Go for Launch: Getting Started with Practical APOLLO Analysis

Sarah Edwards | github.com/mac4n6/APOLLO
@iamevltwin | 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?

KnowledgeC.db
runtime DBs
netusage.db
location DBs
InteractionsC.db
PowerLogs
ADDataStore.sqlite.db
healthdb_secure.sqlite.db

Aggregation Metadata
Locations
Network Usage
Device Status
Health Metadata

App Usage

Intents & Activities

APOLLO Database
APOLLO Module

- Module Metadata
- Notes & Authorship
- Database Metadata
- Database Filename
- Versioning
- Query Metadata
- Key Timestamp
- SQL Query
- Sometimes many!
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 APOLO_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/.fseventsd: Operation not permitted
find: /private/var/mobile/Library/Mobile Documents/com-apple-CloudDocs/Documents/airdrop_test/david/fsevents/.fseventsd: 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)

RecommendaLon:
Use SSH Keys
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:

...Parsing Modules in...
...Creating /tmp_apollo...
...Finding files on root
find: /private/var/.fsevents
...Writing Operation not permitted
...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

What about remote macOS collection?
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

...Parsing Modules in...
...Creating /tmp_apollo...
...Finding files on root
find: /private/var/.fsevents
find: /private/var/mobile

...Writing ios_files.txt
...Searching for and copying
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

What about remote macOS collection?
Edit the hard-coded ‘root’ to appropriate username.
Gather on AppleTV (iOS 13.4, checkra1n'ed)

```
 overarching-MBP APOLO_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/.fseventsd: Operation not permitted
...Writing ios_files.txt...
...Searching for and copying databases into tmp_apollo...
root@192.168.1.157's password: 
ADDataStore.sqlite
root@192.168.1.157's password: 
ADDataStore.sqlite-shm
root@192.168.1.157's password: 
ADDataStore.sqlite-wal
root@192.168.1.157's password: 
knowledgeC.db
root@192.168.1.157's password: 
knowledgeC.db-shm
```

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Throughput</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADDataStore.sqlite</td>
<td>1420KB</td>
<td>5.3MB/s</td>
<td>00:00</td>
</tr>
<tr>
<td>ADDataStore.sqlite-shm</td>
<td>32KB</td>
<td>372.2KB/s</td>
<td>00:00</td>
</tr>
<tr>
<td>ADDataStore.sqlite-wal</td>
<td>0</td>
<td>0.0KB/s</td>
<td>00:00</td>
</tr>
<tr>
<td>knowledgeC.db</td>
<td>2636KB</td>
<td>6.0MB/s</td>
<td>00:00</td>
</tr>
<tr>
<td>knowledgeC.db-shm</td>
<td>32KB</td>
<td>1.8MB/s</td>
<td>00:00</td>
</tr>
</tbody>
</table>

No SSH Keys 😭
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.sqilitedb: SQL Query 8,9,10,11,12,13,14
  [2] modules/aggregate_dictionary_scalars.txt on ADDataStore.sqilitedb: SQL Query 8,9,10,11,12,13,14
  [3] modules/call_history.txt on CallHistory.storedata: 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@qwerty-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_dictionarydistributed_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.storedata: SQL Query 9,10,11,12,13,14
[4] modules/datausage_zlivenusage.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@qwerty-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.sqledb: SQL Query 8,9,10,11,12,13,14
  [2] modules/aggregate_dictionary_scalars.txt on ADDataStore.sqledb: SQL Query 8,9,10,11,12,13,14
  [3] modules/call_history.txt on CallHistory.storedata: 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
Where to start?
Where to start? November 16, 2020
Filter or Query? Choose Your own Adventure!

