

Go for Launch: Getting Started with Practical APOLLO Analysis



Sarah Edwards | github.com/mac4n6/APOLLO

@iamevtwin | mac4n6.com | sarah@blackbagtech.com | FOR518.com

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

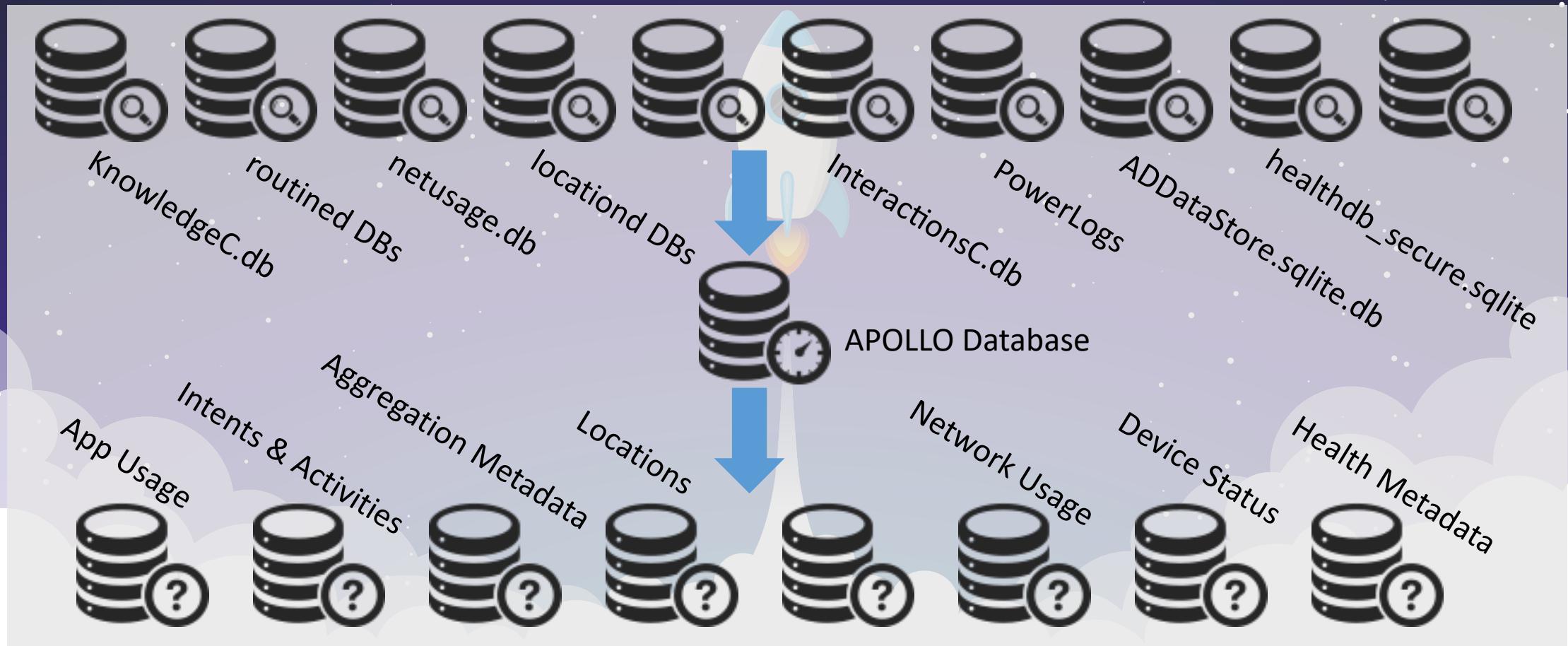
Camera/Flashlight
Usage

User Activities

Apple Pattern of Life Lazy Output'er (APOLLO)

- Quick Correlation
 - Not perfect nor pretty - but it works! (usually)
- Low Bar to Entry – Easy contribution for busy forensic investigators
 - Almost anyone can develop a SQL Query
- Easy to update and configure SQL queries
 - Across Devices & Across OS Versions
- SQL Script Sharing
 - Each query is a separate APOLLO Module
- Python & SQL scripts here: github.com/mac4n6/APOLLO

How Does it Work?



APOLLO Module

- Module Metadata
 - Notes & Authorship
- Database Metadata
 - Database Filename
 - Versioning
- Query Metadata
 - Key Timestamp
- SQL Query
 - Sometimes many!

```
59 [Module Metadata]
60 AUTHOR=Sarah Edwards/mac4n6.com/@iamevtwin
61 MODULE_NOTES=Application Usage, shows application in focus on device.
62
63 [Database Metadata]
64 DATABASE=knowledgeC.db
65 PLATFORM=IOS,MACOS
66 VERSIONS=11,12,13,10.13,10.14,10.15
67
68 [Query Metadata]
69 QUERY_NAME=knowledge_app_inFocus
70 ACTIVITY=Application In Focus
71 KEY_TIMESTAMP=START
72
73 [SQL Query 11,12,13,10.13,10.14,10.15]
74 QUERY=
75     SELECT
76         DATETIME(ZOBJECT.ZSTARTDATE+978307200,'UNIXEPOCH') AS "START",
77         DATETIME(ZOBJECT.ZENDDATE+978307200,'UNIXEPOCH') AS "END",
78         ZOBJECT.ZVALUESTRING AS "BUNDLE ID",
79         (ZOBJECT.ZENDDATE-ZOBJECT.ZSTARTDATE) AS "USAGE IN SECONDS",
80         (ZOBJECT.ZENDDATE-ZOBJECT.ZSTARTDATE)/60.00 AS "USAGE IN MINUTES",
81         ZSTRUCTUREDMETADATA .Z_DKAPPLICATIONMETADATATEKEY__LAUNCHREASON AS "LAUNCH REASON",
82         ZSTRUCTUREDMETADATA .Z_DKAPPLICATIONMETADATATEKEY__EXTENSIONCONTAININGBUNDLEIDENTIFIER AS "EXTENSION CONTAINING BUNDLE ID",
83         ZSTRUCTUREDMETADATA .Z_DKAPPLICATIONMETADATATEKEY__EXTENSIONHOSTIDENTIFIER AS "EXTENSION HOST ID",
84         CASE ZOBJECT.ZSTARTDAYOFWEEK
85             WHEN "1" THEN "Sunday"
86             WHEN "2" THEN "Monday"
87             WHEN "3" THEN "Tuesday"
88             WHEN "4" THEN "Wednesday"
89             WHEN "5" THEN "Thursday"
90             WHEN "6" THEN "Friday"
91             WHEN "7" THEN "Saturday"
92             END "DAY OF WEEK",
93             ZOBJECT.ZSECONDSFROMGMT/3600 AS "GMT OFFSET",
94             DATETIME(ZOBJECT.ZCREATIONDATE+978307200,'UNIXEPOCH') AS "ENTRY CREATION",
95             ZOBJECT.ZUUID AS "UUID",
96             ZSTRUCTUREDMETADATA.ZMETADATAHASH,
97             ZOBJECT.Z_PK AS "ZOBJECT TABLE ID"
98     FROM ZOBJECT
99     LEFT JOIN
100        ZSTRUCTUREDMETADATA
101        ON ZOBJECT.ZSTRUCTUREDMETADATA = ZSTRUCTUREDMETADATA.Z_PK
102     LEFT JOIN
103        ZSOURCE
104        ON ZOBJECT.ZSOURCE = ZSOURCE.Z_PK
105        WHERE ZSTREAMNAME IS "/app/inFocus"
```

New in Version 1.4

- Specific Action Commands
 - Gather
 - Gather on Jailbroken iOS Device (remote or tethered via iproxy), or macOS (possibly on other platforms?)
 - Extract
- Improved Overall Processing



- Output
 - JSON in SQLite
 - Improved CSV
- More Modules, now ~246
- Module Updates for iOS 14 and macOS 11

Gather on macOS 11.

```
[oompa@qwerty-MBP APOLLO_v1_4 % sudo python3 apollo.py gather_macos modules / --ignore /System/Data/Volume  
--ignore ~/miphone_13_5 --ignore ~/Downloads --ignore ~/Library/Mobile\ Documents  
[Password:
```



```
APOLLO Modules Version: 11182020  
Action: gather_macos  
Data Directory: /  
    Ignoring Directory: /System/Data/Volume  
    Ignoring Directory: /Users/oompa/miphone_13_5  
    Ignoring Directory: /Users/oompa/Downloads  
    Ignoring Directory: /Users/oompa/Library/Mobile Documents  
Modules Directory: modules  
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```

```
...Parsing Modules in...modules  
...Creating /tmp_apollo in: /Users/oompa/Downloads/APOLLO_v1_4/tmp_apollo  
...Searching for and copying databases into tmp_apollo...  
...chmod/chown all the things...
```

Gather on macOS 11.

```
[oompa@qwerty-MBP APOLLO_v1_4 % sudo python3 apollo.py gather_macos modules / --ignore /System/Data/Volume  
--ignore ~/miphone_13_5 --ignore ~/Downloads --ignore ~/Library/Mobile Documents  
[Password:
```



```
APOLLO Modules Version: 11182020  
Action: gather_macos  
Data Directory: /  
    Ignoring Directory: /System/Data/Volume  
    Ignoring Directory: /Users/oompa/miphone_13_5  
    Ignoring Directory: /Users/oompa/Downloads  
    Ignoring Directory: /Users/oompa/Library/Mobile Documents  
Modules Directory: modules  
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```

```
...Parsing Modules in...modules  
...Creating /tmp_apollo in: /Users/oompa/Downloads/APOLLO_v1_4/tmp_apollo  
...Searching for and copying databases into tmp_apollo...  
...chmod/chown all the things...
```

Gather on macOS 11.

```
[oompa@qwerty-MBP APOLLO_v1_4 % sudo python3 apollo.py gather_macos modules / --ignore /System/Data/Volume  
--ignore ~/miphone_13_5 --ignore ~/Downloads --ignore ~/Library/Mobile\ Documents  
[Password:  
]
```

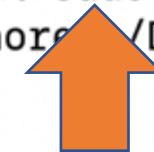


```
APOLLO Modules Version: 11182020  
Action: gather_macos  
Data Directory: /  
    Ignoring Directory: /System/Data/Volume  
    Ignoring Directory: /Users/oompa/miphone_13_5  
    Ignoring Directory: /Users/oompa/Downloads  
    Ignoring Directory: /Users/oompa/Library/Mobile Documents  
Modules Directory: modules  
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```

```
...Parsing Modules in...modules  
...Creating /tmp_apollo in: /Users/oompa/Downloads/APOLLO_v1_4/tmp_apollo  
...Searching for and copying databases into tmp_apollo...  
...chmod/chown all the things...
```

Gather on macOS 11.

```
[oompa@qwerty-MBP APOLLO_v1_4 % sudo python3 apollo.py gather_macos modules / --ignore /System/Data/Volume  
--ignore ~/miphone_13_5 --ignore ~/Downloads --ignore ~/Library/Mobile\ Documents  
[Password:  
]
```



```
APOLLO Modules Version: 11182020  
Action: gather_macos  
Data Directory: /  
    Ignoring Directory: /System/Data/Volume  
    Ignoring Directory: /Users/oompa/miphone_13_5  
    Ignoring Directory: /Users/oompa/Downloads  
    Ignoring Directory: /Users/oompa/Library/Mobile Documents  
Modules Directory: modules  
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```

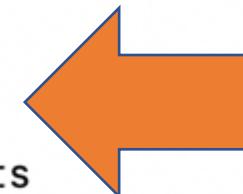
```
...Parsing Modules in...modules  
...Creating /tmp_apollo in: /Users/oompa/Downloads/APOLLO_v1_4/tmp_apollo  
...Searching for and copying databases into tmp_apollo...  
...chmod/chown all the things...
```

Gather on macOS 11.

```
[oompa@qwerty-MBP APOLLO_v1_4 % sudo python3 apollo.py gather_macos modules / --ignore /System/Data/Volume  
--ignore ~/miphone_13_5 --ignore ~/Downloads --ignore ~/Library/Mobile\ Document  
[Password:
```



```
APOLLO Modules Version: 11182020  
Action: gather_macos  
Data Directory: /  
    Ignoring Directory: /System/Data/Volume  
    Ignoring Directory: /Users/oompa/miphone_13_5  
    Ignoring Directory: /Users/oompa/Downloads  
    Ignoring Directory: /Users/oompa/Library/Mobile Documents  
Modules Directory: modules  
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```



```
...Parsing Modules in...modules  
...Creating /tmp_apollo in: /Users/oompa/Downloads/APOLLO_v1_4/tmp_apollo  
...Searching for and copying databases into tmp_apollo...  
...chmod/chown all the things...
```

Gather on macOS 11.

```
[oompa@qwerty-MBP APOLLO_v1_4 % sudo python3 apollo.py gather_macos modules / --ignore /System/Data/Volume  
--ignore ~/miphone_13_5 --ignore ~/Downloads --ignore ~/Library/Mobile\ Documents  
[Password:
```

```
APOLLO Modules Version: 11182020  
Action: gather_macos  
Data Directory: /  
Ignoring Directory: /System/Data/Volume  
Ignoring Directory: /Users/oompa/miphone_13_5  
Ignoring Directory: /Users/oompa/Downloads  
Ignoring Directory: /Users/oompa/Library/Mobile Documents  
Modules Directory: modules  
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```

```
...Parsing Modules in...modules  
...Creating /tmp_apollo in: /Users/oompa/Downloads/APOLLO_v1_4/tmp_apollo  
...Searching for and copying databases into tmp_apollo...  
...chmod/chown all the things...
```



Gather on iOS 14.2 [checkra1n'ed]

```
oompa@qwerty-MBP APOLLO_v1_4 % python3 apollo.py gather_ios --ip 127.0.0.1 --port 4242 modules /private/var
```

```
-----  
APOLLO Modules Version: 11182020
```

```
Action: gather_ios
```

```
Data Directory: /private/var
```

```
Modules Directory: modules
```

```
Jailbroken Device IP/Domain: 127.0.0.1
```

```
Jailbroken Device Port: 4242
```

```
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```

```
...Parsing Modules in...modules
```

```
...Creating /tmp_apollo in: /Users/oompa/Downloads/APOLLO_v1_4/tmp_apollo
```

```
...Finding files on root@127.0.0.1:4242 in /private/var
```

```
find: /private/var/.fsevents: Operation not permitted
```

```
find: /private/var/mobile/Library/Mobile Documents/com~apple~CloudDocs/Documents/airdrop_test/david/fsevents/.fseve
```

```
nts: Operation not permitted
```

```
...Writing ios_files.txt...
```

```
...Searching for and copying databases into tmp_apollo...
```

netusage.sqlite	100%	216KB	18.9MB/s	00:00
netusage.sqlite-shm	100%	32KB	8.2MB/s	00:00
netusage.sqlite-wal	100%	974KB	22.4MB/s	00:00
Cache.sqlite-wal	100%	2499KB	22.4MB/s	00:00
Cache.sqlite-shm	100%	32KB	9.3MB/s	00:00
Cache.sqlite	100%	2216KB	22.1MB/s	00:00
Local.sqlite	100%	852KB	21.4MB/s	00:00
Cloud-V2.sqlite-wal	100%	2157KB	17.5MB/s	00:00
Cloud-V2.sqlite-shm	100%	32KB	10.1MB/s	00:00
Cloud-V2.sqlite	100%	2788KB	22.2MB/s	00:00
Local.sqlite-shm	100%	32KB	11.3MB/s	00:00
Local.sqlite-wal	100%	149KB	18.1MB/s	00:00

Gather on iOS 14.2 [checkra1n'ed]

```
[oompa@qwerty-MBP APOLLO_v1_4 % python3 apollo.py gather_ios --ip 127.0.0.1 --port 4242 modules /private/var
```

```
-----  
APOLLO Modules Version: 11182020
```

```
Action: gather_ios
```

```
Data Directory: /private/var
```

```
Modules Directory: modules
```

```
Jailbroken Device IP/Domain: 127.0.0.1
```

```
Jailbroken Device Port: 4242
```

```
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```

```
...Parsing Modules in...modules
```

```
...Creating /tmp_apollo in: /Users/oompa/Downloads/APOLLO_v1_4/tmp_apollo
```

```
...Finding files on root@127.0.0.1:4242 in /private/var
```

```
find: /private/var/.fsevents: Operation not permitted
```

```
find: /private/var/mobile/Library/Mobile Documents/com~apple~CloudDocs/Documents/airdrop_test/david/fsevents/.fsevents: Operation not permitted
```

```
...Writing ios_files.txt...
```

```
...Searching for and copying databases into tmp_apollo...
```

netusage.sqlite	100%	216KB	18.9MB/s	00:00
netusage.sqlite-shm	100%	32KB	8.2MB/s	00:00
netusage.sqlite-wal	100%	974KB	22.4MB/s	00:00
Cache.sqlite-wal	100%	2499KB	22.4MB/s	00:00
Cache.sqlite-shm	100%	32KB	9.3MB/s	00:00
Cache.sqlite	100%	2216KB	22.1MB/s	00:00
Local.sqlite	100%	852KB	21.4MB/s	00:00
Cloud-V2.sqlite-wal	100%	2157KB	17.5MB/s	00:00
Cloud-V2.sqlite-shm	100%	32KB	10.1MB/s	00:00
Cloud-V2.sqlite	100%	2788KB	22.2MB/s	00:00
Local.sqlite-shm	100%	32KB	11.3MB/s	00:00
Local.sqlite-wal	100%	149KB	18.1MB/s	00:00

Gather on iOS 14.2 [checkra1n'ed]

```
oompa@qwerty5-MBP APOLLO_v1_4 % python3 apollo.py gather_ios --ip 127.0.0.1 --port 4242 modules /private/var
```

```
Apollo Modules Version: 11182020
Action: gather_ios
Data Directory: /private/var
Modules Directory: modules
Jailbroken Device IP/Domain: 127.0.0.1
Jailbroken Device Port: 4242
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```

