys.ROWID = metadata_values.key_id
13 where samples.data_type = 7 and key is null
14 AND "START DATE" LIKE '%2018-09-16%'
15 ORDER BY "Start Date"
```

	Start Date	End Date	Data Type	Steps	Samples Table ID
168	2018-09-16 20:18:01	2018-09-16 20:19:02	7	133.0	3637721
169	2018-09-16 20:19:02	2018-09-16 20:20:04	7	169.0	3637722
170	2018-09-16 20:20:04	2018-09-16 20:21:05	7	138.0	3637723
171	2018-09-16 20:21:05	2018-09-16 20:22:06	7	111.0	3637724
172	2018-09-16 20:22:06	2018-09-16 20:23:08	7	168.0	3637725
173	2018-09-16 20:23:08	2018-09-16 20:24:09	7	114.0	3637726
174	2018-09-16 20:24:09	2018-09-16 20:25:48	7	131.0	3637727
175	2018-09-16 20:24:54	2018-09-16 20:34:52	7	442.0	3637711
176	2018-09-16 20:25:48	2018-09-16 20:28:38	7	14.0	3637728
177	2018-09-16 20:29:47	2018-09-16 20:30:48	7	33.0	3637729
178	2018-09-16 20:30:48	2018-09-16 20:40:11	7	1018.0	3637785
179	2018-09-16 20:34:52	2018-09-16 20:43:01	7	699.0	3637712

```
1  select datetime(samples.start_date+978307200,'unixepoch','utc') as "Start Date",
2  datetime(samples.end_date+978307200,'unixepoch','utc') as "End Date",
3  samples.data_type as "Data Type",
4  quantity as "Distance in Meters",
5  samples.data_id as "Samples Table ID"
6  from samples
7  left outer join quantity_samples on samples.data_id = quantity_samples.data_id
8  left outer join unit_strings on quantity_samples.original_unit = unit_strings.RowID
9  left outer join correlations on samples.data_id = correlations.object
10 left outer join metadata_values on metadata_values.object_id = samples.data_id
11 left outer join metadata_keys on metadata_keys.ROWID = metadata_values.key_id
12 where samples.data_type = 8 and key is null
13 AND "START DATE" LIKE '%2018-09-16%'
14 ORDER BY "Start Date"
```

	Start Date	End Date	Data Type	Distance in Meters	Samples Table ID
150	2018-09-16 19:25:30	2018-09-16 19:35:23	8	78.6573735140264	3634387
151	2018-09-16 19:35:23	2018-09-16 19:45:20	8	416.445916654542	3634938
152	2018-09-16 19:45:20	2018-09-16 19:55:18	8	238.186128458008	3635697
153	2018-09-16 19:55:18	2018-09-16 20:05:16	8	200.604227676522	3636274
154	2018-09-16 20:05:16	2018-09-16 20:15:15	8	700.755024724873	3636847
155	2018-09-16 20:15:15	2018-09-16 20:25:07	8	1113.33662894019	3637479
156	2018-09-16 20:24:54	2018-09-16 20:34:52	8	299.481329584727	3637996
157	2018-09-16 20:25:07	2018-09-16 20:26:08	8	6.43414319492877	3637716
158	2018-09-16 20:29:47	2018-09-16 20:30:48	8	21.5141206183471	3637717
159	2018-09-16 20:30:48	2018-09-16 20:40:11	8	658.256004666211	3637784
160	2018-09-16 20:34:52	2018-09-16 20:43:01	8	502.089796816697	3637997
161	2018-09-16 20:40:11	2018-09-16 20:43:09	8	38.4893803959712	3637786
162	2018-09-16 21:09:58	2018-09-16 21:11:00	8	14.7879310355056	3637795

DEVICE STATUS – WHATS ON? KNOWLEDGEC.DB – NOW PLAYING

	START	END	USAGE IN SECONDS	BUNDLE ID	NOW PLAYING ALBUM	IOW PLAYING ARTIS	NOW PLAYING GENRE	NOW PLAYING TITLE	NOW PLAYING DURATION	STREAM NAME
238	2018-08-28 09:12:07	2018-08-28 09:12:48	41	com.apple.Music	Nervous System	Julia Michaels	Pop	Issues	176.378775510204	/media/nowPlaying
239	2018-08-28 18:52:49	2018-08-28 19:32:09	2360	org.npr.nprnews	WHRV • Live	NULL	NULL	WHRV-FM NPR for Eastern Virginia	0.0	/media/nowPlaying
240	2018-08-28 19:32:12	2018-08-28 19:32:12	0	org.npr.nprnews	WHRV • Live	NULL	NULL	WHRV-FM NPR for Eastern Virginia	0.0	/media/nowPlaying
241	2018-08-28 19:35:51	2018-08-28 19:35:52	1	org.npr.nprnews	WHRV • Live	NULL	NULL	WHRV-FM NPR for Eastern Virginia	0.0	/media/nowPlaying
242	2018-08-28 19:35:52	2018-08-28 19:39:58	246	com.apple.Music	Love Stuff	Elle King	Alternative	America's Sweetheart	245.542	/media/nowPlaying
243	2018-08-28 19:39:58	2018-08-28 19:40:03	5	com.apple.Music	Evacuate the Dancefloor	Cascada	Dance	Evacuate the Dancefloor	207.865034013605	/media/nowPlaying
244	2018-08-28 19:40:03	2018-08-28 19:40:05	2	com.apple.Music	With Teeth	Nine Inch Nails	Rock	The Hand That Feeds	211.789206349206	/media/nowPlaying
245	2018-08-28 19:40:05	2018-08-28 19:40:06	1	com.apple.Music	7/27 (Deluxe)	Fifth Harmony	Pop	Work from Home (feat. Ty Dolla $i...	214.529160997732	/media/nowPlaying
246	2018-08-28 19:40:06	2018-08-28 19:40:07	1	com.apple.Music	Nice to Meet You - EP	Seeb & Dagny	Pop	Drink About	182.323083900227	/media/nowPlaying
247	2018-08-28 19:40:07	2018-08-28 19:41:39	92	com.apple.Music	Blackout (feat. Steph Jones) ...	Tritonal	Dance	Blackout (feat. Steph Jones)	211.742766439909	/media/nowPlaying
248	2018-08-28 19:41:39	2018-08-29 04:15:40	30841	com.apple.Music	Blackout (feat. Steph Jones) ...	Tritonal	Dance	Blackout (feat. Steph Jones)	211.742766439909	/media/nowPlaying
249	2018-08-29 04:15:40	2018-08-29 04:15:43	3	com.apple.Music	Blackout (feat. Steph Jones) ...	Tritonal	Dance	Blackout (feat. Steph Jones)	211.69	/media/nowPlaying
