
iOS Location Forensics

Sarah Edwards | mac4n6.com | [@iamevltwin](https://twitter.com/iamevltwin) | oompa@csh.rit.edu



PRESENTATION SCOPE

Data Locations

- Native iOS Location Features
- 3rd Party Applications

Looking in Unexpected Files

“Creative” Keyword Searching

Ease of Data Availability

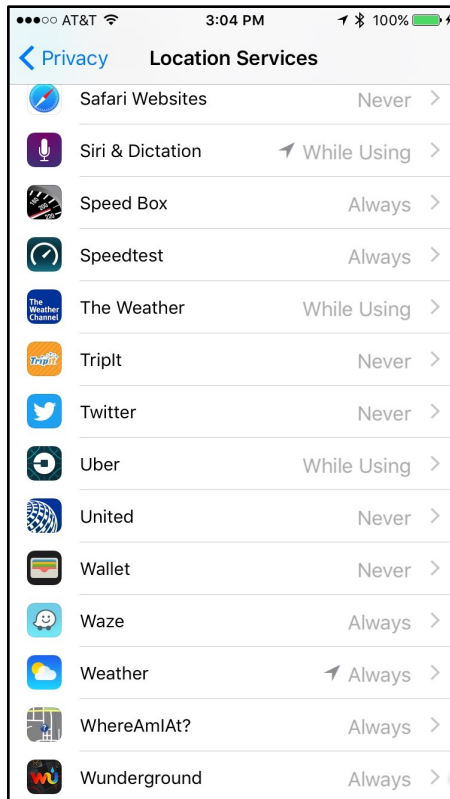
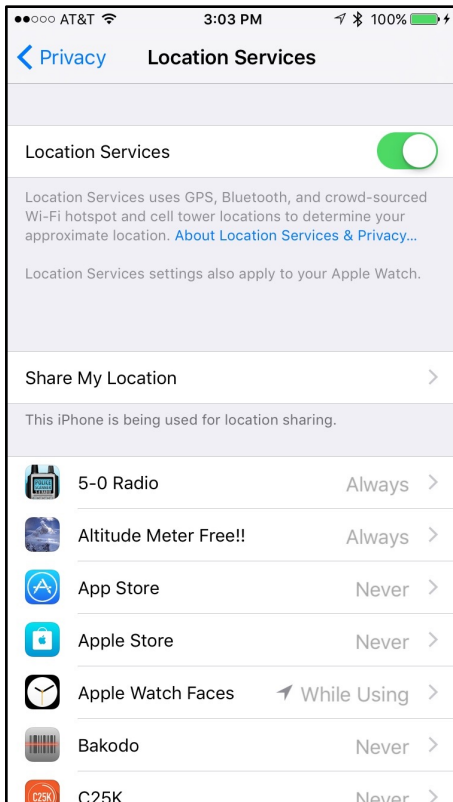
- iOS Backups/Logical Extraction
- Physical Access (ie: Jailbreak)

WHERE TO START? CLIENTS.PLIST

- Which apps are using Location Services?
 - Native iOS & 3rd Party Applications/Bundles/Frameworks/etc.
- File Paths:
 - Backup: /root/Library/Caches/locationd/clients.plist
 - Physical: /private/var/root/Library/Caches/locationd/clients.plist

Key	Type	Value
▼ Root	Dictionary	(95 items)
▶ com.apple.locationd.executable-/usr/libexec/locationd	Dictionary	(1 item)
▶ com.apple.locationd.bundle-/System/Library/LocationBundles/PassbookRelevancy.bundle	Dictionary	(6 items)
▶ com.myfitnesspal.mfp	Dictionary	(7 items)
▶ com.weather.TWC	Dictionary	(10 items)
▶ com.yourcompany.SpeedBoxLite	Dictionary	(9 items)
▶ com.marriott.iphoneprod	Dictionary	(5 items)
▶ com.apple.mobileslideshow	Dictionary	(6 items)
▶ com.ookla.speedtest	Dictionary	(8 items)
▶ com.apple.PassbookUIService	Dictionary	(1 item)
▶ com.facebook.Facebook	Dictionary	(7 items)
▶ com.zillow.ZillowMap	Dictionary	(6 items)
▶ com.apple.AppStore	Dictionary	(7 items)
▶ RunKeeperPro	Dictionary	(9 items)
▶ com.wunderground.weatherunderground	Dictionary	(8 items)
▶ com.apple.springboard	Dictionary	(1 item)
▶ com.zenlabs.c25k	Dictionary	(7 items)
▶ com.google.Maps	Dictionary	(8 items)
▶ com.redfin.redfin	Dictionary	(10 items)
▶ com.apple.mobileme.fmf1	Dictionary	(7 items)
▶ com.apple.locationd.bundle-/System/Library/PrivateFrameworks/HomeKitDaemon.framework	Dictionary	(6 items)
▶ com.glympse.iphone.glympse	Dictionary	(12 items)
▶ com.apple.locationd.bundle-/System/Library/LocationBundles/MotionCalibration.bundle	Dictionary	(7 items)

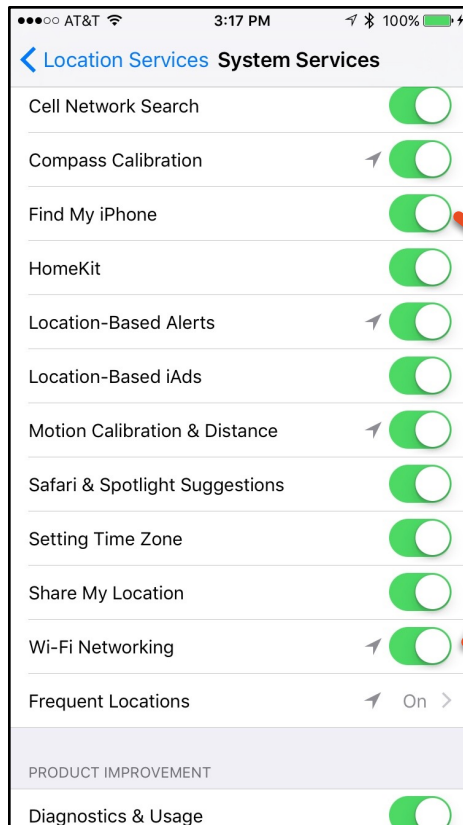
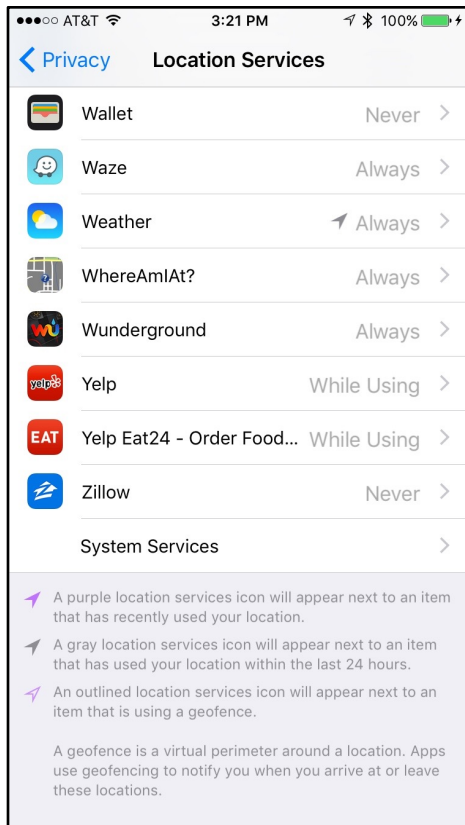
WHERE TO START? CLIENTS.PLIST – LOCATION SERVICES SETTINGS | PRIVACY | LOCATION SERVICES



Authorization:
 1 – Never
 2 – While Using
 4 – Always

Key	Type	Value
Whitelisted	Boolean	NO
BundleId	String	com.wunderground.weatherunderground
SupportedAuthorizationMask	Number	7
LocationTimeStopped	Number	484,834,287.043168
Authorization	Number	4
TrialPeriodNeedsReprompt	Boolean	NO
Registered	String	/private/var/mobile/Containers/Bundle/Application/39C72
Executable	String	/private/var/mobile/Containers/Bundle/Application/39C72

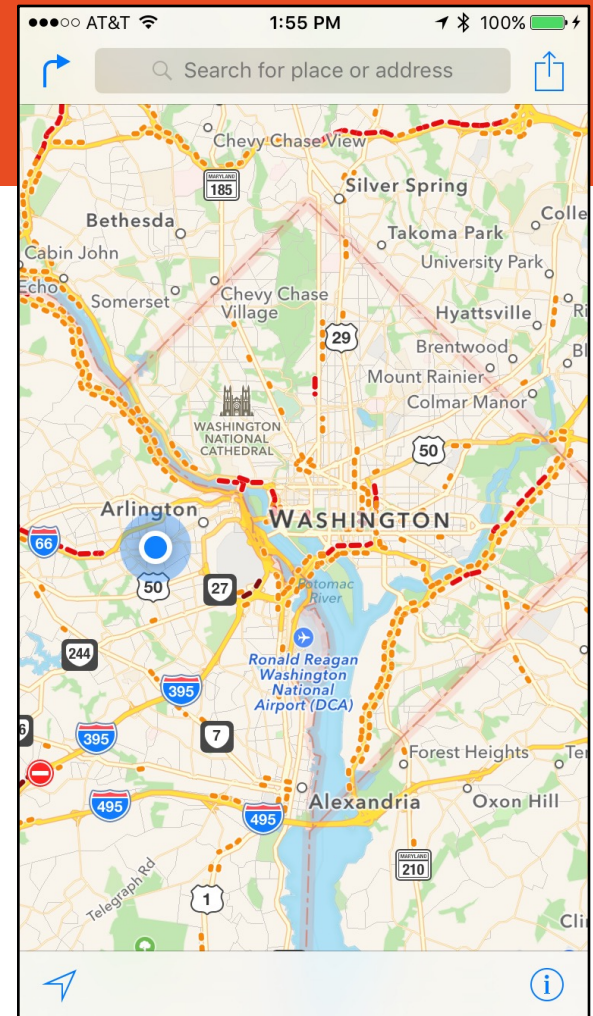
WHERE TO START? CLIENTS.PLIST – LOCATION SERVICES SETTINGS | PRIVACY | LOCATION SERVICES | SYSTEM SERVICES



```
com.apple.locationd.bundle-/System/Library/PrivateFrameworks/FindMyDevice.framework
com.apple.locationd.bundle-/System/Library/LocationBundles/AppGenius.bundle
com.apple.locationd.bundle-/System/Library/LocationBundles/NavdLocationBundleiOS.bundle
com.apple.locationd.bundle-/System/Library/PrivateFrameworks/MobileWiFi.framework
com.apple.locationd.executable-/System/Library/PrivateFrameworks/Search.framework/searchd
com.apple.locationd.bundle-/System/Library/LocationBundles/CompassCalibration.bundle
com.apple.locationd.bundle-/System/Library/LocationBundles/AppleWatchFaces.bundle
```

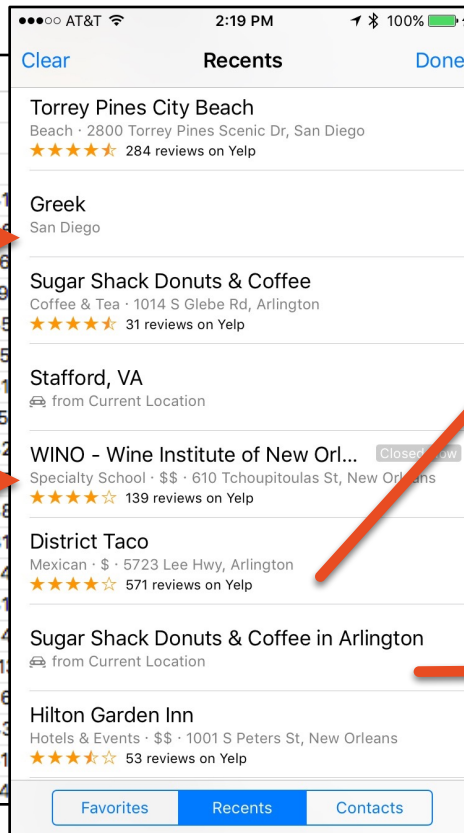
NATIVE IOS APPLE MAPS

- File Paths:
 - Backup: /mobile/Applications/com.apple.Maps/*
 - Physical: /private/var/mobile/Containers/Data/Applications/<GUID>/*
 - iCloud: SyncedPreferences
- File Types:
 - Plist Files
 - Proprietary Data Files
- Data Type
 - Bookmarks/Favorites
 - Search History
 - Last Locations / Search Query