```
...Parsing Modules in...modules
...Creating /tmp_apollo in: /Users/oompa/Downloads/APOLLO_v1_4/tmp_apollo
...Finding files on root@127.0.0.1:4242 in /private/var
find: /private/var/.fsevents.d: Operation not permitted
find: /private/var/mobile/Library/Mobile Documents/com~apple~CloudDocs/Documents/airdrop_test/david/fsevents/.fsevents.d: Operation not permitted
...Writing ios_files.txt...
...Searching for and copying databases into tmp_apollo...
netusage.sqlite
netusage.sqlite-shm
netusage.sqlite-wal
Cache.sqlite-wal
Cache.sqlite-shm
Cache.sqlite
Local.sqlite
Cloud-V2.sqlite-wal
Cloud-V2.sqlite-shm
Cloud-V2.sqlite
Local.sqlite-shm
Local.sqlite-wal
```

	100%	216KB	18.9MB/s	00:00
netusage.sqlite-shm	100%	32KB	8.2MB/s	00:00
netusage.sqlite-wal	100%	974KB	22.4MB/s	00:00
Cache.sqlite-wal	100%	2499KB	22.4MB/s	00:00
Cache.sqlite-shm	100%	32KB	9.3MB/s	00:00
Cache.sqlite	100%	2216KB	22.1MB/s	00:00
Local.sqlite	100%	852KB	21.4MB/s	00:00
Cloud-V2.sqlite-wal	100%	2157KB	17.5MB/s	00:00
Cloud-V2.sqlite-shm	100%	32KB	10.1MB/s	00:00
Cloud-V2.sqlite	100%	2788KB	22.2MB/s	00:00
Local.sqlite-shm	100%	32KB	11.3MB/s	00:00
Local.sqlite-wal	100%	149KB	18.1MB/s	00:00

Gather on iOS 14.2 [checkra1n'ed]

```
oompa@qwerty-MBP APOLLO_v1_4 % python3 apollo.py gather_ios --ip 127.0.0.1 --port 4242 modules /private/var
```

```
-----  
APOLLO Modules Version: 11182020
```

```
Action: gather_ios
```

```
Data Directory: /private/var
```

```
Modules Directory: modules
```

```
Jailbroken Device IP/Domain: 127.0.0.1
```

```
Jailbroken Device Port: 4242
```

```
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```

```
...Parsing Modules in...modules
```

```
...Creating /tmp_apollo in: /Users/oompa/Downloads/APOLLO_v1_4/tmp_apollo
```

```
...Finding files on root@127.0.0.1:4242 in /private/var
```

```
find: /private/var/.fsevents: Operation not permitted
```

```
find: /private/var/mobile/Library/Mobile Documents/com~apple~CloudDocs/Documents/airdrop_test/david/fsevents/.fseve
```

```
nts: Operation not permitted
```

```
...Writing ios_files.txt...
```

```
...Searching for and copying databases into tmp_apollo... ←
```

netusage.sqlite	100%	216KB	18.9MB/s	00:00
netusage.sqlite-shm	100%	32KB	8.2MB/s	00:00
netusage.sqlite-wal	100%	974KB	22.4MB/s	00:00
Cache.sqlite-wal	100%	2499KB	22.4MB/s	00:00
Cache.sqlite-shm	100%	32KB	9.3MB/s	00:00
Cache.sqlite	100%	2216KB	22.1MB/s	00:00
Local.sqlite	100%	852KB	21.4MB/s	00:00
Cloud-V2.sqlite-wal	100%	2157KB	17.5MB/s	00:00
Cloud-V2.sqlite-shm	100%	32KB	10.1MB/s	00:00
Cloud-V2.sqlite	100%	2788KB	22.2MB/s	00:00
Local.sqlite-shm	100%	32KB	11.3MB/s	00:00
Local.sqlite-wal	100%	149KB	18.1MB/s	00:00

Gather on 14.2 [checkra1n'ed]

```
oompa@qwerty-MBP APOLLO_v1_4 % python3 apollo.py gather_ios --ip 127.0.0.1 --port 4242 modules /private/var
```

```
-----  
APOLLO Modules Version: 11182020
```

```
Action: gather_ios
```

```
Data Directory: /private/var
```

```
Modules Directory: modules
```

```
Jailbroken Device IP/Domain: 127.0.0.1
```

```
Jailbroken Device Port: 4242
```

```
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```

```
...Parsing Modules in...modules
```

```
...Creating /tmp_apollo in: /Users/oompa/Downloads/APOLLO_v1_4/tmp_apollo
```

```
...Finding files on root@127.0.0.1:4242 in /private/var
```

```
find: /private/var/.fsevents: Operation not permitted
```

```
find: /private/var/mobile/Library/Mobile Documents/com~apple~CloudDocs/Documents/airdrop_test/david/fsevents/.fseve
```

```
nts: Operation not permitted
```

```
...Writing ios_files.txt...
```

```
...Searching for and copying databases into tmp_apollo... ←
```

```
netusage.sqlite
```

```
netusage.sqlite-shm
```

```
netusage.sqlite-wal
```

```
Cache.sqlite-wal
```

```
Cache.sqlite-shm
```

```
Cache.sqlite
```

```
Local.sqlite
```

```
Cloud-V2.sqlite-wal
```

```
Cloud-V2.sqlite-shm
```

```
Cloud-V2.sqlite
```

```
Local.sqlite-shm
```

```
Local.sqlite-wal
```

100%	216KB	18.9MB/s	00:00
100%	32KB	8.2MB/s	00:00
100%	974KB	22.4MB/s	00:00
100%	2499KB	22.4MB/s	00:00
100%	32KB	9.3MB/s	00:00
100%	2216KB	22.1MB/s	00:00
100%	852KB	21.4MB/s	00:00
100%	2157KB	17.5MB/s	00:00
100%	32KB	10.1MB/s	00:00
100%	2788KB	22.2MB/s	00:00
100%	32KB	11.3MB/s	00:00
100%	149KB	18.1MB/s	00:00

Recommendation:
Use SSH Keys

Gather on iOS 14.2 (checkra1n'ed)

```
[oompa@qwerty5-MBP APOLLO_v1_4 % python3 apollo.py gather_ios --ip 127.0.0.1 --port 4242 modules /private/var
```

```
-----  
APOLLO Modules Version: 11182020  
Action: gather_ios  
Data Directory: /private/var  
Modules Directory: modules  
Jailbroken Device IP/Domain: 127.0.0.1  
Jailbroken Device Port: 4242
```

```
Current Working Director
```

```
...Parsing Modules in...  
...Creating /tmp_apollo  
...Finding files on root  
find: /private/var/.fsevents: Operation not permitted  
find: /private/var/mobile/Library/Mobile Documents/com~apple~CloudDocs/Documents/didrop_test/david/fsevents/.fsevents: Operation not permitted  
ntsd: Operation not permitted  
...Writing ios_files.txt...  
...Searching for and copying databases into tmp_apollo...
```

What about remote macOS collection?

netusage.sqlite	100%	216KB	18.9MB/s	00:00
netusage.sqlite-shm	100%	32KB	8.2MB/s	00:00
netusage.sqlite-wal	100%	974KB	22.4MB/s	00:00
Cache.sqlite-wal	100%	2499KB	22.4MB/s	00:00
Cache.sqlite-shm	100%	32KB	9.3MB/s	00:00
Cache.sqlite	100%	2216KB	22.1MB/s	00:00
Local.sqlite	100%	852KB	21.4MB/s	00:00
Cloud-V2.sqlite-wal	100%	2157KB	17.5MB/s	00:00
Cloud-V2.sqlite-shm	100%	32KB	10.1MB/s	00:00
Cloud-V2.sqlite	100%	2788KB	22.2MB/s	00:00
Local.sqlite-shm	100%	32KB	11.3MB/s	00:00
Local.sqlite-wal	100%	149KB	18.1MB/s	00:00

Gather on iOS 14.2 [checkra1n'ed]

```
[oompa@qwerty-MBP APOLLO_v1_4 % python3 apollo.py gather_ios --ip 127.0.0.1 --port 4242 modules /private/var
```

```
-----  
APOLLO Modules Version: 11182020  
Action: gather_ios  
Data Directory: /private/var  
Modules Directory: modules  
Jailbroken Device IP/Domain: 127.0.0.1  
Jailbroken Device Port: 4242  
Current Working Director
```

```
...Parsing Modules in...  
...Creating /tmp_apollo  
...Finding files on root  
find: /private/var/.fsevents  
find: /private/var/mobile  
ntsd: Operation not perm...  
...Writing ios_files.txt  
...Searching for and cop...  
netusage.sqlite  
netusage.sqlite-shm  
netusage.sqlite-wal  
Cache.sqlite-wal  
Cache.sqlite-shm  
Cache.sqlite
```

What about remote macOS collection?

Edit the hard-coded 'root' to appropriate username.

```
st/david/fsevents/.fseve
```

B	18.9MB/s	00:00
B	8.2MB/s	00:00
B	22.4MB/s	00:00
B	22.4MB/s	00:00
100%	32KB	9.3MB/s
100%	2216KB	22.1MB/s
100%	852KB	21.4MB/s
100%	2157KB	17.5MB/s
100%	32KB	10.1MB/s
100%	2788KB	22.2MB/s
100%	32KB	11.3MB/s
100%	149KB	18.1MB/s

Gather on AppleTV [iOS 13.4, checkra1n'ed]

```
oompa@qwerty-MBP APOLLO_v1_4 % python3 apollo.py gather_ios --ip 192.168.1.157 --port 44 modules /private/var  
-----  
APOLLO Modules Version: 11182020  
Action: gather_ios  
Data Directory: /private/var  
Modules Directory: modules  
Jailbroken Device IP/Domain: 192.168.1.157  
Jailbroken Device Port: 44  
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4  
-----  
...Parsing Modules in...modules  
...Creating /tmp_apollo in: /Users/oompa/Downloads/APOLLO_v1_4/tmp_apollo  
...Finding files on root@192.168.1.157:44 in /private/var  
[root@192.168.1.157's password:  
find: /private/var/.fsevents.d: Operation not permitted  
...Writing ios_files.txt...  
...Searching for and copying databases into tmp_apollo...  
[root@192.168.1.157's password:  
ADDDataStore.sqlite3  
100% 1420KB 5.3MB/s 00:00  
[root@192.168.1.157's password:  
ADDDataStore.sqlite3-shm  
100% 32KB 372.2KB/s 00:00  
[root@192.168.1.157's password:  
ADDDataStore.sqlite3-wal  
100% 0 0.0KB/s 00:00  
[root@192.168.1.157's password:  
knowledgeC.db  
100% 2636KB 6.0MB/s 00:00  
[root@192.168.1.157's password:  
knowledgeC.db-shm  
100% 32KB 1.8MB/s 00:00  
[root@192.168.1.157's password: ?]  
-----
```

No SSH Keys



Extract the data!

```
oompa@qwertys-MBP APOLLO_v1_4 % python3 apollo.py extract -o sql_json -v 14 -k modules tmp_apollo_ios14
```

APOLLO Modules Version: 111820



Action: extract

Platform: apple

Version: 14

Output: sql_json

Data Directory: tmp_apollo_ios14

Modules Directory: modules

KMZ: TRUE

Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4

...Parsing Modules in...modules

==> Parsing 233 modules (Note: Some modules may be run on more than one database.)

- [1] modules/aggregate_dictionary_distributed_keys.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14
- [2] modules/aggregate_dictionary_scalars.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14
- [3] modules/call_history.txt on CallHistory.storeddata: SQL Query 9,10,11,12,13,14
- [4] modules/datausage_zliveusage.txt on DataUsage-watch.sqlite: SQL Query 8,9,10,11,12,13,14

Extract the data!

```
oompa@qwertys-MBP APOLLO_v1_4 % python3 apollo.py extract -o sql_json -v 14 -k modules tmp_apollo_ios14
```



```
APOLLO Modules Version: 11182020
Action: extract
Platform: apple
Version: 14
Output: sql_json
Data Directory: tmp_apollo_ios14
Modules Directory: modules
KMZ: TRUE
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```

```
...Parsing Modules in...modules
```

```
==> Parsing 233 modules (Note: Some modules may be run on more than one database.)
```

```
[1] modules/aggregate_dictionary_distributed_keys.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14
[2] modules/aggregate_dictionary_scalars.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14
[3] modules/call_history.txt on CallHistory.storeddata: SQL Query 9,10,11,12,13,14
[4] modules/datausage_zliveusage.txt on DataUsage-watch.sqlite: SQL Query 8,9,10,11,12,13,14
```

Extract the data!

```
oompa@qwertys-MBP APOLLO_v1_4 % python3 apollo.py extract -o sql_json -v 14 -k modules tmp_apollo_ios14
```

```
APOLLO Modules Version: 11182020
Action: extract
Platform: apple
Version: 14
Output: sql_json
Data Directory: tmp_apollo_ios14
Modules Directory: modules
KMZ: TRUE
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```

```
...Parsing Modules in...modules
```

```
==> Parsing 233 modules (Note: Some modules may be run on more than one database.)
```

```
[1] modules/aggregate_dictionary_distributed_keys.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14
[2] modules/aggregate_dictionary_scalars.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14
[3] modules/call_history.txt on CallHistory.storeddata: SQL Query 9,10,11,12,13,14
[4] modules/datausage_zliveusage.txt on DataUsage-watch.sqlite: SQL Query 8,9,10,11,12,13,14
```



Other Outputs:
CSV & SQLite
('|' delimited data output)

Extract the data!

```
oompa@qwertys-MBP APOLLO_v1_4 % python3 apollo.py extract -o sql_json -v 14 -k modules tmp_apollo_ios14
```

```
APOLLO Modules Version: 11182020
Action: extract
Platform: apple
Version: 14
Output: sql_json
Data Directory: tmp_apollo_ios14
Modules Directory: modules
KMZ: TRUE
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```

```
...Parsing Modules in...modules
```

```
==> Parsing 233 modules (Note: Some modules may be run on more than one database.)
```

- [1] modules/aggregate_dictionary_distributed_keys.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14
- [2] modules/aggregate_dictionary_scalars.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14
- [3] modules/call_history.txt on CallHistory.storeddata: SQL Query 9,10,11,12,13,14
- [4] modules/datausage_zliveusage.txt on DataUsage-watch.sqlite: SQL Query 8,9,10,11,12,13,14



- macOS11 = 10.16
- “yolo” option

Extract the data!

```
oompa@qwertys-MBP APOLLO_v1_4 % python3 apollo.py extract -o sql_json -v 14 -k modules tmp_apollo_ios14
```



```
APOLLO Modules Version: 11182020
Action: extract
Platform: apple
Version: 14
Output: sql_json
Data Directory: tmp_apollo_ios14
Modules Directory: modules
KMZ: TRUE
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```

```
...Parsing Modules in...modules
```

```
==> Parsing 233 modules (Note: Some modules may be run on more than one database.)
```

```
[1] modules/aggregate_dictionary_distributed_keys.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14
[2] modules/aggregate_dictionary_scalars.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14
[3] modules/call_history.txt on CallHistory.storeddata: SQL Query 9,10,11,12,13,14
[4] modules/datausage_zliveusage.txt on DataUsage-watch.sqlite: SQL Query 8,9,10,11,12,13,14
```

Extract the data!

```
oompa@qwertys-MBP APOLLO_v1_4 % python3 apollo.py extract -o sql_json -v 14 -k modules tmp_apollo_ios14
```



```
APOLLO Modules Version: 11182020
Action: extract
Platform: apple
Version: 14
Output: sql_json
Data Directory: tmp_apollo_ios14
Modules Directory: modules
KMZ: TRUE
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4
```

```
...Parsing Modules in...modules
```

```
==> Parsing 233 modules (Note: Some modules may be run on more than one database.)
```

```
[1] modules/aggregate_dictionary_distributed_keys.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14
[2] modules/aggregate_dictionary_scalars.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14
[3] modules/call_history.txt on CallHistory.storeddata: SQL Query 9,10,11,12,13,14
[4] modules/datausage_zliveusage.txt on DataUsage-watch.sqlite: SQL Query 8,9,10,11,12,13,14
```

Extract the data!

```
oompa@qwertys-MBP APOLLO_v1_4 % python3 apollo.py extract -o sql_json -v 14 -k modules tmp_apollo_ios14
```



```
-----  
APOLLO Modules Version: 11182020  
Action: extract  
Platform: apple  
Version: 14  
Output: sql_json  
Data Directory: tmp_apollo_ios14  
Modules Directory: modules  
KMZ: TRUE  
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4  
-----
```

...Parsing Modules in...modules

==> Parsing 233 modules (Note: Some modules may be run on more than one database.)

```
[1] modules/aggregate_dictionary_distributed_keys.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14  
[2] modules/aggregate_dictionary_scalars.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14  
[3] modules/call_history.txt on CallHistory.storeddata: SQL Query 9,10,11,12,13,14  
[4] modules/datausage_zliveusage.txt on DataUsage-watch.sqlite: SQL Query 8,9,10,11,12,13,14
```

Extract the data!

```
oompa@qwertys-MBP APOLLO_v1_4 % python3 apollo.py extract -o sql_json -v 14 -k modules tmp_apollo_ios14
```

```
-----  
APOLLO Modules Version: 11182020  
Action: extract  
Platform: apple  
Version: 14  
Output: sql_json  
Data Directory: tmp_apollo_ios14  
Modules Directory: modules  
KMZ: TRUE  
Current Working Directory: /Users/oompa/Downloads/APOLLO_v1_4  
-----
```

```
...Parsing Modules in...modules
```

```
==> Parsing 233 modules (Note: Some modules may be run on more than one database.) ←  
[1] modules/aggregate_dictionary_distributed_keys.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14  
[2] modules/aggregate_dictionary_scalars.txt on ADDataStore.sqlitedb: SQL Query 8,9,10,11,12,13,14  
[3] modules/call_history.txt on CallHistory.storeddata: SQL Query 9,10,11,12,13,14  
[4] modules/datausage_zliveusage.txt on DataUsage-watch.sqlite: SQL Query 8,9,10,11,12,13,14
```

Extract the data!