250	2018-08-29 04:15:44	2018-08-29 04:19:16	212	com.apple.Music	Blackout (feat. Steph Jones) ...	Tritonal	Dance	Blackout (feat. Steph Jones)	211.69	/media/nowPlaying
251	2018-08-29 04:26:42	2018-08-29 04:26:42	0	com.apple.Music	Alex Rider: Operation Stormb...	Curve	Soundtrack	Chinese Burn (Lunatic Calm Mix)	445.637369614512	/media/nowPlaying
252	2018-08-29 04:26:42	2018-08-29 04:30:24	222	com.apple.Music	Lest We Forget: The Best of ...	Marilyn Manson	Rock	The Beautiful People	222.841904761905	/media/nowPlaying
253	2018-08-29 04:30:25	2018-08-29 04:34:02	217	com.apple.Music	Version 2.0 (20th Anniversar...	Garbage	Rock	I Think I'm Paranoid	218.1979138322	/media/nowPlaying
254	2018-08-29 04:37:54	2018-08-29 04:37:54	0	com.apple.Music	Funk Wav Bounces Vol. 1	Calvin Harris	Dance	Slide (feat. Frank Ocean & Migos)	230.876009070295	/media/nowPlaying

DEVICE STATUS – LOCKED, PLUGGED IN? KNOWLEDGEC.DB

	ENTRY CREATION	DAY OF WEEK	START	END	USAGE IN SECONDS	IS LOCKED	STREAM NAME	ZOBJECT TABLE ID
57	2018-08-22 04:41:45	Tuesday	2018-08-22 04:39:48	2018-08-22 04:41:44	116	UNLOCKED	/device/isLocked	296308
58	2018-08-22 04:48:53	Tuesday	2018-08-22 04:41:44	2018-08-22 04:48:52	428	LOCKED	/device/isLocked	296314
59	2018-08-22 04:49:22	Tuesday	2018-08-22 04:48:52	2018-08-22 04:49:20	28	UNLOCKED	/device/isLocked	296317
60	2018-08-22 04:50:09	Tuesday	2018-08-22 04:49:20	2018-08-22 04:50:08	48	LOCKED	/device/isLocked	296319
61	2018-08-22 04:52:02	Tuesday	2018-08-22 04:50:08	2018-08-22 04:52:00	112	UNLOCKED	/device/isLocked	296322

	ENTRY CREATION	DAY OF WEEK	START	END	USAGE IN SECONDS	IS PLUGGED IN	STREAM NAME	ZOBJECT TABLE ID
67	2018-09-01 05:29:23	Friday	2018-09-01 05:26:44	2018-09-01 05:29:20	156	PLUGGED IN	/device/isPluggedIn	307290
68	2018-09-01 10:08:25	Friday	2018-09-01 05:29:20	2018-09-01 10:08:24	16744	UNPLUGGED	/device/isPluggedIn	307699
69	2018-09-01 15:52:47	Friday	2018-09-01 10:08:24	2018-09-01 15:52:44	20660	PLUGGED IN	/device/isPluggedIn	307792
70	2018-09-01 16:25:30	Saturday	2018-09-01 15:52:44	2018-09-01 16:25:28	1964	UNPLUGGED	/device/isPluggedIn	307816
71	2018-09-01 21:09:29	Saturday	2018-09-01 16:25:28	2018-09-01 21:09:28	17040	PLUGGED IN	/device/isPluggedIn	307876
72	2018-09-02 11:10:56	Saturday	2018-09-01 21:09:28	2018-09-02 11:10:56	50488	UNPLUGGED	/device/isPluggedIn	308178

DEVICE STATUS – PASSCODE UNLOCK ADDATASTORE.DB

```
2    date(daysSince1970*86400,'unixepoch','utc') as day,
3    Key,
4    Value
5    from Scalars
6    where key like "%passcode%"
```

	day	key	value
1	2018-09-12	com.apple.springboard.lockscreen.passcodeUI.activationCount	9
2	2018-09-12	com.apple.passcode.PasscodeType	3
3	2018-09-12	com.apple.passcode.NumPasscodeEntered	1
4	2018-09-13	com.apple.springboard.lockscreen.passcodeUI.activationCount	7
5	2018-09-13	com.apple.passcode.PasscodeType	3
6	2018-09-13	com.apple.passcode.NumPasscodeEntered	1
7	2018-09-14	com.apple.springboard.lockscreen.passcodeUI.activationCount	15
8	2018-09-14	com.apple.passcode.PasscodeType	3
9	2018-09-14	com.apple.passcode.NumPasscodeEntered	3
10	2018-09-15	com.apple.passcode.PasscodeType	3
11	2018-09-15	com.apple.springboard.lockscreen.passcodeUI.activationCount	10
12	2018-09-16	com.apple.passcode.PasscodeType	3
13	2018-09-16	com.apple.springboard.lockscreen.passcodeUI.activationCount	12
14	2018-09-17	com.apple.passcode.PasscodeType	0
15	2018-09-17	com.apple.springboard.lockscreen.passcodeUI.activationCount	7
16	2018-09-17	com.apple.passcode.NumPasscodeEntered	2

```
1    select
2    date(daysSince1970*86400,'unixepoch','utc') as day,
3    Key,
4    Value
5    from Scalars
6    where key like "%fingerprint%"
```

0 rows returned in 26ms from: select
date(daysSince1970*86400,'unixepoch','utc') as day,
Key,
Value
from Scalars
where key like "%fingerprint%"

DEVICE STATUS – BATTERY LEVEL CURRENTPOWERLOG.PLSQL

```
1  SELECT
2    DATETIME(TIMESTAMP, 'unixepoch') AS TIMESTAMP,
3    LEVEL,
4    ID AS "PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI TABLE ID"
5  FROM
6    PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI
```

	TIMESTAMP	Level	3ATTERYAGENT_EVENTBACKWARD_BATTERYUI TABLE
753	2018-09-13 01:31:41	85.0	51178
754	2018-09-13 01:37:26	84.0	51179
755	2018-09-13 01:42:41	84.0	51180
756	2018-09-13 01:48:42	84.0	51181
757	2018-09-13 01:54:18	84.0	51182
758	2018-09-13 01:59:36	84.0	51183
759	2018-09-13 02:04:42	84.0	51184
760	2018-09-13 02:09:48	83.0	51185
761	2018-09-13 02:15:08	82.0	51186
762	2018-09-13 02:20:08	81.0	51187
763	2018-09-13 02:25:08	79.0	51188
764	2018-09-13 02:30:08	79.0	51189
765	2018-09-13 02:35:28	77.0	51190
766	2018-09-13 02:40:38	77.0	51191
767	2018-09-13 02:46:00	78.0	51192

APOLLO:
APPLE PATTERN OF LIFE LAZY OUTPUT'ER

Low Bar to Entry – Easy contribution for busy Forensic Investigators

- Almost anyone can develop a SQL Query

Quick Correlation - Not perfect, but works!

