Lucky (iOS) 13

Time To Press Your Bets

Jared Barnhart @bizzybarney
Parsons Corporation Test Engineer, Principal

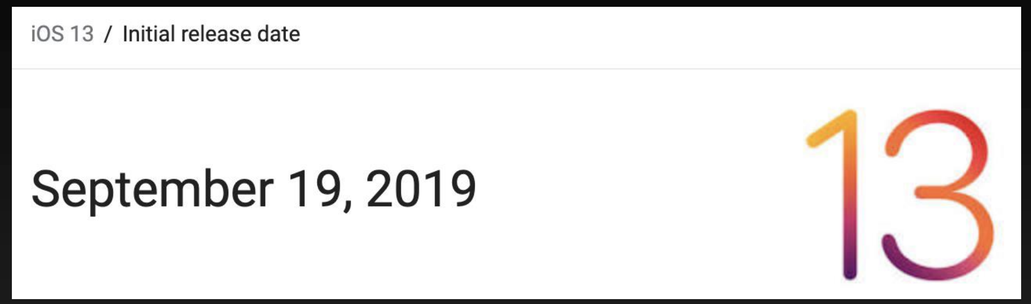
“Introducing checkm8, a permanent unpatchable bootrom exploit for hundreds of millions of iOS devices.”

@axi0mx

checkm8

Oh, the timing.

- 8 days after official iOS 13 release
- iOS research culture change
- Apple can’t fix it
- This is awesome
- @mattiaep has free resources available for more info!



Credit: regmedia.co.uk

Go All In!

Research all the things!

“Ask not what the DFIR community can do for you, ask what you can do for your DFIR community.”

JFK-ish

What does checkm8 mean for iOS forensics?

Everything.

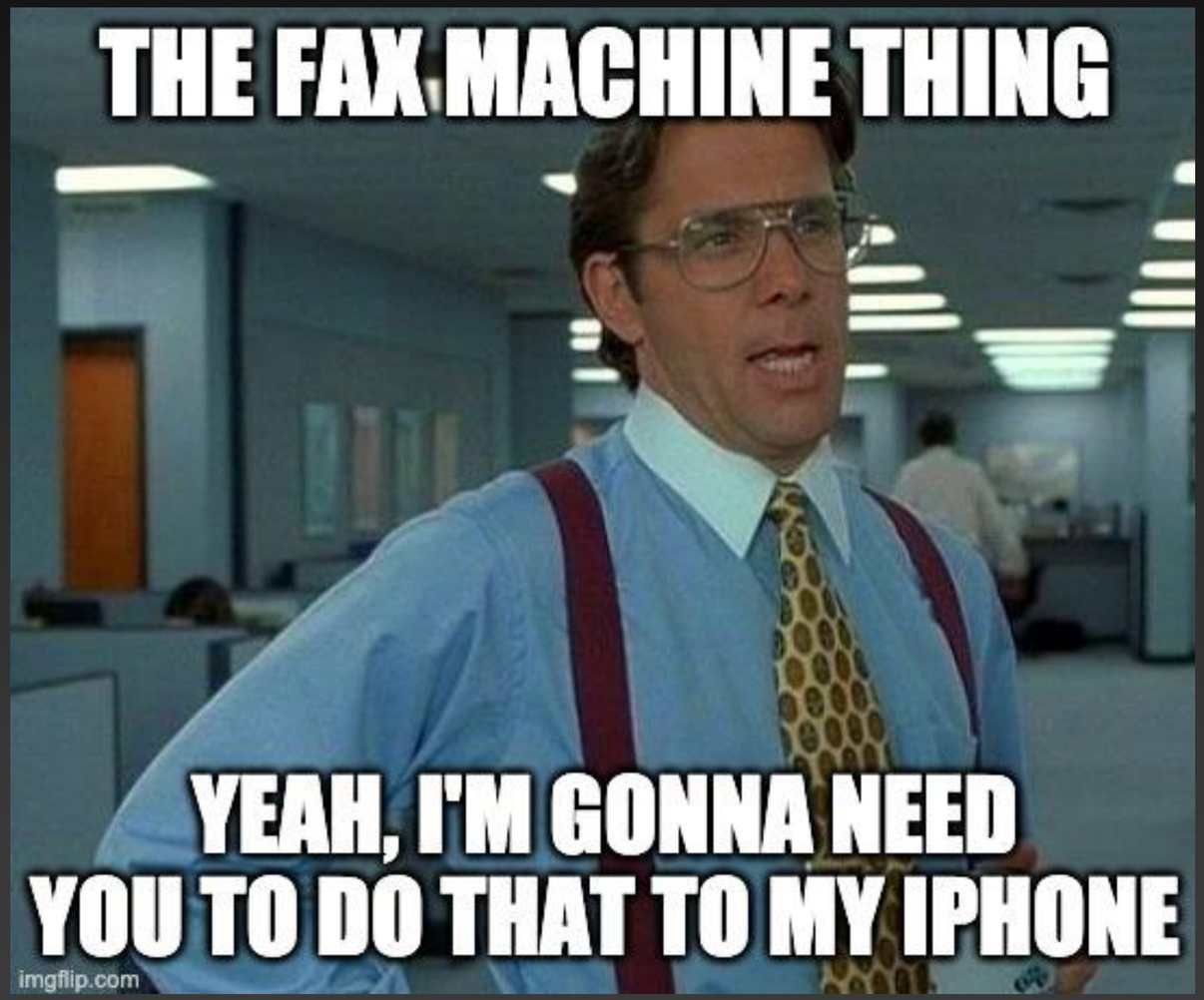
- Get an iPhone X (A11 chip) to maximize the longevity of this exploit
- Prompt and unlimited access to the full iOS file system
  - Native = Apple's applications, directories and files
  - Upon release, we have almost immediate access to jailbreak the OS
- Affordable Forensic Research
  - For the cost of an iPhone 4s thru iPhone X you can do otherwise free forensic research and analysis
- TEST AND VERIFY!

Let’s forensicate!

iOS 13 Artifacts

Something old, something new, something borrowed, something really creepy.

- Facial Recognition in Photos
- Recoverable Deleted Images
- Personalization Portrait
- 3Bars - Rough WiFi Location Tracking



Type to enter a caption.

Photos Analysis

Give me all the faces.

Type to enter a caption.

Photos

Path: /private/var/mobile/Media/..

- The Native Photos application has evolved into an extremely intelligent repository of processed data about the images it contains
- Keyword searching
- Facial recognition and categorization of specific people
- “Moment” type categorization - Concerts, Museums, Sporting Events, Trips, Theme Parks, Birthdays, Timeframes, and many more!
- Place designations based on location data

What happens when you take a picture?

Taking Photo

```
FSE_CREATE_FILE    3876   "Camera" /private/var/mobile/Media/PhotoData/takingphoto
FSE_CREATE_FILE    3876   "Camera" /private/var/mobile/Media/DCIM/.MISC/Incoming/61548763015__6E0F08AB-79E3-4BA5-A062-5DCD0678595C.HEIC
FSE_CONTENT_MODIFIED  3876   "Camera"/private/var/mobile/Media/DCIM/.MISC/Incoming/61548763015__6E0F08AB-79E3-4BA5-A062-5DCD0678595C.HEIC
FSE_XATTR_MODIFIED  3876   "Camera" /private/var/mobile/Media/DCIM/.MISC/Incoming/61548763015__6E0F08AB-79E3-4BA5-A062-5DCD0678595C.HEIC
FSE_STAT_CHANGED    3876   "Camera" /private/var/mobile/Media/DCIM/.MISC/Incoming/61548763015__6E0F08AB-79E3-4BA5-A062-5DCD0678595C.HEIC
FSE_CREATE_FILE    3876   "Camera" /private/var/mobile/Media/DCIM/.MISC/Incoming/61548763015__6E0F08AB-79E3-4BA5-A062-5DCD0678595C.MDATA
FSE_CONTENT_MODIFIED  3876   "Camera"/private/var/mobile/Media/DCIM/.MISC/Incoming/61548763015__6E0F08AB-79E3-4BA5-A062-5DCD0678595C.MDATA
FSE_STAT_CHANGED    3799   "assetsd" /private/var/mobile/Media/PhotoData/Photos.sqlite
FSE_DELETE  3799   "assetsd" /private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/58E8EF6B-2C96-42C5-86EB-880AD19C572B
FSE_CONTENT_MODIFIED  3799   "assetsd"/private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/58E8EF6B-2C96-42C5-86EB-880AD19C572B
FSE_CONTENT_MODIFIED  3799   "assetsd"/private/var/mobile/Media/PhotoData/MISC/.PreviewWellImage.tiff-6H6U
FSE_CREATE_FILE    3799   "assetsd" /private/var/mobile/Media/PhotoData/MISC/.PreviewWellImage.tiff-6H6U
FSE_XATTR_MODIFIED  3799   "assetsd" /private/var/mobile/Media/PhotoData/MISC/PreviewWellImage.tiff
FSE_CREATE_FILE    3799   "assetsd" /private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/EF5FC828-1F3F-4391-B67B-24CFF7D77F17
FSE_STAT_CHANGED    3799   "assetsd" /private/var/mobile/Media/PhotoData/Photos.sqlite-wal
FSE_DELETE  3799   "assetsd" /private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/EF5FC828-1F3F-4391-B67B-24CFF7D77F17
FSE_CONTENT_MODIFIED  3799   "assetsd"/private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/EF5FC828-1F3F-4391-B67B-24CFF7D77F17
^CLa-di-da-di-da:/private/var/mobile/Media root# /usr/bin/fsmon /private/var/mobile/Media/
FSE_CREATE_FILE    3876   "Camera" /private/var/mobile/Media/PhotoData/takingphoto
FSE_CREATE_FILE    3876   "Camera" /private/var/mobile/Media/DCIM/.MISC/Incoming/61548768822__41BE5297-788F-456A-A638-CE0381F0B0D8.HEIC
FSE_CONTENT_MODIFIED  3876   "Camera"/private/var/mobile/Media/DCIM/.MISC/Incoming/61548768822__41BE5297-788F-456A-A638-CE0381F0B0D8.HEIC
FSE_XATTR_MODIFIED  3876   "Camera" /private/var/mobile/Media/DCIM/.MISC/Incoming/61548768822__41BE5297-788F-456A-A638-CE0381F0B0D8.HEIC
FSE_STAT_CHANGED    3876   "Camera" /private/var/mobile/Media/DCIM/.MISC/Incoming/61548768822__41BE5297-788F-456A-A638-CE0381F0B0D8.HEIC
FSE_CREATE_FILE    3876   "Camera" /private/var/mobile/Media/DCIM/.MISC/Incoming/61548768822__41BE5297-788F-456A-A638-CE0381F0B0D8.MDATA
FSE_CONTENT_MODIFIED  3876   "Camera"/private/var/mobile/Media/DCIM/.MISC/Incoming/61548768822__41BE5297-788F-456A-A638-CE0381F0B0D8.MDATA
FSE_CREATE_FILE    3799   "assetsd" /private/var/mobile/Media/PhotoData/MISC/.PreviewWellImage.tiff-vvgE
FSE_CONTENT_MODIFIED  3799   "assetsd"/private/var/mobile/Media/PhotoData/MISC/.PreviewWellImage.tiff-vvgE
FSE_CREATE_FILE    3799   "assetsd" /private/var/mobile/Media/PhotoData/MISC/.PreviewWellImage.tiff-vvgE
FSE_XATTR_MODIFIED  3799   "assetsd" /private/var/mobile/Media/PhotoData/MISC/PreviewWellImage.tiff
FSE_CREATE_FILE    3799   "assetsd" /private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/0204B38C-6BE6-4C3B-9A7C-F7442167750D
FSE_DELETE  3799   "assetsd" /private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/0204B38C-6BE6-4C3B-9A7C-F7442167750D
FSE_CONTENT_MODIFIED  3799   "assetsd"/private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/0204B38C-6BE6-4C3B-9A7C-F7442167750D
```

What happens when you take a picture?