NATIVE – APPLE MAPS – RECENTS GEOHISTORY.MAPSDATA (PLIST FILE)

Key	Type	Value
▼ Root	Dictionary	(2 items)
MSPHistoryVersion	Number	1
▼ MSPHistory	Array	(20 items)
Item 0	Data	<08021224 443641
Item 1	Data	<08031224 454375
Item 2	Data	<08021224 374546
Item 3	Data	<08011224 324239
Item 4	Data	<08021224 433045
Item 5	Data	<08031224 373235
Item 6	Data	<08031224 424431
Item 7	Data	<08011224 463735
Item 8	Data	<08031224 453632
Item 9	Data	<08021224 333033
Item 10	Data	<08031224 453438
Item 11	Data	<08031224 444531
Item 12	Data	<08021224 354244
Item 13	Data	<08031224 443031
Item 14	Data	<08031224 354334
Item 15	Data	<08021224 313231
Item 16	Data	<08021224 303636
Item 17	Data	<08031224 394643
Item 18	Data	<08021224 343331
Item 19	Data	<08011224 333644



```

36 32 39 36 ...$DE115720-59A8-4928-8476-6296
0E 12 B4 0E F2ED7692.....A!.....AB.....
30 01 3A BE .....[".."].....(.0.:.
41 69 41 58 ...com.yelp..Fs_XnZbSlRywMaPAiAX
6C 52 79 77 hNQ"%yelp5.3://biz/Fs_XnZbSlRyw
58 6E 5A 62 MaPAiAXhNQ"#yelp4://biz/Fs_XnZb
2F 46 73 5F SlRywMaPAiAXhNQ"%yelp://biz/Fs_
79 65 6C 70 XnZbSlRywMaPAiAXhNQ"*http://yelp
68 4E 51 42 .com/biz/Fs_XnZbSlRywMaPAiAXhNQ
1A 14 08 03 @...District Taco..Mexican...
6E 30 99 F9 .....?.....@*.Arlington0..
D1 02 28 00 ..... (.0.
77 4D 61 50 0:....com.yelp..Fs
6E 5A 62 57 AiAXhNQ"%yelp5.3://
2F 46 73 5F lRywMaPAiAXhNQ"#yelp
70 31 2F 2F XnZbSlRywMaPAiAXhNQ
41 69 41 58 yelp.com/biz/Fs_XnZ
49 32 17 08 hNQ.2.....?..
01 10 00 20 .....@.....@
62 53 6C 52 .....(.0.:....com.yel
2F 46 73 5F ywMaPAiAXhNQ"%yelp5
2F 2F 62 69 XnZbSlRywMaPAiAXhNQ
6C 70 3A 2F z/Fs_XnZbSlRywMaPAi
22 2A 68 74 //biz/Fs_XnZbSlRywM
79 77 4D 61 tp://yelp.com/biz/F
32 1B 68 74 PAiAXhNQB.....+17
05 65 6E 2D tp://www.districtta
  
```

```

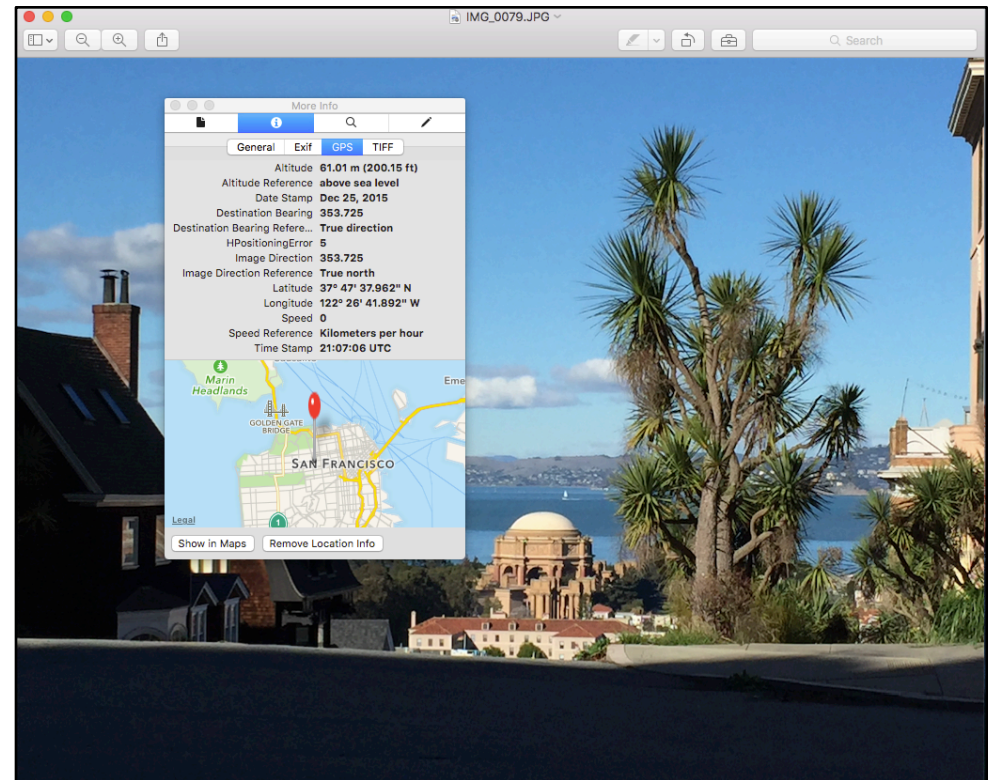
43 39 45 41 ...$5BDEA8A2-4A9D-483E-9F7A-C9EA
40 0A CF 40 176ED341.....P..A!....P..A:;.@.
C0 28 01 12 .....pC@.7Hl..FS.(.
EA 70 43 40 N.L".Current Location*$.)....pC@
12 09 C0 E2 17Hl..FS.9.....pC@A7Hl..FS.J....
48 6C 8D B1 ...pC@.7Hl..FS.....pC@.7Hl..
12 09 72 83 FS.....?.....M...r
74 61 74 65 ~4nC@.....ES."....United State
6F 6E 32 09 s..US..Virginia".VA*.Arlington2.
69 6B 65 52 Arlington:22204B.Columbia PikeR
65 62 65 20 S Glebe RdZ.1014b.1014 S Glebe
20 50 69 6B Rd..Douglas Park...Columbia Pik
65 65 32 0F e*.Sugar Shack Donuts & Coffee2.
56 41 20 20 1014 S Glebe Rd2.Arlington, VA
CA F3 D1 F8 222042.United States...=.....
20 C0 D1 02 ..... (.0.:....com.yel
20 C0 D1 02 (.0.:.... (.0.:.... (.0.:....
6D 2E 79 65 (.0.:.... (.0.:....com.ye
79 65 6C 70 lp..7cic-y9jf10nE2ldkZtd4g"%yelp
5A 74 64 34 5.3://biz/7cic-y9jf10nE2ldkZtd4
45 32 6C 64 g"%yelp4://biz/7cic-y9jf10nE2ld
66 31 4F 6E kZtd4g"%yelp://biz/7cic-y9jf10n
62 69 7A 2F E2ldkZtd4g"*http://yelp.com/biz/
08 02 08 03 7cic-y9jf10nE2ldkZtd4gB.J.....
10 E0 EA 04 .....B.J.....
6C 70 12 16 ..... (.0.:....com.yelp.
35 2E 33 3A 7cic-y9jf10nE2ldkZtd4g"%yelp5.3:
67 22 23 79 //biz/7cic-y9jf10nE2ldkZtd4g"#y
  
```

NATIVE IOS – PHOTOS PHOTO EXIF DATA

File Paths:

- Backup: /mobile/Media/DCIM/####APPLE/*
- Physical:
/private/var/mobile/Media/DCIM/####APPLE/

```
byte:100APPLE oompa$ exiftool IMG_0079.JPG | grep GPS
GPS Latitude Ref      : North
GPS Longitude Ref    : West
GPS Altitude Ref     : Above Sea Level
GPS Time Stamp       : 21:07:06
GPS Speed Ref        : km/h
GPS Speed            : 0
GPS Img Direction Ref : True North
GPS Img Direction    : 353.7246377
GPS Dest Bearing Ref : True North
GPS Dest Bearing     : 353.7246377
GPS Date Stamp       : 2015:12:25
GPS Horizontal Positioning Error: 5 m
GPS Altitude         : 61 m Above Sea Level
GPS Date/Time        : 2015:12:25 21:07:06Z
GPS Latitude         : 37 deg 47' 37.96" N
GPS Longitude        : 122 deg 26' 41.89" W
GPS Position         : 37 deg 47' 37.96" N, 122 deg 26' 41.89" W
```

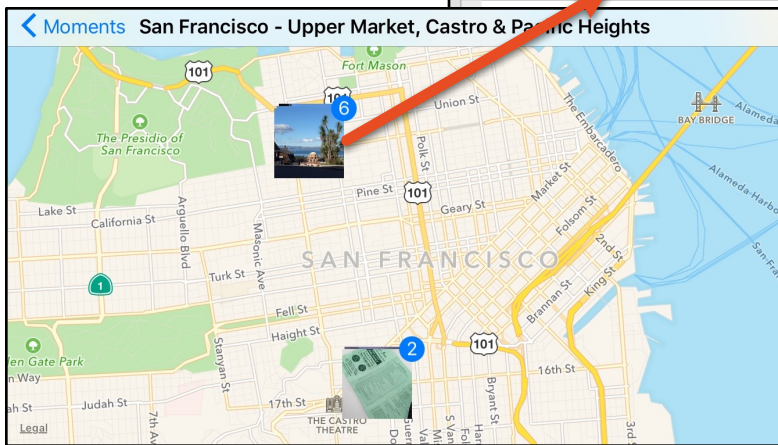


NATIVE IOS - PHOTOS PHOTOS APPLICATION DATABASE

- File Paths:
 - Backup: /mobile/Media/PhotoData/Photos.sqlite
 - Physical: /private/var/mobile/Media/PhotoData/Photos.sqlite

Table: ZADDITIONALASSETATTRIBUTES

ORIGINALASSETSUL	ZORIGINALFILENAME	ZORIGINALPATH	PUBLICGLOBALUU	ZTIMEZONENAME	ZTITLE	ZFACEREGIONS	ZORIGINALHASH	ACEANNOTATIOND	ZREVERSELOCATIONDATA
1	IMG_0079.JPG	DCIM/100APPLE	F8E1D7B3-7410-...	NULL	NULL	NULL	NULL	NULL	BLOB



Edit database cell

Import Export Binary Clear

```

0000 62 70 6c 69 73 74 30 30 d5 01 02 03 04 05 06 07 bplist00.....
0010 08 09 0a 56 69 73 48 6f 6d 65 5a 70 72 6f 76 69 ...VisHome2provi
0020 64 65 72 49 64 5b 70 72 6f 76 69 64 65 72 56 65 derid[providerVe
0030 72 5e 67 65 6f 50 6c 61 63 65 52 65 73 75 6c 74 r"geoPlaceResult
0040 57 76 65 72 73 69 6f 6e 08 54 37 36 31 38 10 09 WVersion.27618..
0050 4f 11 03 41 0a ad 02 18 39 22 11 32 37 35 39 20 O..A...9".2759
0060 42 72 6f 64 65 72 69 63 6b 20 53 74 32 e4 01 5a Broderick St2..Z
0070 11 32 37 35 39 20 42 72 6f 64 65 72 69 63 6b 20 .2759 Broderick
0080 53 74 5a 18 53 61 6e 20 46 72 61 6e 63 69 73 63 Stz.San Francisc
0090 6f 2c 20 43 41 20 20 39 34 31 32 33 5a 0d 55 6e o, CA 94123Z.Un
00a0 69 74 65 64 20 53 74 61 74 65 73 7a a5 01 0a 0d ited Statesz....
00b0 55 6e 69 74 65 64 20 53 74 61 74 65 73 12 02 55 United States..U
00c0 53 1a 0a 43 61 6c 69 66 6f 72 6e 69 61 22 02 43 S..California".C
00d0 41 2a 0d 53 61 6e 20 46 72 61 6e 63 69 73 63 61 A".San Francisco
00e0 32 0d 53 61 6e 20 46 72 61 6e 63 69 73 63 61 3a 2.San Francisco:
00f0 05 39 34 31 32 33 42 0f 50 61 63 69 66 69 63 20 .94123B.Pacific
0100 48 65 69 67 68 74 73 52 0c 42 72 6f 64 65 72 69 HeightsR.Broderi
0110 63 6b 20 53 74 5a 04 32 37 35 39 62 11 32 37 35 ck Stz.2759b.275
0120 39 20 42 72 6f 64 65 72 69 63 6b 20 53 74 6a 04 9 Broderick Stj.
0130 33 38 30 33 8a 01 0f 50 61 63 69 66 69 63 20 48 3803...Pacific H
    
```