Easy to update and configure SQL queries

- Across Devices & Across OS Versions

SQL Script Sharing

Dumb Script – Nothin' fancy going on here, the real work is done by the modules

- Pro Tip: It can be used with any SQL Database and Query…Android, Windows…even Blackberry!?
- …but I'm keeping the name because its badass.

Modules Directory – SQL Query Configuration Files, **already 70+ created!**

python apollo.py –output [csv, sql] <modules directory> <data directory>

EXAMPLE APOLLO CONFIG FILE

```
[Module Metadata]
AUTHOR=Sarah Edwards/mac4n6.com/@iamevltwin
MODULE_NOTES=Application Usage, shows application in focus on device.

[Database Metadata]
DATABASE=knowledgeC.db
PLATFORM=IOS
VERSIONS=11

[Query Metadata]
QUERY_NAME= knowledge_app_inFocus
ACTIVITY=Application In Focus
KEY_TIMESTAMP=START

[SQL Query]
QUERY=
    SELECT
    datetime(ZOBJECT.ZCREATIONDATE+978307200,'UNIXEPOCH') as "ENTRY CREATION",
    ZOBJECT.ZVALUESTRING AS "BUNDLE ID",
    CASE ZOBJECT.ZSTARTDAYOFWEEK
        WHEN "1" THEN "Sunday"
        WHEN "2" THEN "Monday"
        WHEN "3" THEN "Tuesday"
        WHEN "4" THEN "Wednesday"
        WHEN "5" THEN "Thursday"
        WHEN "6" THEN "Friday"
        WHEN "7" THEN "Saturday"
    END "DAY OF WEEK",
    ZOBJECT.ZSECONDSFROMGMT/3600 AS "GMT OFFSET",
    datetime(ZOBJECT.ZSTARTDATE+978307200,'UNIXEPOCH') as "START",
    datetime(ZOBJECT.ZENDDATE+978307200,'UNIXEPOCH') as "END",
    (ZOBJECT.ZENDDATE-ZOBJECT.ZSTARTDATE) as "USAGE IN SECONDS"
    FROM ZOBJECT
    WHERE ZSTREAMNAME IS "/app/inFocus"
```

RUNNING APOLLO

```
MBP-18:APoLLO oompa$ time python apollo.py -output sql modules ~/miphonex_iOS_11_1_2_untar/
Parsing Module: knowledge_app_install.txt
        Executing module on: /Users/oompa/miphonex_iOS_11_1_2_untar/private/var/mobile/Library/Assistant/knowledgeC.db
        Executing module on: /Users/oompa/miphonex_iOS_11_1_2_untar/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db
        Executing module on: /Users/oompa/miphonex_iOS_11_1_2_untar/private/var/mobile/Containers/Data/Application/20C355DE-25C9-4883-B132-C74D769BA639/Library/Caches/News/knowledgeC.db
Parsing Module: powerlog_torch_state.txt
Parsing Module: routined_local_learned_location_of_interest_transition_start.txt
        Executing module on: /Users/oompa/miphonex_iOS_11_1_2_untar/private/var/mobile/Library/Caches/com.apple.routined/Local.sqlite
Parsing Module: aggregate_dictionary_distributed_keys.txt
        Executing module on: /Users/oompa/miphonex_iOS_11_1_2_untar/private/var/mobile/Library/AggregateDictionary/ADDataStore.sqlitedb
Parsing Module: knowledge_application_portrait.txt
        Executing module on: /Users/oompa/miphonex_iOS_11_1_2_untar/private/var/mobile/Library/Assistant/knowledgeC.db
        Executing module on: /Users/oompa/miphonex_iOS_11_1_2_untar/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db
        Executing module on: /Users/oompa/miphonex_iOS_11_1_2_untar/private/var/mobile/Containers/Data/Application/20C355DE-25C9-4883-B132-C74D769BA639/Library/Caches/News/knowledgeC.db
Parsing Module: powerlog_network_usage.txt
Parsing Module: powerlog_battery_level.txt
Parsing Module: powerlog_mobilebackup.txt
Parsing Module: routined_local_learned_location_of_interest_transition_stop.txt
        Executing module on: /Users/oompa/miphonex_iOS_11_1_2_untar/private/var/mobile/Library/Caches/com.apple.routined/Local.sqlite
Parsing Module: coreduetdclassd_device_plugin_state.txt
        Executing module on: /Users/oompa/miphonex_iOS_11_1_2_untar/private/var/mobile/Library/CoreDuet/coreduetdClassD.db
Parsing Module: coreduetd_device_airplane_state.txt
        Executing module on: /Users/oompa/miphonex_iOS_11_1_2_untar/private/var/mobile/Library/CoreDuet/coreduetd.db
Parsing Module: health_workout_locations_end.txt
        Executing module on: /Users/oompa/miphonex_iOS_11_1_2_untar/private/var/mobile/Library/Health/healthdb_secure.sqlite
Parsing Module: routined_cloud_visit_outbound_stop.txt
        Executing module on: /Users/oompa/miphonex_iOS_11_1_2_untar/private/var/mobile/Library/Caches/com.apple.routined/Cloud.sqlite
Parsing Module: interaction_contact_interactions.txt
        Executing module on: /Users/oompa/miphonex_iOS_11_1_2_untar/private/var/mobile/Library/CoreDuet/People/interactionC.db
```

```
===> Lazily outputted to SQLite file: apollo.db


real    87m33.030s
user    12m58.050s
sys     45m35.350s
MBP-18:APoLLO oompa$
```

Much faster if you extract the databases instead of whole disk dump! (>5m)

APOLLO OUTPUT EXAMPLE [1]

```
1  select datetime(key,'localtime') as localtime,
2  Activity, Output from APOLLO
3  where localtime like '%2018-09-16%'
4  and Activity not like '%aggregate%'
5  order by localtime
```

~25k Data Points for 09/16/2018

	localtime	Activity	Output
17	2018-09-16 00:00:00	Application Usage	[TIMESTAMP: 2018-09-16 04:00:00] [BUNDLE ID: com.atebits.Tweetie2] [CONNECTION TYPE: wwan] [IS DROPPED: None] [LINK QUALITY: None] [Priority: 10] [Topic: com.atebits.Tweetie2] [SERV...