Closing Camera App

```
FSE_DELETE      3799    "assetsd"       /private/var/mobile/Media/PhotoData/CPL/pauseICloudPhotos
FSE_CREATE_FILE 3799    "assetsd"       /private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/B5A7D264-0C4F-4B56-B555-EFC7F93A6942
FSE_DELETE      3799    "assetsd"       /private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/B5A7D264-0C4F-4B56-B555-EFC7F93A6942
FSE_CONTENT_MODIFIED    3799    "assetsd"       /private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/B5A7D264-0C4F-4B56-B555-EFC7F93A6942
FSE_CREATE_FILE 3799    "assetsd"       /private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/8C215702-FB69-4D67-A360-1962E3BCE032
FSE_XATTR_MODIFIED      3799    "assetsd"       /private/var/mobile/Media/DCIM/116APPLE/IMG_6650.HEIC
FSE_XATTR_MODIFIED      3799    "assetsd"       /private/var/mobile/Media/DCIM/116APPLE/IMG_6648.HEIC
FSE_XATTR_MODIFIED      3799    "assetsd"       /private/var/mobile/Media/DCIM/116APPLE/IMG_6649.HEIC
FSE_DELETE      3799    "assetsd"       /private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/8C215702-FB69-4D67-A360-1962E3BCE032
FSE_CONTENT_MODIFIED    3799    "assetsd"       /private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/8C215702-FB69-4D67-A360-1962E3BCE032
FSE_CREATE_FILE 3799    "assetsd"       /private/var/mobile/Media/PhotoData/CPL/.dat.nosync0ed7.3rZxDR
FSE_CREATE_FILE 3799    "assetsd"       /private/var/mobile/Media/PhotoData/CPL/.dat.nosync0ed7.3rZxDR
FSE_CHOWN       3799    "assetsd"       /private/var/mobile/Media/PhotoData/CPL/DownloadCounts.plist
FSE_CHOWN       2477    "cloudphotod"   /private/var/mobile/Media/PhotoData/CPL/storage/.fileStorageCrashMarker.plist
FSE_CREATE_FILE 2477    "cloudphotod"   /private/var/mobile/Media/PhotoData/CPL/storage/.dat.nosync09ad.jQVgRI
FSE_CREATE_FILE 3799    "assetsd"       /private/var/mobile/Media/PhotoData/CPL/.dat.nosync0ed7.mQ34Kj
FSE_CHOWN       2477    "cloudphotod"   /private/var/mobile/Media/PhotoData/CPL/storage/.fileStorageCrashMarker.plist
FSE_CHOWN       3799    "assetsd"       /private/var/mobile/Media/PhotoData/CPL/DownloadCounts.plist
FSE_DELETE      2477    "cloudphotod"   /private/var/mobile/Media/PhotoData/CPL/storage/.fileStorageCrashMarker.plist
FSE_CREATE_FILE 3799    "assetsd"       /private/var/mobile/Media/PhotoData/CPL/.dat.nosync0ed7.pZjxNY
FSE_CONTENT_MODIFIED    3799    "assetsd"       /private/var/mobile/Media/PhotoData/CPL/.dat.nosync0ed7.pZjxNY
FSE_CREATE_FILE 3799    "assetsd"       /private/var/mobile/Media/PhotoData/CPL/.dat.nosync0ed7.pZjxNY
FSE_CHOWN       3799    "assetsd"       /private/var/mobile/Media/PhotoData/CPL/mobileCPL.plist
FSE_CREATE_FILE 3799    "assetsd"       /private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/0A7B3A52-2013-4FF4-BC81-981CDE0FD553
FSE_DELETE      3799    "assetsd"       /private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/0A7B3A52-2013-4FF4-BC81-981CDE0FD553
FSE_CONTENT_MODIFIED    3799    "assetsd"       /private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/0A7B3A52-2013-4FF4-BC81-981CDE0FD553
FSE_CREATE_DIR  2477    "cloudphotod"   /private/var/mobile/Media/PhotoData/CPL/derivatives
```

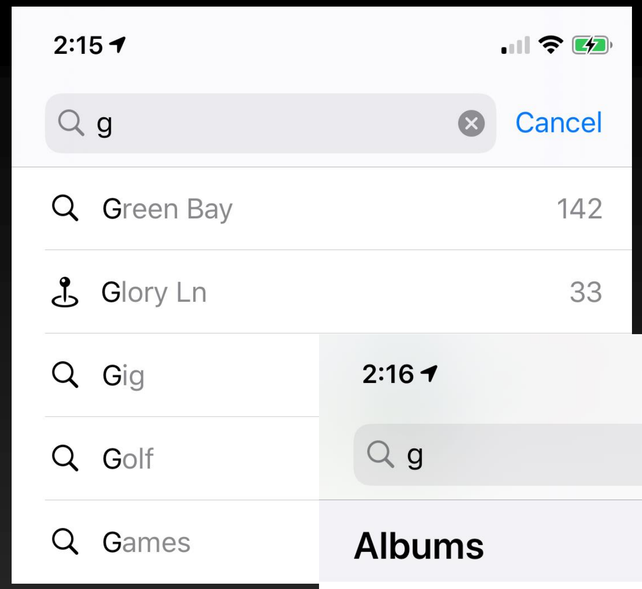
Photo Taken
Now What?

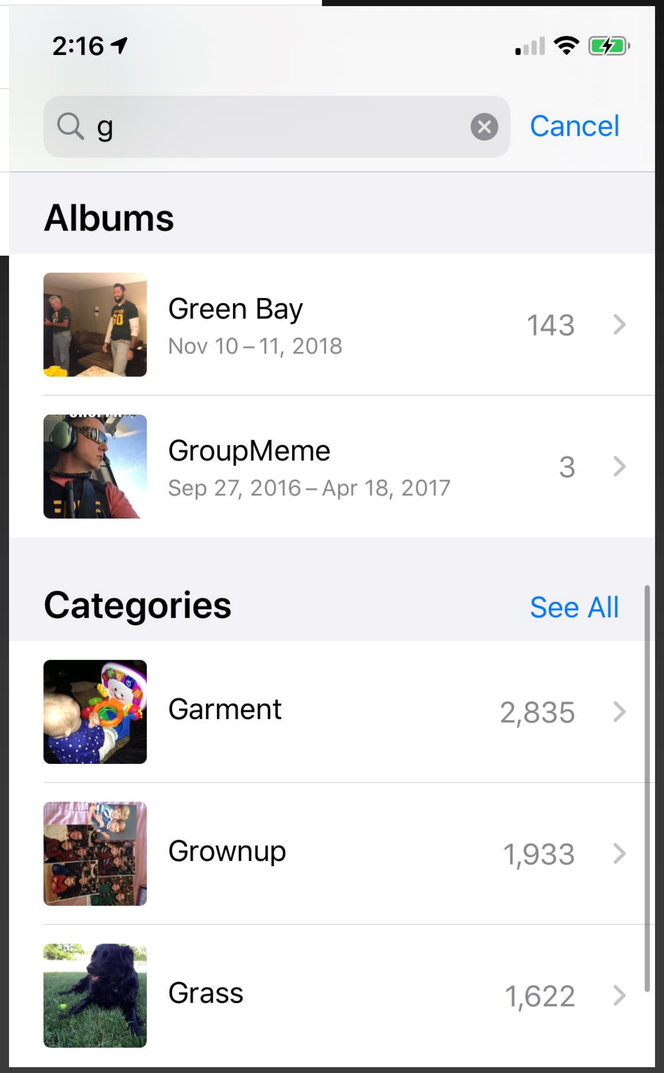
- Ultimately writes the newly taken photo to /private/var/mobile/Media/DCIM/1**APPLE/IMG_0001.HEIC / .JPG
- User settings determine if HEIC (High Efficiency Image Format / Container) or JPEG is default file type
- Start of user's photos reside in ../100APPLE/ , but directories iterate upwards to 101APPLE, 102APPLE, etc. (mine is 116APPLE)
- iCloud synced Photos being enabled shows additional on-disk activity as the Cloud Photo Library (CPL)

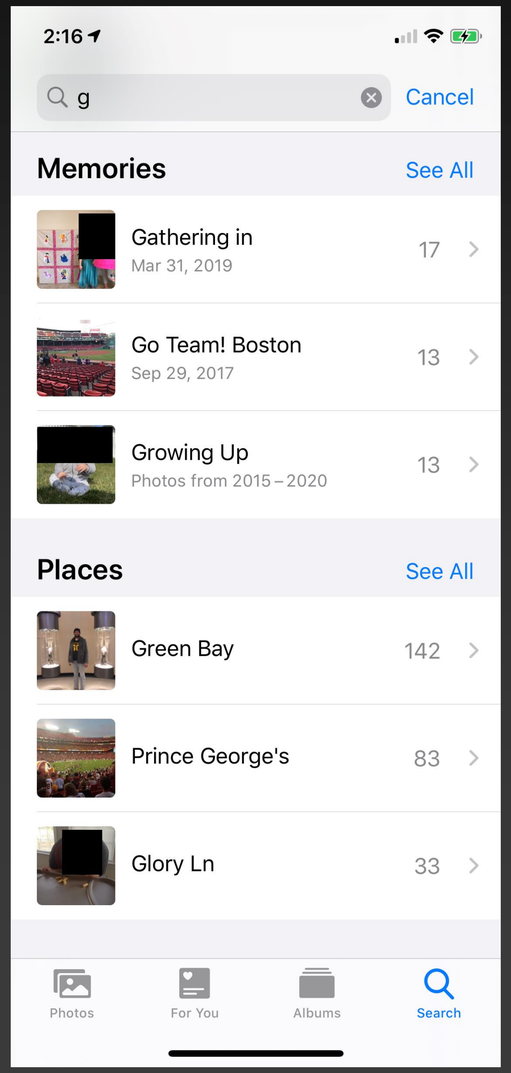
Easy Stuff ✓

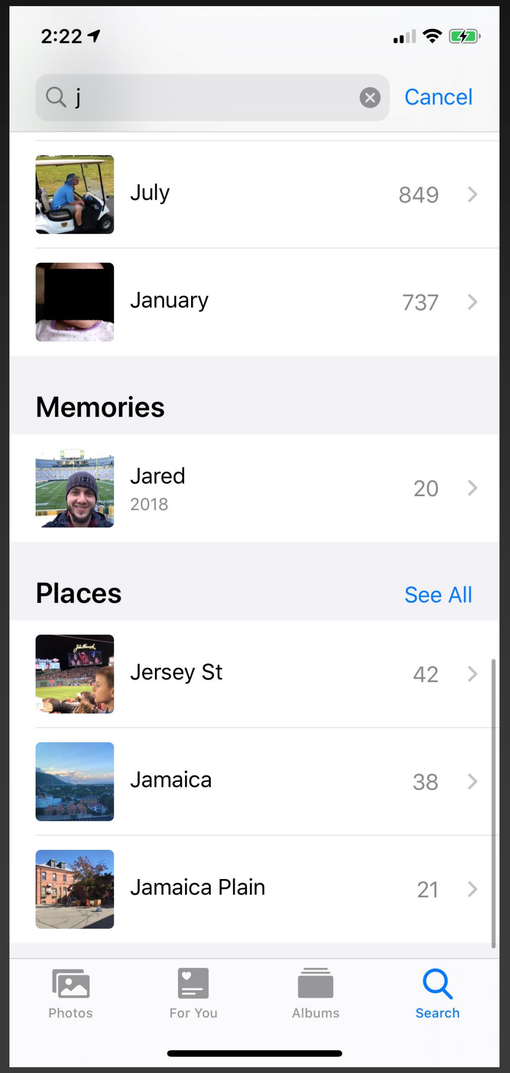
Here comes the goodness..