NATIVE IOS – WALLET / PASSES PKPASS FILES

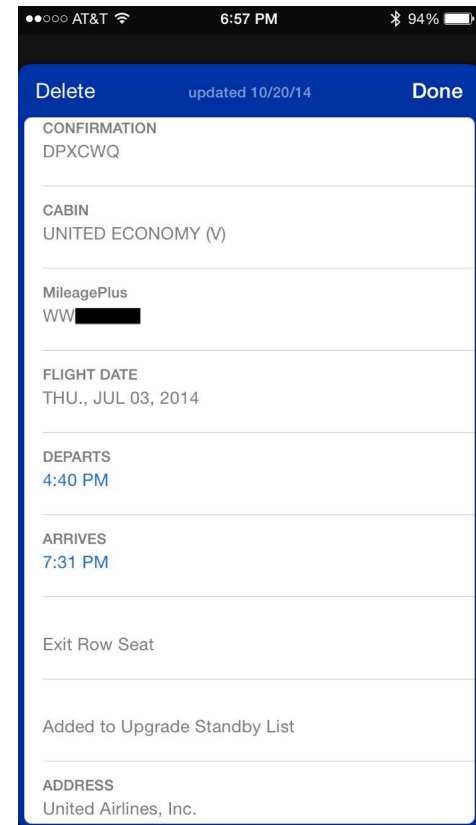
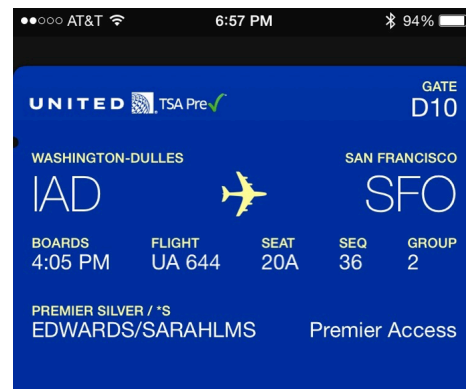
- File Paths:

- Backup:

/mobile/Library/Passes/Cards/*

- Physical:

/private/var/mobile/Library/Passes
/Cards/*



```
miPhone5s:/private/var/mobile/Library/Passes/Cards root# pwd
/private/var/mobile/Library/Passes/Cards
miPhone5s:/private/var/mobile/Library/Passes/Cards root# ls -l
total 0
drwxr-xr-x 2 mobile mobile 204 Jul 16 2014 0-cM9ac3eFNA9iCZ0mbkGqaN10E=.cache
drwxr-xr-x 2 mobile mobile 306 Jul 16 2014 0-cM9ac3eFNA9iCZ0mbkGqaN10E=.pkpass
drwxr-xr-x 2 mobile mobile 204 Jul 26 2014 07DvKQIpN4QMgdtfi5miHNJWHmQ=.cache
drwxr-xr-x 2 mobile mobile 306 Jul 26 2014 07DvKQIpN4QMgdtfi5miHNJWHmQ=.pkpass
drwxr-xr-x 2 mobile mobile 204 Aug 10 2014 0cxFFcwnrkg7WihgBX07v4qr7I=.cache
drwxr-xr-x 2 mobile mobile 408 Aug 10 2014 0cxFFcwnrkg7WihgBX07v4qr7I=.pkpass
drwxr-xr-x 2 mobile mobile 204 Apr 23 2014 8D3SZgmt2S5FQ2hS+9ZUTjvqVm8=.cache
drwxr-xr-x 2 mobile mobile 408 Apr 2 2014 8D3SZgmt2S5FQ2hS+9ZUTjvqVm8=.pkpass
```

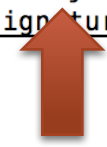
NATIVE IOS – WALLET / PASSES

PASS.JSON

```
{
  "boardingPass": {
    "transitType": "PKTransitTypeAir",
    "auxiliaryFields": [
      {
        "label": "BOARDS",
        "key": "boardingTime",
        "value": "4:05 PM"
      },
      {
        "label": "FLIGHT",
        "key": "flight",
        "value": "UA 644"
      },
      {
        "label": "SEAT",
        "key": "seat",
        "value": "20A"
      },
      {
        "label": "SEQ",
        "key": "seq",
        "value": "36"
      },
      {
        "label": "GROUP",
        "key": "group",
        "value": "2"
      }
    ]
  },
}
```

```
-rwxr-x--x 1 oompa staff 11264 Oct 26 2014 Thumbs.db
-rwxr-x--x 1 oompa staff 6150 Oct 26 2014 footer.png
-rwxr-x--x 1 oompa staff 13133 Oct 26 2014 footer@2x.png
-rwxr-x--x 1 oompa staff 2870 Oct 26 2014 icon.png
-rwxr-x--x 1 oompa staff 4406 Oct 26 2014 icon@2x.png
-rwxr-x--x 1 oompa staff 5467 Oct 26 2014 logo.png
-rwxr-x--x 1 oompa staff 8842 Oct 26 2014 logo@2x.png
-rwxr-x--x 1 oompa staff 448 Oct 26 2014 manifest.json
-rwxr-x--x 1 oompa staff 3551 Oct 26 2014 pass.json
-rwxr-x--x 1 oompa staff 3239 Oct 26 2014 signature
```

```
"headerFields": [
  {
    "label": "GATE",
    "key": "gate",
    "value": "D10",
    "changeMessage": "Your gate has changed to %@"
  }
],
"primaryFields": [
  {
    "label": "WASHINGTON-DULLES",
    "key": "origin",
    "value": "IAD"
  },
  {
    "label": "SAN FRANCISCO",
    "key": "destination",
    "value": "SFO"
  }
]
```

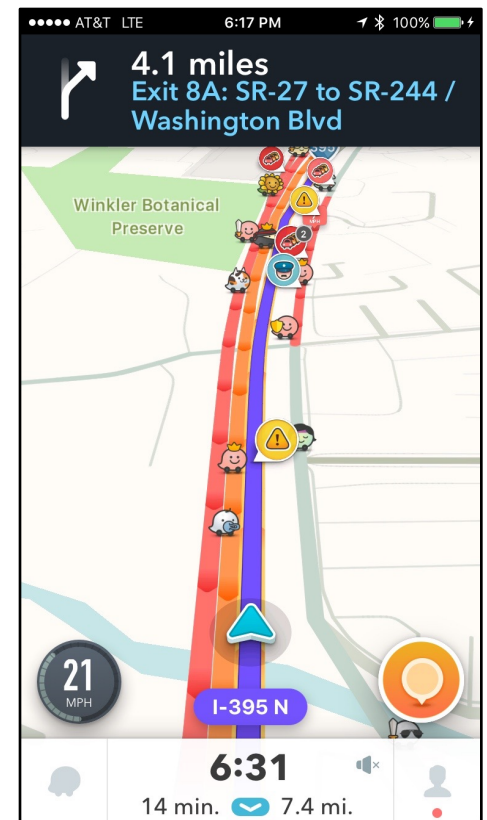
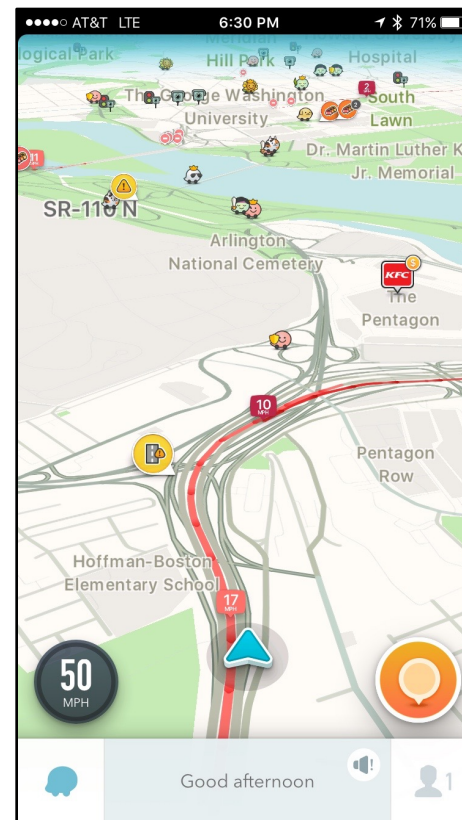


```
"secondaryFields": [
  {
    "label": "PREMIER SILVER / *S",
    "key": "passenger",
    "value": "EDWARDS/SARAHLMs"
  },
  {
    "key": "status",
    "value": "Premier Access"
  }
],
"backFields": [
  {
    "label": "CONFIRMATION",
    "key": "confirmation",
    "value": "DPXCWQ"
  },
  {
    "label": "CABIN",
    "key": "cabin",
    "value": "UNITED ECONOMY (V)"
  },
  {
    "label": "MileagePlus",
    "key": "mileagePlusNumber",
    "value": "Ww [REDACTED]"
  },
  {
    "label": "FLIGHT DATE",
    "key": "flightDate",
    "value": "THU., JUL 03, 2014"
  },
  {
    "label": "DEPARTS",
    "key": "departTime",
    "value": "4:40 PM"
  },
  {
    "label": "ARRIVES",
    "key": "arriveTime",
    "value": "7:31 PM"
  },
  {
    "key": "exitRow",
    "value": "Exit Row Seat"
  }
]
```

3RD PARTY APPS

WAZE

- Crowdsourced Traffic App
- Location Data:
 - /Documents/session (Plaintext File)
 - /Documents/user.db (SQLite Database)

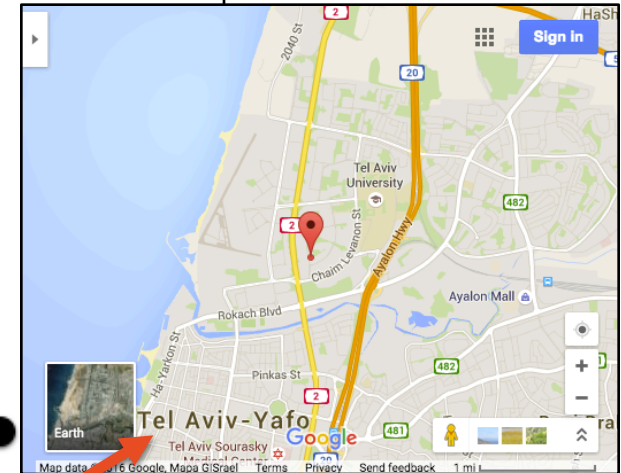


3RD PARTY APPS – WAZE

/Documents/session

- /Documents/session (Plaintext File)
 - “Parking” Position
 - Address Position
 - Current Position
 - Home/Work Positions
 - Waypoints
 - Etc.
- Long,Lat (w/o Decimals)
- Default Location:
 - “34794810, 32106010”
 - 32.106010, 34.794810 = Tel Aviv, Israel



```
byte:Documents oompa$ cat session | grep -i position
Parking.Dest position: 0,0
Parking.Last GPS position: 0,0
GPS.Position: -771[REDACTED],388[REDACTED]
Destination.Position: 0, 0
Departure.Position: 0, 0
Address.Position: -771[REDACTED],388[REDACTED]
Selection.Position: -774[REDACTED],384[REDACTED]
Hold.Position: 34794810, 32106010
HoldLock.Position: 34794810, 32106010
Location.Position: -771[REDACTED],388[REDACTED]
ORIG_GPS.Position: -771[REDACTED],388[REDACTED]
Marked_Location.Position: 34794810, 32106010
Alt-Routes.Position: 34794810, 32106010
AlertSelection.Position: -771[REDACTED],387[REDACTED]
AlertSelectionGps.Position: -771[REDACTED],387[REDACTED]
WayPoint.Position: 0, 0
Parked.Position: -771[REDACTED],388[REDACTED]
preview_pin.Position: -772[REDACTED],386[REDACTED]
RouteOverview.Position: 34794810, 32106010
VenueMapPin.Position: 0, 0
Home.Position: -771[REDACTED],388[REDACTED]
Work.Position: 34794810, 32106010
Navigation.Last position: -771[REDACTED],388[REDACTED]
Navigation.Last waypoint position: 0, 0
```