18	2018-09-16 00:00:00	Application Usage	[TIMESTAMP: 2018-09-16 04:00:00] [BUNDLE ID: com.atebits.Tweetie2] [CONNECTION TYPE: wwan] [IS DROPPED: None] [LINK QUALITY: None] [Priority: 10] [Topic: com.atebits.Tweetie2] [SERV...
19	2018-09-16 00:00:00	Network Usage	[TIMESTAMP: 2018-09-16 04:00:00] [BULLETIN BUNDLE ID: com.atebits.Tweetie2] [TIME INTERVAL IN SECONDS: 60.0] [Count: 3] [POST TYPE: 7] [PLSPRINGBOARDAGENT_AGGREGATE_SBBUL...
20	2018-09-16 00:00:00	Network Usage	[TIMESTAMP: 2018-09-16 04:00:00] [BULLETIN BUNDLE ID: com.atebits.Tweetie2] [TIME INTERVAL IN SECONDS: 60.0] [Count: 40] [POST TYPE: 1] [PLSPRINGBOARDAGENT_AGGREGATE_SBBU...
21	2018-09-16 00:00:01	Location	[TIMESTAMP: 2018-09-16 04:00:01] [COORDINATES: 39.11 -76.61] [ALTITUDE: -5.4] [COURSE: 211.8] [SPEED: 0.0] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCURACY: ...
22	2018-09-16 00:00:02	Location	[TIMESTAMP: 2018-09-16 04:00:02] [COORDINATES: 39.11 , -76.61] [ALTITUDE: -5.4] [COURSE: 211.8] [SPEED: 0.0] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCURACY: ...
23	2018-09-16 00:00:04	Location	[TIMESTAMP: 2018-09-16 04:00:04] [COORDINATES: 39.11 , -76.61] [ALTITUDE: -5.4] [COURSE: 211.8] [SPEED: 0.0] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCURACY: ...
24	2018-09-16 00:00:06	Location	[TIMESTAMP: 2018-09-16 04:00:06] [COORDINATES: 39.11 , -76.61] [ALTITUDE: -5.4] [COURSE: 211.8] [SPEED: 0.0] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCURACY: ...
25	2018-09-16 00:00:06	Device Status	[TIMESTAMP: 2018-09-16 04:00:06] [TIMESTAMP END: 2018-09-16 04:01:06] [topic: com.apple.private.alloy.timesync] [priority: URGENT] [INCOMING MESSAGES: 1] [OUTGOING MESSAGES: 4] [...
26	2018-09-16 00:00:06	Device Status	[TIMESTAMP: 2018-09-16 04:00:06] [TIMESTAMP END: 2018-09-16 04:01:06] [topic: com.apple.private.alloy.maps.proxy] [priority: URGENT] [INCOMING MESSAGES: 10] [OUTGOING MESSAGES: ...
27	2018-09-16 00:00:06	Device Status	[TIMESTAMP: 2018-09-16 04:00:06] [TIMESTAMP END: 2018-09-16 04:01:06] [topic: com.apple.private.alloy.nsurlsessionproxy] [priority: Default] [INCOMING MESSAGES: 19] [OUTGOING MESSA...
28	2018-09-16 00:00:08	Device State	[TIMESTAMP: 2018-09-16 04:00:08] [LEVEL: 80.0] [RAW LEVEL: 77.0635500365] [IS CHARGING: 1] [FULLY CHARGED: 0] [PLBATTERYAGENT_EVENTBACKWARD_BATTERY TABLE ID: 494058]
29	2018-09-16 00:00:08	Location	[TIMESTAMP: 2018-09-16 04:00:08] [COORDINATES: 39.11 , -76.61] [ALTITUDE: -5.4] [COURSE: 211.8] [SPEED: 0.0] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCURACY: ...
30	2018-09-16 00:00:09	Application Activity	[ENTRY CREATION: 2018-09-16 04:00:09] [DAY OF WEEK: Sunday] [BUNDLE ID: com.apple.Maps] [ACTIVITY TYPE: com.apple.Maps] [TITLE: Dropped Pin on] [EXP...
31	2018-09-16 00:00:09	Application Activity	[ENTRY CREATION: 2018-09-16 04:00:09] [DAY OF WEEK: Sunday] [BUNDLE ID: com.apple.Maps] [ACTIVITY TYPE: com.apple.Maps] [TITLE: Fairfax DrDirection from My Location] [EXPIRATI...
32	2018-09-16 00:00:10	Location	[TIMESTAMP: 2018-09-16 04:00:10] [COORDINATES: 39.11 , -76.61] [ALTITUDE: -5.4] [COURSE: 211.8] [SPEED: 0.0] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCURACY: ...
33	2018-09-16 00:00:11	Location	[TIMESTAMP: 2018-09-16 04:00:11] [COORDINATES: 39.11 , -76.61] [ALTITUDE: -5.4] [COURSE: 211.8] [SPEED: 0.0] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCURACY: ...
34	2018-09-16 00:00:13	Location	[TIMESTAMP: 2018-09-16 04:00:13] [COORDINATES: 39.11 , -76.61] [ALTITUDE: -5.4] [COURSE: 211.8] [SPEED: 0.0] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCURACY: ...
35	2018-09-16 00:00:14	Location	[TIMESTAMP: 2018-09-16 04:00:14] [COORDINATES: 39.11 , -76.61] [ALTITUDE: -5.4] [COURSE: 211.8] [SPEED: 0.0] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCURACY: ...

APOLLO OUTPUT EXAMPLE [2] DISTRACTED DRIVING?

	Activity	Output
316	Location	[TIMESTAMP: 2018-09-16 04:03:48] [COORDINATES: 39.1153389157401, -76.6329456498558] [ALTITUDE: 30.4] [COURSE: 151.890029907] [SPEED: 15.8448888889] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCUR..
317	Location	[TIMESTAMP: 2018-09-16 04:03:49] [COORDINATES: 39.1152105275425, -76.632857958339] [ALTITUDE: 30.5] [COURSE: 152.069168091] [SPEED: 15.9477777778] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCURA...
318	Location	[TIMESTAMP: 2018-09-16 04:03:50] [COORDINATES: 39.1150827819936, -76.6327722606686] [ALTITUDE: 30.7] [COURSE: 152.069168091] [SPEED: 15.9477777778] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCURA...