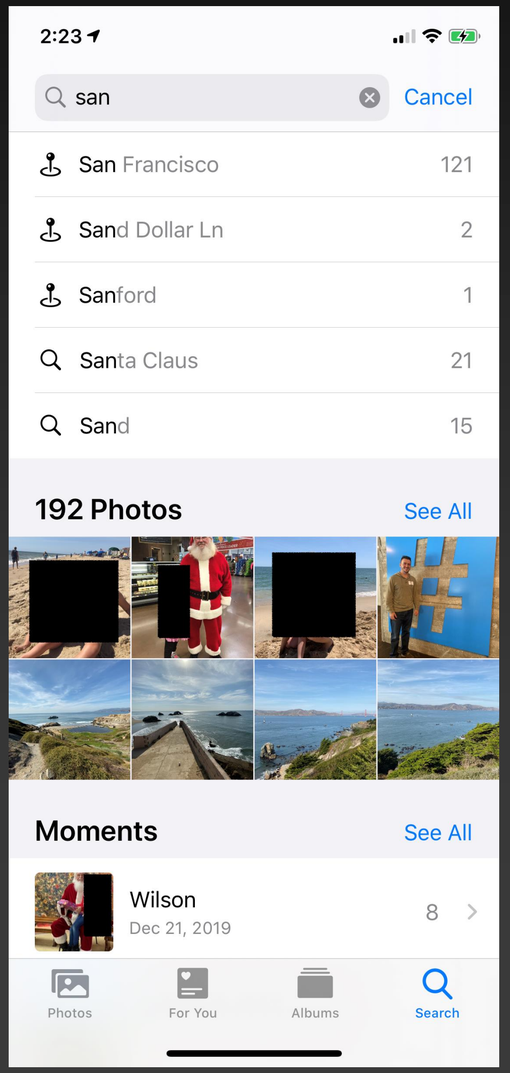
Media Analysis











mediaanalysis.db

Path: /private/var/mobile/Media/MediaAnalysis/mediaanalysis.db

- Scoring and analysis for each photo occurs in this file
- Different factors such as sharpness, quality, shot type, human confidence, and more

Table: Assets

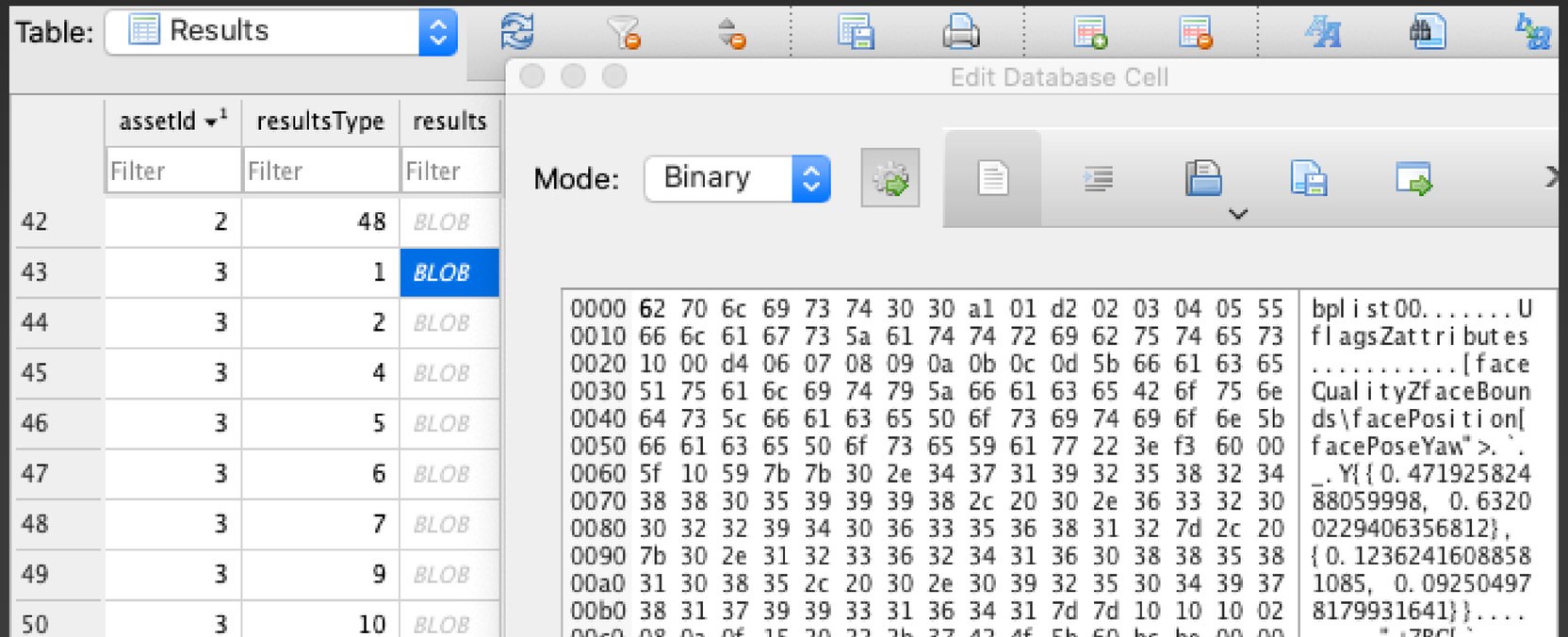
Filter in any column

	id	localIdentifier	version	dateModified	dateAnalyzed	analysisTypes	flags	quality	masterFingerprint	adjustedFingerprint	statsFlags
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	4A2F3C70-DE73-48F5-B622-E570600469E1/L0/001	33	590777493.894	590802996.924663	33430492	0	0.990000009536743	AYyKETvcJhqV2J145c27wHnRrWE6	NULL	9308543322822658
2	2	7C78D7AD-1F16-4D66-95F9-DCD12251984A/L0/001	33	590777503.918	590803000.473422	33430492	0	0.990000009536743	AZweX25/yLhBSbqzrwjQM9lHgiAE	NULL	9308749588367362
3	3	C2327791-D91B-426D-8D00-8536F3EFD730/L0/001	33	589901723.792	590829414.731938	33430492	536870944	0.990000009536743	Af7kEplJY6fOLcofR/rnYdZHPx7m	NULL	72366043699906562
4	4	435B1C5D-7803-4FC0-9D09-7C653E09DF90/L0/001	33	589379603.46637	590829432.031046	33430492	536870944	0.980000019073486	AdM1QmhzbF1YC0JXZ/5ruD2lPZF9	NULL	72365751575021570
5	5	B23D57EB-5D29-4BFB-8DBC-408DFEBFC90F/L0/001	33	589379655.505108	590829427.50958	33430492	536870912	0.959999978542328	AYRPCE2PhWP/53zjus1E2vF6466f	NULL	9308749588367362
6	6	77C86CC3-88A4-448A-9E6C-F0F9AC7D746D/L0/001	33	589379930.501177	590829427.149943	33430492	536870944	0.970000028610229	AVHW1+1HPE3Vg+VHAgLZWDYytOgm	NULL	72365751642130434
7	7	C214CD73-E69F-4724-A78D-5CE759428C35/L0/001	33	589379523.91729	590829432.403203	33430492	536870912	0.970000028610229	AS031EGLwyawDFQPS+J1nXodulY4	NULL	9308749521258498
8	8	26D4F146-58DC-42E8-83F2-E23CBC21B27D/L0/001	33	589304030.014245	590829434.806824	33430492	536870944	0.930000007152557	ARZUuWUa6e3LD4fz8UcqoLi/mCjl	NULL	9308749588367362
9	9	B53BC62C-F679-4D05-AA0A-B5A124AE8816/L0/001	33	589203467.202021	590829438.231955	33430492	536870946	0.939999997615814	AR5oFa4QzmbJ5SmnWvps4jZ4YcK8	NULL	9308749521258498
10	10	94120CD0-39F1-4CE1-9FEF-58F8F841DDD7/L0/001	33	589203453.538258	590829438.737093	33430492	536870950	0.959999978542328	ARjO6i+m3sEjr5iaG4I1HOl/wwr0	NULL	9308749588367362

mediaanalysis.db

Path: /private/var/mobile/Media/MediaAnalysis/mediaanalysis.db

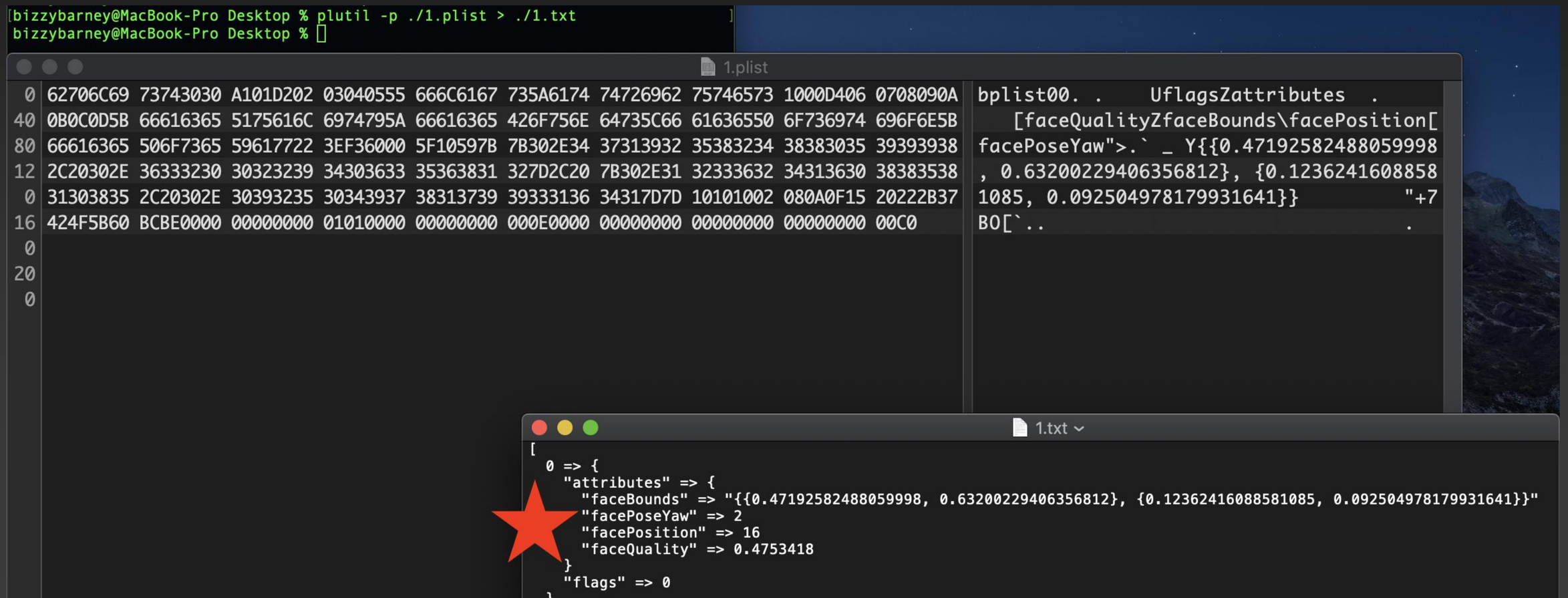
- ‘Results’ table tracks the results of the analysis, and joins to the ‘Assets’
- Multiple results listed for each ‘assetId’
- Each ‘resultsType’ value represents a different measure of the analysis performed on the individual asset, the result type is stored in the ‘results’ BLOB



mediaanalysis.db

‘results’ column BLOB’s

- BLOB’s can be printed to .txt using ‘plutil’
- BLOB where ‘resultsType’ = 1 involves attributes about faces