3RD PARTY APPS – WAZE

/Documents/user.db

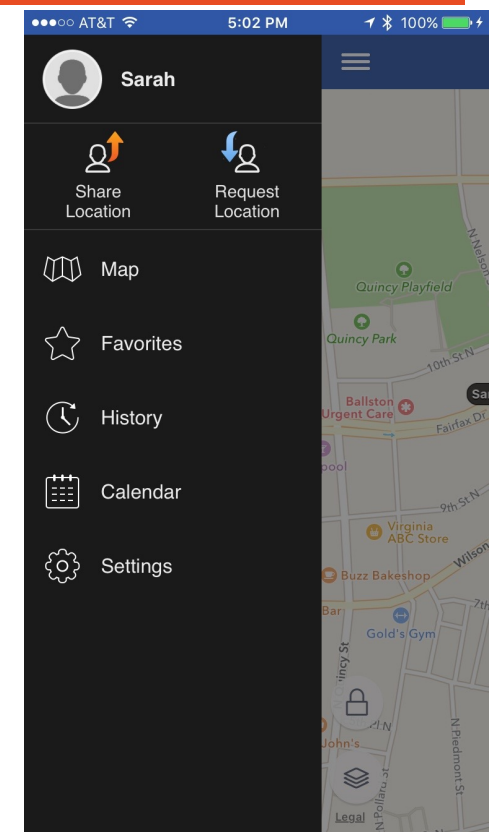
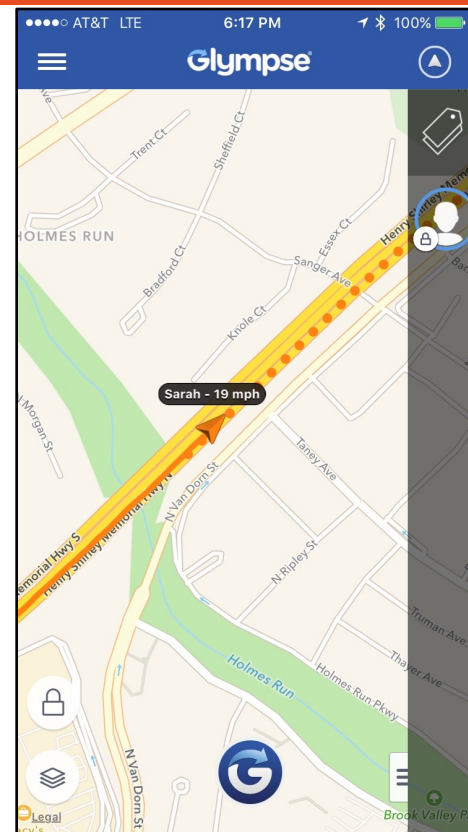
- /Documents/user.db (SQLite Database)
 - Places Table
 - Home / Work (Correlate with Favorites Table)
 - Searches (Correlate with Recents Table)

Table:  

id	name	street	city	state	country	house	longitude	latitude	venue_id	created_time	
<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	
1	1	<input type="text" value="REDACTED"/>	Arlington	Virginia	US	<input type="text" value="REDACTED"/>	-771 <input type="text" value="REDACTED"/>	388 <input type="text" value="REDACTED"/>	venues.1854...	1461945578	
2	2	Wegman's - Potomac Town Center	Dining Way	Neabsco	VA	US	14801	-77289095	38631001	venues.1852...	1463001807

3RD PARTY APPS GLYMPSE

- Location Sharing App
- Location Data:
 - /Documents/Glympse/places_v2.dat
 - /Documents/ImageCache/glympse_place_<lat>_<long>_<Name>.jpg

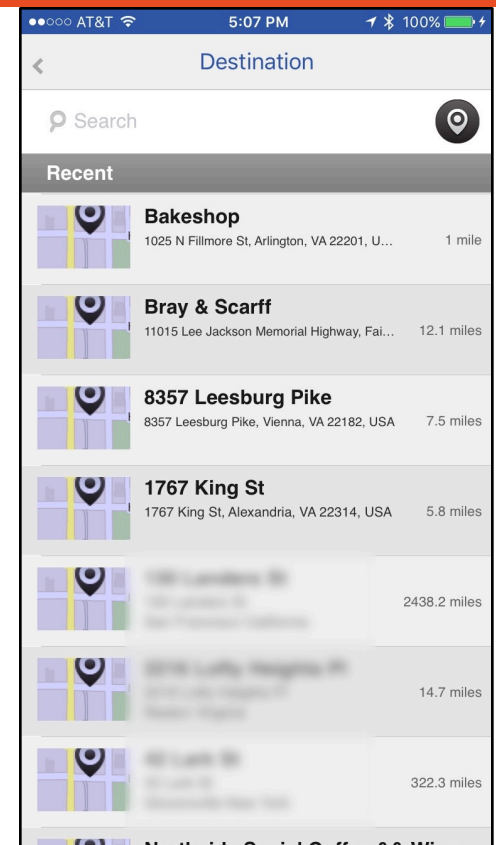


3RD PARTY APPS – GLYMPSE

/Documents/Glympse/places_v2.dat

- /Documents/Glympse/places_v2.dat (JSON)
- Recents & Searches

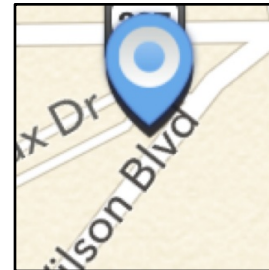
```
{
  "al1": "1025.N.Fillmore.St,.Arlington,.VA.22201,.United.States",
  "ln": -77.092659,
  "lt": 38.885443,
  "nm": "Bakeshop"
},
{
  "al1": "11015.Lee.Jackson.Memorial.Highway,.Fairfax,.VA.22031,.United.States",
  "imgurl": "glympse-place:38.852007_-77.325539_Bray.&.Scarff.jpg",
  "ln": -77.325539,
  "lt": 38.852007,
  "nm": "Bray.&.Scarff"
},
{
  "al1": "8357.Leesburg.Pike,.Vienna,.VA.22182,.USA",
  "imgurl": "glympse-place:38.921152_-77.234453_8357.Leesburg.Pike.jpg",
  "ln": -77.234453,
  "lt": 38.921152,
  "nm": "8357.Leesburg.Pike"
},
{
  "al1": "1767.King.St,.Alexandria,.VA.22314,.USA",
  "ln": -77.05949,
  "lt": 38.806899,
  "nm": "1767.King.St"
},
}
```



3RD PARTY APPS – GLYMPSE

/Documents/Glympse/ImageCache/*

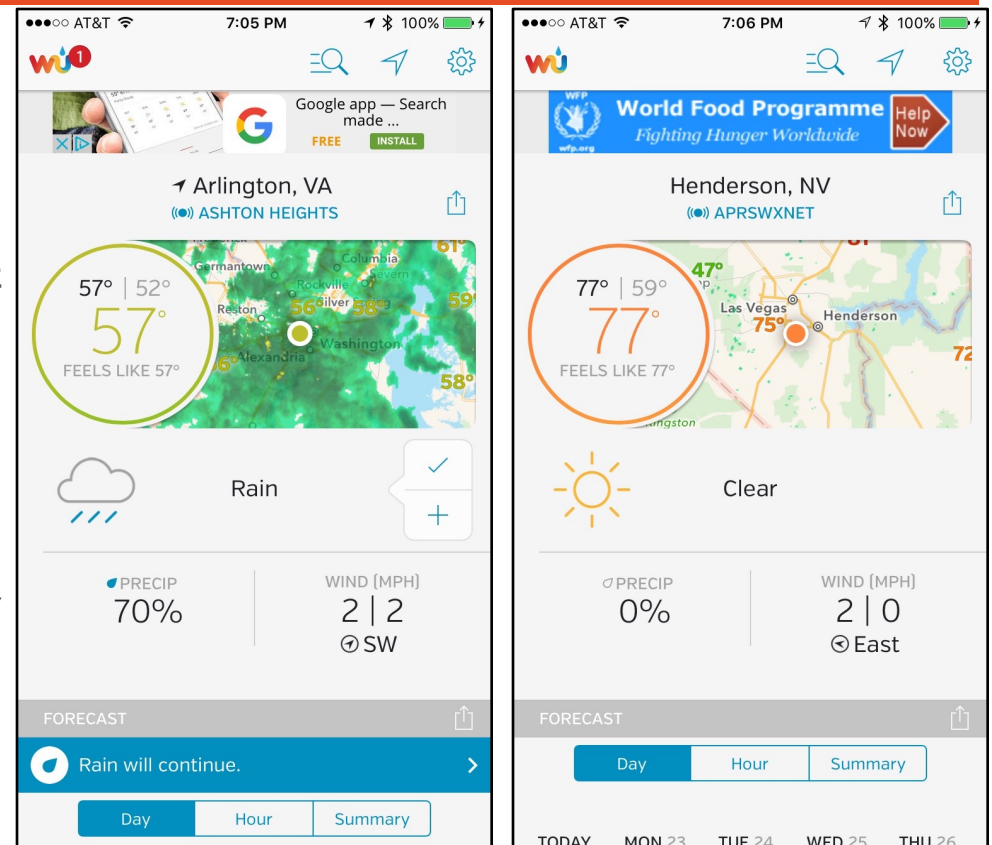
- /Documents/Glympse/ImageCache/glympse_place_<lat>_<long>_<Name>.jpg
- Recents & Searches
- Icons of Locations
- WARNING:
 - Locations not necessarily visited, just searched
- Redundant data in image_cache_index_v2.dat (JSON)



```
glympse_place_38.852007__77.325539_Bray___Scarff.jpg  
glympse_place_38.885492__77.097700_Northside_Social_Coffee____Wine.jpg  
glympse_place_38.921152__77.234453_8357_Leesburg_Pike.jpg  
glympse_place_38.9[REDACTED]__77.3[REDACTED].jpg  
glympse_place_43.993275__102.241745_Wall_Drug_Store.jpg  
glympse_place_47.620560__122.349457_Seattle_Space_Needle.jpg  
glympse_place_48.858532_2.294748_Eiffel_Tower.jpg
```

3RD PARTY APPS WUNDERGROUND

- Weather Application
- Location Data:
 - /Library/Preferences/com.wunderground.weatherunderground.plist
 - /Library/Preferences/group.com.wunderground.widgets.plist (Shared Data)
 - Snapshots Directory
 - /Library/Caches/com.wunderground.weatherunderground/cache.db