```
modules/knowledge_event_tombstone.txt on knowledgeC.db for [SQL Query 12,13,10.14,10.15,10.16,14]: 2 databases.  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/Assistant/knowledgeC.db  
Number of Records: 0  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db  
Number of Records: 10000  
  
modules/knowledge_audio_input_route.txt on knowledgeC.db for [SQL Query 11,12,13,14]: 2 databases.  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/Assistant/knowledgeC.db  
Number of Records: 0  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db  
Number of Records: 27  
  
==> Total Number of Records: 2750612  
==> Total Number of Location Records: 24476  
==> Lazily outputted to SQLite file: apollo.db
```

```
oompa@qwertys-MBP APOLLO_v1_4 % ls *.kmz  
knowledge_app_location_activity.kmz  
locationd_cacheencryptedAB_ltecelllocation.kmz  
locationd_cacheencryptedAB_ltecelllocationlocal.kmz  
locationd_cacheencryptedAB_wifilocation.kmz  
routined_cache_zrtcllocationmo.kmz  
routined_cache_zrthintmo.kmz  
routined_cache_zrvvisitmo.kmz  
routined_local_learned_location_of_interest_entry.kmz  
routined_local_learned_location_of_interest_exit.kmz  
routined_local_learned_location_of_interest_transition_start.kmz  
routined_local_learned_location_of_interest_transition_stop.kmz  
routined_local_vehicle_parked.kmz  
routined_local_vehicle_parked_history.kmz
```

Extract the data!

```
modules/knowledge_event_tombstone.txt on knowledgeC.db for [SQL Query 12,13,10.14,10.15,10.16,14]: 2 databases.  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/Assistant/knowledgeC.db  
Number of Records: 0  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db  
Number of Records: 10000  
  
modules/knowledge_audio_input_route.txt on knowledgeC.db for [SQL Query 11,12,13,14]: 2 databases.  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/Assistant/knowledgeC.db  
Number of Records: 0  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db  
Number of Records: 27  
  
==> Total Number of Records: 2750612  
==> Total Number of Location Records: 24476  
==> Lazily outputted to SQLite file: apollo.db
```



```
oompa@qwertys-MBP APOLLO_v1_4 % ls *.kmz  
knowledge_app_location_activity.kmz  
locationd_cacheencryptedAB_ltecelllocation.kmz  
locationd_cacheencryptedAB_ltecelllocationlocal.kmz  
locationd_cacheencryptedAB_wifilocation.kmz  
routined_cache_zrtcllocationmo.kmz  
routined_cache_zrthintmo.kmz  
routined_cache_zrvvisitmo.kmz  
routined_local_learned_location_of_interest_entry.kmz  
routined_local_learned_location_of_interest_exit.kmz  
routined_local_learned_location_of_interest_transition_start.kmz  
routined_local_learned_location_of_interest_transition_stop.kmz  
routined_local_vehicle_parked.kmz  
routined_local_vehicle_parked_history.kmz
```

Extract the data!

```
modules/knowledge_event_tombstone.txt on knowledgeC.db for [SQL Query 12,13,10.14,10.15,10.16,14]: 2 databases.  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/Assistant/knowledgeC.db  
Number of Records: 0  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db  
Number of Records: 10000  
  
modules/knowledge_audio_input_route.txt on knowledgeC.db for [SQL Query 11,12,13,14]: 2 databases.  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/Assistant/knowledgeC.db  
Number of Records: 0  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db  
Number of Records: 27  
  
==> Total Number of Records: 2750612  
==> Total Number of Location Records: 24476  
==> Lazily outputted to SQLite file: apollo.db
```

```
oompa@qwertys-MBP APOLLO_v1_4 % ls *.kmz  
knowledge_app_location_activity.kmz  
locationd_cacheencryptedAB_ltecelllocation.kmz  
locationd_cacheencryptedAB_ltecelllocationlocal.kmz  
locationd_cacheencryptedAB_wifilocation.kmz  
routined_cache_zrtcllocationmo.kmz  
routined_cache_zrthintmo.kmz  
routined_cache_zrvvisitmo.kmz  
routined_local_learned_location_of_interest_entry.kmz  
routined_local_learned_location_of_interest_exit.kmz  
routined_local_learned_location_of_interest_transition_start.kmz  
routined_local_learned_location_of_interest_transition_stop.kmz  
routined_local_vehicle_parked.kmz  
routined_local_vehicle_parked_history.kmz
```

Extract the data!

```
modules/knowledge_event_tombstone.txt on knowledgeC.db for [SQL Query 12,13,10.14,10.15,10.16,14]: 2 databases.  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/Assistant/knowledgeC.db  
Number of Records: 0  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db  
Number of Records: 10000  
  
modules/knowledge_audio_input_route.txt on knowledgeC.db for [SQL Query 11,12,13,14]: 2 databases.  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/Assistant/knowledgeC.db  
Number of Records: 0  
Executing module on: tmp_apollo_ios14/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db  
Number of Records: 27  
  
==> Total Number of Records: 2750612  
==> Total Number of Location Records: 24476  
==> Lazily outputted to SQLite file: apollo.db
```



```
oompa@qwertys-MBP APOLLO_v1_4 % ls *.kmz  
knowledge_app_location_activity.kmz  
locationd_cacheencryptedAB_ltecelllocation.kmz  
locationd_cacheencryptedAB_ltecelllocationlocal.kmz  
locationd_cacheencryptedAB_wifilocation.kmz  
routined_cache_zrtcllocationmo.kmz  
routined_cache_zrthintmo.kmz  
routined_cache_zrvvisitmo.kmz  
routined_local_learned_location_of_interest_entry.kmz  
routined_local_learned_location_of_interest_exit.kmz  
routined_local_learned_location_of_interest_transition_start.kmz  
routined_local_learned_location_of_interest_transition_stop.kmz  
routined_local_vehicle_parked.kmz  
routined_local_vehicle_parked_history.kmz
```

Where to start?

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: APOLLO

Refresh Clear Filters Clear Sorting Save Table As Print New Record Delete Record Toggle Format Toolbar Find in cells Replace Filter in any column

	Key	Activity	Output	Database	Module
1	2021-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
2	2021-10-20 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
3	2020-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
4	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
5	2020-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
6	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
7	2020-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
8	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
9	2020-10-21 06:46:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
10	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14

Mode: JSON

Word Wrap Autoformat

```
1 {  
2   "APP CATEGORY": null,  
3   "APP NAME": null,  
4   "APP SUBCATEGORY": null,  
5   "BUNDLE ID": "com.apple.MobileStore",  
6   "DAY OF WEEK": "Wednesday",  
7   "END": "2020-10-21 06:45:00",  
8   "ENTRY CREATION": "2020-10-21 06:45:46",  
9   "GMT OFFSET": -4,  
10  "IS INSTALL": 1,  
11  "START": "2020-10-21 06:45:00",  
12  "UUID": "6412214C-956F-492E-AFC7-FF5A07354703",  
13  "ZMETADATAHASH":  
14  "11a36377e14012e46d38c87e315c8c78",  
15  "ZOBJECT TABLE ID": 99854  
}
```

Where to start?

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: APOLLO Refresh Clear Filters Clear Sorting Save Table As Print New Record Delete Record Toggle Format Toolbar Find in cells Replace Filter in any column

	Key	Activity	Output	Database	Module
1	2020-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
2	2020-10-21 13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
3	2020-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
4	2020-10-21 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
5	2020-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
6	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
7	2020-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
8	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
9	2020-10-21 06:46:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
10	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14

Edit Database Cell

Mode: JSON Word Wrap Autoformat

```
1 {
2   "APP CATEGORY": null,
3   "APP NAME": null,
4   "APP SUBCATEGORY": null,
5   "BUNDLE ID": "com.apple.MobileStore",
6   "DAY OF WEEK": "Wednesday",
7   "END": "2020-10-21 06:45:00",
8   "ENTRY CREATION": "2020-10-21 06:45:46",
9   "GMT OFFSET": -4,
10  "IS INSTALL": 1,
11  "START": "2020-10-21 06:45:00",
12  "UUID": "6412214C-956F-492E-AFC7-FF5A07354703",
13  "ZMETADATAHASH": "11a36377e14012e46d38c87e315c8c78",
14  "ZOBJECT TABLE ID": 99854
15 }
```

Where to start?

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: APOLLO

Refresh Clear Filters Clear Sorting Save Table As Print New Record Delete Record Toggle Format Toolbar Find in cells Replace Filter in any column

	Key	Activity	Output	Database	Module
1	2020-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
2	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
3	2020-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
4	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
5	2020-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
6	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
7	2020-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
8	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
9	2020-10-21 06:46:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
10	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14

Mode: JSON Word Wrap Autoformat

```
1 {  
2   "APP CATEGORY": null,  
3   "APP NAME": null,  
4   "APP SUBCATEGORY": null,  
5   "BUNDLE ID": "com.apple.MobileStore",  
6   "DAY OF WEEK": "Wednesday",  
7   "END": "2020-10-21 06:45:00",  
8   "ENTRY CREATION": "2020-10-21 06:45:46",  
9   "GMT OFFSET": -4,  
10  "IS INSTALL": 1,  
11  "START": "2020-10-21 06:45:00",  
12  "UUID": "6412214C-956F-492E-AFC7-FF5A07354703",  
13  "ZMETADATAHASH":  
14  "11a36377e14012e46d38c87e315c8c78",  
15  "ZOBJECT TABLE ID": 99854  
}
```

Where to start?

Screenshot of a database interface showing a table and a JSON editor.

The table has columns: Key, Activity, Output, Database, and Module. An orange arrow points to the "Output" column header. The JSON editor on the right shows a single row's data in JSON format, with another orange arrow pointing to it.

Table Headers: Database Structure, Browse Data, Edit Pragmas, Execute SQL

Table Columns: Key, Activity, Output, Database, Module

JSON Editor Data (Row 1):

```
1 {  
2   "APP CATEGORY": null,  
3   "APP NAME": null,  
4   "APP SUBCATEGORY": null,  
5   "BUNDLE ID": "com.apple.MobileStore",  
6   "DAY OF WEEK": "Wednesday",  
7   "END": "2020-10-21 06:45:00",  
8   "ENTRY CREATION": "2020-10-21 06:45:46",  
9   "GMT OFFSET": -4,  
10  "IS INSTALL": 1,  
11  "START": "2020-10-21 06:45:00",  
12  "UUID": "6412214C-956F-492E-AFC7-FF5A07354703",  
13  "ZMETADATAHASH":  
14  "11a36377e14012e46d38c87e315c8c78",  
15  "ZOBJECT TABLE ID": 99854  
}
```

Where to start?

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: APOLLO

Refresh Clear Filters Clear Sorting Save Table As Print New Record Delete Record Toggle Format Toolbar Find in cells Replace Filter in any column

	Key	Activity	Output	Database	Module
1	2020-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
2	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
3	2020-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
4	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
5	2020-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
6	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
7	2020-10-21 06:45:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
8	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
9	2020-10-21 06:46:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
10	2020-11-10 17:13:00	Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14

Mode: JSON

Word Wrap Autoformat

```
1 {  
2   "APP CATEGORY": null,  
3   "APP NAME": null,  
4   "APP SUBCATEGORY": null,  
5   "BUNDLE ID": "com.apple.MobileStore",  
6   "DAY OF WEEK": "Wednesday",  
7   "END": "2020-10-21 06:45:00",  
8   "ENTRY CREATION": "2020-10-21 06:45:46",  
9   "GMT OFFSET": -4,  
10  "IS INSTALL": 1,  
11  "START": "2020-10-21 06:45:00",  
12  "UUID": "6412214C-956F-492E-AFC7-FF5A07354703",  
13  "ZMETADATAHASH":  
14  "11a36377e14012e46d38c87e315c8c78",  
15  "ZOBJECT TABLE ID": 99854  
}
```

Where to start?

The screenshot shows a database interface with a table of logs and a JSON editor.

Table View:

Key	Activity	Output	Database	Module
1	2020-10-21 06:45:00 Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
2	2020-11-10 17:13:00 Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
3	2020-10-21 06:45:00 Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
4	2020-11-10 17:13:00 Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
5	2020-10-21 06:45:00 Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
6	2020-11-10 17:13:00 Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
7	2020-10-21 06:45:00 Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
8	2020-11-10 17:13:00 Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
9	2020-10-21 06:46:00 Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14
10	2020-11-10 17:13:00 Application Install	{...}	tmp_apollo_ios14/private/var/mobile/Library/CoreDue...	modules/knowledge_app_install.txt#knowledgeC.db#SQL Query 11,12,13,14

JSON Editor:

```
1 {  
2   "APP CATEGORY": null,  
3   "APP NAME": null,  
4   "APP SUBCATEGORY": null,  
5   "BUNDLE ID": "com.apple.MobileStore",  
6   "DAY OF WEEK": "Wednesday",  
7   "END": "2020-10-21 06:45:00",  
8   "ENTRY CREATION": "2020-10-21 06:45:46",  
9   "GMT OFFSET": -4,  
10  "IS INSTALL": 1,  
11  "START": "2020-10-21 06:45:00",  
12  "UUID": "6412214C-956F-492E-AFC7-FF5A07354703",  
13  "ZMETADATAHASH":  
14  "11a36377e14012e46d38c87e315c8c78",  
15  "ZOBJECT TABLE ID": 99854  
}
```

An orange arrow points from the table towards the JSON editor, indicating a connection or relationship between the two.

Where to start? November 16, 2020

Filter or Query? Choose Your own Adventure!

Table: APOLLO

Refresh Clear Filters Clear Sorting

	Key	Activity	Output
	2020-11-16	Filter	Filter
1	2020-11-16	Aggregate ...	{...}
2	2020-11-16	Aggregate ...	{...}
3	2020-11-16	Aggregate ...	{...}
4	2020-11-16	Aggregate ...	{...}
5	2020-11-16	Aggregate ...	{...}
6	2020-11-16	Aggregate ...	{...}
7	2020-11-16	Aggregate ...	{...}
8	2020-11-16	Aggregate ...	{...}
9	2020-11-16	Aggregate ...	{...}
10	2020-11-16	Aggregate ...	{...}
11	2020-11-16	Aggregate ...	{...}
12	2020-11-16	Aggregate ...	{...}
13	2020-11-16	Aggregate ...	{...}
14	2020-11-16	Aggregate ...	{...}
15	2020-11-16	Aggregate ...	{...}
16	2020-11-16	Aggregate ...	{...}
17	2020-11-16	Aggregate ...	{...}
18	2020-11-16	Aggregate ...	{...}
19	2020-11-16	Aggregate ...	{...}
20	2020-11-16	Aggregate ...	{...}
21	2020-11-16	Aggregate ...	{...}
22	2020-11-16	Aggregate ...	{...}
23	2020-11-16	Aggregate ...	{...}
24	2020-11-16	Aggregate ...	{...}
25	2020-11-16	Aggregate ...	{...}
26	2020-11-16	Aggregate ...	{...}
27	2020-11-16	Aggregate ...	{...}
28	2020-11-16	Aggregate ...	{...}
29	2020-11-16	Aggregate ...	{...}
30	2020-11-16	Aggregate ...	{...}
31	2020-11-16	Aggregate ...	{...}
32	2020-11-16	Aggregate ...	{...}
33	2020-11-16	Aggregate ...	{...}
34	2020-11-16	Aggregate ...	{...}
35	2020-11-16	Aggregate ...	{...}
36	2020-11-16	Aggregate ...	{...}
37	2020-11-16	Aggregate ...	{...}
38	2020-11-16	Aggregate ...	{...}
39	2020-11-16	Aggregate ...	{...}
40	2020-11-16	Aggregate ...	{...}
41	2020-11-16	Aggregate ...	{...}
42	2020-11-16	Aggregate ...	{...}
43	2020-11-16	Aggregate ...	{...}
44	2020-11-16	Aggregate ...	{...}
45	2020-11-16	Aggregate ...	{...}
46	2020-11-16	Aggregate ...	{...}
47	2020-11-16	Aggregate ...	{...}
48	2020-11-16	Aggregate ...	{...}
49	2020-11-16	Aggregate ...	{...}
50	2020-11-16	Aggregate ...	{...}
51	2020-11-16	Aggregate ...	{...}
52	2020-11-16	Aggregate ...	{...}
53	2020-11-16	Aggregate ...	{...}
54	2020-11-16	Aggregate ...	{...}
55	2020-11-16	Aggregate ...	{...}
56	2020-11-16	Aggregate ...	{...}
57	2020-11-16	Aggregate ...	{...}
58	2020-11-16	Aggregate ...	{...}
59	2020-11-16	Aggregate ...	{...}
60	2020-11-16	Aggregate ...	{...}
61	2020-11-16	Aggregate ...	{...}
62	2020-11-16	Aggregate ...	{...}
63	2020-11-16	Aggregate ...	{...}
64	2020-11-16	Aggregate ...	{...}
65	2020-11-16	Aggregate ...	{...}
66	2020-11-16	Aggregate ...	{...}
67	2020-11-16	Aggregate ...	{...}
68	2020-11-16	Aggregate ...	{...}
69	2020-11-16	Aggregate ...	{...}
70	2020-11-16	Aggregate ...	{...}
71	2020-11-16	Aggregate ...	{...}
72	2020-11-16	Aggregate ...	{...}
73	2020-11-16	Aggregate ...	{...}
74	2020-11-16	Aggregate ...	{...}
75	2020-11-16	Aggregate ...	{...}
76	2020-11-16	Aggregate ...	{...}
77	2020-11-16	Aggregate ...	{...}
78	2020-11-16	Aggregate ...	{...}
79	2020-11-16	Aggregate ...	{...}
80	2020-11-16	Aggregate ...	{...}
81	2020-11-16	Aggregate ...	{...}
82	2020-11-16	Aggregate ...	{...}
83	2020-11-16	Aggregate ...	{...}
84	2020-11-16	Aggregate ...	{...}
85	2020-11-16	Aggregate ...	{...}
86	2020-11-16	Aggregate ...	{...}
87	2020-11-16	Aggregate ...	{...}
88	2020-11-16	Aggregate ...	{...}
89	2020-11-16	Aggregate ...	{...}
90	2020-11-16	Aggregate ...	{...}
91	2020-11-16	Aggregate ...	{...}
92	2020-11-16	Aggregate ...	{...}
93	2020-11-16	Aggregate ...	{...}
94	2020-11-16	Aggregate ...	{...}
95	2020-11-16	Aggregate ...	{...}
96	2020-11-16	Aggregate ...	{...}
97	2020-11-16	Aggregate ...	{...}
98	2020-11-16	Aggregate ...	{...}
99	2020-11-16	Aggregate ...	{...}
100	2020-11-16	Aggregate ...	{...}