---

**Table: APOLLO**

<table>
<thead>
<tr>
<th>Key</th>
<th>Activity</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-11-16</td>
<td>Filter</td>
<td>Filter</td>
</tr>
</tbody>
</table>

---

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

---

```
<table>
<thead>
<tr>
<th>Key</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-11-16 19:15:03</td>
<td>Routined</td>
</tr>
<tr>
<td>2020-11-16 19:15:03</td>
<td>Routined</td>
</tr>
<tr>
<td>2020-11-16 19:15:34</td>
<td>Routined</td>
</tr>
<tr>
<td>2020-11-16 19:15:34</td>
<td>Routined</td>
</tr>
<tr>
<td>2020-11-16 19:16:51</td>
<td>Routined</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Key</th>
<th>Activity</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-11-16</td>
<td>Show rowid column</td>
<td></td>
</tr>
<tr>
<td>2020-11-16</td>
<td>Hide column(s)</td>
<td></td>
</tr>
<tr>
<td>2020-11-16</td>
<td>Show all columns</td>
<td></td>
</tr>
<tr>
<td>2020-11-16</td>
<td>Select column</td>
<td></td>
</tr>
<tr>
<td>2020-11-16</td>
<td>Edit display format</td>
<td></td>
</tr>
<tr>
<td>2020-11-16</td>
<td>Set encoding</td>
<td></td>
</tr>
<tr>
<td>2020-11-16</td>
<td>Set encoding for all tables</td>
<td></td>
</tr>
</tbody>
</table>

```
SELECT 
datetime('Key', 'localtime') as Key,
Activity, Output, Database, Module
FROM APOLLO
WHERE key LIKE '2020-11-16%'
```