319	App Usage	[ZINTERACTIONS CREATION DATE: 2018-09-16 04:03:52] [ZBUNDLEID: com.apple.assistant_service] [ZDISPLAYNAME: None] [ZIDENTIFIER: None] [ZPERSONID: None] [ZDIRECTION: 3] [ZISRESPONSE: 0] [ZMECHANISM:...
320	App Usage	[ZINTERACTIONS CREATION DATE: 2018-09-16 04:03:52] [ZBUNDLEID: com.apple.MobileSMS] [ZDISPLAYNAME: None] [ZIDENTIFIER: None] [ZPERSONID: None] [ZDIRECTION: 1] [ZISRESPONSE: 0] [ZMECHANISM: 4] [Z...
321	Location	[TIMESTAMP: 2018-09-16 04:03:51] [COORDINATES: 39.1149556073617, -76.6326878872086] [ALTITUDE: 30.8] [COURSE: 152.069244385] [SPEED: 16.0506666667] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCUR...
322	Location	[TIMESTAMP: 2018-09-16 04:03:52] [COORDINATES: 39.1148244918474, -76.6326033291797] [ALTITUDE: 30.8] [COURSE: 152.069168091] [SPEED: 15.9992222222] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCUR...
323	Application Activity	[ENTRY CREATION: 2018-09-16 04:03:52] [DAY OF WEEK: Sunday] [START: 2018-09-16 04:03:51] [END: 2018-09-16 04:03:51] [USAGE IN SECONDS: 0] [APP NAME: Messages] [INTENT CLASS: INSendMessageIntent] [IN..
324	Location	[TIMESTAMP: 2018-09-16 04:03:53] [COORDINATES: 39.1147407013582, -76.632554927344] [ALTITUDE: 30.8] [COURSE: 152.069168091] [SPEED: 15.6391111111] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCURACY..
325	Application Usage	[ADJUSTED_TIMESTAMP: 2018-09-16 04:03:53] [BUNDLE_ID: com.apple.MobileSMS] [APPROLE: 1] [DISPLAY: 3] [LEVEL: 1.0] [ORIENTATION: None] [SCREENWEIGHT: 0.89] [ORIGINAL_SCREEN_STATE_TIMESTAMP: 2018...
326	Location	[TIMESTAMP: 2018-09-16 04:03:54] [COORDINATES: 39.1145646633985, -76.6324465294773] [ALTITUDE: 30.7] [COURSE: 156.159225464] [SPEED: 15.6391111111] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCURA...
327	Application Activity	[ENTRY CREATION: 2018-09-16 04:03:54] [DAY OF WEEK: Sunday] [START: 2018-09-16 04:03:15] [END: 2018-09-16 04:03:54] [USAGE IN SECONDS: 39] [BUNDLE ID: com.apple.Music] [NOW PLAYING ALBUM: Sugar] [...
328	Device Status	[ENTRY CREATION: 2018-09-16 04:03:54] [DAY OF WEEK: Sunday] [START: 2018-09-16 04:03:12] [END: 2018-09-16 04:03:52] [USAGE IN SECONDS: 40] [AUDIO IDENTIFIER: 74:6F:F7:20:6D:77-Audio-AudioMain-43483...
329	Location	[TIMESTAMP: 2018-09-16 04:03:55] [COORDINATES: 39.114432869852, -76.6323719029567] [ALTITUDE: 30.4] [COURSE: 156.159301758] [SPEED: 16.1021111111] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCURACY...
330	App Usage	[TIMESTAMP: 2018-09-16 04:03:55] [TIMESTAMP LOGGED: 2018-09-16 04:03:55] [APPLICATION NAME / BUNDLE ID: assistantd] [ASERTION ID: 38188] [ASSERTION NAME: com.apple.audio.sid:0x379e0cb, assistantd(14...
331	App Usage	[TIMESTAMP: 2018-09-16 04:03:55] [TIMESTAMP LOGGED: 2018-09-16 04:03:55] [APPLICATION NAME / BUNDLE ID: com.apple.Music] [ASERTION ID: 38320] [ASSERTION NAME: com.apple.audio.sid:0x379e4db, Music(...
332	Location	[TIMESTAMP: 2018-09-16 04:03:56] [COORDINATES: 39.1142981795731, -76.6322985162874] [ALTITUDE: 30.2] [COURSE: 157.228683472] [SPEED: 16.5136666667] [HORIZONTAL ACCURACY: 5.0] [VERTICAL ACCURA..

APOLLO OUTPUT EXAMPLE [3] DEVICE STATUS

	localtime	Activity	Output
11970	2018-09-16 10:44:40	Device State	[TIMESTAMP: 2018-09-16 14:44:40] [LEVEL: 100.0] [RAW LEVEL: 95.4379562044] [IS CHARGING: 0] [FULLY CHARGED: 0] [PLBATTERYAGENT_EVENTBACKWARD_BATTERY TABLE ID: 494989]
11971	2018-09-16 10:44:47	Device Status	[TIMESTAMP: 2018-09-16 14:44:47] [Brightness: 62.7914428711] [PLDISPLAYAGENT_EVENTFORWARD_DISPLAY TABLE ID: 95723]
11972	2018-09-16 10:44:47	Device State	[TIMESTAMP: 2018-09-16 14:44:47] [Screen: 9] [PLSPRINGBOARDAGENT_EVENTFORWARD_SBSCREEN TABLE ID: 84444]
11973	2018-09-16 10:44:48	Device Status	[TIMESTAMP: 2018-09-16 14:44:48] [TIMESTAMP END: 2018-09-16 14:44:48] [TIMESTAMP LOGGED: 2018-09-16 14:44:48] [BUNDLE ID: com.waze.iphone] [Type: Location] [LOCATION DESIRE...
11974	2018-09-16 10:44:48	Device Status	[TIMESTAMP: 2018-09-16 14:44:48] [accessory: 1] [cell: 1] [gps: 1] [gps_coarse: 0] [lac: 0] [mcc: 0] [nmea: 1] [pipeline: 0] [skyhook: 0] [wifi: 1] [wifi2: 0] [PLLOCATIONAGENT_EVENTFORWARD_T...
11975	2018-09-16 10:44:48	Device Status	[TIMESTAMP: 2018-09-16 14:44:48] [accessory: 0] [cell: 0] [gps: 0] [gps_coarse: 0] [lac: 0] [mcc: 0] [nmea: 0] [pipeline: 0] [skyhook: 0] [wifi: 0] [wifi2: 0] [PLLOCATIONAGENT_EVENTFORWARD...
11976	2018-09-16 10:44:48	Device Status	[TIMESTAMP: 2018-09-16 14:44:48] [accessory: 0] [cell: 1] [gps: 0] [gps_coarse: 0] [lac: 0] [mcc: 0] [nmea: 1] [pipeline: 0] [skyhook: 0] [wifi: 1] [wifi2: 0] [PLLOCATIONAGENT_EVENTFORWARD_...