resultsType Values

BLOB Data Summary

1. Face Bounds / Position / Quality
2. Shot Type
3. Duration / Quality / Start - Timescale 1600
4. Duration / Quality / Start - Timescale 600
5. Duration / Quality / Start
6. Duration / Flags / Start
7. Duration / Flags / Start
8. No Data Available
9. Attributes = ‘junk’
10. Attributes = ‘sharpness’
11. No Data
12. Attributes = ‘featureVector’
13. No Data
14. Attributes = ‘Data’
15. Duration / Quality / Start - Timescale 600
16. Attributes = ‘orientation’, Duration / Start
17. Quality
18. Attributes = ‘objectBounds’, Duration / Start
19. Duration / Quality / Start
20. Saliency Bounds / Saliency Confidence
21. No Data
22. Attributes / Duration / Start
23. Duration / Quality / Start
24. Duration / Quality / Start
25. Duration / Quality / Start
26. No Data
27. Duration / Quality / Start
28. Attributes = ‘faceId’ , ‘facePrint’
29. Attributes = ‘petsBounds’, ‘petsConfidence’
30. Attributes = ‘contentScore’, ‘exposureScore’, ‘faceQualityScore’, ‘FaceResults’, ‘frameQualityScore’, ‘globalQualityScore’, ‘penaltyScore’, ‘sharpnessScore’, ‘textureScore’, ‘timestamp’, ‘visualPleasingScore’
31. No Data
32. Attributes = bestPlaybackCrop, Duration / Flags / Quality / Start
33. Attributes = keyFrameScore, keyFrameTime, Duration / Quality / Start
34. Attributes = underExpose
35. Attributes = longExposureSuggestionState, loopSuggestionState
36. Duration / Quality / Start
37. Duration / Quality / Start
38. Duration/ Quality / Start
39. Duration/ Quality / Start
40. Attributes = ‘petsBounds’, ‘petsConfidence’
41. Attributes = ‘humanBounds’, ‘humanConfidence’, Flags
42. No Data
43. Attributes = ‘absoluteScore’, ‘humanScore’, ‘relativeScore’, Duration / Start
44. Attributes = ‘energyValues’, ‘peakValues’, Duration / Start
45. No Data
46. Attributes = ‘sceneprint’, ‘EspressoModelImageprint’
47. Attributes = ‘flashFired’, ‘sharpness’, ‘stillTime’, ‘texture’
48. Duration / Quality / Start
49. No Data

mediaanalysis.db

SQL Query

```sql
select
    a.id,
    a.localIdentifier as "Local Identifier",
    a.analysisTypes as "Analysis Types",
    datetime(a.dateModified+978307200, 'unixepoch') as "Date Modified (UTC)",
    datetime(a.dateAnalyzed+978307200, 'unixepoch') as "Date Analyzed (UTC)",
CASE
    when results.resultsType = 1 then "Face Bounds / Position / Quality"
    when results.resultsType = 2 then "Shot Type"
    when results.resultsType = 3 then "Duration / Quality / Start"
    when results.resultsType = 4 then "Duration / Quality / Start"
    when results.resultsType = 5 then "Duration / Quality / Start"
    when results.resultsType = 6 then "Duration / Flags / Start"
    when results.resultsType = 7 then "Duration / Flags / Start"
    when results.resultsType = 15 then "Duration / Quality / Start"
    when results.resultsType = 19 then "Duration / Quality / Start"
    when results.resultsType = 22 then "Duration / Quality / Start"
    when results.resultsType = 23 then "Duration / Quality / Start"
    when results.resultsType = 24 then "Duration / Quality / Start"
    when results.resultsType = 25 then "Duration / Quality / Start"
    when results.resultsType = 27 then "Duration / Quality / Start"
    when results.resultsType = 36 then "Duration / Quality / Start"
    when results.resultsType = 37 then "Duration / Quality / Start"
    when results.resultsType = 38 then "Duration / Quality / Start"
    when results.resultsType = 39 then "Duration / Quality / Start"
    when results.resultsType = 48 then "Duration / Quality / Start"
    when results.resultsType = 8 then "UNK"
    when results.resultsType = 11 then "UNK"
    when results.resultsType = 13 then "UNK"
    when results.resultsType = 21 then "UNK"
    when results.resultsType = 26 then "UNK"
    when results.resultsType = 31 then "UNK"
    when results.resultsType = 42 then "UNK"
    when results.resultsType = 45 then "UNK"
    when results.resultsType = 49 then "UNK"
    when results.resultsType = 9 then "Attributes - junk"
    when results.resultsType = 10 then 'Attributes - sharpness'
    when results.resultsType = 12 then "Attributes - featureVector"
    when results.resultsType = 14 then "Attributes - Data"
    when results.resultsType = 16 then "Attributes - orientation"
    when results.resultsType = 17 then 'Quality'
    when results.resultsType = 18 then "Attributes - objectBounds"
    when results.resultsType = 20 then "Saliency Bounds and Confidence"
    when results.resultsType = 28 then "Attributes - faceId / facePrint"
    when results.resultsType = 29 then "Attributes - petsBounds and Confidence"
    when results.resultsType = 30 then "Various Scoring Values"
    when results.resultsType = 32 then "Attributes - bestPlaybackCrop"
    when results.resultsType = 33 then "Attributes - keyFrameScore / keyFrameTime"
    when results.resultsType = 34 then "Attributes - underExpose"
    when results.resultsType = 35 then "Attributes - longExposureSuggestionState / loopSuggestionState"
    when results.resultsType = 40 then "Attributes - petBounds and Confidence"
    when results.resultsType = 41 then "Attributes - humanBounds and Confidence"
    when results.resultsType = 43 then "Attributes - absoluteScore/ humanScore/ relativeScore"
    when results.resultsType = 44 then "Attributes - energyValues/ peakValues"
    when results.resultsType = 46 then "Attributes - sceneprint/ EspressoModelImagePrint"
    when results.resultsType = 47 then "Attributes - flashFired, sharpness, stillTime, texture"
end as "Results Type",
    hex(results.results) as "Results BLOB"
from assets a
left join results on results.assetId=a.id
```

mediaanalysis.db

Focused Results on ‘humanBounds and ‘humanConfidence’ - 5019 rows returned

```
59    from assets a
60    left join results on results.assetId=a.id
61    where results.resultsType = 41
```

	id	Local Identifier	Analysis Types	Date Modified (UTC)	Date Analyzed (UTC)	Results Type
5004	17…	09A5EEE9-63BE-4411-9ECF-90929545264C/L0/001	4856588	2020-06-16 22:43:53	2020-06-17 03:34:54	Attributes – humanBounds and Confidence
5005	17…	513AA776-DE0A-4B75-9C4A-30EAC0670A68/L0/001	4856588	2020-06-16 22:43:17	2020-06-17 03:34:55	Attributes – humanBounds and Confidence
5006	17…	7C1715F2-F6A9-4521-A900-91FE82E9BEE9/L0/001	4856588	2020-06-16 22:42:14	2020-06-17 03:34:55	Attributes – humanBounds and Confidence
5007	17…	D995CC71-89AD-4F5B-9D23-E05925251597/L0/001	4856588	2020-06-16 22:42:00	2020-06-17 03:34:56	Attributes – humanBounds and Confidence
5008	17…	B7437C42-BFCB-4F1E-BA25-70D7F7F4B2AE/L0/001	4856588	2020-06-18 21:56:19	2020-06-19 02:31:22	Attributes – humanBounds and Confidence
5009	17…	4395CFA5-21DF-4DC0-8EA6-EBA4CEAE20C6/L0/001	4856588	2020-06-18 21:56:18	2020-06-19 02:31:23	Attributes – humanBounds and Confidence
5010	17…	BC5281C0-0005-429D-B581-20B76BD1A1D9/L0/001	4856588	2020-06-18 21:56:19	2020-06-19 02:31:23	Attributes – humanBounds and Confidence
5011	17…	4E74FAAC-CC1B-449F-B40A-E82E32E1C4F4/L0/001	4856588	2020-06-18 21:56:19	2020-06-19 02:31:24	Attributes – humanBounds and Confidence
5012	17…	5027AAFA-6287-41D4-83DE-DB42F39FBEBD/L0/001	4856588	2020-06-19 16:44:04	2020-06-19 16:45:31	Attributes – humanBounds and Confidence
5013	17…	07CEE772-AAF5-4A7E-B729-2C065F0407DB/L0/001	4856588	2020-06-19 16:44:29	2020-06-19 16:45:31	Attributes – humanBounds and Confidence
5014	17…	BFA80CFB-5505-46FD-AAD3-17BB1191F23F/L0/001	4856588	2013-06-16 15:23:40	2020-06-19 17:31:03	Attributes – humanBounds and Confidence
5015	17…	2A6B58E9-348C-40AE-BE34-B1136AE1744C/L0/001	31774940	2020-06-19 23:01:47	2020-06-20 03:43:04	Attributes – humanBounds and Confidence
5016	17…	89E1C122-9144-4698-8DAE-EB46BDA646A6/L0/001	4856588	2020-06-22 00:12:48	2020-06-22 03:22:24	Attributes – humanBounds and Confidence
5017	17…	EEFDB451-7C5E-457F-9D39-A1B9E15DE081/L0/001	4856588	2020-06-24 15:35:22	2020-06-24 15:35:56	Attributes – humanBounds and Confidence
5018	17…	4853FDFB-3BC6-4B66-B3BB-53D3D85A8E40/L0/001	4856588	2020-06-27 21:56:31	2020-06-28 23:50:37	Attributes – humanBounds and Confidence
5019	17…	109C89B0-8887-4A7F-86D0-8FA98E776353/L0/001	4856588	2020-06-30 01:34:39	2020-06-30 03:29:56	Attributes – humanBounds and Confidence

How often does this media analysis happen?

- Seems to be a constant process of analyzing the content of photos and videos
- This auger is feeding into the ‘Memories’ and ‘People’ categorization of Photos
- But how does the keyword search work?

Table: KeyValueStore

	id	key	value
	Filter	Filter	Filter
1	1	MediaAnalysisVersion	33
2	2	LatestVersionTimeStamp	590721799
3	7223	DailyProcessTimeStamp	595843835
4	17552	NumberOfMoviesPartiallyAnalyzedToday	304
5	17553	NumberOfMoviesPartiallyAnalyzedInLatestVersion	846
6	17554	MovieDurationPartiallyAnalyzedToday	7774
7	17555	TotalTimeSpentPartiallyAnalyzingMovieInLatestVersion	106826
8	17556	MovieDurationPartiallyAnalyzedInLatestVersion	38462
9	18113	NumberOfLivePhotosPartiallyAnalyzedToday	139
10	18114	NumberOfLivePhotosPartiallyAnalyzedInLatestVersion	276
11	18115	TotalTimeSpentPartiallyAnalyzingLivePhotoInLatestVersion	3936
12	20682	NumberOfLivePhotosFullyAnalyzedToday	7
13	20683	NumberOfLivePhotosFullyAnalyzedInLatestVersion	49
14	20684	TotalTimeSpentFullyAnalyzingLivePhotoInLatestVersion	562
15	22083	NumberOfMoviesFullyAnalyzedToday	75
16	22084	NumberOfMoviesFullyAnalyzedInLatestVersion	150
17	22085	MovieDurationFullyAnalyzedToday	2849
18	22086	TotalTimeSpentFullyAnalyzingMovieInLatestVersion	27749
19	22087	MovieDurationFullyAnalyzedInLatestVersion	5415
20	22356	NumberOfAssetsPartiallyAnalyzedToday	802
21	22357	NumberOfImagesPartiallyAnalyzedToday	359
22	22358	NumberOfImagesPartiallyAnalyzedInLatestVersion	6251
23	22359	TotalTimeSpentPartiallyAnalyzingImageInLatestVersion	5254
24	22360	TotalTimeRunningWithPendingAnalysisToday	8906497
25	22361	NumberOfTimesScheduledWithPendingAnalysisToday	224
26	22362	TotalTimeRunningWithPendingAnalysisInLatestVersion	8983136
27	22363	NumberOfTimesScheduledWithPendingAnalysisInLatestVersion	356
28	22364	NumberOfAssetsFullyAnalyzedToday	2204
29	22365	NumberOfImagesFullyAnalyzedToday	2122
30	22366	NumberOfImagesFullyAnalyzedInLatestVersion	9928
31	22367	TotalTimeSpentFullyAnalyzingImageInLatestVersion	6763
32	22368	TotalTimeRunningWithoutPendingAnalysisToday	8
33	22369	NumberOfTimesScheduledWithoutPendingAnalysisToday	8
34	22370	TotalTimeRunningWithoutPendingAnalysisInLatestVersion	14
35	22371	NumberOfTimesScheduledWithoutPendingAnalysisInLatestVersion	14

psi.sqlite

Path: /private/var/mobile/Media/PhotoData/Caches/search/psi.sqlite

- Textual strings related to the searchable terms can be found in this file
- Do NOT mistake the terms in this file for user created content, but the context found in this file is derived from Apple's analysis of the media files
- Apple is analyzing the content of the images and video files in Photos and attaching search strings to certain files
- There are sub-terms generated to point to the established keywords so if the user searches for "truck" it might default to "Automobile" or "Vehicle"

psi.sqlite
‘word_embedding’ table

- The ‘word’ column is ultimately the term that is being searched
- The ‘exended word’ column is pointing back to the ‘word’ column
- BLOB’s in the database when exported to CSV show the words
- These values are not pre-populated, as the media files are analyzed new entries are written here