```
1 SELECT
2 Key,Activity,Output,Database,Module
3 FROM APOLLO
4 where key like '2020-11-16%'
```

	Key	
1	2020-11-16 19:15:03	Routined
2	2020-11-16 19:15:03	Routined
3	2020-11-16 19:15:34	Routined
4	2020-11-16 19:15:34	Routined
5	2020-11-16 19:16:51	Routined

Execution finished without errors.
Result: 145706 rows returned in 1000ms
At line 1:
SELECT
Key,Activity,Output,Database,Module
FROM APOLLO
where key like '2020-11-16%'

Where to start? November 16, 2020

Can I change from UTC to localtime? Yes!

Table: APOLLO

	Key ^{v1}	Activity	Output
	2020-11-16		
1	2020-11-16		
2	2020-11-16		
3	2020-11-16		
4	2020-11-16		
5	2020-11-16		
6	2020-11-16		

- Show rowid column
- Hide column(s)
- Show all columns
- Select column
- Edit display format**
- Set encoding
- Set encoding for all tables
- Aggregate



```
1 SELECT
2   datetime(Key,'localtime') as Key,
3   Activity, Output, Database, Module
4   FROM APOLLO
5   where key like '2020-11-16%'
```

Choose display format

Display format

Choose a display format for the column 'Key' which is applied to each value prior to showing it.

Custom

```
1 datetime("Key", "localtime")
```

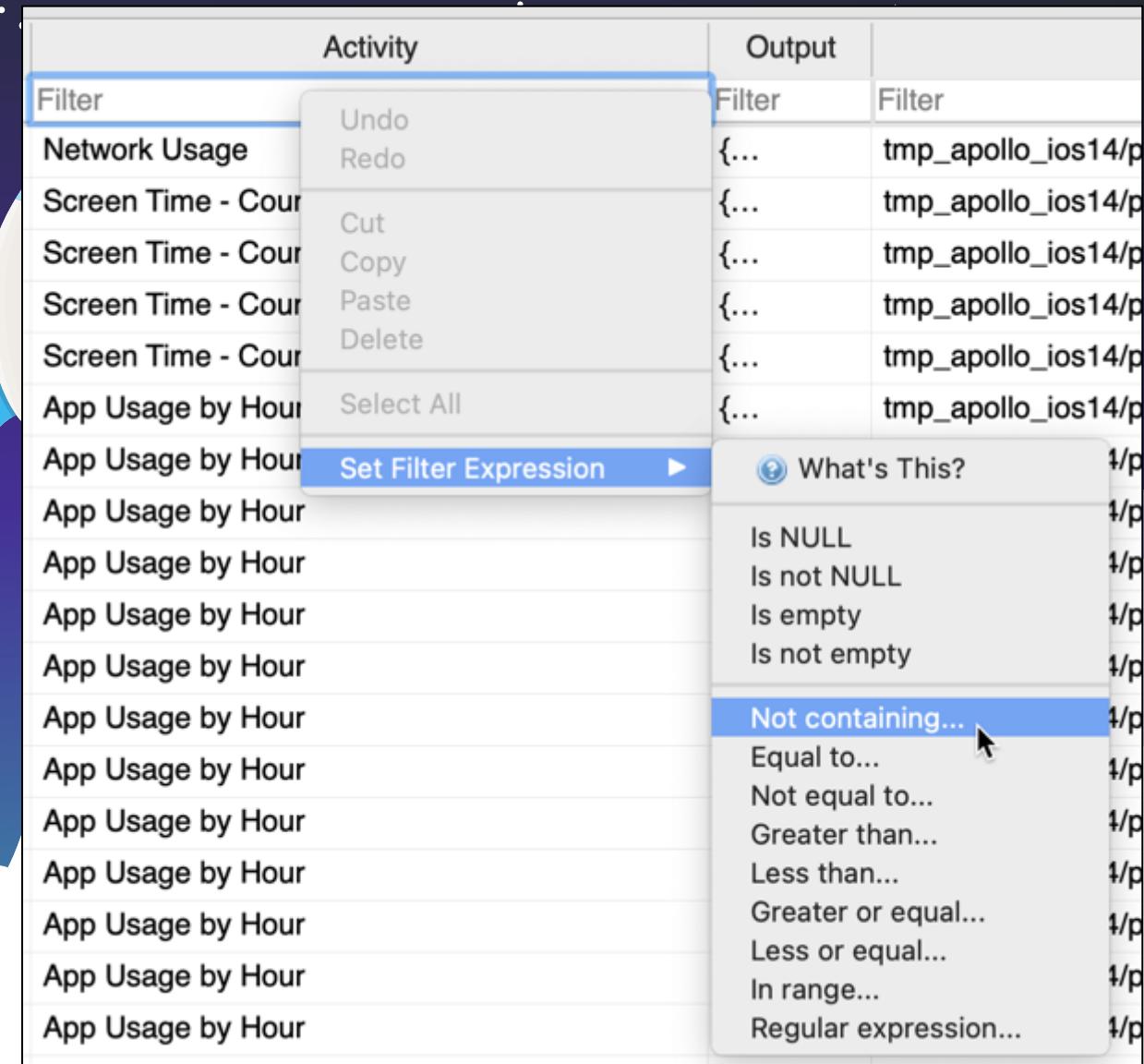
Cancel OK

	Key	Activity
1	2020-11-16 14:15:03	Routined Location - Entry
2	2020-11-16 14:15:03	Routined Location - Entry

Where to start? November 16, 2020

• Remove the Noise

- DB Browser for SQLite
 - Powerful filtering w/o need for SQL Query creation.
- Could also not process modules.
 - Remove them the /modules directory
- Add custom SQL Queries as modules.
 - (Hey, why not add that into the APOLLO project too? Help a fellow investigator!)



Where to start? November 16, 2020

Remove the Noise

- Original Events: 2,750,612
- Filter by Day -> 145,706
- Filter out Noise -> 36,076



Table: APOLLO

Refresh Clear Filters Clear Sorting Save Table As Print New Record Delete Record Toggle Format Toolbar

	Key	Activity
	2020-11-16	/^((?!Aggregate Screen Time Kernel Assertion Coalition App Usage by Hour Process Data Usage).)*\$/
793	2020-11-16 01:31:18	WiFi Connection
794	2020-11-16 01:31:18	WiFi Connection
795	2020-11-16 01:31:18	Battery Level UI
796	2020-11-16 01:31:20	Routined Location

793 - 795 of 36076 Go to: 1

Where to start? November 16, 2020

- Key-in on a specific event...

- “Sarah was observed getting into her vehicle.”



Table:	APOLLO	Refresh	Clear Filters	Clear Sorting	Save Table As	Print	New Record	Delete Record	Toggle Format Toolbar	>> Filt...
Key	Activity	Output	Database	Module						
2020-11-16	Process Data Usage.)*\$/	Filter	Filter	carplay						
1	2020-11-16 14:10:52	CarPlay Connection Status	{...}	tmp_apollo_ios14/...	modules/knowledge_device_carplay_connected.txt#k					
2	2020-11-16 14:22:24	CarPlay Connection Status	{...}	tmp_apollo_ios14/...	modules/knowledge_device_carplay_connected.txt#k					
3	2020-11-16 15:24:00	CarPlay Connection Status	{...}	tmp_apollo_ios14/...	modules/knowledge_device_carplay_connected.txt#k					

Mode: JSON Word Wrap Autoformat Import

```
1  {
2    "CARPLAY CONNECTED": "CONNECTED",
3    "DAY OF WEEK": "Monday",
4    "END": "2020-11-16 19:22:24",
5    "ENTRY CREATION": "2020-11-16 19:22:27",
6    "GMT OFFSET": -5,
7    "START": "2020-11-16 19:10:52",
8    "USAGE IN MINUTES": 11.533333333333333,
9    "USAGE IN SECONDS": 692,
10   "UUID": "78D5A0BB-0567-4E97-BD05-DECAA742EF8E",
11   "ZOBJECT TABLE ID": 188834
12 }
```

Where to start? November 16, 2020

- Key-in on a specific event...

- “Sarah was observed getting into her vehicle.”

Table: APOLLO

Refresh Clear Filters Clear Sorting Save Table As Print New Record Delete Record Toggle Format Toolbar Filter Mode: JSON Word Wrap Autoformat Import

	Key	Activity	Output	Database	Module
1	2020-11-16	Process Data Usage.)*\$/	Filter	Filter	carplay
2	2020-11-16 14:10:52	CarPlay Connection Status	{...}	tmp_apollo_ios14/...	modules/knowledge_device_carplay_connected.txt#k
3	2020-11-16 14:22:24	CarPlay Connection Status	{...}	tmp_apollo_ios14/...	modules/knowledge_device_carplay_connected.txt#k
	2020-11-16 15:24:00	CarPlay Connection Status	{...}	tmp_apollo_ios14/...	modules/knowledge_device_carplay_connected.txt#k

```
1 {  
2   "CARPLAY CONNECTED": "DISCONNECTED",  
3   "DAY OF WEEK": "Monday",  
4   "END": "2020-11-16 20:24:00",  
5   "ENTRY CREATION": "2020-11-16 20:24:01",  
6   "GMT OFFSET": -5,  
7   "START": "2020-11-16 19:22:24",  
8   "USAGE IN MINUTES": 61.6, ←  
9   "USAGE IN SECONDS": 3696,  
10  "UUID": "AFA92E89-A8CB-480F-A433-B27873C46415",  
11  "ZOBJECT TABLE ID": 189488  
12 }
```

```
1 {  
2   "CARPLAY CONNECTED": "CONNECTED",  
3   "DAY OF WEEK": "Monday",  
4   "END": "2020-11-16 19:22:24",  
5   "ENTRY CREATION": "2020-11-16 19:22:27",  
6   "GMT OFFSET": -5,  
7   "START": "2020-11-16 19:10:52",  
8   "USAGE IN MINUTES": 11.533333333333333,  
9   "USAGE IN SECONDS": 692,  
10  "UUID": "78D5A0BB-0567-4E97-BD05-DECAA742EF8E",  
11  "ZOBJECT TABLE ID": 188834  
12 }
```

No CarPlay Disconnect on second connection. 

Where to start? November 16, 2020

- Key-in on a specific event...

- “Sarah was observed getting into her vehicle.”
 - What if it didn’t have CarPlay?



Table: APOLLO Refresh Clear Filters Clear Sorting Save Table As Print New Record Mode: JSON Word Wrap

	Key ▾ ¹	Activity	Output	Database	
93	2020-11-16	Process Data Usage.)*\$/	Filter	Filter	motionstatehistory
94	2020-11-16 14:10:53	Motion State History	{...}	tmp_apollo_ios14/...	modules/...
95	2020-11-16 14:10:54	Motion State History	{...}	tmp_apollo_ios14/...	modules/...
96	2020-11-16 14:11:51	Motion State History	{...}	tmp_apollo_ios14/...	modules/...
97	2020-11-16 14:11:52	Motion State History	{...}	tmp_apollo_ios14/...	modules/...
98	2020-11-16 14:13:33	Motion State History	{...}	tmp_apollo_ios14/...	modules/...
99	2020-11-16 14:14:11	Motion State History	{...}	tmp_apollo_ios14/...	modules/...
100	2020-11-16 14:14:21	Motion State History	{...}	tmp_apollo_ios14/...	modules/...
	2020-11-16 14:14:41	Motion State History	{...}	tmp_apollo_ios14/...	modules/...

```
1  {
2    "CONFIDENCE": 3,
3    "IS MOVING": 1,
4    "IS VEHICULAR": 1,
5    "MOTIONSTATEHISTORY TABLE ID": 744,
6    "MOUNTED": 0,
7    "MOUNTED CONFIDENCE": 0,
8    "START TIME": "2020-11-16 19:10:54",
9    "TIMESTAMP": 119332.38947675,
10   "TURN": 0,
11   "TYPE": 4096,
12   "VEHICLE EXIT STATE": 0,
13   "VEHICULAR FLAGS DATA": 16
14 }
```

Where did I go? Check for Routined Locations

	Key 	Activity	Output	Database	Module
	2020-11-16 14:10 ⓘ Process Data Usage.)*\$/ 		Filter	Filter	Filter
36	2020-11-16 14:10:51 Device Plugin Status	{...}	tmp_apollo_ios14/...	modules/knowledge_device_pluggedin.txt#knowledgeC.db#SQL Query ...	
37	2020-11-16 14:10:51 Device Plugin Status	{...}	tmp_apollo_ios14/...	modules/knowledge_device_pluggedin.txt#knowledgeC.db#SQL Query ...	
38	2020-11-16 14:10:51 Routined Location	{...}	tmp_apollo_ios14/...	modules/routined_cache_zrthintmo.txt#Cache.sqlite#SQL Query ...	
39	2020-11-16 14:10:51 App Audio Routing	{...}	tmp_apollo_ios14/...	modules/powerlog_app_audio.txt#CurrentPowerlog.PLSQL#SQL Query ...	
40	2020-11-16 14:10:52 CarPlay Connection Status	{...}	tmp_apollo_ios14/...	modules/knowledge_device_carplay_connected.txt#knowledgeC.db#SQL ...	
41	2020-11-16 14:10:52 App Audio Routing	{...}	tmp_apollo_ios14/...	modules/powerlog_app_audio.txt#CurrentPowerlog.PLSQL#SQL Query ...	
42	2020-11-16 14:10:52 App Audio Routing	{...}	tmp_apollo_ios14/...	modules/powerlog_app_audio.txt#CurrentPowerlog.PLSQL#SQL Query ...	
43	2020-11-16 14:10:53 Motion State History	{...}	tmp_apollo_ios14/...	modules/...	
44	2020-11-16 14:10:53 Battery Level	{...}	tmp_apollo_ios14/...	modules/powerlog_battery_level.txt#CurrentPowerlog.PLSQL#SQL Query ...	
45	2020-11-16 14:10:53 Screen Brightness	{...}	tmp_apollo_ios14/...	modules/powerlog_display_brightness.txt#CurrentPowerlog.PLSQL#SQL ...	
46	2020-11-16 14:10:53 IDS Messages	{...}	tmp_apollo_ios14/...	modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query...	
47	2020-11-16 14:10:53 IDS Messages	{...}	tmp_apollo_ios14/...	modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query...	
48	2020-11-16 14:10:53 IDS Messages	{...}	tmp_apollo_ios14/...	modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query...	
49	2020-11-16 14:10:53 IDS Messages	{...}	tmp_apollo_ios14/...	modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query...	
50	2020-11-16 14:10:53 IDS Messages	{...}	tmp_apollo_ios14/...	modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query...	
51	2020-11-16 14:10:53 IDS Messages	{...}	tmp_apollo_ios14/...	modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query...	
52	2020-11-16 14:10:53 IDS Messages	{...}	tmp_apollo_ios14/...	modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query...	
53	2020-11-16 14:10:53 IDS Messages	{...}	tmp_apollo_ios14/...	modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query...	
54	2020-11-16 14:10:53 Battery Level UI	{...}	tmp_apollo_ios14/...	modules/powerlog_battery_level_ui.txt#CurrentPowerlog.PLSQL#SQL Quer...	
55	2020-11-16 14:10:54 Motion State History	{...}	tmp_apollo_ios14/...	modules/...	
56	2020-11-16 14:10:54 Now Playing	{...}	tmp_apollo_ios14/...	modules/knowledge_audio_media_nowplaying.txt#knowledgeC.db#SQL ...	
57	2020-11-16 14:10:54 Now Playing	{...}	tmp_apollo_ios14/...	modules/knowledge_audio_media_nowplaying.txt#knowledgeC.db#SQL ...	
58	2020-11-16 14:10:54 Device Volume	{...}	tmp_apollo_ios14/...	modules/powerlog_device_volume.txt#CurrentPowerlog.PLSQL#SQL Quer...	
59	2020-11-16 14:10:54 Airdrop Connection	{...}	tmp_apollo_ios14/...	modules/powerlog_airdrop.txt#CurrentPowerlog.PLSQL#SQL Query ...	
60	2020-11-16 14:10:54 Location Technology	{...}	tmp_apollo_ios14/...	modules/powerlog_location_tech_status.txt#CurrentPowerlog.PLSQL#SQL ...	
61	2020-11-16 14:10:54 Audio Input	{...}	tmp_apollo_ios14/...	modules/knowledge_audio_input_route.txt#knowledgeC.db#SQL Query ...	
62	2020-11-16 14:10:55 Routined Location	{...}	tmp_apollo_ios14/...	modules/routined_cache_zrtcllocationmo.txt#Cache.sqlite#SQL Query ...	
63	2020-11-16 14:10:55 App Location Usage	{...}	tmp_apollo_ios14/...	modules/powerlog_location_client_status.txt#CurrentPowerlog.PLSQL#SQ...	
64	2020-11-16 14:10:55 App Location Usage	{...}	tmp_apollo_ios14/...	modules/powerlog_location_client_status.txt#CurrentPowerlog.PLSQL#SQ...	

Where did I go? Check for Routined Locations

- Correlate timestamp with CarPlay Disconnect event or Motion State History

Table: APOLLO

Key ▾¹ Activity Output Database Module

2020-11-16 14:22 Process Data Usage.)*\$/ Filter Filter zrtcllocation

	Key ▾ ¹	Activity	Output	Database	Module
18	2020-11-16 14:22:17	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#
19	2020-11-16 14:22:18	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#
20	2020-11-16 14:22:19	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#
21	2020-11-16 14:22:20	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#
22	2020-11-16 14:22:21	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#
23	2020-11-16 14:22:22	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#
24	2020-11-16 14:22:23	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#
25	2020-11-16 14:22:24	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#
26	2020-11-16 14:22:25	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#
27	2020-11-16 14:22:26	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#
28	2020-11-16 14:22:27	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#
29	2020-11-16 14:22:28	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#
30	2020-11-16 14:22:29	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#

Mode: JSON