11977	2018-09-16 10:44:48	Device Status	[TIMESTAMP: 2018-09-16 14:44:48] [accessory: 0] [cell: 0] [gps: 0] [gps_coarse: 0] [lac: 0] [mcc: 0] [nmea: 0] [pipeline: 0] [skyhook: 0] [wifi: 0] [wifi2: 0] [PLLOCATIONAGENT_EVENTFORWARD...
11978	2018-09-16 10:44:51	Device Status	[TIMESTAMP: 2018-09-16 14:44:51] [Brightness: 72.7005004883] [PLDISPLAYAGENT_EVENTFORWARD_DISPLAY TABLE ID: 95724]
11979	2018-09-16 10:44:52	Device Status	[TIMESTAMP: 2018-09-16 14:44:52] [BUTTON TYPE: 48] [EVENT TYPE: 1] [PLBUTTONAGENT_EVENTPOINT_BUTTONTABLE TABLE ID: 22343]
11980	2018-09-16 10:44:52	Device Status	[TIMESTAMP: 2018-09-16 14:44:52] [BUTTON TYPE: 48] [EVENT TYPE: 0] [PLBUTTONAGENT_EVENTPOINT_BUTTONTABLE TABLE ID: 22344]
11981	2018-09-16 10:44:52	Device Status	[TIMESTAMP: 2018-09-16 14:44:52] [Brightness: 73.7777709961] [PLDISPLAYAGENT_EVENTFORWARD_DISPLAY TABLE ID: 95725]
11982	2018-09-16 10:44:53	Device Status	[TIMESTAMP: 2018-09-16 14:44:53] [Brightness: 75.2227783203] [PLDISPLAYAGENT_EVENTFORWARD_DISPLAY TABLE ID: 95726]
11983	2018-09-16 10:44:53	Device Status	[TIMESTAMP: 2018-09-16 14:44:53] [Brightness: 0.0] [PLDISPLAYAGENT_EVENTFORWARD_DISPLAY TABLE ID: 95727]
11984	2018-09-16 10:44:53	Device State	[TIMESTAMP: 2018-09-16 14:44:53] [Screen: 0] [PLSPRINGBOARDAGENT_EVENTFORWARD_SBSCREEN TABLE ID: 84445]
11985	2018-09-16 10:44:55	Device Status	[TIMESTAMP: 2018-09-16 14:44:55] [TIMESTAMP END: 2018-09-16 14:48:25] [topic: com.apple.private.alloy.photos.proxy] [priority: Sync] [INCOMING MESSAGES: 2] [OUTGOING MESSAGES: 2]...
11986	2018-09-16 10:44:55	Device Status	[TIMESTAMP: 2018-09-16 14:44:55] [TIMESTAMP END: 2018-09-16 14:48:25] [topic: com.apple.private.alloy.nsurlsessionproxy] [priority: Default] [INCOMING MESSAGES: 11] [OUTGOING MESS...
11987	2018-09-16 10:44:55	Device Status	[TIMESTAMP: 2018-09-16 14:44:55] [TIMESTAMP END: 2018-09-16 14:48:25] [topic: com.apple.private.alloy.coreduet] [priority: Default] [INCOMING MESSAGES: 1] [OUTGOING MESSAGES: 0] [I...
11988	2018-09-16 10:44:55	Device Status	[TIMESTAMP: 2018-09-16 14:44:55] [TIMESTAMP END: 2018-09-16 14:48:25] [topic: com.apple.private.alloy.news] [priority: Default] [INCOMING MESSAGES: 2] [OUTGOING MESSAGES: 1] [INC...

APOLLO OUTPUT EXAMPLE [4]
APP USAGE & BROWSING

	localtime	Activity	Output
12139	2018-09-16 10:54:15	Application Usage	[ADJUSTED_TIMESTAMP: 2018-09-16 14:54:15] [BUNDLE_ID: com.apple.lock-screen] [APPROLE: 3] [DISPLAY: 0] [LEVEL: 1050.0] [ORIENTATION: 1] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_S...
12140	2018-09-16 10:54:16	Device Status	[ENTRY CREATION: 2018-09-16 14:54:16] [DAY OF WEEK: Sunday] [START: 2018-09-16 13:56:56] [END: 2018-09-16 14:54:16] [USAGE IN SECONDS: 3440] [IS LOCKED: LOCKED] [STREAM NA...
12141	2018-09-16 10:54:16	Application Usage	[ADJUSTED_TIMESTAMP: 2018-09-16 14:54:16] [BUNDLE_ID: com.apple.springboard.home-screen] [APPROLE: 1] [DISPLAY: 0] [LEVEL: 0.0] [ORIENTATION: 1] [SCREENWEIGHT: 1.0] [ORIGINAL_...
12142	2018-09-16 10:54:17	Application Usage	[ADJUSTED_TIMESTAMP: 2018-09-16 14:54:17] [BUNDLE_ID: com.apple.mobilemail] [APPROLE: 1] [DISPLAY: 0] [LEVEL: 1.0] [ORIENTATION: 1] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATE...
12143	2018-09-16 10:54:18	Application In Focus	[ENTRY CREATION: 2018-09-16 14:54:22] [BUNDLE ID: com.apple.mobilemail] [DAY OF WEEK: Sunday] [GMT OFFSET: -4] [START: 2018-09-16 14:54:18] [END: 2018-09-16 14:54:22] [USAGE IN ...
12144	2018-09-16 10:54:22	Application Activity	[ENTRY CREATION: 2018-09-16 14:54:22] [DAY OF WEEK: Sunday] [BUNDLE ID: com.apple.mobilemail] [ACTIVITY TYPE: com.apple.mail.mailbox] [TITLE: None] [EXPIRATION DATE: 2018-10-16 1...
12145	2018-09-16 10:54:22	Application Usage	[ADJUSTED_TIMESTAMP: 2018-09-16 14:54:22] [BUNDLE_ID: com.apple.springboard.home-screen] [APPROLE: 1] [DISPLAY: 0] [LEVEL: 0.0] [ORIENTATION: 1] [SCREENWEIGHT: 1.0] [ORIGINAL_...