```
<table>
<thead>
<tr>
<th>Key</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-11-16 14:15:03</td>
<td>Routined Location - Entry</td>
</tr>
<tr>
<td>2020-11-16 14:15:03</td>
<td>Routined Location - Entry</td>
</tr>
</tbody>
</table>
```
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
Where to start? November 16, 2020

Key in on a specific event...

• “Sarah was observed getting into her vehicle.”
Where to start? November 16, 2020

Key in on a specific event...

• “Sarah was observed getting into her vehicle.”

***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 I didn’t have CarPlay?

Table: APOLLO

<table>
<thead>
<tr>
<th>Key</th>
<th>Activity</th>
<th>Output</th>
<th>Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-11-16</td>
<td>Motion State History</td>
<td>... tmp_apollo_ios14/...</td>
<td>modules/...</td>
</tr>
<tr>
<td>2020-11-16</td>
<td>Motion State History</td>
<td>... tmp_apollo_ios14/...</td>
<td>modules/...</td>
</tr>
<tr>
<td>2020-11-16</td>
<td>Motion State History</td>
<td>... tmp_apollo_ios14/...</td>
<td>modules/...</td>
</tr>
<tr>
<td>2020-11-16</td>
<td>Motion State History</td>
<td>... tmp_apollo_ios14/...</td>
<td>modules/...</td>
</tr>
<tr>
<td>2020-11-16</td>
<td>Motion State History</td>
<td>... tmp_apollo_ios14/...</td>
<td>modules/...</td>
</tr>
<tr>
<td>2020-11-16</td>
<td>Motion State History</td>
<td>... tmp_apollo_ios14/...</td>
<td>modules/...</td>
</tr>
<tr>
<td>2020-11-16</td>
<td>Motion State History</td>
<td>... tmp_apollo_ios14/...</td>
<td>modules/...</td>
</tr>
<tr>
<td>2020-11-16</td>
<td>Motion State History</td>
<td>... tmp_apollo_ios14/...</td>
<td>modules/...</td>
</tr>
<tr>
<td>Key</td>
<td>Activity</td>
<td>Output</td>
<td>Database</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------</td>
<td>----------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>36</td>
<td>Device Plugin Status</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/knowledge_device_pluggedin.txt#knowledgeC.dbf#SQL Query ...</td>
</tr>
<tr>
<td>37</td>
<td>Device Plugin Status</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/knowledge_device_pluggedin.txt#knowledgeC.dbf#SQL Query ...</td>
</tr>
<tr>
<td>38</td>
<td>Routed Location</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/routed_cache_zrtinito.txt#Cache.sqlite#SQL Query ...</td>
</tr>
<tr>
<td>39</td>
<td>App Audio Routing</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_app_audio.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>40</td>
<td>CarPlay Connection Status</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/knowledge_device_carplay_connected.txt#knowledgeC.dbf#SQL ...</td>
</tr>
<tr>
<td>41</td>
<td>App Audio Routing</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_app_audio.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>42</td>
<td>App Audio Routing</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_app_audio.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>43</td>
<td>Motion State History</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/...</td>
</tr>
<tr>
<td>44</td>
<td>Battery Level</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_battery_level.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>45</td>
<td>Screen Brightness</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_display_brightness.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>46</td>
<td>IDS Messages</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>47</td>
<td>IDS Messages</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>48</td>
<td>IDS Messages</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>49</td>
<td>IDS Messages</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>50</td>
<td>IDS Messages</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>51</td>
<td>IDS Messages</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>52</td>
<td>IDS Messages</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>53</td>
<td>IDS Messages</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_ids_messages.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>54</td>
<td>Battery Level UI</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_battery_level.ui.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>55</td>
<td>Motion State History</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/...</td>
</tr>
<tr>
<td>56</td>
<td>Now Playing</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/knowledge_audio_media_nowplaying.txt#knowledgeC.dbf#SQL Query ...</td>
</tr>
<tr>
<td>57</td>
<td>Now Playing</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/knowledge_audio_media_nowplaying.txt#knowledgeC.dbf#SQL Query ...</td>
</tr>
<tr>
<td>58</td>
<td>Device Volume</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_device_volume.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>59</td>
<td>Airdrop Connection</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_airdrop.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>60</td>
<td>Location Technology</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_location_tech_status.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>61</td>
<td>Audio Input</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/knowledge_audio_input_route.txt#knowledgeC.dbf#SQL Query ...</td>
</tr>
<tr>
<td>62</td>
<td>Routed Location</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/routed_cache_zrtlocationmo.txt#Cache.sqlite#SQL Query ...</td>
</tr>
<tr>
<td>63</td>
<td>App Location Usage</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_location_client_status.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
<tr>
<td>64</td>
<td>App Location Usage</td>
<td>(...) tmp_apollo_ios14/...</td>
<td>modules/powerlog_location_client_status.txt#CurrentPowerlog.PLSQL#SQL Query ...</td>
</tr>
</tbody>
</table>
Where did I go? Check for Routined Locations

• Correlate timestamp with CarPlay Disconnect event or Motion State History
Where did I go?
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_zrtnlocationmo.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 was I doing in the park?
What apps did I use?

<table>
<thead>
<tr>
<th>Key</th>
<th>Activity</th>
<th>Output</th>
<th>Database</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-11-16 14:21:07</td>
<td>Application Activity</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_activity.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:21:08</td>
<td>Application Activity</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_activity.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:21:21</td>
<td>Application In Focus</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_inFocus.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:21:26</td>
<td>Application In Focus</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_inFocus.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:21:30</td>
<td>Application In Focus</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_inFocus.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:21:53</td>
<td>Application In Focus</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_inFocus.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:21:53</td>