```
1 {  
2   "ALTITUDE": 67.41794834612082,  
3   "COORDINATES": "38.8742205507249, -77.1337143400014",  
4   "COURSE": 30.439660111699805,  
5   "HORIZONTAL ACCURACY": 8.001208273680877,  
6   "LATITUDE": 38.87422055072489,  
7   "LONGITUDE": -77.13371434000143,  
8   "SPEED (KMPH)": 0.8600284337997437,  
9   "SPEED (M/S)": 0.23889678716659546,  
10  "SPEED (MPH)": 0.5343977790844441,  
11  "TIMESTAMP": "2020-11-16 19:22:24",  
12  "VERTICAL ACCURACY": 3.0,  
13  "ZRTCLLOCATIONMO TABLE ID": 81858  
14 }
```

Where did I go?

The image shows a Google Maps search result for the coordinates 38.8742205507249, -77.1337143. The search bar at the top of the browser window displays these coordinates. The left side of the screen shows a street view image of a white car parked in a parking lot with trees in the background. Below the image are the coordinates and a link to the exact location. On the right is a map of the Bluemont Park area in Arlington, Virginia. A red pin marks the location at the intersection of Wilson Blvd and 9th St N. The map also shows Union Hills Park, Bon Air Park, and Rose Garden. Other landmarks include Sunrise at Bluemont Park, Bluemont Junction Park, and Ashlawn Elementary School. The map includes standard controls for zooming and panning.

38.8742205507249, -77.1337143

38°52'27.2"N 77°08'01.4"W
38.874221, -77.133714

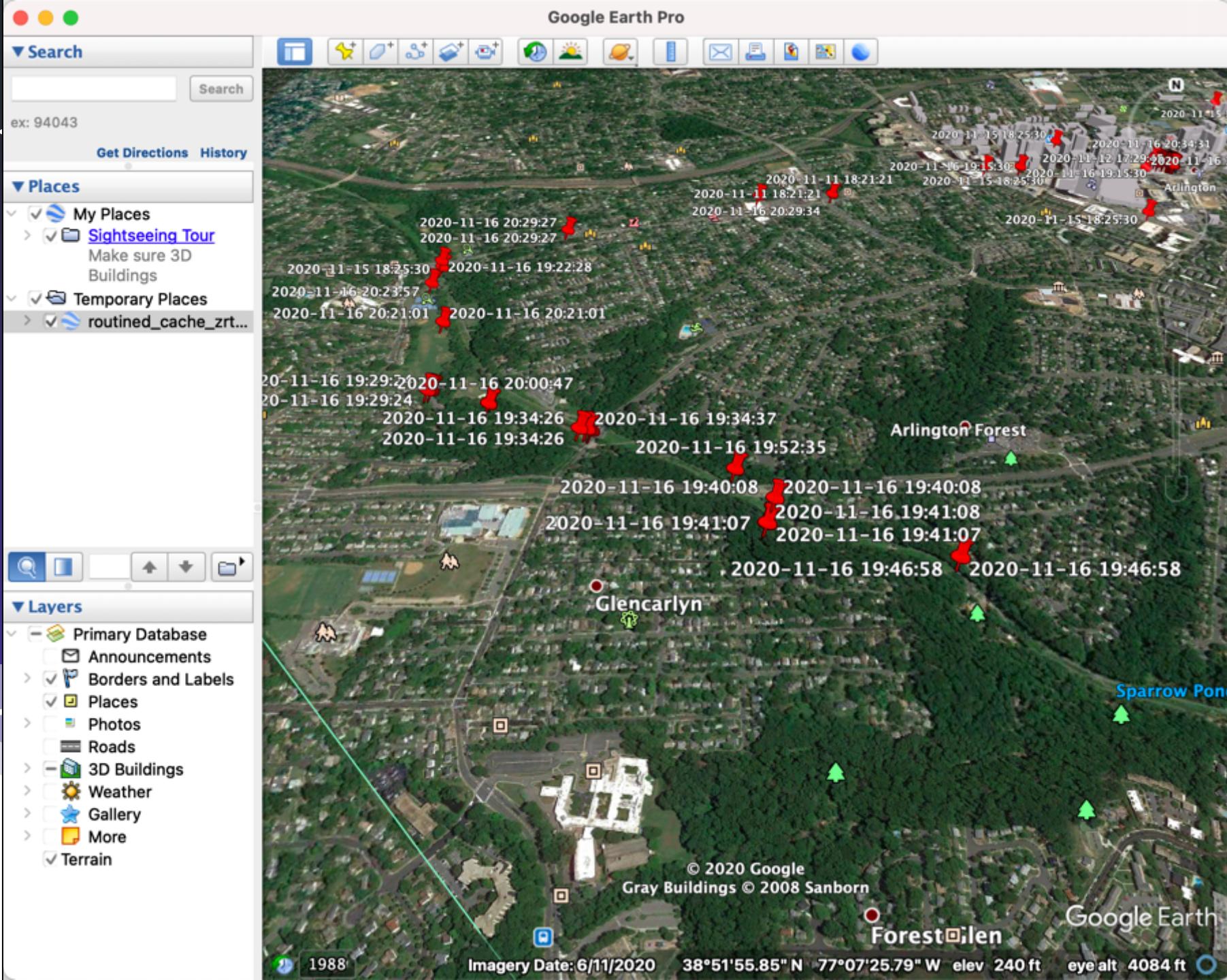
Directions Save Nearby Send to your phone Share

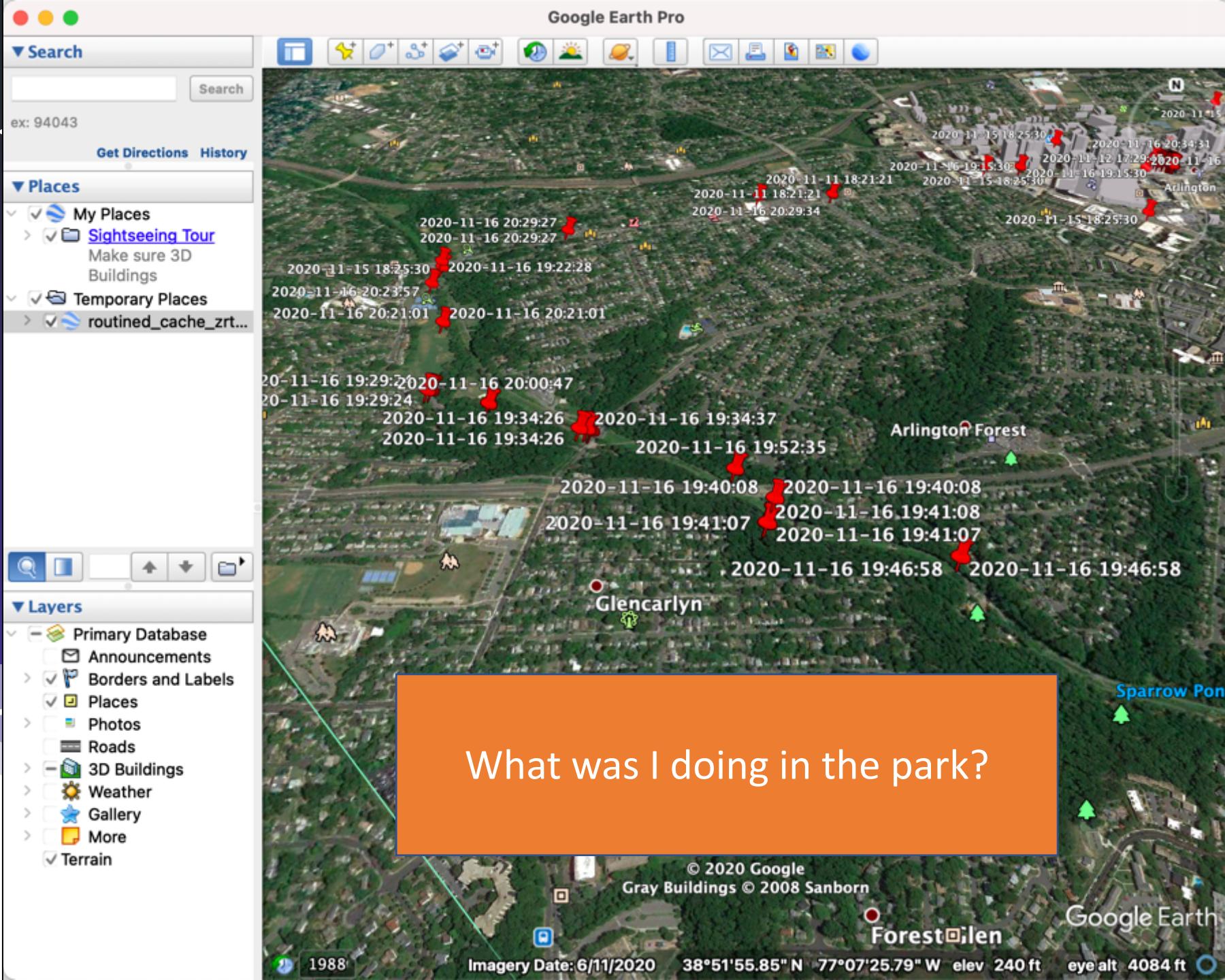
Boulevard Manor, Arlington, VA 22203
VVF8+MG Arlington, Virginia
Add a missing place

Union Hills Park
Bon Air Park
Rose Garden
Sunrise at Bluemont Park
Wilson Blvd
9th St N
N Lexington St
9th Rd N
N Kensington St
N Kentucky St
N Arlington Mill Dr
Blvd
8th Rd N
7th St N
5th Rd N
N Montana St
5th St N
Bluemont Junction Park
Bluemont Park:
Asher's Baseball Field
Satellite
Map data ©2020
United States
Send feedback
Google
500 ft

Where did I go? KMZ Files

```
[oompa@qwerty-MBP APOLLO_v1_4 % ls *.kmz
knowledge_app_location_activity.kmz
locationd_cacheencryptedAB_ltecelllocation.kmz
locationd_cacheencryptedAB_ltecelllocationlocal.kmz
locationd_cacheencryptedAB_wifilocation.kmz
routined_cache_zrtcllocationmo.kmz
routined_cache_zrthintmo.kmz ←
routined_cache_zrvisitmo.kmz
routined_local_learned_location_of_interest_entry.kmz
routined_local_learned_location_of_interest_exit.kmz
routined_local_learned_location_of_interest_transition_start.kmz
routined_local_learned_location_of_interest_transition_stop.kmz
routined_local_vehicle_parked.kmz
routined_local_vehicle_parked_history.kmz
```





What apps did I use?

Key 	Activity	Output	Database	Module
2020-11-16 14:14:14  App	Application Activity	{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_activity.txt	knowledgeC.db#modules/knowledge_app_activity.txt
2020-11-16 14:21:07 Application Activity		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_activity.txt	knowledgeC.db#modules/knowledge_app_activity.txt
2020-11-16 14:21:08 Application Activity		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_inFocus.txt	knowledgeC.db#modules/knowledge_app_inFocus.txt
2020-11-16 14:21:21 Application In Focus		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_inFocus.txt	knowledgeC.db#modules/knowledge_app_inFocus.txt
2020-11-16 14:21:26 Application In Focus		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_inFocus.txt	knowledgeC.db#modules/knowledge_app_inFocus.txt
2020-11-16 14:21:30 Application In Focus		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_inFocus.txt	knowledgeC.db#modules/knowledge_app_inFocus.txt
2020-11-16 14:21:53 Application In Focus		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_inFocus.txt	knowledgeC.db#modules/knowledge_app_inFocus.txt
2020-11-16 14:21:53 Application Usage		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_usage.txt	knowledgeC.db#modules/knowledge_app_usage.txt
2020-11-16 14:21:57 Application In Focus		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_inFocus.txt	knowledgeC.db#modules/knowledge_app_inFocus.txt
2020-11-16 14:21:57 Application Usage		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_usage.txt	knowledgeC.db#modules/knowledge_app_usage.txt
2020-11-16 14:22:09 Application In Focus		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_inFocus.txt	knowledgeC.db#modules/knowledge_app_inFocus.txt
2020-11-16 14:22:15 Application In Focus		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_inFocus.txt	knowledgeC.db#modules/knowledge_app_inFocus.txt
2020-11-16 14:23:19 Application Usage		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_usage.txt	knowledgeC.db#modules/knowledge_app_usage.txt
2020-11-16 14:29:23 Application In Focus		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_inFocus.txt	knowledgeC.db#modules/knowledge_app_inFocus.txt
2020-11-16 14:29:23 Application Usage		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_usage.txt	knowledgeC.db#modules/knowledge_app_usage.txt
2020-11-16 14:34:03 Application Intents		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_intents.txt	knowledgeC.db#modules/knowledge_app_intents.txt
2020-11-16 14:34:09 Application In Focus		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_inFocus.txt	knowledgeC.db#modules/knowledge_app_inFocus.txt
2020-11-16 14:34:09 Application Usage		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_usage.txt	knowledgeC.db#modules/knowledge_app_usage.txt
2020-11-16 14:34:14 Application In Focus		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_inFocus.txt	knowledgeC.db#modules/knowledge_app_inFocus.txt
2020-11-16 14:34:14 Application Usage		{...}	tmp_apollo... knowledgeC.db#modules/knowledge_app_usage.txt	knowledgeC.db#modules/knowledge_app_usage.txt

```

1  {
2      "BUNDLE ID": "com.apple.camera",
3      "DAY OF WEEK": "Monday",
4      "END": "2020-11-16 19:29:40",
5      "ENTRY CREATION": "2020-11-16 19:29:40",
6      "EXTENSION CONTAINING BUNDLE ID": null,
7      "EXTENSION HOST ID": null,
8      "GMT OFFSET": -5,
9      "LAUNCH REASON": "com.apple.springboard.lock-screen.scroll",
10     "START": "2020-11-16 19:29:23",
11     "USAGE IN MINUTES": 0.2833333333333333,
12     "USAGE IN SECONDS": 17,
13     "UUID": "164CC3B6-4559-4372-B519-12542D50FA26",
14     "ZMETADATAHASH": "10af4e48852bb6b6b633d53709403b0c",
15     "ZOBJECT TABLE ID": 188858
16 }
```

What apps did I use?

```
1  {
2      "BUNDLE ID": "com.apple.podcasts",
3      "DAY OF WEEK": "Monday",
4      "END": "2020-11-16 19:34:11",
5      "ENTRY CREATION": "2020-11-16 19:34:11",
6      "EXTENSION CONTAINING BUNDLE ID": null,
7      "EXTENSION HOST ID": null,
8      "GMT OFFSET": -5,
9      "LAUNCH REASON": "com.apple.SpringBoard.transitionReason.homescreen",
10     "START": "2020-11-16 19:34:09",
11     "USAGE IN MINUTES": 0.03333333333333333,
12     "USAGE IN SECONDS": 2,
13     "UUID": "A9283F3F-7508-4F52-81EF-94DC39D04F0A",
14     "ZMETADATAHASH": "24ce9df611b359a77ddacb4a83926e43",
15     "ZOBJECT TABLE ID": 188876
16 }
```

What apps did I use?

```
1  {
2      "BUNDLE ID": "com.apple.podcasts",
3      "DAY OF WEEK": "Monday",
4      "END": "2020-11-16 19:34:11",
5      "ENTRY CREATION": "2020-11-16 19:34:11",
6      "EXTENSION CONTAINING BUNDLE ID": null,
7      "EXTENSION HOST ID": null,
8      "GMT OFFSET": -5,
9      "LAUNCH REASON": "com.apple.SpringBoard.transitionReason.homescreen",
10     "START": "2020-11-16 19:34:09",
11     "USAGE IN MINUTES": 0.03333333333333333
12  {
13      "BUNDLE ID": "com.apple.Music",
14      "DAY OF WEEK": "Monday",
15      "END": "2020-11-16 19:34:24",
16      "ENTRY CREATION": "2020-11-16 19:34:24",
```

What apps did I use?

```
1  {
2      "BUNDLE ID": "com.apple.podcasts",
3      "DAY OF WEEK": "Monday",
4      "END": "2020-11-16 19:34:11",
5      "ENTRY CREATION": "2020-11-16 19:34:11",
6      "EXTENSION CONTAINING BUNDLE ID": null,
7      "EXTENSION HOST ID": null,
8      "GMT OFFSET": -5,
9      "LAUNCH REASON": "com.apple.SpringBoard.transitionReason.homescreen",
10     "START": "2020-11-16 19:34:09",
11     "USAGE IN MINUTES": 0.03333333333333333
```

```
12    {
13        "BUNDLE ID": "com.apple.Music",
14        "DAY OF WEEK": "Monday",
15        "END": "2020-11-16 19:34:24",
16        "ENTRY CREATION": "2020-11-16 19:34:24",
17        "EXTENSION CONTAINING BUNDLE ID": null,
18        "EXTENSION HOST ID": null,
19        "GMT OFFSET": -5,
20        "LAUNCH REASON": "com.apple.SpringBoard.transitionReason.homescreen",
21        "START": "2020-11-16 19:34:14",
22        "USAGE IN MINUTES": 0.1666666666666666,
23        "USAGE IN SECONDS": 10,
24        "UUID": "A3770BF6-8E47-4346-BF95-252126B0F422",
25        "ZMETADATAHASH": "24ce9df611b359a77ddacb4a83926e43",
26        "ZOBJECT TABLE ID": 188934
27    }
```

```
1  {
2      "BUNDLE ID": "us.zoom.videomeetings",
3      "DAY OF WEEK": "Monday",
4      "END": "2020-11-16 19:53:08",
5      "ENTRY CREATION": "2020-11-16 19:53:08",
6      "EXTENSION CONTAINING BUNDLE ID": null,
7      "EXTENSION HOST ID": null,
8      "GMT OFFSET": -5,
9      "LAUNCH REASON": "com.apple.SpringBoard.transitionReason.spotlight",
10     "START": "2020-11-16 19:53:05",
11     "USAGE IN MINUTES": 0.05,
12     "USAGE IN SECONDS": 3,
13     "UUID": "774F9D12-3333-4561-880B-3294F07BA316",
14     "ZMETADATAHASH": "2de493f45d5787a7efcc60688bbb4eeb",
15     "ZOBJECT TABLE ID": 188977
16 }
```

What apps did I use?