Database View

Table: word_embedding

	word	extended_word	score
	Filter	Filter	Filter
1	BLOB	BLOB	0.667262881994247
2	BLOB	BLOB	0.649745374917984
3	BLOB	BLOB	0.638536334037781
4	BLOB	BLOB	0.5925452709198
5	BLOB	BLOB	0.583393573760986
6	BLOB	BLOB	0.576670140028
7	BLOB	BLOB	0.576606273651123
8	BLOB	BLOB	0.572214603424072
9	BLOB	BLOB	0.564599871635437
10	BLOB	BLOB	0.562753558158875
11	BLOB	BLOB	0.555677831172943
12	BLOB	BLOB	0.550348252058029
13	BLOB	BLOB	0.57157564163208
14	BLOB	BLOB	0.568598747253418
15	BLOB	BLOB	0.558833867311478
16	BLOB	BLOB	0.0
17	BLOB	BLOB	0.588809549808502
18	BLOB	BLOB	0.560436338186264
19	BLOB	BLOB	0.607523620128632
20	BLOB	BLOB	0.574867755174637
21	BLOB	BLOB	0.569831848144531
22	BLOB	BLOB	0.567874252796173

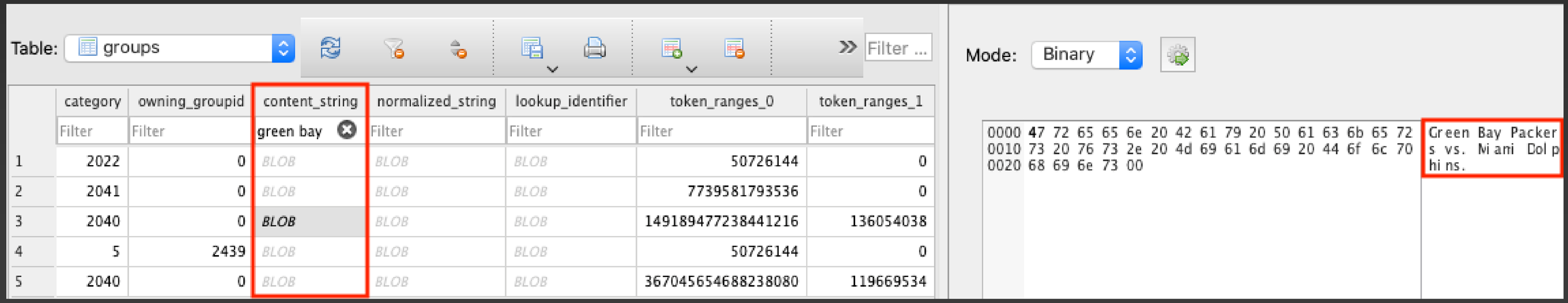
CSV View

word_embedding_all

word	extended_word	score
Celebration	festivity	0.667262881994247
Celebration	celebrating	0.649745374917984
Celebration	celebrate	0.638536334037781
Celebration	parade	0.5925452709198
Celebration	revelry	0.583393573760986
Celebration	commemoration	0.576670140028
Celebration	fete	0.576606273651123
Celebration	celebratory	0.572214603424072
Celebration	feast	0.564599871635437
Celebration	festive	0.562753558158875
Celebration	commemorate	0.555677831172943
Celebration	anniversary	0.550348252058029
Holiday	festive	0.57157564163208
Holiday	thanksgiving	0.568598747253418
Holiday	festivity	0.558833867311478
Stadium	__STUB__	0.0
Adult	child	0.588809549808502
Adult	teen	0.560436338186264
Lamp	fluorescent	0.607523620128632
Lamp	dimmer	0.574867755174637
Lamp	glow	0.569831848144531
Lamp	lampshade	0.567874252796173
Lamp	lighting	0.562241286039352
Lamp	pendant	0.554966658353806
Lamp	nightstand	0.554882675409317
Baseball Bat	__STUB__	0.0

psi.sqlite
‘groups’ table

- ‘groups’ table contains some naming information related to the revolving categories that are constantly offered in Photos such as the names of People, Places, Events, Holidays, Seasons, etc.
- In the example below, I searched for ‘green bay’ and one of the BLOB results listed is “Green Bay Packers vs. Miami Dolphins”. Extremely specific, and exactly accurate. This device went to one NFL football game in Green Bay, Wisconsin and the Packers played the Miami Dolphins.



	category	owning_groupid	content_string	normalized_string	lookup_identifier	token_ranges_0	token_ranges_1
	Filter	Filter	green bay	Filter	Filter	Filter	Filter
1	2022	0	BLOB	BLOB	BLOB	50726144	0
2	2041	0	BLOB	BLOB	BLOB	7739581793536	0
3	2040	0	BLOB	BLOB	BLOB	149189477238441216	136054038
4	5	2439	BLOB	BLOB	BLOB	50726144	0
5	2040	0	BLOB	BLOB	BLOB	367045654688238080	119669534

You will never smile for another iPhone photo again.

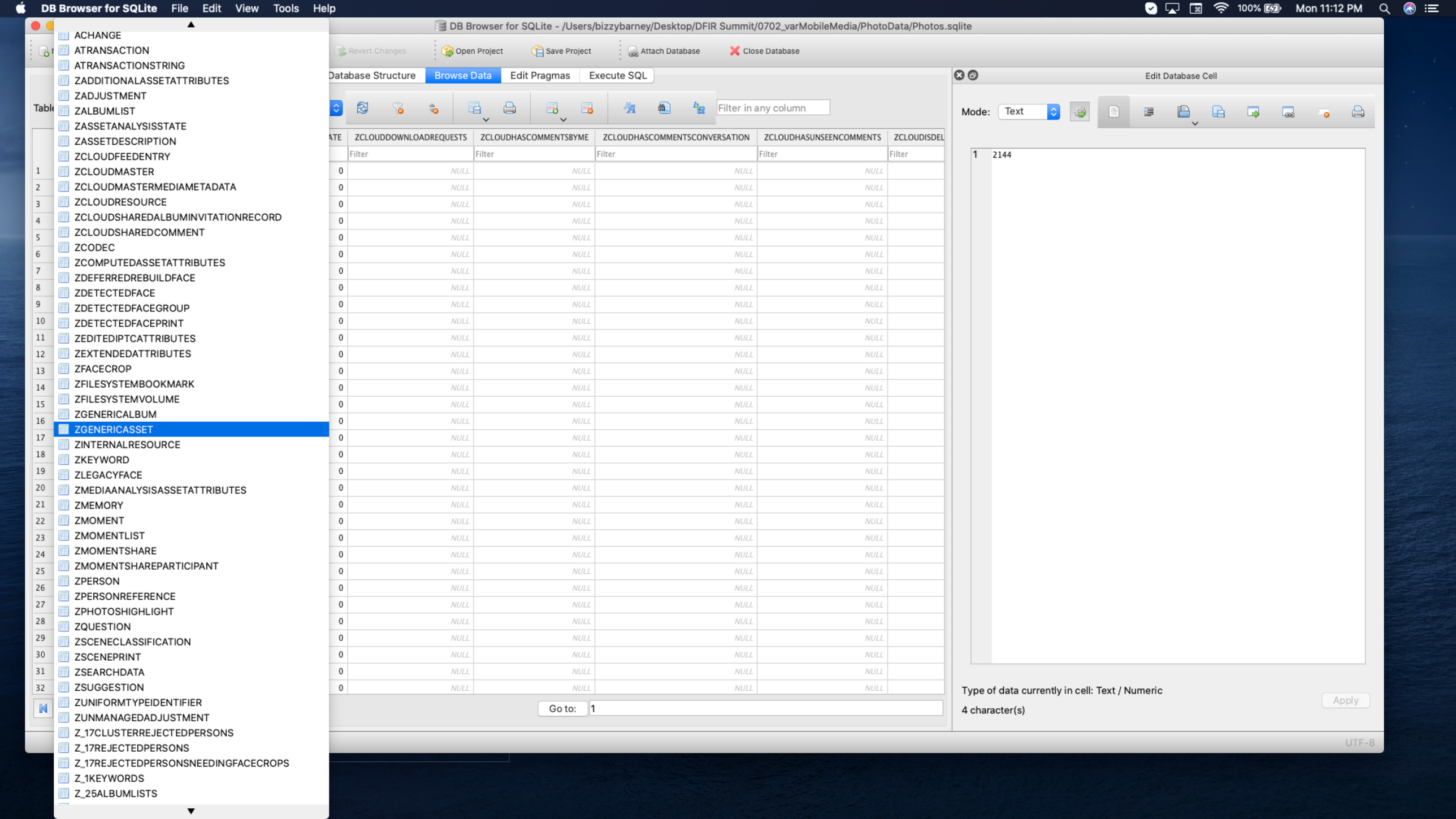
You might, but later you will regret it.

Photos.sqlite

It gets creepy now.

- ~67 tables full of data about the native Photos and Cloud Photo Library
- Potentially several hundred MB’s in size (mine was ~324MB)
- It knows when a stranger is looking at your baby..