<td>Application Usage</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_usage.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:21:57</td>
<td>Application In Focus</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_inFocus.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:21:57</td>
<td>Application Usage</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_usage.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:22:09</td>
<td>Application In Focus</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_inFocus.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:22:15</td>
<td>Application In Focus</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_inFocus.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:23:19</td>
<td>Application Usage</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_usage.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:29:23</td>
<td>Application In Focus</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_inFocus.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:29:23</td>
<td>Application Usage</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_usage.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:34:03</td>
<td>Application Intents</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_intents.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:34:09</td>
<td>Application In Focus</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_inFocus.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:34:09</td>
<td>Application Usage</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_usage.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:34:14</td>
<td>Application In Focus</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_inFocus.txt#knowledgeC.db</td>
<td></td>
</tr>
<tr>
<td>2020-11-16 14:34:14</td>
<td>Application Usage</td>
<td>tmp_apollo...</td>
<td>modules/knowledge_app_usage.txt#knowledgeC.db</td>
<td></td>
</tr>
</tbody>
</table>
What apps did I use?

<table>
<thead>
<tr>
<th>Bundle ID</th>
<th>Day of Week</th>
<th>Start Time</th>
<th>End Time</th>
<th>Usage in Minutes</th>
<th>UUID</th>
<th>ZObject Table ID</th>
</tr>
</thead>
</table>
Connected Audio Bluetooth Devices?
<table>
<thead>
<tr>
<th>Key</th>
<th>Activity</th>
<th>Output</th>
<th>Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>27</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>28</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>29</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>30</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>31</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>32</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>33</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>34</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>35</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>36</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>37</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>38</td>
<td>App Now Playing</td>
<td>@phillmoore modules/powerlog_app_nowplaying.txt</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>39</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>40</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>41</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>42</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>43</td>
<td>App Now Playing</td>
<td>@phillmoore modules/powerlog_app_nowplaying.txt</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>44</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
<tr>
<td>45</td>
<td>Now Playing</td>
<td>@phillmoore tmp_apollo</td>
<td>modules/knowledge_audio_media_nowplaying</td>
</tr>
</tbody>
</table>

Shout out to @phillmoore at thisweekin4n6.com!
What did I listen to?

**BUNDLE ID**: "com.apple.Music",
**DAY OF WEEK**: "Monday",
**DURATION**: 195.65133786848074,
**ELAPSED**: null,
**END**: "2020-11-16 19:50:07",
**ENTRY CREATION**: "2020-11-16 19:50:07",
**GMT OFFSET**: -5,
**IDENTIFIER**: null,
**IS AIRPLAY VIDEO**: 0,
**MEDIA TYPE**: "M4MediaRemoteMediaTypeMusic",
**NOW PLAYING ALBUM**: "Get Wet",
**NOW PLAYING ARTIST**: "Krewella",
**NOW PLAYING DURATION**: "195.65133786848074",
**NOW PLAYING GENRE**: "Dance",
**NOW PLAYING TITLE**: "Human",
**OUTPUT DEVICE IDS (HEX)**:
"62706c697374303030d4010203040506070a582476657273696f6e5e100f4e534656756644172633669766572d108065472e674f800686647354e532e6f626f6e6573747356246436c617373a116002a1e24011f8600680075f101636303a83533a17333a42353a43373a7365734e534754616265654172637285745e5417546686866f66167279a322ac2854e5346896374966f6e17005300e064000b073007e06500070080008000d00f001e100f000f040fc01050010a12001240131031e600000000000",
**PLAYING**: 1,
**START**: "2020-11-16 19:50:05",
**USAGE IN MINUTES**: 0.033333333333333333,
**USAGE IN SECONDS**: 2,
**UUID**: "8e69b8c8-aaca-46b4-9b57-a54dd2c40355",
**ZMETADATASHA**: "164a9a9a54df79ac2cb9b15979eb3d",
**ZOBJECT TABLE ID**: 188967
<table>
<thead>
<tr>
<th>Key</th>
<th>Activity</th>
<th>Output</th>
<th>Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>2030</td>
<td>App Usage</td>
<td>...</td>
<td>modules/powerlog_app_usage.txt#Cpu</td>
</tr>
<tr>
<td>3037</td>
<td>Routined Location</td>
<td>...</td>
<td>modules/routined_cache_zrtcllocation</td>
</tr>
<tr>
<td>3038</td>
<td>Routined Location</td>
<td>...</td>
<td>modules/routined_cache_zrtcllocation</td>
</tr>
<tr>
<td>3039</td>
<td>Routined Location</td>
<td>...</td>
<td>modules/routined_cache_zrtcllocation</td>
</tr>
<tr>
<td>3040</td>
<td>Application In Focus</td>
<td>...</td>
<td>modules/knowledge_app_inFocus.txt</td>
</tr>
<tr>
<td>3041</td>
<td>Health Heart Rate</td>
<td>...</td>
<td>modules/health_heart_rate.txt#health</td>
</tr>
<tr>
<td>3042</td>
<td>Application Usage</td>
<td>...</td>
<td>modules/powerlog_app_usage.txt#Cpu</td>
</tr>
<tr>
<td>3043</td>
<td>Springboard Screen State</td>
<td>...</td>
<td>modules/powerlog_device_scren.txt</td>
</tr>
<tr>
<td>3044</td>
<td>App Usage</td>
<td>...</td>
<td>modules/powerlog_app_usage.txt#Cpu</td>
</tr>
<tr>
<td>3045</td>
<td>Routined Location</td>
<td>...</td>
<td>modules/routined_cache_zrtcllocation</td>
</tr>
<tr>
<td>3046</td>
<td>Routined Location</td>
<td>...</td>
<td>modules/routined_cache_zrtcllocation</td>
</tr>
<tr>
<td>3047</td>
<td>Routined Location</td>
<td>...</td>
<td>modules/routined_cache_zrtcllocation</td>
</tr>
<tr>
<td>3048</td>
<td>Routined Location</td>
<td>...</td>
<td>modules/routined_cache_zrtcllocation</td>
</tr>
<tr>
<td>3049</td>
<td>Routined Location</td>
<td>...</td>
<td>modules/routined_cache_zrtcllocation</td>
</tr>
<tr>
<td>3050</td>
<td>Application Intents</td>
<td>...</td>
<td>modules/application_intents.txt</td>
</tr>
<tr>
<td>3051</td>
<td>App Usage</td>
<td>...</td>
<td>modules/powerlog_app_usage.txt#Cpu</td>
</tr>
<tr>
<td>3052</td>
<td>Routined Location</td>
<td>...</td>
<td>modules/routined_cache_zrtcllocation</td>
</tr>
<tr>
<td>3053</td>
<td>Health Heart Rate</td>
<td>...</td>
<td>modules/health_heart_rate.txt#health</td>
</tr>
<tr>
<td>3054</td>
<td>Health Heart Rate</td>
<td>...</td>
<td>modules/health_heart_rate.txt#health</td>
</tr>
</tbody>
</table>

Who was I Zoom'ing with?
Who was I Zoom’ing with?

• Deep down into multiple levels of binary plist inception...
• Verify with Zoom or Twitter app data
Lee sliding into my Zoom session...