```
1  {
2      "BUNDLE ID": "com.apple.podcasts",
3      "DAY OF WEEK": "Monday",
4      "END": "2020-11-16 19:34:11",
5      "ENTRY CREATION": "2020-11-16 19:34:11",
6      "EXTENSION CONTAINING BUNDLE ID": null,
7      "EXTENSION HOST ID": null,
8      "GMT OFFSET": -5,
9      "LAUNCH REASON": "com.apple.SpringBoard.transitionReason.spotlight",
10     "START": "2020-11-16 19:34:09",
11     "USAGE IN MINUTES": 0.03333333333333333
```

```
12    {
13        "BUNDLE ID": "com.apple.Music",
14        "DAY OF WEEK": "Monday",
15        "END": "2020-11-16 19:34:24",
16        "ENTRY CREATION": "2020-11-16 19:34:24",
17        "EXTENSION CONTAINING BUNDLE ID": null,
18        "EXTENSION HOST ID": null,
19        "GMT OFFSET": -5,
20        "LAUNCH REASON": "com.apple.SpringBoard.transitionReason.spotlight",
21        "START": "2020-11-16 19:34:14",
22        "USAGE IN MINUTES": 0.1666666666666666,
23        "USAGE IN SECONDS": 10,
24        "UUID": "A3770BF6-8E47-4346-BF95-252126B01C9D",
25        "ZMETADATAHASH": "24ce9df611b359a77ddacb4a83926e43",
26        "ZOBJECT TABLE ID": 188934
27    }
```

```
1  {
2      "BUNDLE ID": "us.zoom.videomeetings",
3      "DAY OF WEEK": "Monday",
4      "END": "2020-11-16 19:53:08",
5      "ENTRY CREATION": "2020-11-16 19:53:08",
6      "EXTENSION CONTAINING BUNDLE ID": null,
7      "EXTENSION HOST ID": null,
8      "GMT OFFSET": -5,
9      "LAUNCH REASON": "com.apple.SpringBoard.transitionReason.spotlight",
10     "START": "2020-11-16 19:53:05",
11     "USAGE IN MINUTES": 0.03333333333333333
```

```
12    {
13        "BUNDLE ID": "com.apple.MobileSMS",
14        "DAY OF WEEK": "Monday",
15        "END": "2020-11-16 19:55:39",
16        "ENTRY CREATION": "2020-11-16 19:55:39",
17        "EXTENSION CONTAINING BUNDLE ID": null,
18        "EXTENSION HOST ID": null,
19        "GMT OFFSET": -5,
20        "LAUNCH REASON": "com.apple.SpringBoard.transitionReason.homescreen",
21        "START": "2020-11-16 19:54:58",
22        "USAGE IN MINUTES": 0.6833333333333333,
23        "USAGE IN SECONDS": 41,
24        "UUID": "FD1AA318-B642-4812-91B3-55806262FF44",
25        "ZMETADATAHASH": "24ce9df611b359a77ddacb4a83926e43",
26        "ZOBJECT TABLE ID": 188997
27    }
```

Connected Audio Bluetooth Devices?

Key  1	Activity 	Output 	Database 	Module
2020-11-16 14:	 bluetooth	 Filter	 Filter	 Filter
2020-11-16 14:12:33	Bluetooth State	{...}	tmp_apollo...	modules/powerlog_bluetooth_device_state.txt#Cur
2020-11-16 14:16:31	Bluetooth State	{...}	tmp_apollo...	modules/powerlog_bluetooth_device_state.txt#Cur
2020-11-16 14:16:32	Bluetooth State	{...}	tmp_apollo...	modules/powerlog_bluetooth_device_state.txt#Cur
2020-11-16 14:21:33	Bluetooth State	{...}	tmp_apollo...	modules/powerlog_bluetooth_device_state.txt#Cur
2020-11-16 14:21:50	Bluetooth Connected	{...}	tmp_apollo...	modules/knowledge_audio_bluetooth_connected.tx
2020-11-16 14:22:02	Bluetooth State	{...}	tmp_apollo...	modules/powerlog_bluetooth_device_state.txt#Cur
2020-11-16 14:22:02	Bluetooth State	{...}	tmp_apollo...	modules/powerlog_bluetooth_device_state.txt#Cur
2020-11-16 14:22:08	Bluetooth Connected	{...}	tmp_apollo...	modules/knowledge_audio_bluetooth_connected.tx
2020-11-16 14:22:09	Bluetooth State	{...}	tmp_apollo...	modules/powerlog_bluetooth_device_state.txt#Cur
2020-11-16 14:22:09	Bluetooth State	{...}	tmp_apollo...	modules/powerlog_bluetooth_device_state.txt#Cur
2020-11-16 14:22:13	Bluetooth Connected	{...}	tmp_apollo...	modules/knowledge_audio_bluetooth_connected.tx
2020-11-16 14:22:15	Bluetooth Connected	{...}	tmp_apollo...	modules/knowledge_audio_bluetooth_connected.tx

```
1 1 {  
2 "BLUETOOTH ADDRESS": "60:83:73:B5:B7:32",  
3 "BLUETOOTH NAME": "miAirPods Pro",  
4 "DAY OF WEEK": "Monday",  
5 "DEVICE TYPE": 20,  
6 "END": "2020-11-16 20:24:10",  
7 "ENTRY CREATION": "2020-11-16 20:24:10",  
8 "GMT OFFSET": -5,  
9 "NAME": null,  
10 "START": "2020-11-16 19:22:08",  
11 "USAGE IN MINUTES": 62.03333333333333,  
12 "USAGE IN SECONDS": 3722,  
13 "UUID": "526232C2-4082-40FA-9ACC-786A8A1CE132",  
14 "VALUE": null,  
15 "ZMETADATAHASH": "798ebbd846426c89fb431af7f8210e06",  
16 "ZOBJECT TABLE ID": 189519  
17 }
```

What did I listen to?

Table: APOLLO Refresh Clear Filters Clear Sorting Save Table As Print New Record Delete Record Mode: JSON Word Wrap Autoformat Import

	Key <small>▼1</small>	Activity	Output	Database	Mod
26	2020-11-16 14:14:14	playing	Filter	Filter	
27	2020-11-16 14:14:54	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_now
28	2020-11-16 14:16:15	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_now
29	2020-11-16 14:16:26	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_now
30	2020-11-16 14:20:13	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_now
31	2020-11-16 14:20:30	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_now
32	2020-11-16 14:20:46	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_now
33	2020-11-16 14:20:58	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_now
34	2020-11-16 14:22:10	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_now
35	2020-11-16 14:34:02	App Now Playing	{...}	tmp_apollo...	modules/powerlog_app_nowplaying.txt#
36	2020-11-16 14:34:02	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_now
37	2020-11-16 14:34:02	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_now
38	2020-11-16 14:34:02	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_now
39	2020-11-16 14:34:02	Now Playing	{...}	tmp_apollo...	modules/powerlog_app_nowplaying.txt#
40	2020-11-16 14:34:02	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_now
41	2020-11-16 14:34:02	Now Playing	{...}	tmp_apollo...	modules/powerlog_app_nowplaying.txt#
42	2020-11-16 14:34:02	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_now
43	2020-11-16 14:34:19	App Now Playing	{...}	tmp_apollo...	modules/powerlog_app_nowplaying.txt#
44	2020-11-16 14:34:19	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_now
45	2020-11-16 14:34:39	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_now

Shout out to @phillmoore
 at thisweekin4n6.com!

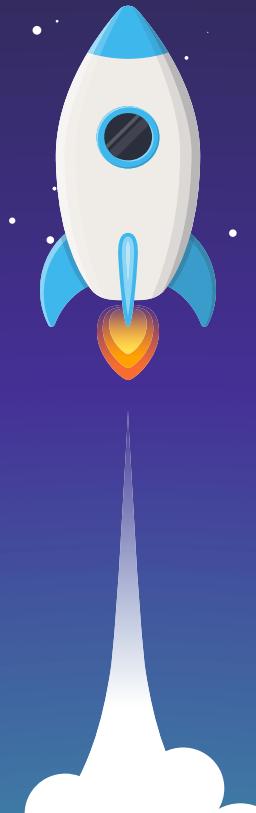
```

1 { "BUNDLE ID": "com.apple.podcasts",
  2 "DAY OF WEEK": "Monday",
  3 "DURATION": 1275.2631292517008,
  4 "ELAPSED": null,
  5 "END": "2020-11-16 19:34:02",
  6 "ENTRY CREATION": "2020-11-16 19:34:02",
  7 "GMT OFFSET": -5,
  8 "IDENTIFIER": null,
  9 "IS AIRPLAY VIDEO": 0,
 10 "MEDIA TYPE": "MRMediaRemoteMediaTypePodcast",
 11 "NOW PLAYING ALBUM": "November 5, 2020",
 12 "NOW PLAYING ARTIST": "This Week In 4n6 » Podcasts",
 13 "NOW PLAYING DURATION": 1275.2631292517008,
 14 "NOW PLAYING GENRE": null,
 15 "NOW PLAYING TITLE": "Month In 4n6 – October – 2020",
 16 "OUTPUT DEVICE IDS (HEX)": "62706C6973743030D4010203040506070A582476657273696F6100F4E534B657965644172636869766572D1080954726F6F748C6B6579735A4E532E6F626A656374735624636C617373A1118002F1E20A11F800680075F101636303A38333A37333A42353A423737365735E4E534D757461626C654172726179A3252728574E534544696374696F6E617279A32A2C285C4E5344696374696F6E610053005E0064006B0073007E008500870089008B008D008F009E100F000F400FC0105010A0120012401310136000000000000002
 18 "PLAYING": 1,
 19 "START": "2020-11-16 19:22:10",
 20 "USAGE IN MINUTES": 11.8666666666666667,
 21 "USAGE IN SECONDS": 712,
 22 "UUID": "E500AAB1-AC4A-49B5-A28B-87CDABE66C52",
 23 "ZMETADATAHASH": "44fe6438ea94e711d8e1f8201f22f339",
 24 "ZOBJECT TABLE ID": 188864
 25 }

```

What did I listen to?

```
1  {  
2      "BUNDLE ID": "com.apple.Music",  
3      "DAY OF WEEK": "Monday",  
4      "DURATION": 195.65133786848074,  
5      "ELAPSED": null,  
6      "END": "2020-11-16 19:50:07",  
7      "ENTRY CREATION": "2020-11-16 19:50:07",  
8      "GMT OFFSET": -5,  
9      "IDENTIFIER": null,  
10     "IS AIRPLAY VIDEO": 0,  
11     "MEDIA TYPE": "MRMediaRemoteMediaTypeMusic",  
12     "NOW PLAYING ALBUM": "Get Wet",  
13     "NOW PLAYING ARTIST": "Krewella",  
14     "NOW PLAYING DURATION": 195.65133786848074,  
15     "NOW PLAYING GENRE": "Dance",  
16     "NOW PLAYING TITLE": "Human",  
17     "OUTPUT DEVICE IDS (HEX)":  
18         "62706C6973743030D4010203040506070A582476657273696F6E5  
19         "100F4E534B657965644172636869766572D1080954726F6F74800  
20         "6B6579735A4E532E6F626A656374735624636C617373A1118002A  
21         "F1E20A11F800680075F101636303A38333A37333A42353A42373A  
22         "7365735E4E534D757461626C654172726179A3252728574E53417  
23         "544696374696F6E617279A32A2C285C4E5344696374696F6E6172  
24         "0053005E0064006B0073007E008500870089008B008D008F00910  
25         "E100F000F400FC0105010A012001240131013600000000000000000020  
18     "PLAYING": 1,  
19     "START": "2020-11-16 19:50:05",  
20     "USAGE IN MINUTES": 0.033333333333333333,  
21     "USAGE IN SECONDS": 2,  
22     "UUID": "8E69BEC8-AACA-46B4-9BA7-A54DD2C40355",  
23     "ZMETADATAHASH": "164a9a9fa545df79ac2cb9b1597aeb3d",  
24     "ZOBJECT TABLE ID": 188967  
25 }
```



```
1  {  
2      "BUNDLE ID": "us.zoom.videomeetings",  
3      "DAY OF WEEK": "Monday",  
4      "DURATION": null,  
5      "ELAPSED": null,  
6      "END": "2020-11-16 20:16:44",  
7      "ENTRY CREATION": "2020-11-16 20:16:44",  
8      "GMT OFFSET": -5,  
9      "IDENTIFIER": null,  
10     "IS AIRPLAY VIDEO": 0,  
11     "MEDIA TYPE": null,  
12     "NOW PLAYING ALBUM": null,  
13     "NOW PLAYING ARTIST": null,  
14     "NOW PLAYING DURATION": null,  
15     "NOW PLAYING GENRE": null,  
16     "NOW PLAYING TITLE": null,  
17     "OUTPUT DEVICE IDS (HEX)":  
18         "62706C6973743030D4010203040506070A582476657273696F6E5  
19         "100F4E534B657965644172636869766572D1080954726F6F74800  
20         "6B6579735A4E532E6F626A656374735624636C617373A1118002A  
21         "F1E20A11F800680075F101636303A38333A37333A42353A42373A  
22         "7365735E4E534D757461626C654172726179A3252728574E53417  
23         "544696374696F6E617279A32A2C285C4E5344696374696F6E6172  
24         "0053005E0064006B0073007E008500870089008B008D008F00910  
25         "E100F000F400FC0105010A0120012401310136000000000000000020  
18     "PLAYING": 1,  
19     "START": "2020-11-16 20:00:48",  
20     "USAGE IN MINUTES": 15.933333333333334,  
21     "USAGE IN SECONDS": 956,  
22     "UUID": "AB8259DE-880A-4B0A-8224-F28D3FA46D7D",  
23     "ZMETADATAHASH": "696a7e160600710e9b2caa75a01e19af",  
24     "ZOBJECT TABLE ID": 189062  
25 }
```

Who was I Zoom'ing with?

Table: APOLLO Refresh Clear Filters Clear Sorting Save Table As Print New Record Delete Record >

	Key ▾ ¹	Activity	Output	Database	Mo
1036	2020-11-16 15:01	App Usage	Filter	tmp_apollo...	modules/powerlog_app_usage.txt#Cu
1037	2020-11-16 15:01:09	Routined Location	{...	tmp_apollo...	modules/routined_cache_zrtcllocation
1038	2020-11-16 15:01:10	Routined Location	{...	tmp_apollo...	modules/routined_cache_zrtcllocation
1039	2020-11-16 15:01:11	Routined Location	{...	tmp_apollo...	modules/routined_cache_zrtcllocation
1040	2020-11-16 15:01:11	Application In Focus	{...	tmp_apollo...	modules/knowledge_app_inFocus.txt#k
1041	2020-11-16 15:01:11	Health Heart Rate	{...	tmp_apollo...	modules/health_heart_rate.txt#health
1042	2020-11-16 15:01:11	Application Usage	{...	tmp_apollo...	modules/knowledge_app_usage.txt#k
1043	2020-11-16 15:01:11	Springboard Screen State	{...	tmp_apollo...	modules/powerlog_device_screen.txt#
1044	2020-11-16 15:01:11	App Usage	{...	tmp_apollo...	modules/powerlog_app_usage.txt#Cu
1045	2020-11-16 15:01:12	Routined Location	{...	tmp_apollo...	modules/routined_cache_zrtcllocation
1046	2020-11-16 15:01:13	Routined Location	{...	tmp_apollo...	modules/routined_cache_zrtcllocation
1047	2020-11-16 15:01:14	Routined Location	{...	tmp_apollo...	modules/routined_cache_zrtcllocation
1048	2020-11-16 15:01:15	Routined Location	{...	tmp_apollo...	modules/routined_cache_zrtcllocation
1049	2020-11-16 15:01:17	Routined Location	{...	tmp_apollo...	modules/routined_cache_zrtcllocation
1050	2020-11-16 15:01:17	Application Intents	{...	tmp_apollo...	modules/knowledge_app_intents.txt#k
1051	2020-11-16 15:01:18	Routined Location	{...	tmp_apollo...	modules/routined_cache_zrtcllocation
1052	2020-11-16 15:01:19	Routined Location	{...	tmp_apollo...	modules/routined_cache_zrtcllocation
1053	2020-11-16 15:01:20	Health Heart Rate	{...	tmp_apollo...	modules/health_heart_rate.txt#health
1054	2020-11-16 15:01:21	Routined Location	{...	tmp_apollo...	modules/routined_cache_zrtcllocation
1055	2020-11-16 15:01:21	Health Heart Rate	{...	tmp_apollo...	modules/health_heart_rate.txt#health

Mode: JSON Word Wrap Autoformat Import E

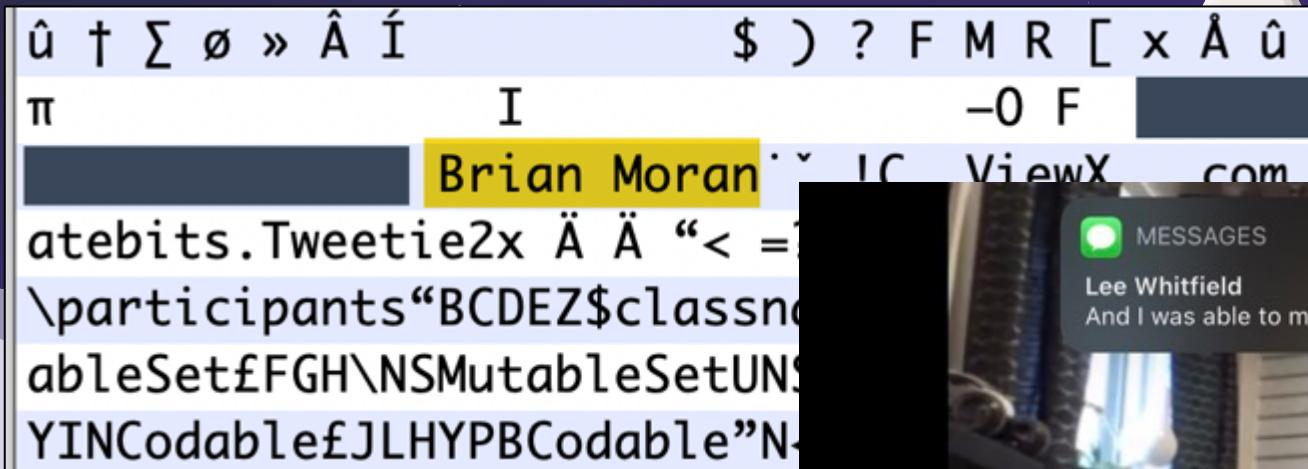
```