Path: /private/var/mobile/Media/PhotoData/Photos.sqlite


DB Browser for SQLite File Edit View Tools Help
Mon 11:12 PM
DB Browser for SQLite - /Users/bizzybarney/Desktop/DFIR Summit/0702_varMobileMedia/PhotoData/Photos.sqlite
Revert Changes
Open Project
Save Project
Attach Database
Close Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Filter in any column
ACHANGE
ATRANSACTION
ATRANSACTIONSTRING
ZADDITIONALASSETATTRIBUTES
ZADJUSTMENT
ZALBUMLIST
ZASSETANALYSISSTATE
ZASSETDESCRIPTION
ZCLOUDFEEDENTRY
ZCLOUDMASTER
ZCLOUDMASTERMEDIAMETADATA
ZCLOUDRESOURCE
ZCLOUDSHAREDALBUMINVITATIONRECORD
ZCLOUDSHAREDCOMMENT
ZCODEC
ZCOMPUTEDASSETATTRIBUTES
ZDEFERREDREBUILDFACE
ZDETECTEDFACE
ZDETECTEDFACEGROUP
ZDETECTEDFACEPRINT
ZEDITEDIPTCATTRIBUTES
ZEXTENDEDATTRIBUTES
ZFACECROP
ZFILESYSTEMBOOKMARK
ZFILESYSTEMVOLUME
ZGENERICALBUM
ZGENERICASSET
ZINTERNALRESOURCE
ZKEYWORD
ZLEGACYFACE
ZMEDIAANALYSISASSETATTRIBUTES
ZMEMORY
ZMOMENT
ZMOMENTLIST
ZMOMENTSHARE
ZMOMENTSHAREPARTICIPANT
ZPERSON
ZPERSONREFERENCE
ZPHOTOSHIGHLIGHT
ZQUESTION
ZSCENECLASSIFICATION
ZSCENEPRINT
ZSEARCHDATA
ZSUGGESTION
ZUNIFORMTYPEIDENTIFIER
ZUNMANAGEDADJUSTMENT
Z_17CLUSTERREJECTEDPERSONS
Z_17REJECTEDPERSONS
Z_17REJECTEDPERSONSNEEDINGFACECROPS
Z_1KEYWORDS
Z_25ALBUMLISTS
ZCLOUDDOWNLOADREQUESTS
ZCLOUDHASCOMMENTSBYME
ZCLOUDHASCOMMENTSCONVERSATION
ZCLOUDHASUNSEENCOMMENTS
ZCLOUDISDEL
Filter
NULL
Go to:
1
Edit Database Cell
Mode:
Text
2144
Type of data currently in cell: Text / Numeric
4 character(s)
Apply
UTF-8

Focusing on Faces
ZDETECTEDFACE Table

- Age
- Hair Color
- Baldness
- Gender
- Eye Glasses
- Facial Hair
- X and Y axis measurements for left eye, right eye, mouth, and center
- Person Identifier - joins to ZPERSON table

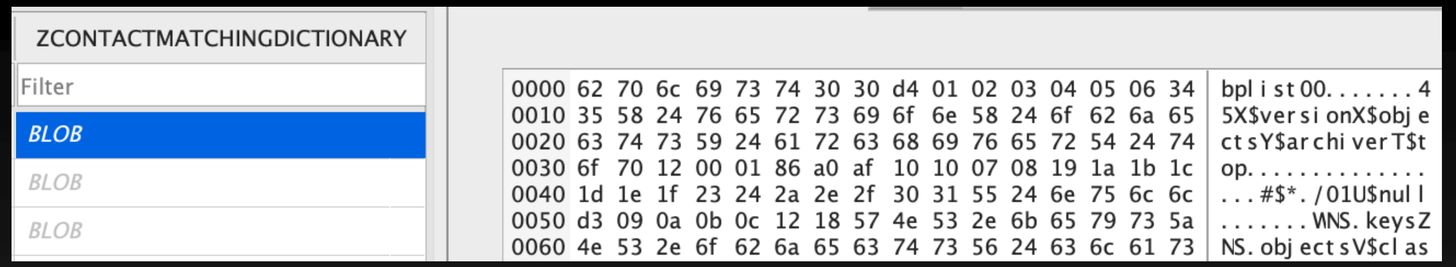
Table: ZDETECTEDFACE

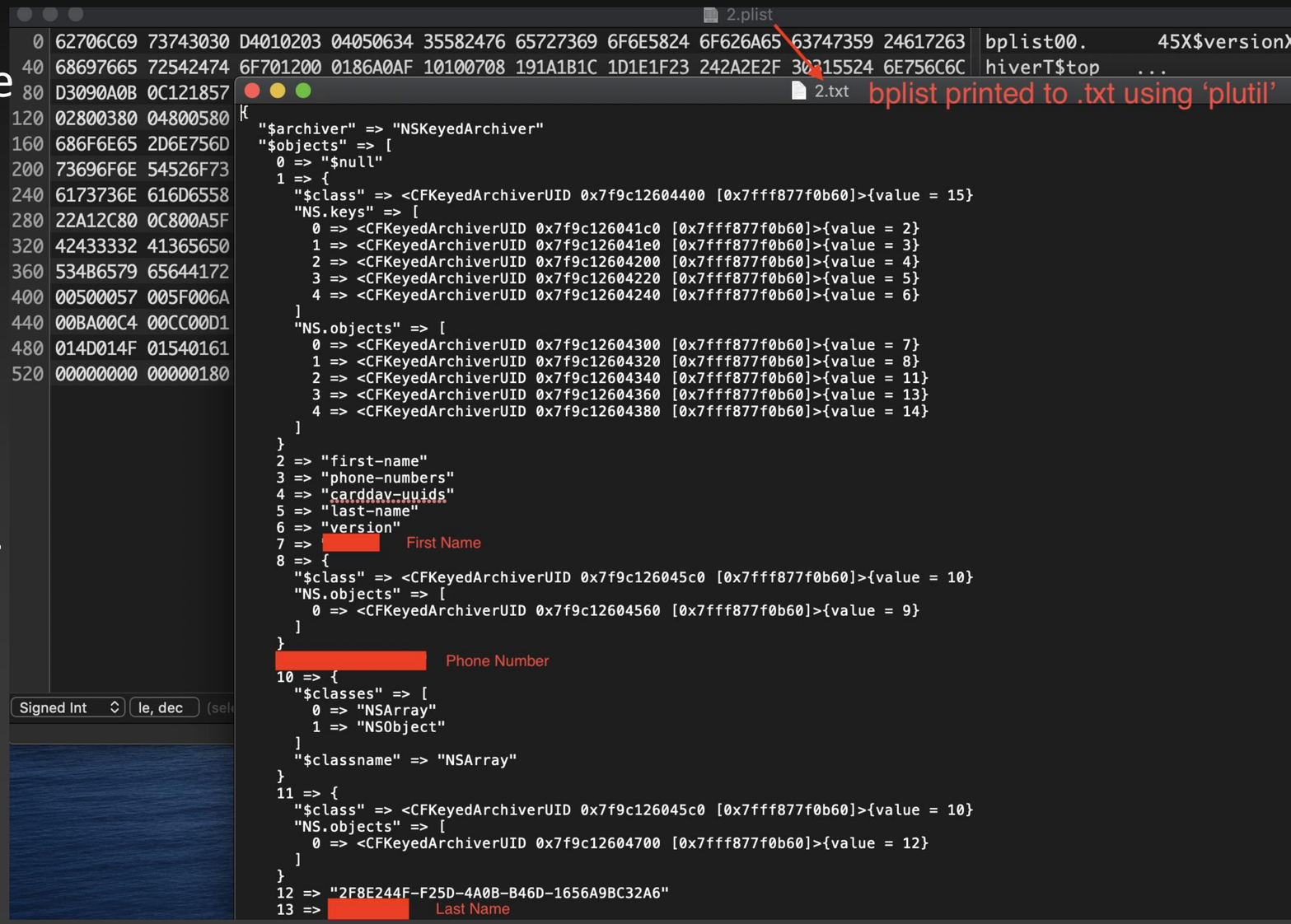
	ZEYESSTATE	ZFACEALGORITHMVERSION	ZFACIALHAIRTYPE	ZGENDERTYPE	ZGLASSESTYPE	ZHAIRCOLORTYPE	ZHASSMILE
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	2	5	1	2	3	3	0
2	1	5	5	1	3	1	0
3	2	5	1	1	2	2	0

Focusing on Faces

ZPERSON Table

- Face Count - Number of times the face is known in the Photos
- Display Name
- Full Name
- Person UUID
- CONTACTMATCHINGDICTIONARY - If yes, possible to get phone number for person from BLOB