```
{"ACCOUNT": "E:oompa@csh.rit.edu",
"CONTACT ID": "",
"DATE DELIVERED": "N/A",
"DATE READ": "2020-11-16 20:25:57",
"FILENAME": "null",
"IS DELIVERED": 1,
"IS FROM ME": 0,
"MESSAGE": "And I was able to mount the evidence file. Hope I didn’t just cursed everything", "MESSAGE DATE": "2020-11-16 20:10:47",
"MIME TYPE": "null",
"SERVICE": "iMessage",
"TOTAL BYTES": "null",
"TRANSFER TYPE": null
}

"BUNDLE ID": "com.apple.MobileSMS",
"DAY OF WEEK": "Monday",
"DEVICE ID (HARDWARE UUID)": "null",
"END": "2020-11-16 20:10:47",
"ENTRY CREATION": "2020-11-16 20:10:48",
"GMT OFFSET": -5,
"ID": "B8060292-B916-49E7-B5E8-936864D7FE16",
"NOTIFICATION TYPE": "Receive",
"START": "2020-11-16 20:10:47",
"UUID": "EEE05CDB-A2A6-415C-88B8-C6776998EA1BF",
"ZMETADATAHASH": "a66d502d0b0643cd9c2f0cd711925584",
"ZOBJECT TABLE ID": 189054
```
...I really was there for a reason!
What about activity other devices?

- Screen Time, Web Visits/Usage, Notifications, App Usage
Bonus Round!
*Checks Time*
Stopped to Take a Selfie

<table>
<thead>
<tr>
<th>Key</th>
<th>Activity</th>
<th>Output</th>
<th>Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-11-16 14:29:25</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:29:25</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:29:41</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:29:41</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:34:27</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:34:27</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:34:38</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:34:38</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:34:38</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:34:39</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:34:53</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:34:54</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:34:54</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:34:54</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:34:57</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:34:57</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:34:58</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:41:08</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:41:08</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:41:09</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:41:09</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:41:09</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:41:09</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:41:09</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
<tr>
<td>2020-11-16 14:41:09</td>
<td>Camera State</td>
<td>...</td>
<td>tmp_apollo... modules/powerlog_camera_st</td>
</tr>
</tbody>
</table>

```json
```
Reviewed and deleted those selfies...
Potential 3rd Party App Calls in Call History