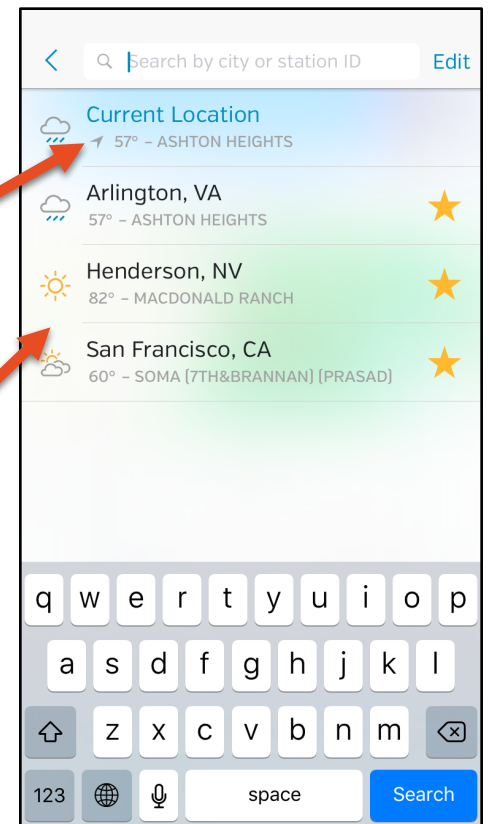
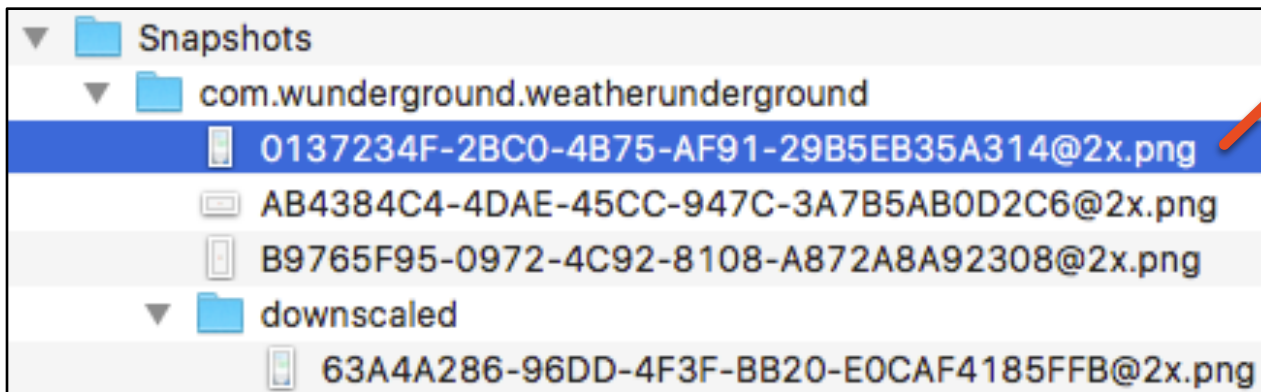
3RD PARTY APPS - WUNDERGROUND PREFERENCE FILES

- /Library/Preferences/group.com.wunderground.widgets.plist (newer)
 - lastKnownUserLocation Key
 - NSKeyedArchive Binary Plists: locationConfigList, recentLocationsList
- /Library/Preferences/com.wunderground.weatherunderground.plist (older)
 - Recents:
 - Locations can be very close to actual location
 - Other Keys
 - customEventsLocation (Location that is being viewed)
 - CurrentLocation2 (Not actual current location in my data)
 - MapViewCenterCoordinate

▼ Recents	Array	(8 items)
▼ Item 0	Dictionary	(3 items)
name	String	Kissimmee, FL
zmw	String	32830.1.99999
gps	String	28.359903,-81.557385
▼ Item 1	Dictionary	(2 items)
name	String	Orlando, Florida
zmw	String	32801.1.99999
▼ Item 2	Dictionary	(3 items)
name	String	Reston, VA
zmw	String	20192.1.99999
gps	String	38.940202,-77.367469
▼ Item 3	Dictionary	(3 items)
name	String	Oakton, VA
zmw	String	22124.2.99999
gps	String	38.917071,-77.366860
▼ Item 4	Dictionary	(3 items)
name	String	Sterling, VA
zmw	String	20102.1.99999
gps	String	38.955814,-77.447092
▼ Item 5	Dictionary	(3 items)
name	String	Seaside, CA
zmw	String	93940.8.99999
gps	String	36.597159,-121.843928
▼ Item 6	Dictionary	(3 items)
name	String	Monterey, CA
zmw	String	93942.1.99999
gps	String	36.600750,-121.895134
▼ Item 7	Dictionary	(3 items)
name	String	Stafford, VA
zmw	String	22554.1.99999
gps	String	38.468674,-77.411728

3RD PARTY APPS - WUNDERGROUND SNAPSHOTS DIRECTORY

- /Library/Caches/Snapshots/<bundleid>/*.png
- Created when:
 - App Moved to Background
 - iOS Device Locked
- Can be very useful in ALL applications!



3RD PARTY APPS - WUNDERGROUND CACHE.DB FILES

- /Library/Caches/com.wunderground.weatherunderground/cache.db
- All apps have a cache.db file
 - Sometime great info, sometimes not.
 - Cached network requests/responses from the iDevice
 - Not usually found in logical/backup acquisitions

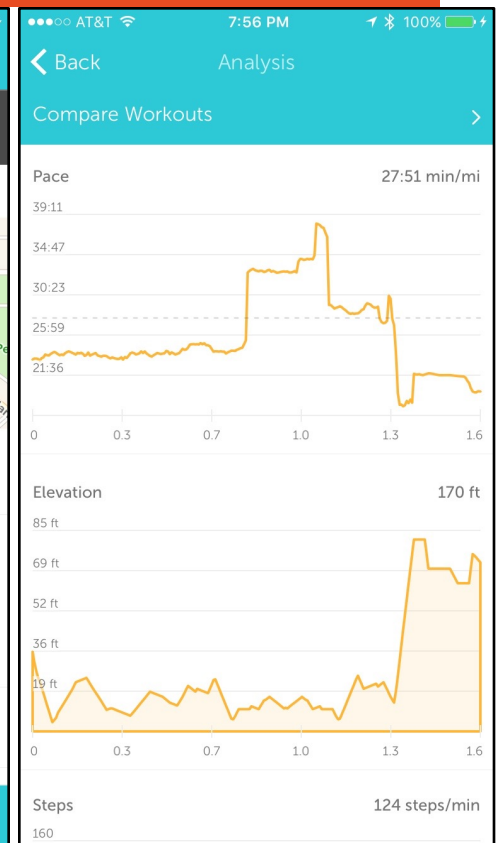
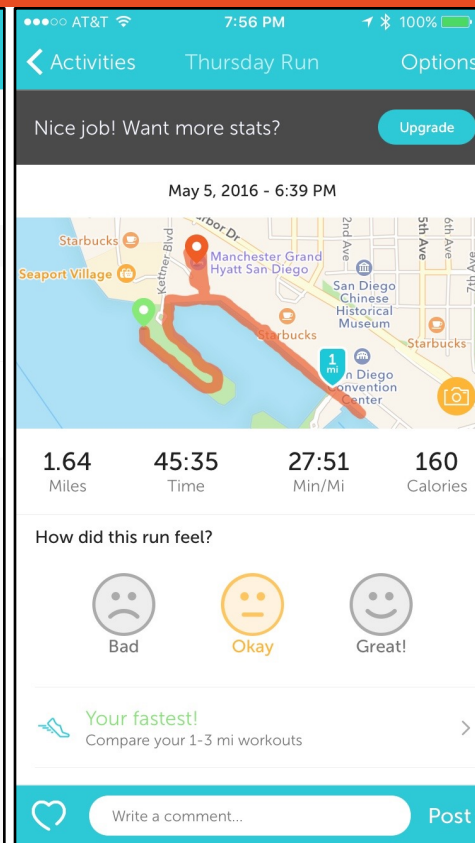
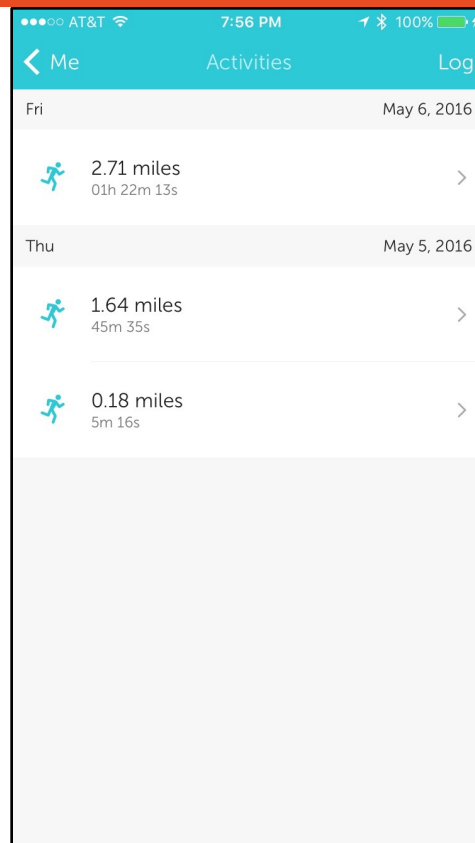
Table: cfurl_cache_response New Record

entry_ID	request_key	time_stamp
Filter	Filter	Filter
1 279	https://pagead2.googlesyndication.com/activeview?avi=B_hZ5FztCV8PwJcSNmQTgzJj4AgCdiarfsAIAABABOAGgBho&id=gmob&p=64%2C28%2C114%2C...	2016-05-22 23:05:01
2 280	http://www.wunderground.com/auto/iphone_app/geo/FavoriteConditions/index.html?q.0.q=38.8[REDACTED],-77.1[REDACTED]&q.1.q=38.8[REDACTED],-77.1[REDACTED]&	2016-05-22 23:05:07
3 281	https://api.wunderground.com/api/c39ea9c961f1a516/geolookup/q/38.8[REDACTED],-77.1[REDACTED].json?DMA=1	2016-05-22 23:05:34
4 282	https://api.wunderground.com/api/c39ea9c961f1a516/history_2016052020160523/q/38.8[REDACTED],-77.1[REDACTED].json?v=wuiapp	2016-05-22 23:05:34
5 283	https://api.wunderground.com/api/c39ea9c961f1a516/conditions/forecast10day/hourly10day/v:2.0/lang:EN/q/38.8[REDACTED],-77.1[REDACTED].json	2016-05-22 23:05:34
6 284	https://api.wunderground.com/api/c39ea9c961f1a516/currenthurricane/view.json	2016-05-22 23:05:34
7 285	https://api.wunderground.com/api/c39ea9c961f1a516/radio/q/38.8[REDACTED],-77.1[REDACTED].json?v=wuiapp	2016-05-22 23:05:34

3RD PARTY APPS

RUNKEEPER

- Exercise Tracking
- Location Data:
- /Documents/RunKeeper.sqlite



3RD PARTY APPS - RUNKEEPER

/Documents/RunKeeper.sqlite

- /Documents/RunKeeper.sqlite – Locations in 'points' Table, correlate trip_id in 'trips' Table for time frame.

Table:

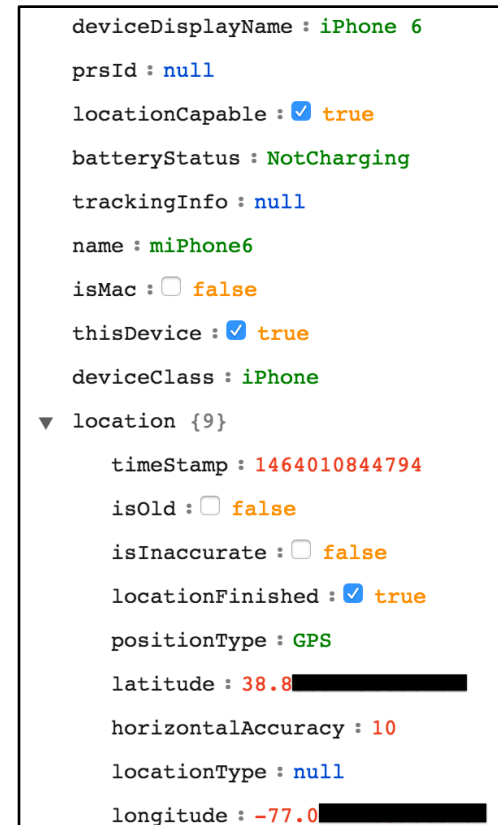
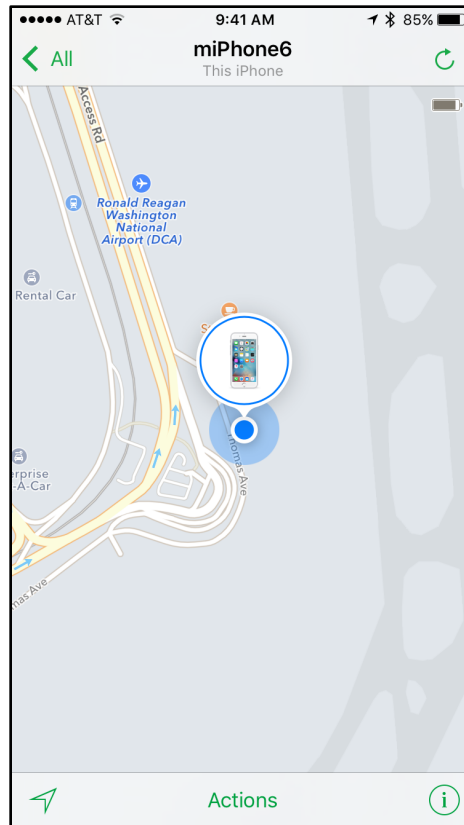
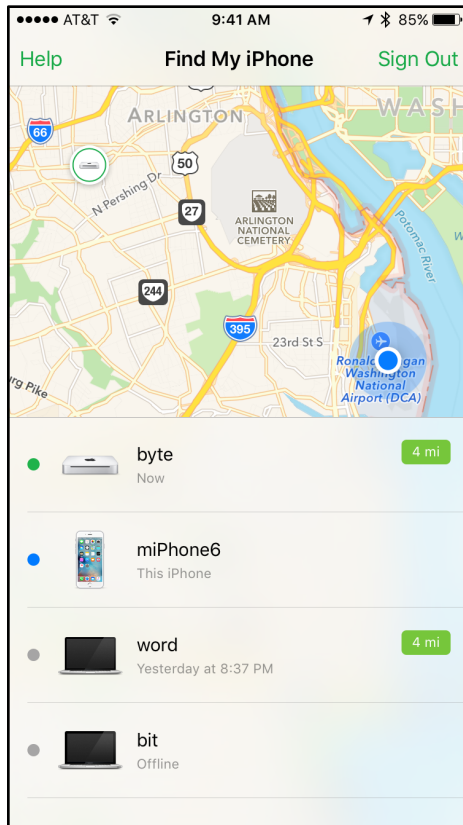
point_id	trip_id	latitude	longitude	altitude	time_interval_at_point	speed_from_last_point
Filter	2	Filter	Filter	Filter	Filter	Filter
166 474	2	32.7065251395411	-117.164410762598	3.81818181818182	1762.907	0.00600226053019198
167 475	2	32.7065891772813	-117.164489049574	3.81818181818182	1772.889	0.00576211446557199
168 476	2	32.7066429890997	-117.164586363469	3.81818181818182	17	
169 477	2	32.7067039674453	-117.164665572454	3.36363636363636	17	
170 478	2	32.7067630598626	-117.164761461427	2.90909090909091	18	
171 479	2	32.7068212302706	-117.164862211903	2.54545454545455	18	

Table:

trip_id	start_date	distance	elapsed_time
Filter	Filter	Filter	Filter
1 1	1462473169.0	289.073021347779	315.999
2 2	1462473578.0	2633.62439359492	2734.999
3 3	1462550655.0	4360.74595377222	4932.64

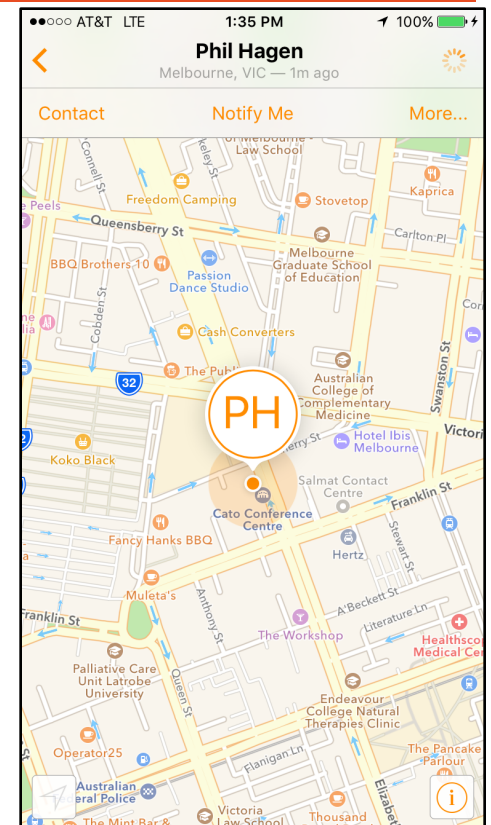
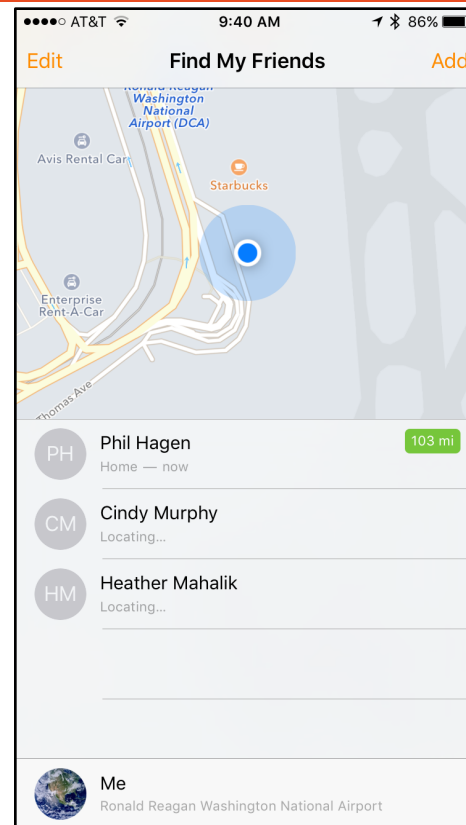
NATIVE IOS – FIND MY IPHONE

/Library/Caches/com.apple.mobileme.fmip | /Cache.db



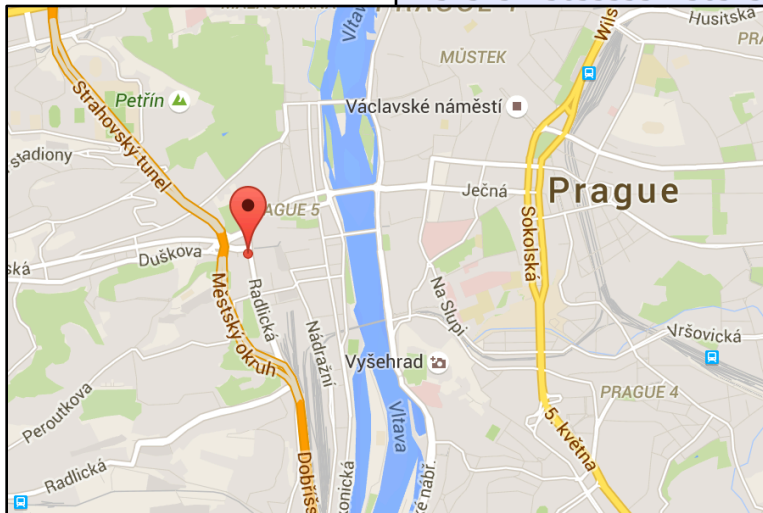
NATIVE IOS FIND MY FRIENDS

- Locate your friends
 - If they allow you.
- Data Locations:
 - /Library/Caches/com.apple.mobileme.fmfI/Cache.db



NATIVE IOS – FIND MY FRIENDS DELETED DATABASE ENTRIES IN CACHE.DB

3A5B5D2C 226D6F64 656C5665
2C223232 223A302C 22313222
223A3134 36333937 36323839



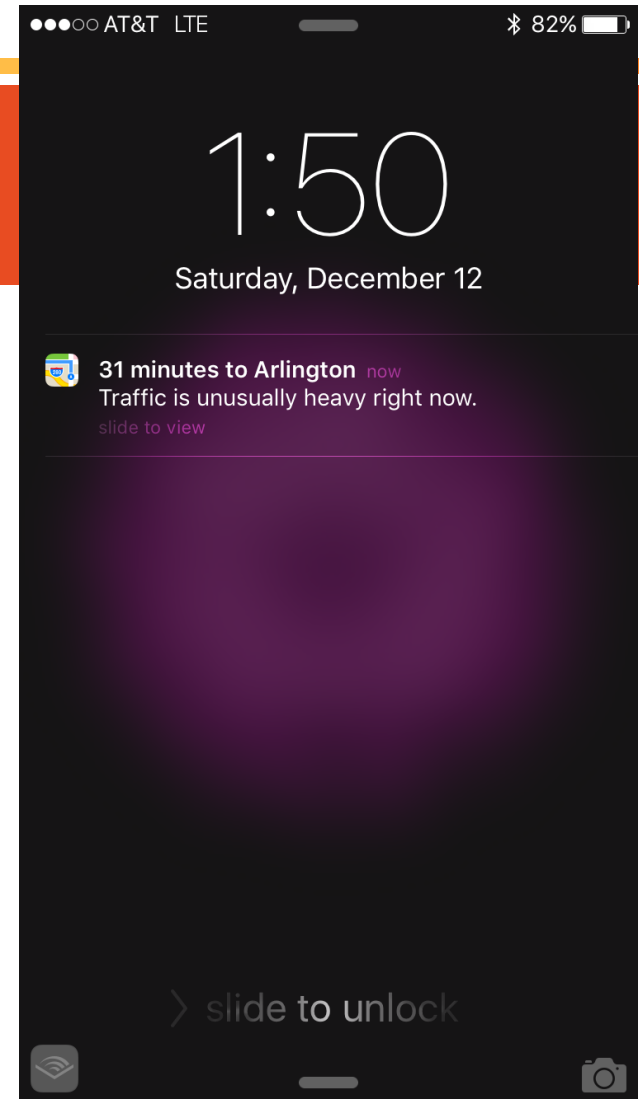
22726164 69757322 3A313030
75646522 3A31342E 34303038
69746174 696F6E46 726F6D48

```

        ô! ≤D{"pendingOffers": [], "modelVersion": "1", "fetchStatus": "200", "dataContext": {"11": 0, "22": 0, "12": 0, "13": 1463963423693, "18": 146396308776411, "19": 1, "0": 1463976289444, "1": 1463976289444, "2": 1463963078431, "5": 0, "6": 33, "8": 1463963248549, "9": "6F84028F9C69827212736D82CD8B9780", "20": 0, "21": 0, "10": 1464010805366}, "myFencesISet": [], "futureFollowing": [], "prefs": {"allowFriendRequests": "Yes", "fenceNotification": "FRIENDS", "hideLocation": "No", "shouldReceiveEmails": "Yes", "primaryEmail": "oompa@csh.rit.edu", "favorites": null}, "myFencesOthersSet": [{"address": "", "followerIds": ["MTE1MzQ3NjkzMQ~~"], "latitude": 50.07145919546399, "locationType": "", "label": "", "trigger": "exit", "type": "NotifyMe", "onetimeonly": true, "updateTimestamp": 1444245024391, "prettyAddress": "", "phoneNumbers": [], "emails": [], "streetName": "", "friendId": "", "fullAddress": {"formattedAddressLines": ["Palác Křiškovský", "Radlická 615/4", "150 00 Prague", "Czech Republic"], "country": "Czech Republic", "streetName": "Radlická", "streetAddress": "Radlická 615/4", "locality": "Prague", "administrativeArea": "Prague"}, "isOnline": true, "id": "90c987be-8690-4fad-ab16-5e4741ec3dfc", "radius": 100.0, "fenceId": null, "createdById": "1153476931", "longitude": 14.40084815694506}], "futureFollowers": [], "followers": [{"invitationFromH
    
```