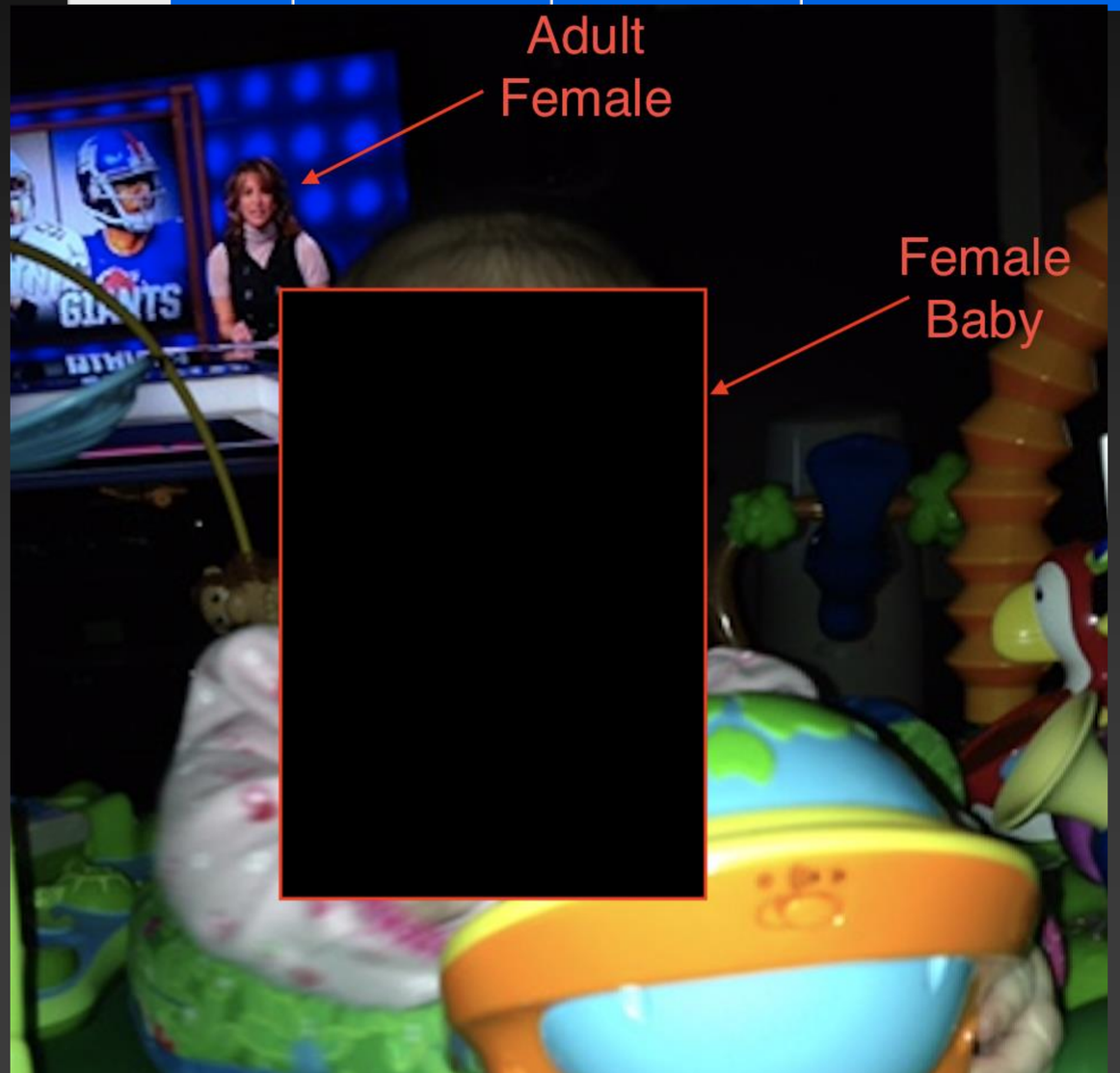
Photos.sqlite
SQL Query

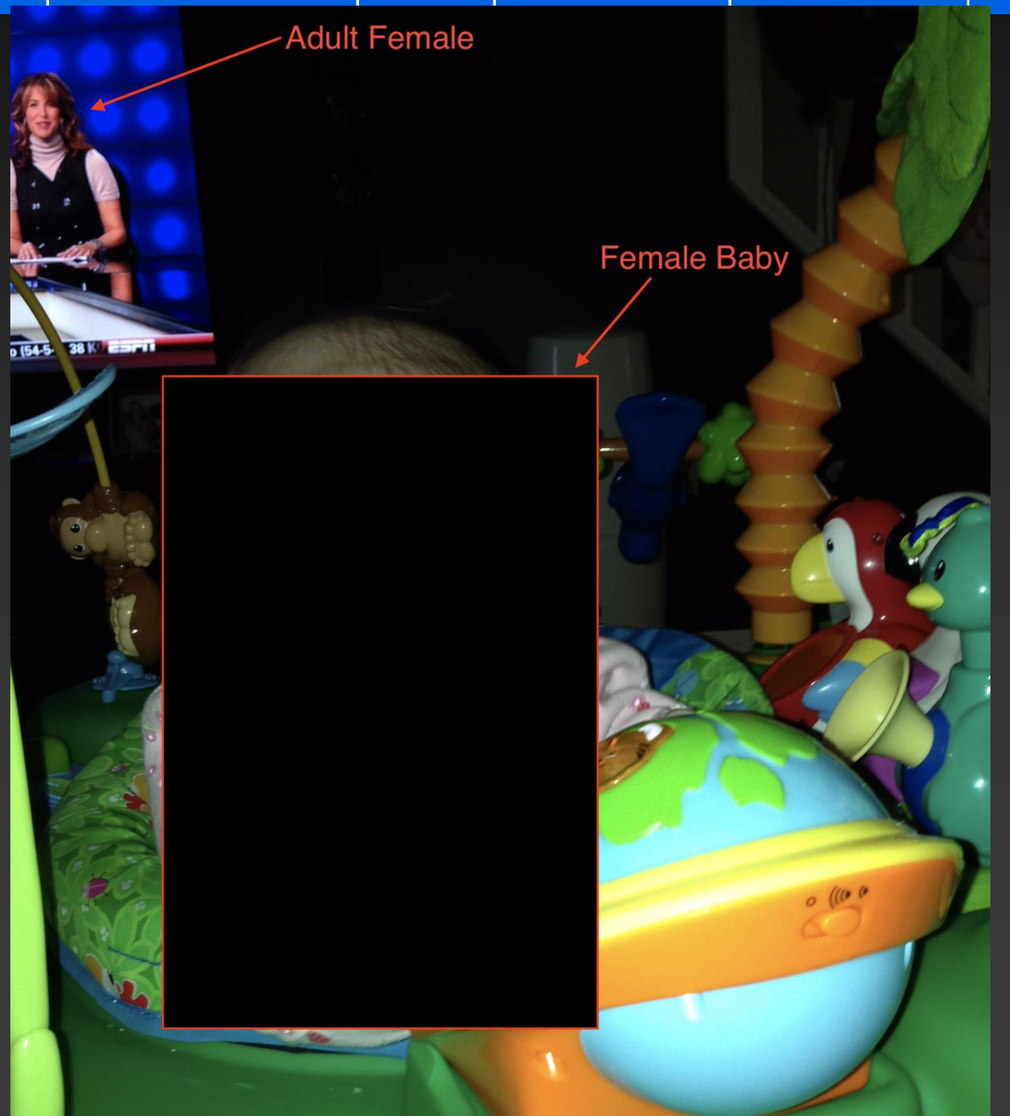
- Query only hits on photos with faces and outputs: file name and directory, age estimate rating, gender, glasses type, facial hair type, baldness, person name, number of times the person's face is recognized in Photos, location coordinates if available, Moment location title.
- Additional research can be done fore hair color, and more.

```
select
    zga.z_pk,
    zga.ZDIRECTORY as "Directory",
    zga.ZFILENAME as "File Name",
CASE
    when zga.ZFACEAREAPOINTS > 0 then "Yes"
    else "N/A"
    end as "Face Detected in Photo",
CASE
    when zdf.ZAGETYPE = 1 then "Baby / Toddler"
    when zdf.ZAGETYPE = 2 then "Baby / Toddler"
    when zdf.ZAGETYPE = 3 then "Child / Young Adult"
    when zdf.ZAGETYPE = 4 then "Young Adult / Adult"
    when zdf.ZAGETYPE = 5 then "Adult"
end as "Age Type Estimate",
case
    when zdf.ZGENDERTYPE = 1 then "Male"
    when zdf.ZGENDERTYPE = 2 then "Female"
    else "UNK"
end as "Gender",
    zp.ZDISPLAYNAME as "Display Name",
    zp.ZFULLNAME as "Full Name",
    zp.ZFACECOUNT as "Face Count",
CASE
    when zdf.ZGLASSESTYPE = 3 then "None"
    when zdf.ZGLASSESTYPE = 2 then "Sun"
    when zdf.ZGLASSESTYPE = 1 then "Eye"
    else "UNK"
end as "Glasses Type",
CASE
    when zdf.ZFACIALHAIRTYPE = 1 then "None"
    when zdf.ZFACIALHAIRTYPE = 2 then "Beard / Mustache"
    when zdf.ZFACIALHAIRTYPE = 3 then "Goatee"
    when zdf.ZFACIALHAIRTYPE = 5 then "Stubble"
    else "UNK"
end as "Facial Hair Type",
CASE
    when zdf.ZBALDTYPE = 2 then "Bald"
    when zdf.ZBALDTYPE = 3 then "Not Bald"
end as "Baldness",
CASE
    when zga.zlatitude = -180
    then 'N/A'
    else zga.ZLATITUDE
end as "Latitude",
CASE
    when zga.ZLONGITUDE = -180
    then 'N/A'
    else zga.ZLONGITUDE
end as "Longitude",
    datetime(zga.zaddeddate+978307200, 'unixepoch') as "Date Added",
    ZMOMENT.ztitle as "Location Title"
from zgenericasset zga
left join zmoment on zmoment.Z_PK=zga.ZMOMENT
left join ZDETECTEDFACE zdf on zdf.ZASSET=zga.Z_PK
left join ZPERSON zp on zp.Z_PK=zdf.ZPERSON
where zga.ZFACEAREAPOINTS > 0
```

	Z_PK	Directory	File Name	Face Detected in Photo	Age Type Estimate	Gender	Display Name	Full Name	Face Count	Glasses Type	Facial Hair Type
5496	23518	DCIM/112APPLE	IMG_2640.HEIC	Yes	Adult	Male	Jared	Jared Barnhart	387	Sun	Stubble
5497	23518	DCIM/112APPLE	IMG_2640.HEIC	Yes	Baby / Toddler	Female	[redacted]	[redacted]	562	None	None
5498	23518	DCIM/112APPLE	IMG_2640.HEIC	Yes	Baby / Toddler	Female	[redacted]	[redacted]	1722	None	None

	Z_PK	Directory	File Name	Face Detected in Photo	Age Type Estimate	Gender	Display Name	Full Name	Face Count	Baldness
4	2629	DCIM/101APPLE	IMG_1007.JPG	Yes	Baby / Toddler	Female	*NULL*		2	Not Bald
5	2629	DCIM/101APPLE	IMG_1007.JPG	Yes	Adult	Female	*NULL*		1	Not Bald
6	2630	DCIM/101APPLE	IMG_1008.JPG	Yes	Adult	Female	*NULL*		1	Not Bald
7	2630	DCIM/101APPLE	IMG_1008.JPG	Yes	Baby / Toddler	Female	*NULL*		2	Not Bald





Recoverable Deleted Images

Unallocated space on iOS is encrypted.

Therefore, fully deleted photos are generally gone forever.

General Info - Deleted Photos

- Typically when recovering deleted photos in mobile devices, they are being carved from unallocated space of internal or external flash memory.
- Allocated photos are logically accessible in the file system, meaning the user can still open them, share them, etc.
- Unallocated photos are no longer accessible to the user, but the data that was the photo file can still reside in the unallocated area until clean-up algorithms clear that block of flash memory to be used again by the file system.
- On iOS devices after the iPhone 4, the unallocated space is ENCRYPTED so we cannot address the unallocated area. Thus, why no physical iOS extractions.
- ‘Recently Deleted’ folder = Not Deleted. Simply starts a counter in a database to actually delete at a later time.