```
"ADDRESS": "Zoom Meeting",
"CALL TYPE": 0,
"DURATION (IN MINUTES)": 15.9210706671079,
"DURATION (IN SECONDS)": 955.264240026474,
"ISO COUNTRY CODE": null,
"LOCATION": null,
"ORIGINATED": 1,
"SERVICE PROVIDER": "BJ4HAAB9B3.us.zoom.video meetings",
"TIMESTAMP": "2020-11-16 20:00:48",
"WAS ANSWERED": 0,
"ZCALLRECORD TABLE ID": 71
```
Time to head home…
Dictating text messages to Lee (not via Siri)
Was I speeding or using non-hands free apps?
<table>
<thead>
<tr>
<th>Key</th>
<th>Activity</th>
<th>Output</th>
<th>Database</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>2020-11-16 15:29:02</td>
<td>App Usage</td>
<td>tmp_apollo_build...modules/powerlog_app_usage.txt#{CurrentProcessor}</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>2020-11-16 15:29:03</td>
<td>Routined Location</td>
<td>tmp_apollo_build...modules/routined_cache_zrtlocationmo.txt#</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>2020-11-16 15:29:03</td>
<td>Now Playing</td>
<td>tmp_apollo_build...modules/knowledge_audio_media_nowplay.txt#{CurrentProcessor}</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>2020-11-16 15:29:03</td>
<td>App Location Usage</td>
<td>tmp_apollo_build...modules/powerlog_location_client_status.txt#{CurrentProcessor}</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>2020-11-16 15:29:04</td>
<td>Activity Level</td>
<td>tmp_apollo_build...modules/knowledge_activity_level.txt#{CurrentProcessor}</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>2020-11-16 15:29:04</td>
<td>Audio Routing</td>
<td>tmp_apollo_build...modules/powerlog_audio_routing.txt#{CurrentProcessor}</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>2020-11-16 15:29:04</td>
<td>Audio Input</td>
<td>tmp_apollo_build...modules/knowledge_audio_input_route.txt#{CurrentProcessor}</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>2020-11-16 15:29:05</td>
<td>Routined Location</td>
<td>tmp_apollo_build...modules/routined_cache_zrtlocationmo.txt#{CurrentProcessor}</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>2020-11-16 15:29:05</td>
<td>Routined Location</td>
<td>tmp_apollo_build...modules/routined_cache_zrtlocationmo.txt#{CurrentProcessor}</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>2020-11-16 15:29:06</td>
<td>Routined Location</td>
<td>tmp_apollo_build...modules/routined_cache_zrtlocationmo.txt#{CurrentProcessor}</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>2020-11-16 15:29:07</td>
<td>Telephony Activity</td>
<td>tmp_apollo_build...modules/...</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>2020-11-16 15:29:08</td>
<td>Motion State History</td>
<td>tmp_apollo_build...modules/...</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>2020-11-16 15:29:08</td>
<td>Routined Location</td>
<td>tmp_apollo_build...modules/routined_cache_zrtlocationmo.txt#{CurrentProcessor}</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>2020-11-16 15:29:08</td>
<td>Application Intents</td>
<td>tmp_apollo_build...modules/knowledge_app_intents.txt#{CurrentProcessor}</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>2020-11-16 15:29:08</td>
<td>Siri Service</td>
<td>tmp_apollo_build...modules/knowledge_siri_service.txt#{CurrentProcessor}</td>
<td></td>
</tr>
</tbody>
</table>

*APP NAME*: "Maps",
*APPE ID*: "com.apple.assistant_service",
"DAY OF WEEK": "Monday",
"DERIVED INTENT ID": "null",
"DEVICE ID": "null",
"DIRECTION": "0",
"DONATED BY SIRI": "0",
"END": "2020-11-16 20:29:08",
"ENTRY CREATION": "2020-11-16 20:29:08",
"GMT OFFSET": "-5",
"GROUP ID": "null",
"HANDLING STATUS": "0",
"INTENT CLASS": "Intent",
"INTENT TYPE": "3",
"INTENT VERB": "Navigation",
"ITEM ID": "C93C8F00-DCF4-41CE-806F-1C38FC846876",
"NAME": "null",
"SERIALIZED INTERACTION (HEX):"
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: @iamevltwin, 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