12146	2018-09-16 10:54:25	Device State	[TIMESTAMP: 2018-09-16 14:54:25] [LEVEL: 100.0] [RAW LEVEL: 94.867980662] [IS CHARGING: 0] [FULLY CHARGED: 0] [PLBATTERYAGENT_EVENTBACKWARD_BATTERY TABLE ID: 495004]
12147	2018-09-16 10:54:26	Application In Focus	[ENTRY CREATION: 2018-09-16 14:54:30] [BUNDLE ID: com.apple.MobileSMS] [DAY OF WEEK: Sunday] [GMT OFFSET: -4] [START: 2018-09-16 14:54:26] [END: 2018-09-16 14:54:30] [USAGE I...
12148	2018-09-16 10:54:26	Application Usage	[ADJUSTED_TIMESTAMP: 2018-09-16 14:54:26] [BUNDLE_ID: com.apple.MobileSMS] [APPROLE: 1] [DISPLAY: 0] [LEVEL: 1.0] [ORIENTATION: 1] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STAT...
12149	2018-09-16 10:54:29	Application Usage	[ADJUSTED_TIMESTAMP: 2018-09-16 14:54:29] [BUNDLE_ID: com.apple.mobilesafari] [APPROLE: 1] [DISPLAY: 0] [LEVEL: 1.0] [ORIENTATION: 1] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STA...
12150	2018-09-16 10:54:30	Application In Focus	[ENTRY CREATION: 2018-09-16 14:58:09] [BUNDLE ID: com.apple.mobilesafari] [DAY OF WEEK: Sunday] [GMT OFFSET: -4] [START: 2018-09-16 14:54:30] [END: 2018-09-16 14:58:09] [USAGE I...
12151	2018-09-16 10:54:40	Safari Browsing	[ENTRY CREATION: 2018-09-16 14:54:40] [DAY OF WEEK: Sunday] [URL: https://www.npr.org/2018/09/16/648317623/sunday-puzzle-tba] [BUNDLE ID: com.apple.mobilesafari] [STREAM NAME: ...

APOLLO OUTPUT EXAMPLE [5] CONTEXT WITH INTERACTIONS

	localtime	Activity	Output
12224	2018-09-16 10:59:57	Device State	[TIMESTAMP: 2018-09-16 14:59:57] [LEVEL: 100.0] [RAW LEVEL: 94.2028985507] [IS CHARGING: 0] [FULLY CHARGED: 0] [PLBATTERYAGENT_EVENTBACKWARD_BATTERY TABLE ID: 495018]
12225	2018-09-16 10:59:57	Network Usage	[TIMESTAMP: 2018-09-16 14:59:57] [CURRENT SSID: 0C521C D30989] [CURRENT CHANNEL: 1] [PLWIFIAGENT_EVENTBACKWARD_CUMULATIVEPROPERTIES TABLE I...
12226	2018-09-16 10:59:57	Network Usage	[TIMESTAMP: 2018-09-16 14:59:57] [CURRENT SSID: 0C521C D30989] [CURRENT CHANNEL: 1] [PLWIFIAGENT_EVENTBACKWARD_CUMULATIVEPROPERTIES TABLE I...
12227	2018-09-16 11:00:00	App Usage	[ZINTERACTIONS CREATION DATE: 2018-09-16 16:40:49] [ZBUNDLEID: com.apple.mobilemail] [ZDISPLAYNAME: Redfin] [ZIDENTIFIER: listings@redfin.com] [ZPERSONID: None] [ZDIRECTION: 0...
12228	2018-09-16 11:00:00	App Usage	[ZINTERACTIONS CREATION DATE: 2018-09-16 16:40:49] [ZBUNDLEID: com.apple.mobilemail] [ZDISPLAYNAME: Audi Experience] [ZIDENTIFIER: audiexperience@e.audiusa.com] [ZPERSONID: N...
12229	2018-09-16 11:00:00	App Usage	[ZINTERACTIONS CREATION DATE: 2018-09-16 16:40:49] [ZBUNDLEID: com.apple.mobilemail] [ZDISPLAYNAME:] [ZIDENTIFIER:] [ZPERSONID: None] [ZDIREC...
12230	2018-09-16 11:00:00	App Usage	[ZINTERACTIONS CREATION DATE: 2018-09-16 16:40:49] [ZBUNDLEID: com.apple.mobilemail] [ZDISPLAYNAME: The Container Store] [ZIDENTIFIER: pop@my.containerstore.com] [ZPERSONID: ...
12231	2018-09-16 11:00:00	App Usage	[ZINTERACTIONS CREATION DATE: 2018-09-17 11:43:30] [ZBUNDLEID: com.apple.mobilemail] [ZDISPLAYNAME: Audi Experience] [ZIDENTIFIER: audiexperience@e.audiusa.com] [ZPERSONID: N...
12232	2018-09-16 11:00:00	App Usage	[ZINTERACTIONS CREATION DATE: 2018-09-17 11:43:30] [ZBUNDLEID: com.apple.mobilemail] [ZDISPLAYNAME: The Container Store] [ZIDENTIFIER: pop@my.containerstore.com] [ZPERSONID: ...
12233	2018-09-16 11:00:00	App Usage	[ZINTERACTIONS CREATION DATE: 2018-09-17 11:43:30] [ZBUNDLEID: com.apple.mobilemail] [ZDISPLAYNAME: Redfin] [ZIDENTIFIER: listings@redfin.com] [ZPERSONID: None] [ZDIRECTION: 0]...

APOLLO OUTPUT EXAMPLE [6]
HEART RATE & WORKOUT LOCATION

	localtime	Activity	Output
12746	2018-09-16 11:37:00	Application Usage	[TIMESTAMP: 2018-09-16 15:37:00] [BUNDLE ID: com.atebits.Tweetie2] [CONNECTION TYPE: wwan] [IS DROPPED: None] [LINK QUALITY: None] [Priority: 10] [Topic: com.atebits.Tweetie2] [SER...
12747	2018-09-16 11:37:02	Health Heart Rate	[Start Date: 2018-09-16 15:37:02] [End Date: 2018-09-16 15:37:02] [Data Type: 5] [quantity: 2.35] [original_quantity: 141.0] [unit_string: count/min] [key: HKMetadataKeyHeartRateMotionContext]...
12748	2018-09-16 11:37:02	Health Heart Rate	[Start Date: 2018-09-16 15:37:02] [End Date: 2018-09-16 15:37:02] [Data Type: 5] [quantity: 2.35] [original_quantity: 141.0] [unit_string: count/min] [key: _HKPrivateHeartRateContext] [Samples T...
12749	2018-09-16 11:37:06	Location	[TIMESTAMP: 2018-09-16 15:37:06] [COORDINATES: 38.8802585552204, -77.111613813563] [ALTITUDE: 89.7836456299] [COURSE: -1.0] [SPEED: -1.0] [HORIZONTAL ACCURACY: 65.0] [VER...