1  {
2    "APP NAME": null,
3    "BUNDLE ID": "com.atebits.Tweetie2",
4    "DAY OF WEEK": "Monday",
5    "DERIVED INTENT ID": null,
6    "DEVICE ID": null,
7    "DIRECTION": 0,
8    "DONATED BY SIRI": 0,
9    "END": "2020-11-16 20:01:17",
10   "ENTRY CREATION": "2020-11-16 20:01:17",
11   "GMT OFFSET": -5,
12   "GROUP ID": "iamevtwin-456360479",
13   "HANDLING STATUS": 0,
14   "INTENT CLASS": "T1DirectMessageConversationIntent",
15   "INTENT TYPE": 2,
16   "INTENT VERB": null,
17   "ITEM ID": "40056187-ABFC-46D4-9D7D-5F78631F55D2",
18   "NAME": null,
19   "SERIALIZED INTERACTION (HEX)": "62706C6973743030D4010203040506070A582476657273696F6E100F4E534B657965644172636869766572D1080954726F6F74803734F11181762706C6973743030D4010203040506070A58247665000186A05F100F4E534B657965644172636869766572D1080954797A808182868A939495969A9DA0A8ACAFB4B5B655246E756C696E74657276616C56696E74656E745E5F646F6E617465644279526F75704964656E7469666965725A6964656E7469666965725F106E585F736E69707065745F10155F636F6E74657874457874656E742513262728291A2B1C2D2E2F1C1C1F5F101D5F73686F756C6464465766963655549445C6261636B696E6753746F72655F101577574655F10167265636F72644465766963654964656E7469666965F102439443533454537412D364244322D343245372D383637322C654465736372697074696F6E42797465735562797465735F1019706C6973743030D40001000200030004000500060007000A58247312000186A05F100F4E534B657965644172636869766572D10009

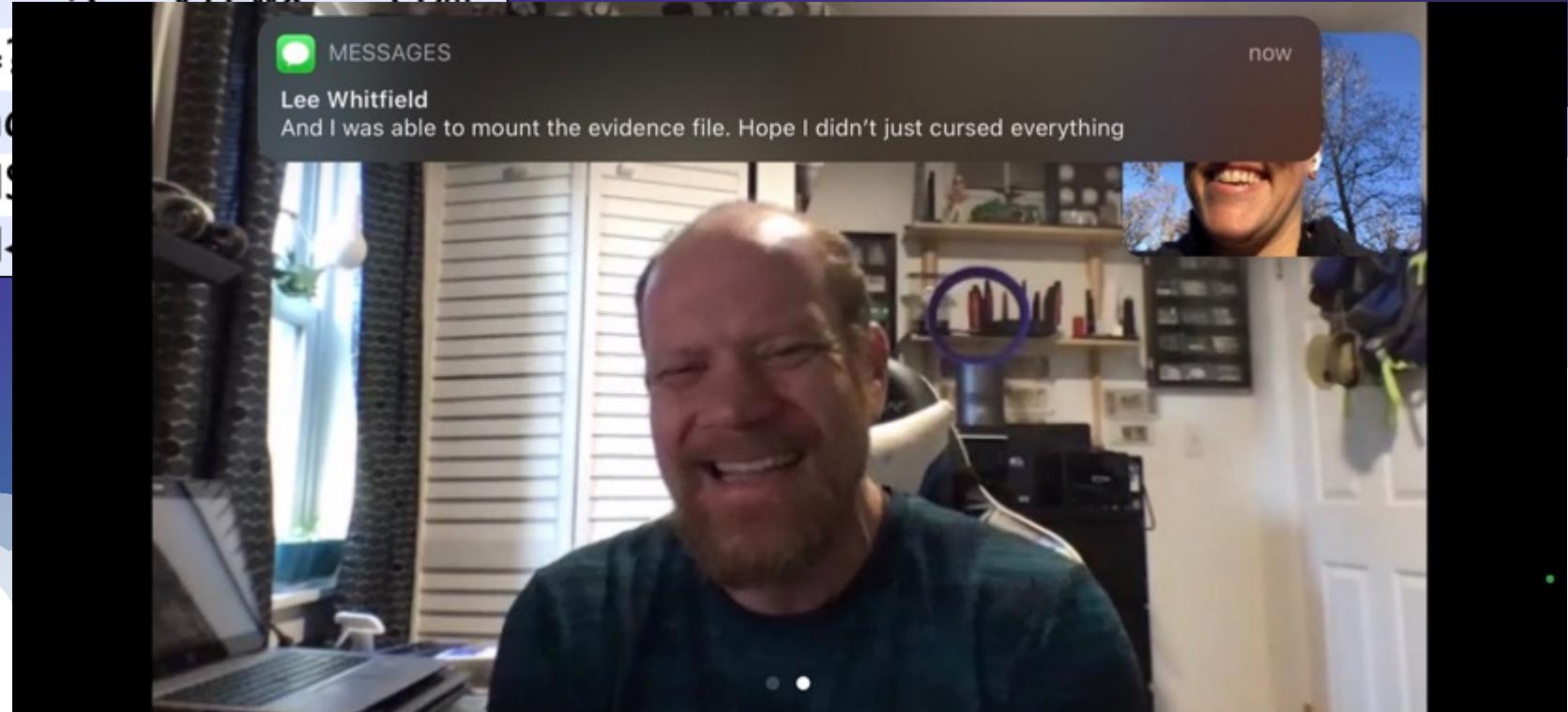
```

Who was I Zoom'ing with?

- Deep down into multiple levels of binary plist inception...
- Verify with Zoom or Twitter app data



```
û t Σ ø » Å Í      $ ) ? F M R [ x Å û  
π          I           -0 F [REDACTED]  
[REDACTED] Brian Moran [REDACTED] ViewX [REDACTED]  
atebits.Tweetie2x Ä Ä “< =  
\participants“BCDEZ$classno  
ableSetFGH\NSMutableSetUNS  
YIN CodablefJLHYPBCodable”N-
```



Lee sliding into my Zoom session...

Key ▾1	Activity	Output	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2020-11-16 15:10	Filter	Filter	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2020-11-16 15:10:47	Routined Location	{...	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2020-11-16 15:10:47	Application Intents	{...	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2020-11-16 15:10:47	Application Intents	{...	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2020-11-16 15:10:47	Application Intents	{...	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2020-11-16 15:10:47	SMS Chat	{...	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2020-11-16 15:10:47	Notification Usage	{...	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2020-11-16 15:10:48	Battery Level	{...	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2020-11-16 15:10:48	Routined Location	{...	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2020-11-16 15:10:49	Routined Location	{...	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

```
1 1 {{"ACCOUNT": "E:oompa@csh.rit.edu",
2 2 "CONTACT ID": "██████████",
3 3 "DATE DELIVERED": "N/A",
4 4 "DATE READ": "2020-11-16 20:25:57",
5 5 "FILENAME": null,
6 6 "IS DELIVERED": 1,
7 7 "IS FROM ME": 0,
8 8 "MESSAGE": "And I was able to mount the evidence file. Hope I didn't just cursed everything",
9 9 "MESSAGE DATE": "2020-11-16 20:10:47",
10 10 "MIME TYPE": null,
11 11 "SERVICE": "iMessage",
12 12 "TOTAL BYTES": null,
13 13 "TRANSFER TYPE": null
14 14
15 15

1 1 {{"BUNDLE ID": "com.apple.MobileSMS",
2 2 "DAY OF WEEK": "Monday",
3 3 "DEVICE ID (HARDWARE UUID)": null,
4 4 "END": "2020-11-16 20:10:47",
5 5 "ENTRY CREATION": "2020-11-16 20:10:48",
6 6 "GMT OFFSET": -5,
7 7 "ID": "B6806292-B916-49E7-B5E8-936864D7FE16",
8 8 "NOTIFICATION TYPE": "Receive",
9 9 "START": "2020-11-16 20:10:47",
10 10 "UUID": "EEE05CDB-A2A6-415C-8B8C-6776998EA1BF",
11 11 "ZMETADATAHASH": "a66d502d0b0643cd9c2f0cd711925584",
12 12 "ZOBJECT TABLE ID": 189054
13 13
14 14}
```

...I really was there for a reason!

Table: APOLLO

Refresh Clear Filters Clear Sorting Save Table As Print New Record Delete Record >>

	Key	Activity	Output	Database	Mo
1	2020-11-16	2020-11-16 14:22:57 Health Workout Time Zone	Filter	Filter	workout
2		2020-11-16 14:22:57 Health Indoor Workout	{...}	tmp_apollo...	modules/health_workout_indoor.txt#he
3		2020-11-16 14:22:57 Health Workout (General)	{...}	tmp_apollo...	modules/health_workout_general.txt#h
4		2020-11-16 14:22:57 Health Workout Humidity	{...}	tmp_apollo...	modules/health_workout_humidity.txt#
5		2020-11-16 14:22:57 Health Workout Location Longitude	{...}	tmp_apollo...	modules/health_workout_location_long
6		2020-11-16 14:22:57 Health Workout Minimum Ground Elevation	{...}	tmp_apollo...	modules/...
7		2020-11-16 14:22:57 Health Workout Time of Day	{...}	tmp_apollo...	modules/health_workout_timeofday.txt
8		2020-11-16 14:22:57 Health Workout Average METs	{...}	tmp_apollo...	modules/health_workout_mets.txt#hea
9		2020-11-16 14:22:57 Health Workout Location Latitude	{...}	tmp_apollo...	modules/health_workout_location_latit
10		2020-11-16 14:22:57 Health Workout Elevation	{...}	tmp_apollo...	modules/health_workout_elevation.txt#
11		2020-11-16 14:22:57 Health Workout Weather	{...}	tmp_apollo...	modules/health_workout_weather.txt#h
12		2020-11-16 14:22:57 Health Workout Temperature	{...}	tmp_apollo...	modules/health_workout_temperature
13		2020-11-16 14:22:57 Health Workout Maximum Ground Elevation	{...}	tmp_apollo...	modules/...

Mode: JSON Word Wrap Autoformat Import Export

```
1  {
2    "CALORIES BURNED": 202.3524922734972,
3    "DISTANCE IN KILOMETERS": 3.352461756184275,
4    "DISTANCE IN MILES": 2.083122513901979,
5    "DURATION (IN MINUTES)": 48.168150049448016,
6    "END DATE": "2020-11-16 20:11:09",
7    "FLIGHTS CLIMBED": null,
8    "GOAL": null,
9    "GOAL TYPE": "OPEN",
10   "START DATE": "2020-11-16 19:22:57",
11   "STEPS": null,
12   "TOTAL BASEL ENERGY BURNED": 77.69843106525619,
13   "WORKOUT TYPE": "INDOOR / OUTDOOR WALK"
14 }
```

What about activity other devices?

- Screen Time, Web Visits/Usage, Notifications, App Usage

Key ^{v1}	Activity	Output	Database	
2020-11-16	/^((?!Portrait Tombstone).)*\$/	502A32AD-	Filter	Filter
2020-11-16 10:00:00	Screen Time - App (By Hour)	{...}	tmp_apollo...	modules/screentime_timed...
2020-11-16 10:00:00	Screen Time - App (By Hour)	{...}	tmp_apollo...	modules/screentime_timed...
2020-11-16 10:00:00	Screen Time - Generic (By Hour)	{...}	tmp_apollo...	modules/screentime_by_ho...
2020-11-16 10:00:00	Screen Time - Counted Item	{...}	tmp_apollo...	modules/screentime_counte...
2020-11-16 10:00:00	Screen Time - Category (By Hour)	{...}	tmp_apollo...	modules/screentime_by_cat...
2020-11-16 10:00:00	Screen Time - Category (By Hour)	{...}	tmp_apollo...	modules/screentime_by_cat...
2020-11-16 10:00:00	Screen Time - Category (By Hour)	{...}	tmp_apollo...	modules/screentime_by_cat...
2020-11-16 10:12:20	Backlight Status	1 { 2 " BUNDLE ID": "com.apple.news", 3 " DAY OF WEEK": "Sunday", 4 " DEVICE ID (HARDWARE UUID)": "502A32AD-3CAF-5585-BC09-053E309F9587", 5 " END": "2020-11-16 03:16:00", 6 " ENTRY CREATION": "2020-11-16 03:16:00", 7 " GMT OFFSET": -5, 8 " NAME": null, 9 " START": "2020-11-16 03:11:29", 10 " USAGE IN MINUTES": 4.5166666666666667, 11 " USAGE IN SECONDS": 271, 12 " UUID": "1FE8A53A-8BF1-46DA-BBC7-A64B51A9809D", 13 " VALUE": null, 14 " ZMETADATAHASH": "15927bd633cdf2bede4122a6a2ec358e", 15 " ZOBJECT TABLE ID": 188025 16 }		1 { 2 " ALT DSID": "001792", 3 " APP USAGE TIME ITEM (MINUTES)": 0.1, 4 " APP USAGE TIME ITEM (SECONDS)": 6, 5 " APPLE ID": "oompa@csh.rit.edu", 6 " BUNDLE ID": "com.atebits.Tweetie2", 7 " CATEGORY ID": "Social Networking", 8 " DEVICE ID": "502A32AD-3CAF-5585-BC09-053E309F9587", 9 " DOMAIN": null, 10 " DSID": 24713276, 11 " FAMILY MEMBER TYPE": "Adult", 12 " FAMILY NAME": "Edwards", 13 " GIVEN NAME": "Sarah", 14 " HOUR": "2020-11-16 15:00:00", 15 " LOCAL USER DEVICE STATE": null, 16 " NAME": "qwerty's MacBook Pro", 17 " NUMBER OF PICKUPS W/O APP USAGE": 0, 18 " PLATFORM": "macOS", 19 " ZUSAGETIMEDITEM TABLE ID": 135198 20 }
2020-11-16 10:12:25	Notification Usage			
2020-11-16 10:15:03	Application Web Usage			
2020-11-16 10:15:03	Application Web Usage			
2020-11-16 10:15:13	Application Web Usage			

Bonus Round!
Checks Time



Thank You OSDFCon!

- Updates Available soon on github.com/mac4n6/APOLLO
- New mac4n6.com Blog Series - “The APOLLO Diaries”
 - Small vignettes of device usage using APOLLO
- Contact Me: @iamevtwin, sarah@blackbagtech.com
- Got BlackBag BlackLight? APOLLO modules are built in!
- Thank you to my test subjects:
 - Phill Moore
 - Brian Moran
 - Lee Whitfield
- FOR518.com – SANS Mac & iOS Forensic Analysis and Incident Response



Stopped to Take a Selfie

Table: APOLLO Refresh Clear Filters Clear Sorting Save Table As Print New Record >

Mode: JSON Word Wrap Autoformat Import

	Key [▼]	Activity	Output	Database	
1	2020-11-16 14	camera	Filter	Filter	Filter
2	2020-11-16 14:29:25	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
3	2020-11-16 14:29:25	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
4	2020-11-16 14:29:41	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
5	2020-11-16 14:29:41	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
6	2020-11-16 14:34:27	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
7	2020-11-16 14:34:27	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
8	2020-11-16 14:34:38	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
9	2020-11-16 14:34:38	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
10	2020-11-16 14:34:39	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
11	2020-11-16 14:34:53	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
12	2020-11-16 14:34:54	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
13	2020-11-16 14:34:54	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
14	2020-11-16 14:34:54	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
15	2020-11-16 14:34:57	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
16	2020-11-16 14:34:58	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
17	2020-11-16 14:41:08	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
18	2020-11-16 14:41:08	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
19	2020-11-16 14:41:09	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
20	2020-11-16 14:41:09	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
21	2020-11-16 14:41:09	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
22	2020-11-16 14:41:09	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
23	2020-11-16 14:41:09	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st
24	2020-11-16 14:41:22	Camera State	{...}	tmp_apollo...	modules/powerlog_camera_st

1 {
2 "ADJUSTED_TIMESTAMP": "2020-11-16 19:41:09",
3 "BUNDLE_ID": "com.apple.camera",
4 "CAMERA_TYPE": "FRONT",
5 "OFFSET_TIMESTAMP": "2020-11-17 17:02:14",
6 "ORIGINAL_CAMERA_TIMESTAMP": "2020-11-16 19:41:01",
7 "PLCAMERAAGENT_EVENTFORWARD_CAMERA_TABLE_ID": 64,
8 "STATE": "ON",
9 "TIME_OFFSET": 8.835574984550476
10 }

Reviewed and deleted those selfies...

	Key 	Activity	Output	Database	Module
1	2020-11-16	 Filter	 Filter	 Filter	photos
2	2020-11-16 15:24:57	Photos Activity	{...}	tmp_apollo...	modules/knowledge_app_activity_photos.tx
3	2020-11-16 15:25:03	Photos Activity	{...}	tmp_apollo...	modules/knowledge_app_activity_photos.tx
4	2020-11-16 15:25:10	Photos Deletes All	{...}	tmp_apollo...	modules/knowledge_photos_deletes_all.txt#
5	2020-11-16 15:25:10	Photos Engagement	{...}	tmp_apollo...	modules/knowledge_photos_engagement.tx
6	2020-11-16 15:25:15	Photos Activity	{...}	tmp_apollo...	modules/knowledge_app_activity_photos.tx
7	2020-11-16 15:25:19	Photos Activity	{...}	tmp_apollo...	modules/knowledge_app_activity_photos.tx
8	2020-11-16 15:25:30	Photos Engagement	{...}	tmp_apollo...	modules/knowledge_photos_engagement.tx
9	2020-11-16 15:25:31	Photos Activity	{...}	tmp_apollo...	modules/knowledge_app_activity_photos.tx
10	2020-11-16 15:25:33	Photos Activity	{...}	tmp_apollo...	modules/knowledge_app_activity_photos.tx
11	2020-11-16 15:25:40	Photos Activity	{...}	tmp_apollo...	modules/knowledge_app_activity_photos.tx
12	2020-11-16 15:25:40	Photos Engagement	{...}	tmp_apollo...	modules/knowledge_photos_engagement.tx
13	2020-11-16 15:25:40	Photos Engagement	{...}	tmp_apollo...	modules/knowledge_photos_engagement.tx
14	2020-11-16 15:25:42	Photos Activity	{...}	tmp_apollo...	modules/knowledge_app_activity_photos.tx