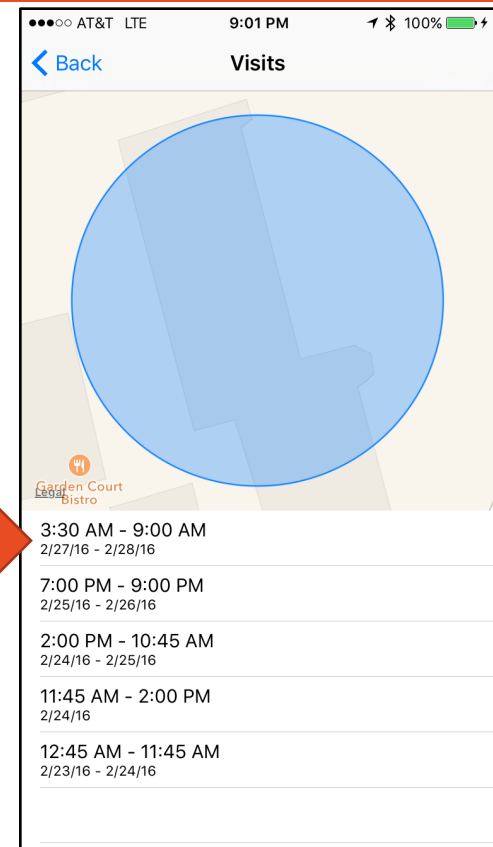
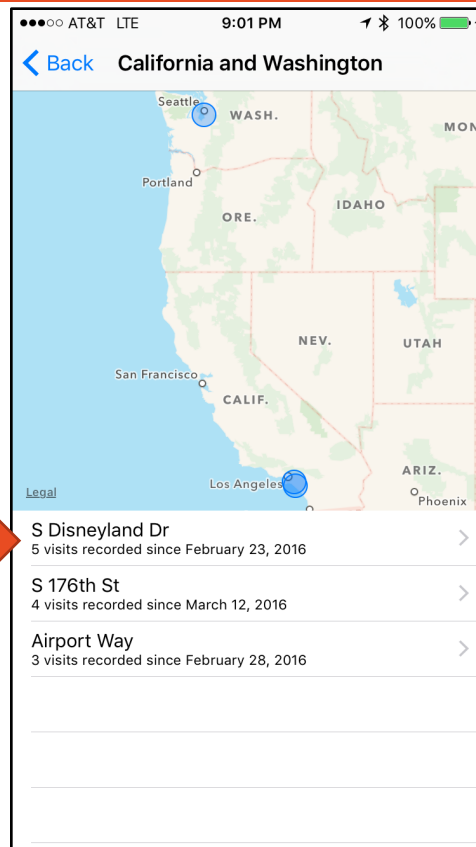
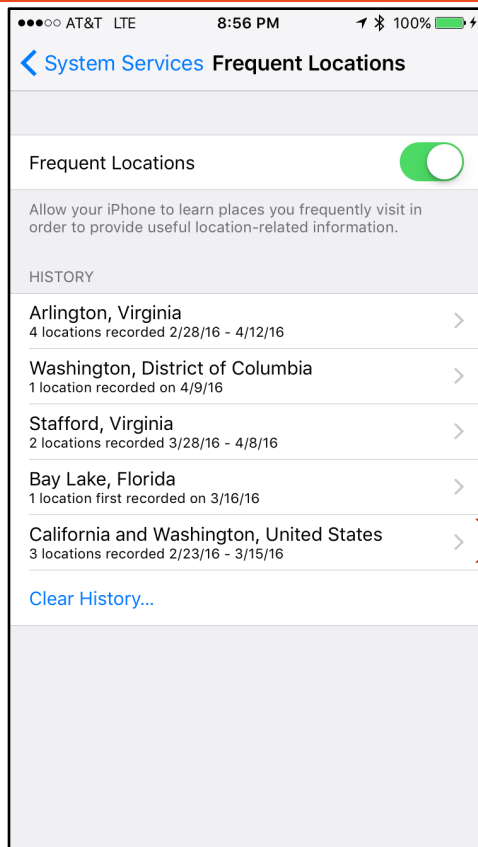
NATIVE IOS - FREQUENT LOCATIONS (ROUTINED)

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



NATIVE IOS - FREQUENT LOCATIONS (ROUTINED)

Settings | Privacy | Location Services | System Services | Frequent Locations



NATIVE IOS - LOCATIONS (ROUTINED)

/private/var/root/library/caches/locationd/cache_encryptedB.db

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

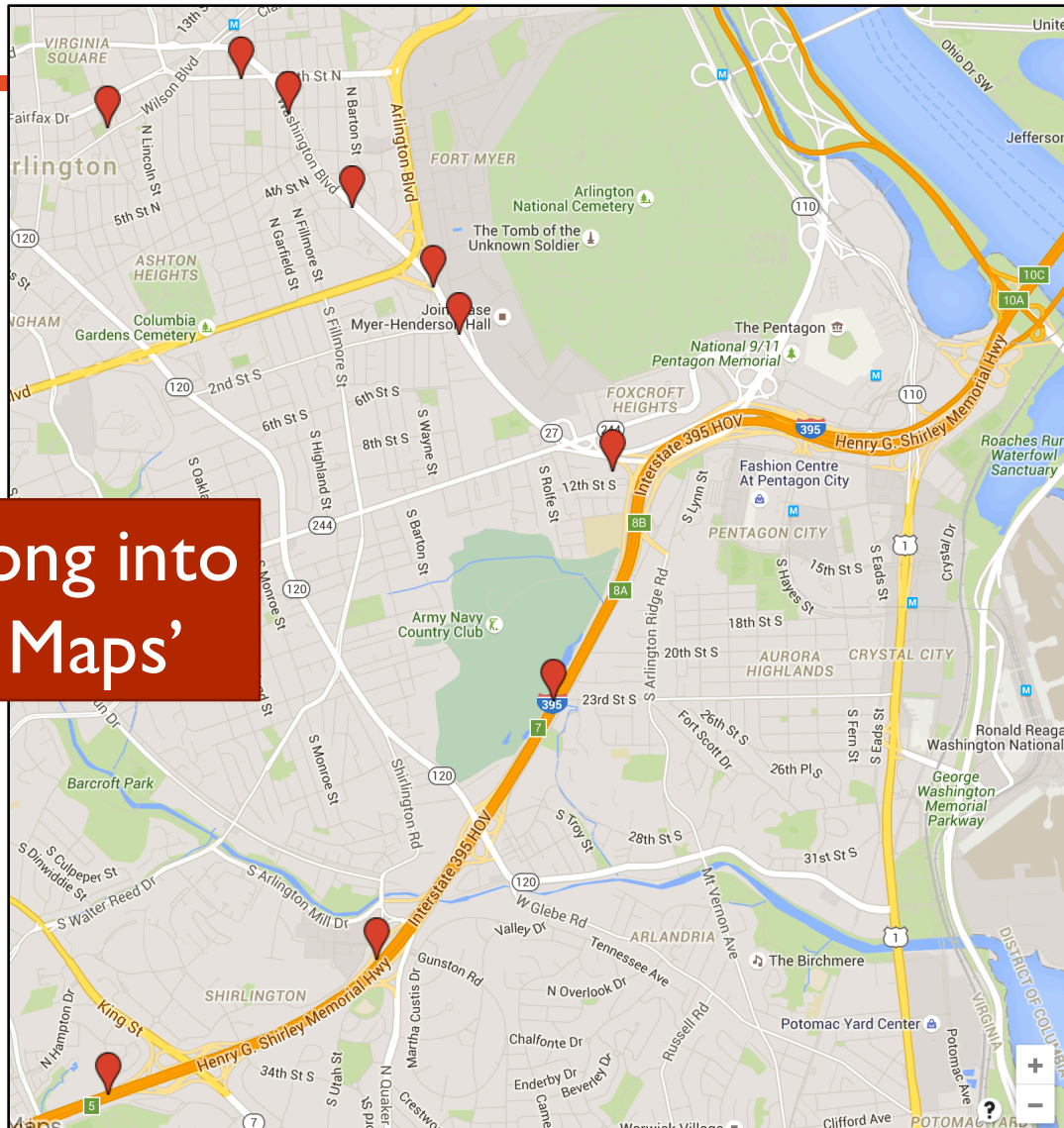
	timestamp	Latitude	Longitude	Altitude	HorizontalAccuracy	VerticalAccuracy
1	2016-04-12 08:00:30	38.8819415801995	-77.1033633413063	83.9911193847656	65.0	49.8430881839981
2	2016-04-12 08:02:09	38.8844267330494	-77.0947589586276	89.2934923546982	5.0	3.66666666666667
3	2016-04-12 08:03:07	38.8826809963573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

Data Retention:
~1 Days

Timestamps:
Accurate*

GPS Accuracy:
Close, but YMMV

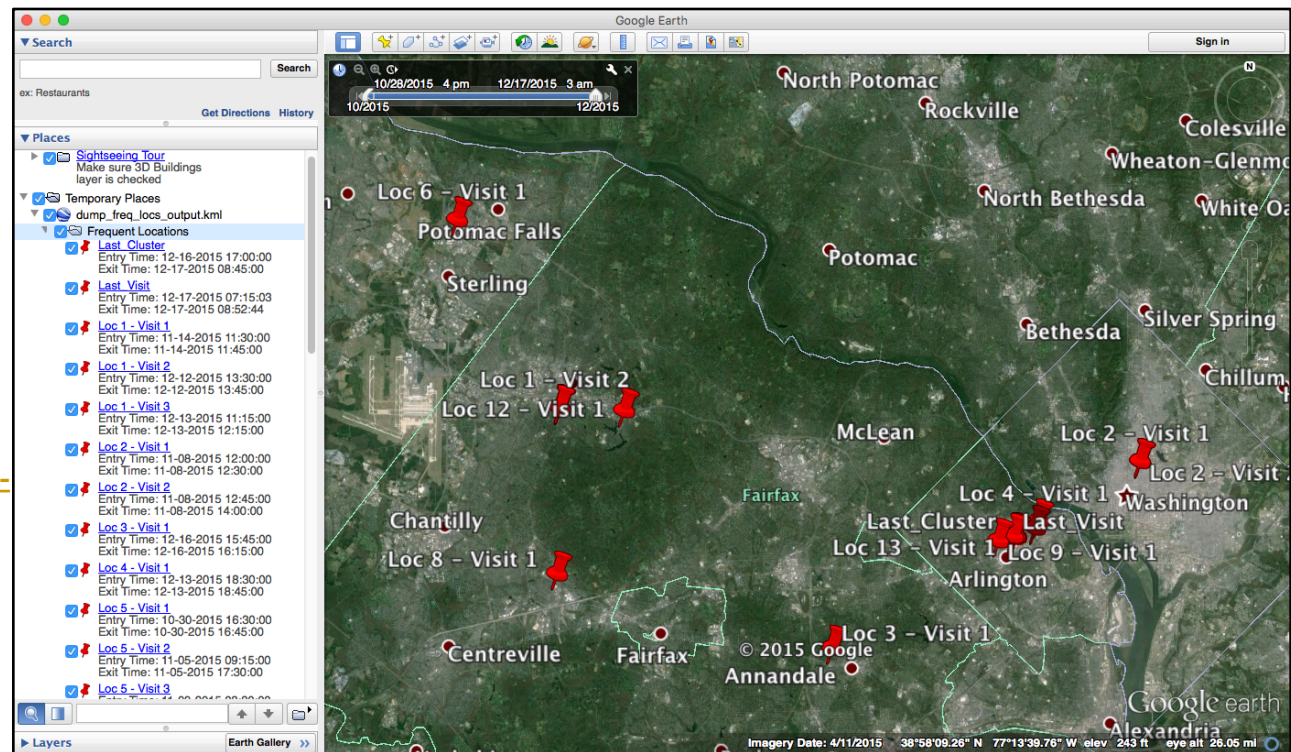
Import Lat/Long into Google 'My Maps'



NATIVE IOS - FREQUENT LOCATIONS

/private/var/mobile/library/caches/com.apple.routined/StateModel#.archive [1 or 2]

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



NATIVE IOS - FREQUENT LOCATIONS

/private/var/mobile/library/caches/com.apple.routined/StateModel#.archive [1 or 2]

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

Location BLOB Contents:
[DataPoints: 0]