12750	2018-09-16 11:37:07	Location	[TIMESTAMP: 2018-09-16 15:37:07] [COORDINATES: 38.8802601822436, -77.1116145815906] [ALTITUDE: 89.753616333] [COURSE: -1.0] [SPEED: -1.0] [HORIZONTAL ACCURACY: 65.0] [VERT...
12751	2018-09-16 11:37:11	Health Heart Rate	[Start Date: 2018-09-16 15:37:11] [End Date: 2018-09-16 15:37:11] [Data Type: 5] [quantity: 2.33333333333] [original_quantity: 140.0] [unit_string: count/min] [key: HKMetadataKeyHeartRateMoti...
12752	2018-09-16 11:37:11	Health Heart Rate	[Start Date: 2018-09-16 15:37:11] [End Date: 2018-09-16 15:37:11] [Data Type: 5] [quantity: 2.33333333333] [original_quantity: 140.0] [unit_string: count/min] [key: _HKPrivateHeartRateContext] ...
12753	2018-09-16 11:37:12	Health Heart Rate	[Start Date: 2018-09-16 15:37:12] [End Date: 2018-09-16 15:37:12] [Data Type: 5] [quantity: 2.33333333333] [original_quantity: 140.0] [unit_string: count/min] [key: HKMetadataKeyHeartRateMot...
12754	2018-09-16 11:37:12	Health Heart Rate	[Start Date: 2018-09-16 15:37:12] [End Date: 2018-09-16 15:37:12] [Data Type: 5] [quantity: 2.33333333333] [original_quantity: 140.0] [unit_string: count/min] [key: _HKPrivateHeartRateContext] ...
12755	2018-09-16 11:37:17	Health Heart Rate	[Start Date: 2018-09-16 15:37:17] [End Date: 2018-09-16 15:37:17] [Data Type: 5] [quantity: 2.33333333333] [original_quantity: 140.0] [unit_string: count/min] [key: HKMetadataKeyHeartRateMot...
12756	2018-09-16 11:37:17	Health Heart Rate	[Start Date: 2018-09-16 15:37:17] [End Date: 2018-09-16 15:37:17] [Data Type: 5] [quantity: 2.33333333333] [original_quantity: 140.0] [unit_string: count/min] [key: _HKPrivateHeartRateContext] ...
12757	2018-09-16 11:37:25	Health Heart Rate	[Start Date: 2018-09-16 15:37:25] [End Date: 2018-09-16 15:37:25] [Data Type: 5] [quantity: 2.35] [original_quantity: 141.0] [unit_string: count/min] [key: HKMetadataKeyHeartRateMotionContext]...
12758	2018-09-16 11:37:25	Health Heart Rate	[Start Date: 2018-09-16 15:37:25] [End Date: 2018-09-16 15:37:25] [Data Type: 5] [quantity: 2.35] [original_quantity: 141.0] [unit_string: count/min] [key: _HKPrivateHeartRateContext] [Samples T...
12759	2018-09-16 11:37:27	Health Heart Rate	[Start Date: 2018-09-16 15:37:27] [End Date: 2018-09-16 15:37:27] [Data Type: 5] [quantity: 2.4] [original_quantity: 144.0] [unit_string: count/min] [key: HKMetadataKeyHeartRateMotionContext] ...
12760	2018-09-16 11:37:27	Health Heart Rate	[Start Date: 2018-09-16 15:37:27] [End Date: 2018-09-16 15:37:27] [Data Type: 5] [quantity: 2.4] [original_quantity: 144.0] [unit_string: count/min] [key: _HKPrivateHeartRateContext] [Samples Ta...
12761	2018-09-16 11:37:58	Location	[TIMESTAMP: 2018-09-16 15:37:58] [COORDINATES: 38.880329507199, -77.1116755548252] [ALTITUDE: 90.4955047722] [COURSE: -1.0] [SPEED: -1.0] [HORIZONTAL ACCURACY: 20.0] [VER...
12762	2018-09-16 11:38:00	Application Usage	[TIMESTAMP: 2018-09-16 15:38:00] [BUNDLE ID: com.atebits.Tweetie2] [CONNECTION TYPE: wwan] [IS DROPPED: None] [LINK QUALITY: None] [Priority: 10] [Topic: com.atebits.Tweetie2] [SER...
12763	2018-09-16 11:38:18	Device State	[TIMESTAMP: 2018-09-16 15:38:18] [LEVEL: 98.0] [RAW LEVEL: 92.9875821768] [IS CHARGING: 0] [FULLY CHARGED: 0] [PLBATTERYAGENT_EVENTBACKWARD_BATTERY TABLE ID: 495078]
12764	2018-09-16 11:38:18	Device Status	[TIMESTAMP: 2018-09-16 15:38:18] [DEVICE CONNECTABLE: 1] [DEVICE CONNECTED: 0] [DEVICE DISCOVERABLE: 0] [DEVICE POWERED: 1] [PLBLUETOOTHAGENT_EVENTFORWARD_DEVICES...

FUTURE IMPROVEMENTS

More Queries!

- More iOS Databases
- Additional tables in currently parsed databases
- MacOS Data
- Additional Databases, perhaps less Pattern-of-Life Data to put context to PoL data
- Additional queries in the same config for various OS versions (possible backwards compatibility)

Additional Testing – This is PoC code at best

Efficiency at full device dumps

Better BLOB Display – Possible "strings" function at least

Automatic Embedded Plist Extraction and Display

Automatic Unarchiving of PowerLog Archive GZip Files

Multiple Database Filenames

Automatic Database Coalescing

Visualization

PERFECTION, THIS ISN'T.

Proof of Concept Code

- Still needs lots of testing on various datasets, iOS versions, iOS devices
- Haven't even started macOS support.

It ain't pretty

- Does not work for small screened laptops.

It ain't fast

- Not speedy on full iOS dumps, but once the specific databases are extracted pretty quick.

Only works on SQL Databases

Mo' Data, Mo' Problems

- Potentially a million+ data points
- SQL Query Filtering (Yo dawg, I hear you like databases so I put your databases into a database.)

Timestamps & Time Zones

- Can't we all just agree to UTC or GTFO?

MAHALO!

Will be released soon at github.com/mac4n6 (I promise!)

@iamevltwin | mac4n6.com

Take a Class! SANS FOR518 – Mac and iOS Forensic Analysis & Incident Response FOR518.com

- Sydney - November
- London – February
- San Francisco – March
- Orlando – April
- San Diego - May
- Amsterdam - May
- Washington, DC – June
- Austin - July