```

1 1 {
2 2   "ACTIVITY TYPE": "com.apple.mobileslideshow.album",
3 3   "ACTIVITY UUID": "87CC6A76-2F3B-4F94-9CCE-585A8BD32F7C",
4 4   "BUNDLE ID": "com.apple.mobileslideshow",
5 5   "DAY OF WEEK": "Monday",
6 6   "ELIGIBLE FOR PREDICTION": 1,
7 7   "END": "2020-11-16 20:24:57",
8 8   "ENTRY CREATION": "2020-11-16 20:25:54",
9 9   "EXPIRATION DATE": "2020-12-16 20:25:43",
10 10  "GMT OFFSET": -5,
11 11  "ITEM IDENTIFIER": "oAglesphkC3P5uuUY4Vng==",
12 12  "PUBLICALLY INDEXABLE": 0,
13 13  "SOURCE ID": "spotlight",
14 14  "START": "2020-11-16 20:24:57",
15 15  "USER ACTIVITY REQUIRED STRING": "v1.0/com.apple.mobileslideshow.album/t='View%20album%20%E2%80%9CRecents%E2%80%9D'&u={'uuid='B97C2D9B-052F-43D9-9E73-7B2FA84B221F}",
16 16  "UUID": "7387FB1A-4D58-4018-ABDB-61B94554C46F",
17 17  "ZMETADATAHASH": "0d27232f72e8f2a2e039fd96154cd18e",
18 18  "ZOBJECT TABLE ID": 189568
19 19 }

```

Potential 3rd Party App Calls in Call History

Table: APOLLO Refresh Clear Filters Clear Sorting Save Table As Print New Record >> Mode: JSON Word Wrap Autoformat Import Export

	Key ^{v1}	Activity	Output	Database	Module
1	2020-11-16	Call History	Filter	Filter	call
2	2020-11-16 12:06:27	Call History	{...}	tmp_apollo...	modules/call_history.txt#CallHistory.sto
3	2020-11-16 15:00:48	Call History	{...}	tmp_apollo...	modules/call_history.txt#CallHistory.sto
4	2020-11-16 15:00:52	In Call Service	{...}	tmp_apollo...	modules/powerlog_incallservice.txt#Cu...
5	2020-11-16 15:16:47	In Call Service	{...}	tmp_apollo...	modules/powerlog_incallservice.txt#Cu...

A green arrow points from the table row at index 3 to the JSON detail view below.

```
1 {  
2   "ADDRESS": "Zoom Meeting",  
3   "CALL TYPE": 0,  
4   "DURATION (IN MINUTES)": 15.9210706671079,  
5   "DURATION (IN SECONDS)": 955.264240026474,  
6   "ISO COUNTRY CODE": null,  
7   "LOCATION": null,  
8   "ORIGINATED": 1,  
9   "SERVICE PROVIDER": "BJ4HAAB9B3.us.zoom.videomeetings",  
10  "TIMESTAMP": "2020-11-16 20:00:48",  
11  "WAS ANSWERED": 0,  
12  "ZCALLRECORD TABLE ID": 71  
13 }
```

```
1 {  
2   "ADJUSTED_TIMESTAMP": "2020-11-16 20:00:52",  
3   "BUNDLE ID": "us.zoom.videomeetings",  
4   "KCALL SUB TYPE": null,  
5   "OFFSET_TIMESTAMP": "2020-11-16 19:16:20",  
6   "ORIGINAL_INCALLSERVICE_TIMESTAMP": "2020-11-16 20:00:45",  
7   "PLXPCAGENT_EVENTFORWARD_INCALLSERVICE TABLE ID": 25,  
8   "PROVIDER IDENTIFIER": "BJ4HAAB9B3.us.zoom.videomeetings",  
9   "STATUS": "callStart",  
10  "TIME_OFFSET": 7.833649039268494,  
11  "VIDEO": 0  
12 }
```

Time to head home....

Table: APOLLO					Mode: JSON
	Key ▾ ¹	Activity	Output	Database	
	2020-11-16 15:2	Filter	Filter	Filter	M
1824	2020-11-16 15:24:59	Application Activity	{...}	tmp_apollo...	"ACTIVITY TYPE": "com.appleMaps", "ACTIVITY UUID": "A02ED595-3FD3-483A-9B90-446EB799D9E2", "BUNDLE ID": "com.appleMaps", "CONTENT DESCRIPTION": null, "CONTENT URL": null, "DAY OF WEEK": "Monday", "ELIGIBLE FOR PREDICTION": 1, "END": "2020-11-16 20:24:59", "ENTRY CREATION": "2020-11-16 20:25:30", "EXPIRATION DATE": "2020-12-16 20:24:59", "GMT OFFSET": -5, "GROUP ID": null, "ITEM IDENTIFIER": "e210U/B9kJcGgxqofeSsjg==", "PUBLICALLY INDEXABLE": 0, "SOURCE ID": "spotlight", "START": "2020-11-16 20:24:59", "SUGGESTED IN VOCATION PHRASE": null, "UNIQUE ID": null, "USER ACTIVITY REQUIRED STRING": "v1.0/com.appleMaps/t='Get%20directions%20to%20Quincy%20St', 'MapsActionKey='MapsDirectionsActionKey', 'MapsActionValue='Get%20directions%20to%20Quincy%20St', 'MapsTableID=189547", "UUID": "DA3D9C11-9A7D-4397-95DC-2B8E2E0DF0DA", "ZMETADATAHASH": "a7068f91098a460bb13d1cba778687c4", "ZOBJECT TABLE ID": 189547 }
1825	2020-11-16 15:25:00	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocation
1826	2020-11-16 15:25:00	DASD Battery Temperature	{...}	tmp_apollo...	modules/knowledge_dasd_battery_te
1827	2020-11-16 15:25:02	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocation
1828	2020-11-16 15:25:02	Health Heart Rate	{...}	tmp_apollo...	modules/health_heart_rate.txt#heal
1829	2020-11-16 15:25:03	Photos Activity	{...}	tmp_apollo...	modules/knowledge_app_activity_pho
1830	2020-11-16 15:25:03	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocation
1831	2020-11-16 15:25:03	Application Activity	{...}	tmp_apollo...	"ACTIVITY TYPE": "com.appleMaps", "ACTIVITY UUID": "A02ED595-3FD3-483A-9B90-446EB799D9E2", "BUNDLE ID": "com.appleMaps", "CONTENT DESCRIPTION": null, "CONTENT URL": null, "DAY OF WEEK": "Monday", "ELIGIBLE FOR PREDICTION": 1, "END": "2020-11-16 20:24:59", "ENTRY CREATION": "2020-11-16 20:25:30", "EXPIRATION DATE": "2020-12-16 20:24:59", "GMT OFFSET": -5, "GROUP ID": null, "ITEM IDENTIFIER": "e210U/B9kJcGgxqofeSsjg==", "PUBLICALLY INDEXABLE": 0, "SOURCE ID": "spotlight", "START": "2020-11-16 20:24:59", "SUGGESTED IN VOCATION PHRASE": null, "UNIQUE ID": null, "USER ACTIVITY REQUIRED STRING": "v1.0/com.appleMaps/t='Get%20directions%20to%20Quincy%20St', 'MapsActionKey='MapsDirectionsActionKey', 'MapsActionValue='Get%20directions%20to%20Quincy%20St', 'MapsTableID=189547", "UUID": "DA3D9C11-9A7D-4397-95DC-2B8E2E0DF0DA", "ZMETADATAHASH": "a7068f91098a460bb13d1cba778687c4", "ZOBJECT TABLE ID": 189547 }
1832	2020-11-16 15:25:04	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocation
1833	2020-11-16 15:25:04	Health Heart Rate	{...}	tmp_apollo...	modules/health_heart_rate.txt#heal
1834	2020-11-16 15:25:05	Application Intents	{...}	tmp_apollo...	modules/knowledge_app_intents.txt#l
1835	2020-11-16 15:25:06	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocation
1836	2020-11-16 15:25:07	Routined Location - Learned ...	{...}	tmp_apollo...	modules/...
1837	2020-11-16 15:25:07	Routined Location - Outbound Stop	{...}	tmp_apollo...	modules/routined_cloud_visit_outbound
1838	2020-11-16 15:25:07	Routined Location - Inbound Stop	{...}	tmp_apollo...	modules/routined_cloud_visit_inbound
1839	2020-11-16 15:25:07	Routined Location - Learned ...	{...}	tmp_apollo...	modules/...

Dictating text messages to Lee (not via Siri)

	Key ^{▼1}	Activity	Output	Database	Module
2051	2020-11-16 15:2	Filter	Filter	Filter	Filter
2052	2020-11-16 15:26:41	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocation
2053	2020-11-16 15:26:41	Application Intents	{...}	tmp_apollo...	modules/knowledge_app_intents.txt#l
2054	2020-11-16 15:26:41	SMS Chat	{...}	tmp_apollo...	modules/sms_chat.txt#sms.db#SQL C
2055	2020-11-16 15:26:42	Audio Routing	{...}	tmp_apollo...	modules/powerlog_audio_routing.txt#
2056	2020-11-16 15:26:42	SMS Chat - Message Delivered	{...}	tmp_apollo...	modules/sms_chat_message_deliver
2056	2020-11-16 15:26:42	Audio Input	{...}	tmp_apollo...	modules/knowledge_audio_input rou
2057	2020-11-16 15:26:43	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocation
2058	2020-11-16 15:26:44	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocation
2059	2020-11-16 15:26:44	App Audio Routing	{...}	tmp_apollo...	modules/powerlog_app_audio.txt#Cu
2060	2020-11-16 15:26:45	App Location Usage	{...}	tmp_apollo...	modules/powerlog_location_client_st
2061	2020-11-16 15:26:45	Health Heart Rate	{...}	tmp_apollo...	modules/health_heart_rate.txt#heal
2062	2020-11-16 15:26:46	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocation
2063	2020-11-16 15:26:47	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocation
2064	2020-11-16 15:26:48	Audio Routing	{...}	tmp_apollo...	modules/powerlog_audio_routing.txt#
2065	2020-11-16 15:26:48	Audio Input	{...}	tmp_apollo...	modules/knowledge_audio_input rou

```

1  {
2      "AUDIO IDENTIFIER": "Built-In Microphone",
3      "AUDIO PORT NAME": "iPhone Microphone",
4      "AUDIO PORT TYPE": "MicrophoneBuiltIn",
5      "DAY OF WEEK": "Monday",
6      "END": "2020-11-16 20:26:48",
7      "ENTRY CREATION": "2020-11-16 20:26:48",
8      "GMT OFFSET": -5,
9      "ROUTE CHANGE REASON": 3,
10     "START": "2020-11-16 20:26:42",
11     "USAGE IN MINUTES": 0.1,
12     "USAGE IN SECONDS": 6,
13     "UUID": "7F8D0250-3CA8-453D-942C-FA3795198A74",
14     "ZMETADATAHASH": "ab89feb5b1b046f7ba6a6b583c480503",
15     "ZOBJECT TABLE ID": 189590
16 }
```

Was I speeding or using non-hands free apps?

The screenshot shows a database viewer on the left and a JSON viewer on the right.

Database View (Left):

	Key	Activity	Output	Database	Module
11	2020-11-16 15:29:02	App Usage	{...}	tmp_apollo...	modules/powerlog_app_usage.txt#CurrentPo
12	2020-11-16 15:29:03	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#
13	2020-11-16 15:29:03	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_nowplayin
14	2020-11-16 15:29:03	App Location Usage	{...}	tmp_apollo...	modules/powerlog_location_client_status.txt#
15	2020-11-16 15:29:04	Activity Level	{...}	tmp_apollo...	modules/knowledge_activity_level.txt#knowle
16	2020-11-16 15:29:04	Audio Routing	{...}	tmp_apollo...	modules/powerlog_audio_routing.txt#Current
17	2020-11-16 15:29:04	Audio Input	{...}	tmp_apollo...	modules/knowledge_audio_input_route.txt#ki
18	2020-11-16 15:29:05	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#

JSON View (Right):

```
1  {
2      "ALTITUDE": 70.4,
3      "COORDINATES": "38.8752015833333, -77.13275145",
4      "COURSE": 71.03408813476563,
5      "HORIZONTAL ACCURACY": 5.0,
6      "LATITUDE": 38.87520158333336,
7      "LONGITUDE": -77.13275144999999,
8      "SPEED (KMPH)": 35.5584,
9      "SPEED (M/S)": 9.877333333333333,
10     "SPEED (MPH)": 22.095002026666666,
11     "TIMESTAMP": "2020-11-16 20:29:05",
12     "VERTICAL ACCURACY": 9.5,
13     "ZRTCLLOCATIONMO TABLE ID": 85337
14 }
```

Nope, Just Asking Siri for Directions

	Key ^{v1}	Activity	Output	Database	Module
11	2020-11-16 15:29:02	App Usage	{...}	tmp_apollo...	modules/powerlog_app_usage.txt#CurrentPo
12	2020-11-16 15:29:03	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocationmo.txt#
13	2020-11-16 15:29:03	Now Playing	{...}	tmp_apollo...	modules/knowledge_audio_media_nowplayin
14	2020-11-16 15:29:03	App Location Usage	{...}	tmp_apollo...	modules/powerlog_location_client_status.txt#
15	2020-11-16 15:29:04	Activity Level	{...}	tmp_apollo...	modules/knowledge_activity_level.txt#knowle
16	2020-11-16 15:29:04	Audio Routing	{...}	tmp_apollo...	modules/powerlog_audio_routing.txt#Current
17	2020-11-16 15:29:04	Audio Input	{...}	tmp_apollo...	modules/knowledge_audio_input_route.txt#ki
18	2020-11-16 15:29:05	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocati
19	2020-11-16 15:29:05	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocati
20	2020-11-16 15:29:06	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocati
21	2020-11-16 15:29:06	App Location Usage	{...}	tmp_apollo...	modules/powerlog_location_client_
22	2020-11-16 15:29:07	Telephony Activity	{...}	tmp_apollo...	modules/...
23	2020-11-16 15:29:08	Motion State History	{...}	tmp_apollo...	modules/...
24	2020-11-16 15:29:08	Routined Location	{...}	tmp_apollo...	modules/routined_cache_zrtcllocati
25	2020-11-16 15:29:08	Application Intents	{...}	tmp_apollo...	modules/knowledge_app_intents.tx
26	2020-11-16 15:29:08	Siri Service	{...}	tmp_apollo...	modules/knowledge_siri_service.tx

```
1  {  
2    "ADJUSTED_TIMESTAMP": "2020-11-16 20:29:02",  
3    "APPROLE": 0,  
4    "BUNDLE_ID": "com.apple.Siri",  
5    "DISPLAY": 3,  
6    "LEVEL": 2.0,  
7    "OFFSET_TIMESTAMP": "2020-11-17 17:02:14",  
8    "ORIENTATION": null,  
9    "ORIGINAL_SCREEN_STATE_TIMESTAMP": "2020-11-16 20:28:54",  
10   "PLSCREENSTATEAGENT_EVENTFORWARD_SCREENSTATE TABLE ID": 960,  
11   "SCREENWEIGHT": 1.0,  
12   "TIME_OFFSET": 8.835574984550476  
13 }
```

```
1  {  
2    "APP NAME": "Maps",  
3    "BUNDLE ID": "com.apple.assistant_service",  
4    "DAY OF WEEK": "Monday",  
5    "DERIVED INTENT ID": null,  
6    "DEVICE ID": null,  
7    "DIRECTION": 0,  
8    "DONATED BY SIRI": 0,  
9    "END": "2020-11-16 20:29:08",  
10   "ENTRY CREATION": "2020-11-16 20:29:08",  
11   "GMT OFFSET": -5,  
12   "GROUP ID": null,  
13   "HANDLING STATUS": 0,  
14   "INTENT CLASS": "INIntent",  
15   "INTENT TYPE": 3,  
16   "INTENT VERB": "Navigation",  
17   "ITEM ID": "C93C8FB0-DCFE-41CE-806F-1C38FC846B76",  
18   "NAME": null,  
19   "SERIALIZED INTERACTION (HEX)":  
"62706C6973743030D4010203040506070A582476657273696F  
0186A05F100F4E534B657965644172636869766572D10809547  
6174615624636C6173734F1104DC62706C6973743030D401020
```

Thanks! Give it a try!

- Updates Available soon on github.com/mac4n6/APOLLO
- New mac4n6.com Blog Series - “The APOLLO Diaries”
 - Small vignettes of device usage using APOLLO
- Contact Me: @iamevtwin, sarah@blackbagtech.com
- Got BlackBag BlackLight? APOLLO modules are built in!
- Thank you to my test subjects:
 - Phill Moore
 - Brian Moran
 - Lee Whitfield
- FOR518.com – SANS Mac & iOS Forensic Analysis and Incident Response