Hexdump Output:
-----
00000000: 0A A5 02 18 39 22 1A 32 33 30 31 E2 80 93 32 33 ....9".2301...23
00000010: 37 37 20 43 6C 61 72 65 6E 64 6F 6E 20 42 6C 76 77 Clarendon Blv
00000020: 64 32 EB 01 5A 1A 32 33 30 31 E2 80 93 32 33 37 d2.Z.2301...237
00000030: 37 20 43 6C 61 72 65 6E 64 6F 6E 20 42 6C 76 64 7 Clarendon Blvd
00000040: 5A 14 41 72 6C 69 6E 67 74 6F 6E 2C 20 56 41 20 Z.Arlington, VA
00000050: 20 32 32 32 30 31 5A 0D 55 6E 69 74 65 64 20 53 22201Z.United S
00000060: 74 61 74 65 73 7A A7 01 0A 0D 55 6E 69 74 65 64 tatesz....United
00000070: 20 53 74 61 74 65 73 12 02 55 53 1A 08 56 69 72 States..US..Vir
00000080: 67 69 6E 69 61 22 02 56 41 2A 09 41 72 6C 69 6E ginia".VA*.Arlin
00000090: 67 74 6F 6E 32 09 41 72 6C 69 6E 67 74 6F 6E 3A gton2.Arlington:
000000A0: 05 32 32 32 30 31 42 0A 43 6F 75 72 74 68 6F 75 .22201B.Courthou
000000B0: 73 65 52 0E 43 6C 61 72 65 6E 64 6F 6E 20 42 6C seR.Clarendon Bl
000000C0: 76 64 5A 0B 32 33 30 31 E2 80 93 32 33 37 37 62 vdZ.2301...2377b
000000D0: 1A 32 33 30 31 E2 80 93 32 33 37 37 20 43 6C 61 .2301...2377 Cla
000000E0: 72 65 6E 64 6F 6E 20 42 6C 76 64 8A 01 14 43 6C rendon Blvd...Cl
000000F0: 61 72 65 6E 64 6F 6E 2D 43 6F 75 72 74 68 6F 75 arendon-Courthou
00000100: 73 65 8A 01 0A 43 6F 75 72 74 68 6F 75 73 65 4A se...CourthouseJ
00000110: 12 09 4A E9 3E A5 EF 71 43 40 11 31 6B 18 F4 94 ..J.>..qC@.1k...
00000120: 45 53 C0 58 02 70 C2 3B ES.X.p.;
None
-----
Hex Output:
[0aa5021839221a32333031e280933233373720436c6172656e646f6e20426c766432eb015a1a323
33031e280933233373720436c6172656e646f6e20426c76645a1441726c696e67746f6e2c2056412
02032323230315a0d556e69746564205374617465737aa7010a0d556e69746564205374617465731
2025531a0856697267696e6961220256412a0941726c696e67746f6e320941726c696e67746f6e3
a053232323031420a436f757274686f757365520e436c6172656e646f6e20426c76645a0b3233303
1e2809332333737621a32333031e280933233373720436c6172656e646f6e20426c76648a0114436
c6172656e646f6e2d436f757274686f7573658a010a436f757274686f7573654a12094ae93ea5ef7
1434011316b18f4944553c0580270c23b]
```

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

Visits (Entry/Exits):
  Visit Number: 1
  Entry Timestamp: 11-11-2015 12:09:33
  Exit Timestamp: 11-11-2015 13:08:03

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

NATIVE IOS - CELL LOCATIONS

/private/var/root/library/caches/locationd/
cache_encryptedA.db & lockCache_encryptedA.db

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

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

Data Retention:

~1 Week
(Varies Per Table)

Timestamps:

Accurate*

GPS Accuracy:

Within General Area (See
Next Slide)

Many Other Tables:

- CDMA
- SCDMA
- LTE
- WIFI
- "Indoor"
- Application/"WTW"

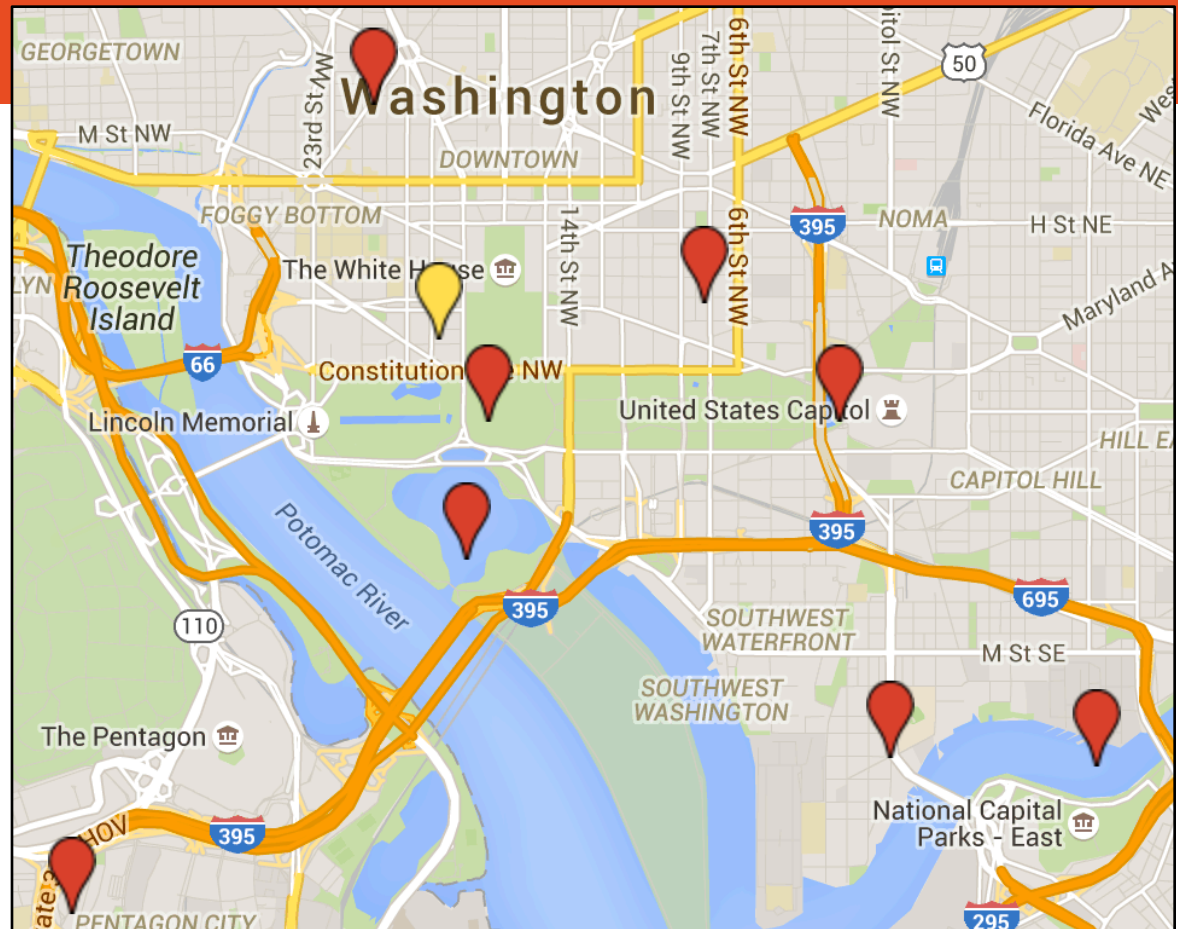
NATIVE IOS - CELL LOCATIONS

cache_encryptedA.db

Yellow Point:
My Actual Location

Red Points:
“LTE Cell Locations”

Warning:
Locations are in
general area, NOT
exact area



NATIVE IOS - WIFI LOCATIONS

/private/var/root/library/caches/locationd/cache_encryptedB.db

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

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

Data Retention:
~4 Days

Timestamps:
Accurate*

GPS Accuracy:
Within General Area

MAC Address:
Stored in Base 10

NATIVE IOS - WIFI LOCATIONS

/private/var/root/library/caches/locationd/cache_encryptedB.db

202552290261808

ASCII Unicode Hide Binary **8 10 16**

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

AND	OR	D	E	F	AC	C
NOR	XOR	A	B	C	RoL	RoR
<<	>>	7	8	9	2's	1's
X<<Y	X>>Y	4	5	6	÷	—
byte flip		1	2	3	×	+
word flip		FF	0	00	=	

0xB838614F3B30

ASCII Unicode Hide Binary **8 10 16**

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

AND	OR	D	E	F	AC	C
NOR	XOR	A	B	C	RoL	RoR
<<	>>	7	8	9	2's	1's
X<<Y	X>>Y	4	5	6	÷	—
byte flip		1	2	3	×	+
word flip		FF	0	00	=	

← → ↻ <https://wigle.net/search>

View
 Uploads
 Info
 Stats
 Tools

Network Search

Query for networks

Latitude: to: Longitude: to:

Search Radius Tolerance(+/- degrees):

BSSID/MAC:

SSID / Network Name (exact match):

SSID / Network Name (wildcards¹: % and _):

Last Observed:

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

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

Street Address: State: Zip:

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

showing records 1 to 1

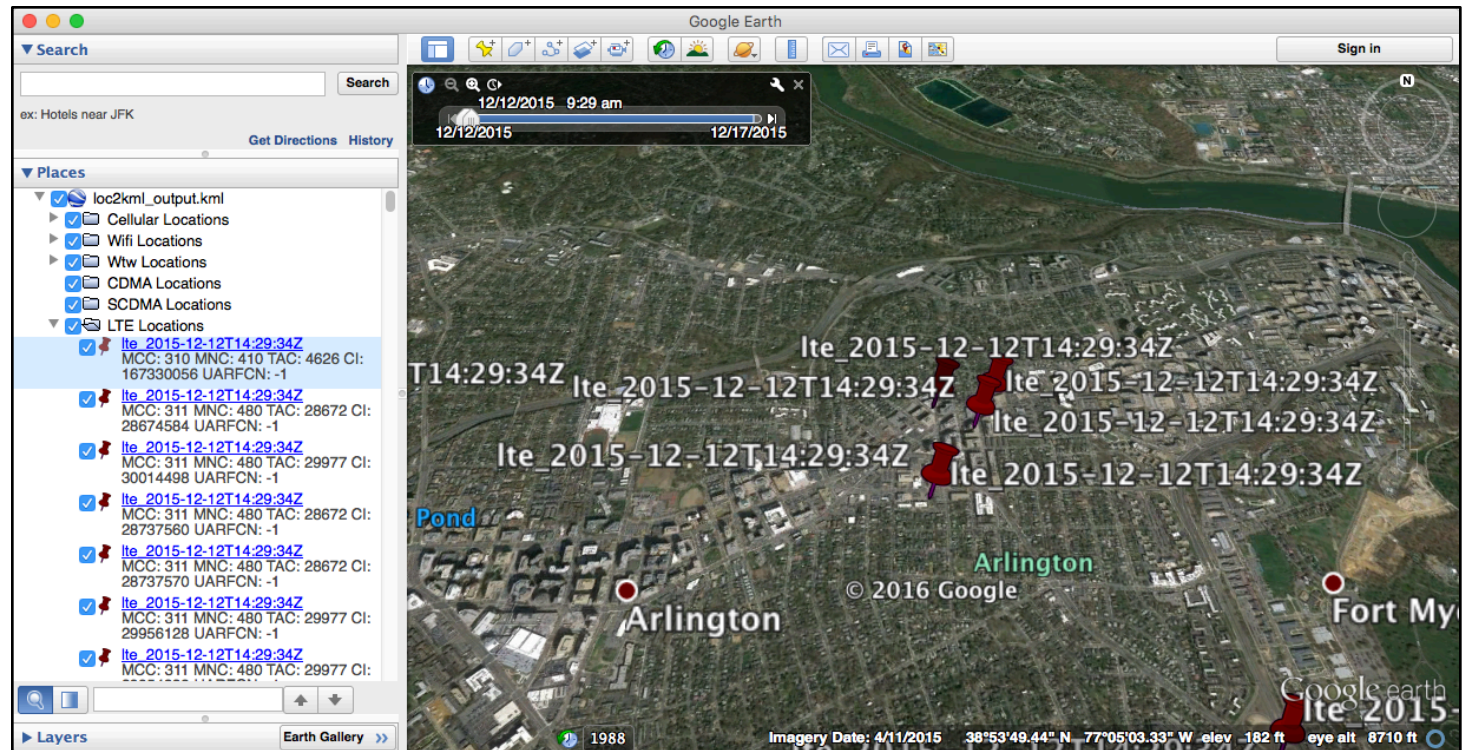
Map	Net ID	SSID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long	Channel	Bcn Int.	QoS	Found by Me	Free	Pay	Comment
map	B8:38:61:4F:3B:30	OAS_OPEN		infra	2014-10-05 15:51:05	2015-05-09 14:45:51		38.89290619	-77.03944397	1		2				<input type="button" value="add comment"/>

Network Location

Click for interactive map

LOCATIONS SCRAPER (COMING SOON!) PYTHON SCRIPT

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



WHEN ALL ELSE FAILS, KEYWORD SEARCH!