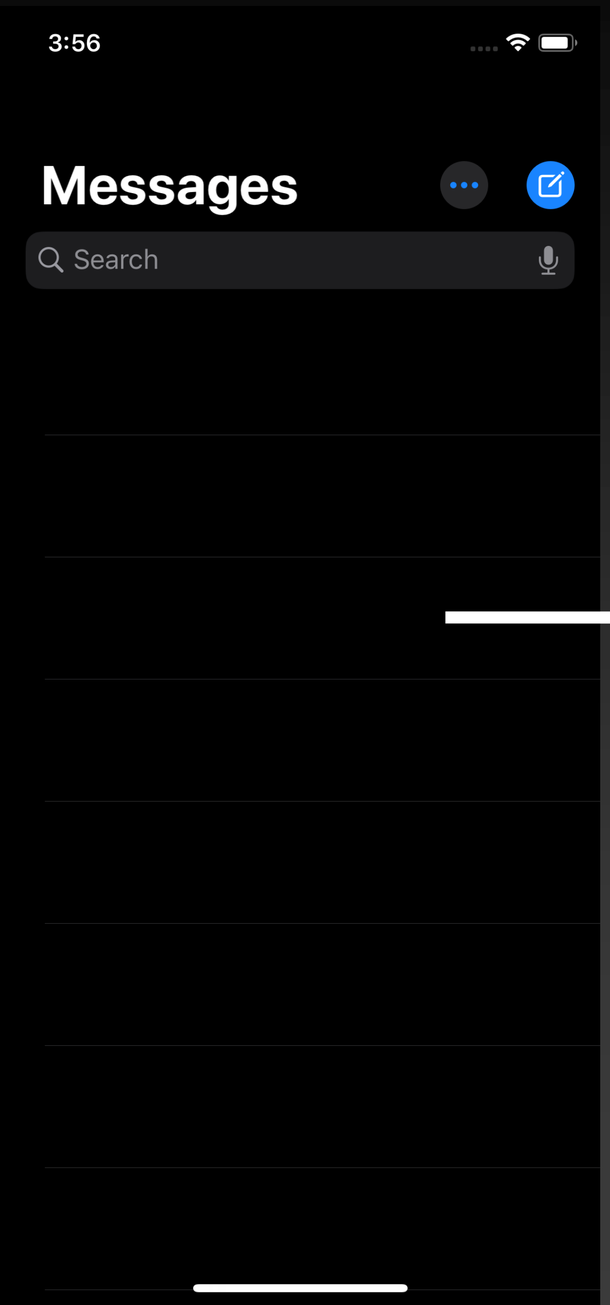
Mobile SMS Previews

Path: /private/var/mobile/Library/Caches/com.apple.MobileSMS/Previews/Search

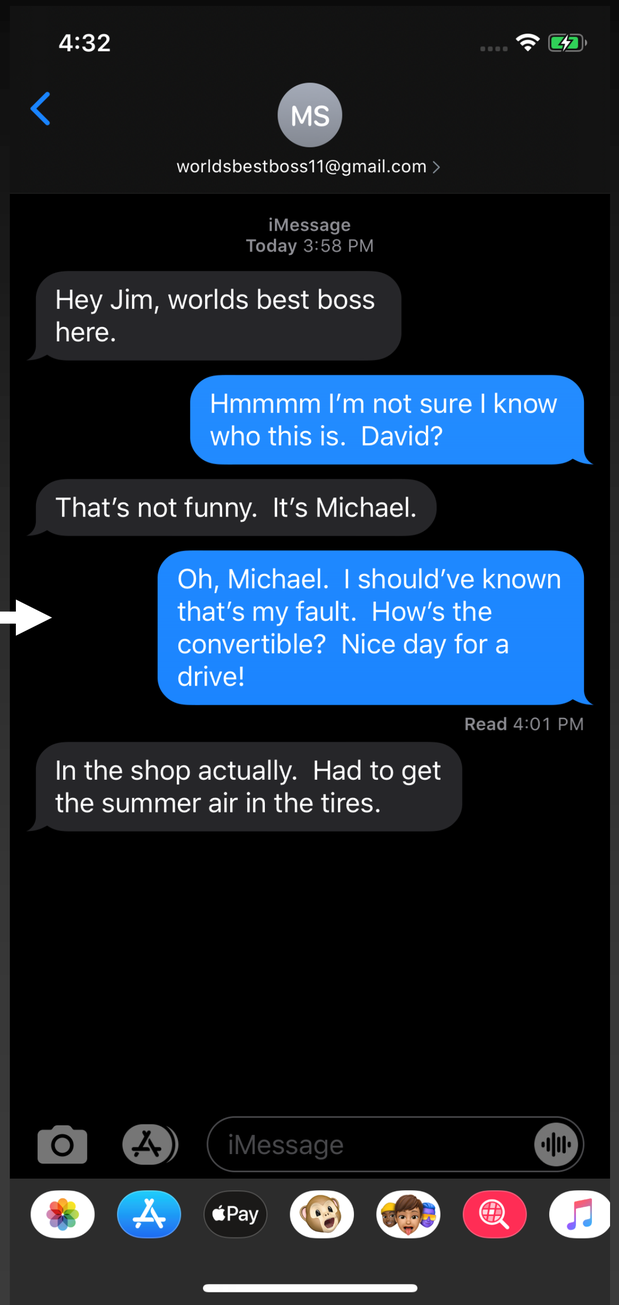
- Not necessarily new, but I didn’t learn about it until very recently and was able to test it on multiple devices with repeated results
- Within Messaging application, if you touch the Contact or Group icon at the top of the screen, and then the small “i” in a circle, it presents among other things the media files exchanged within that thread
- Upon pressing that small “i” in a circle, those photos are written to disk in the path above
- Upon deleting the photo from the thread, and with never having saved the media files, the media files can still be found
- Attribution is the difficult part, but I’ll take a deleted photo all day, every day!

Thanks to Sgt. Ryan Socks for bringing this artifact to my attention!

New Device



iMessage Thread Started



Check of the Directory

```
[-bash-3.2# pwd
/private/var/mobile/Library/Caches/com.apple.MobileSMS
[-bash-3.2# ls -la
total 0
drwxr-xr-x   3 mobile  mobile    96 Jul  9 15:56 .
drwx------  92 mobile  mobile  2944 Jul  9 16:08 ..
drwxr-xr-x   3 mobile  mobile    96 Jul  9 15:56 Plugins
```

../Previews/Search doesn't exist!

Photo Received While Monitoring the ../com.apple.MobileSMS/ directory

```
[-bash-3.2# /usr/bin/fsmon /private/var/mobile/Library/Caches/com.apple.MobileSMS
FSE_CREATE_DIR  72      "imagent"       /private/var/mobile/Library/Caches/com.apple.MobileSMS/Previews
FSE_CREATE_DIR  72      "imagent"       /private/var/mobile/Library/Caches/com.apple.MobileSMS/Previews/Attachments
FSE_CREATE_DIR  72      "imagent"       /private/var/mobile/Library/Caches/com.apple.MobileSMS/Previews/Attachments/73
FSE_CREATE_DIR  72      "imagent"       /private/var/mobile/Library/Caches/com.apple.MobileSMS/Previews/Attachments/73/03
FSE_CREATE_DIR  72      "imagent"       /private/var/mobile/Library/Caches/com.apple.MobileSMS/Previews/Attachments/73/03/1E2B1297-BE1D-47F9-B4CE-E4994BDBE509
```

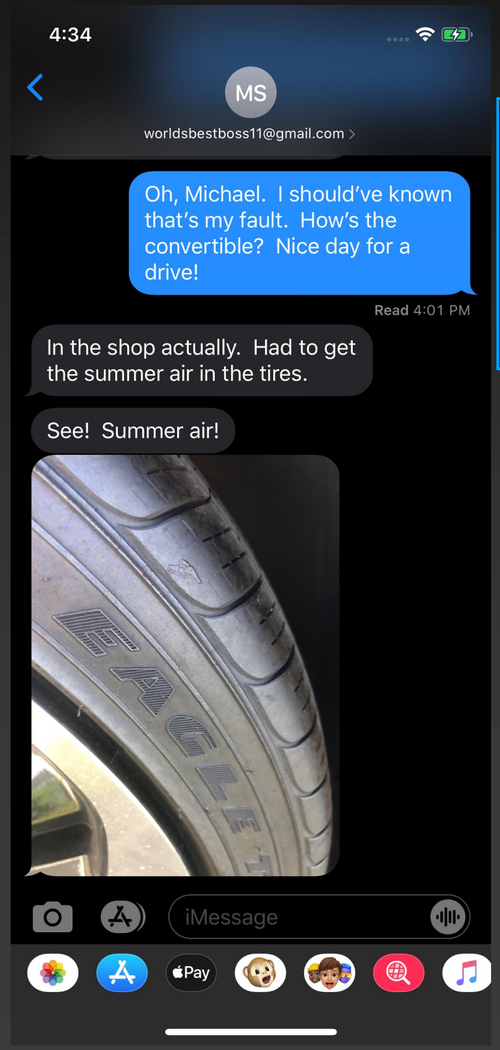
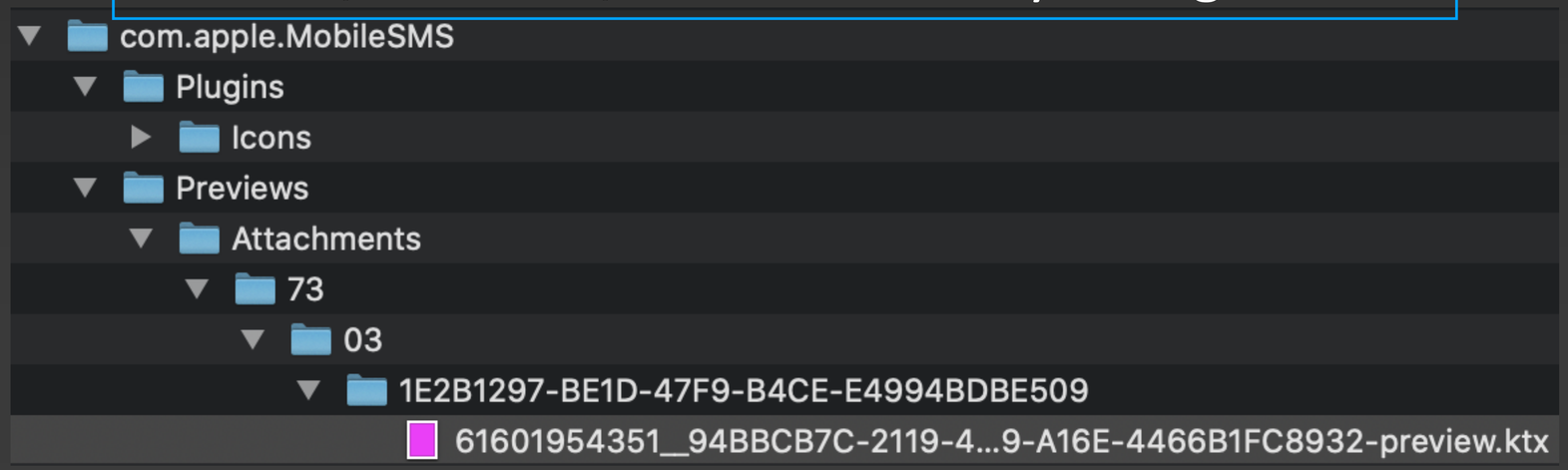
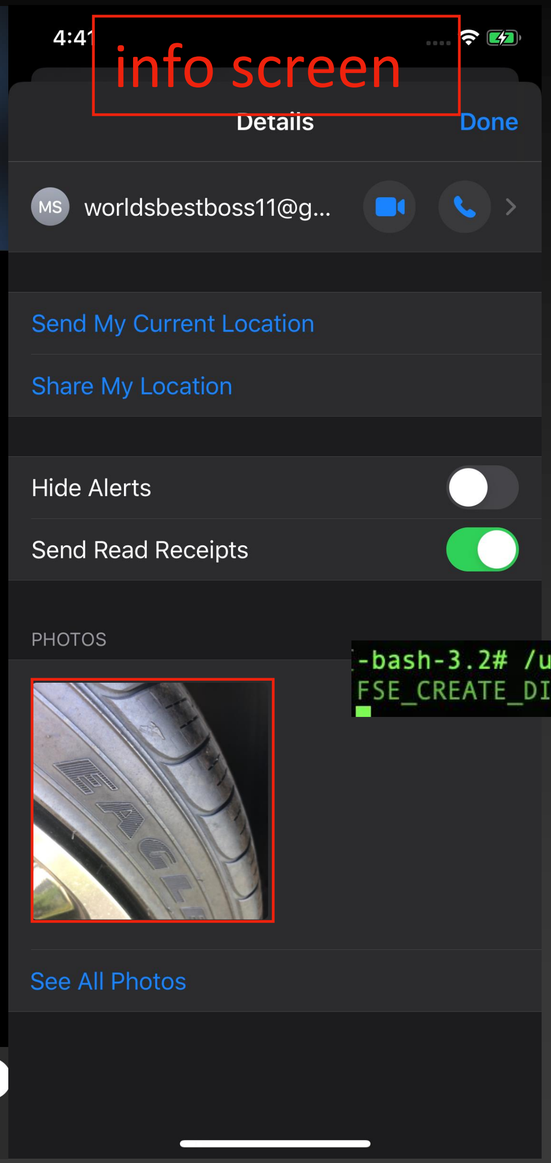


Photo received Message thread populated the ../Previews/Attachments directory and stored a .ktx image file there that was NOT a preview of the attachment, but instead an all pink image.

Still no ../Previews/Search directory though!



Press the small i for info while monitoring the ../com.apple.MobileSMS/ directory

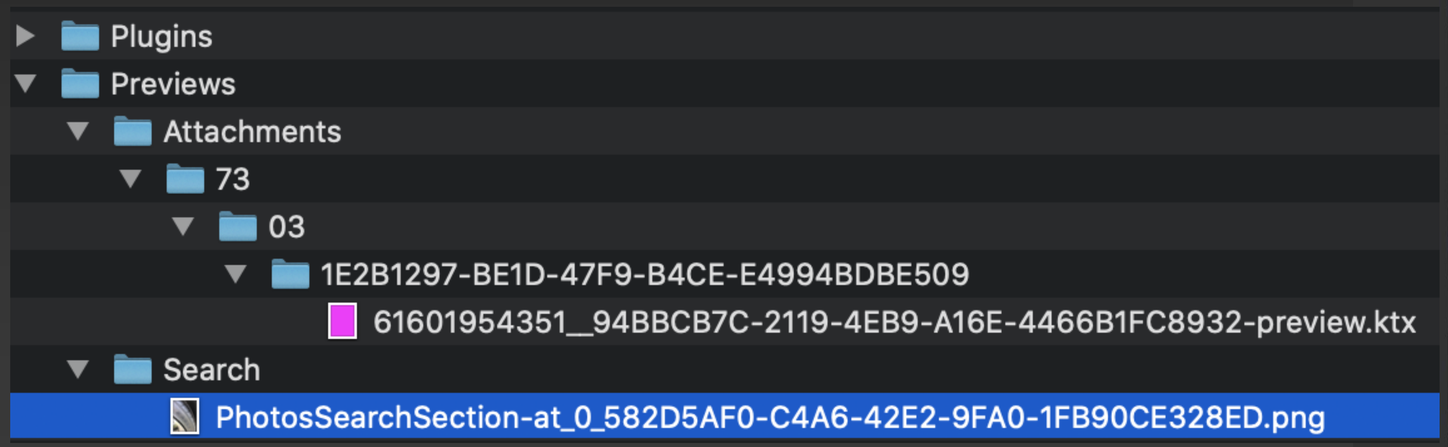


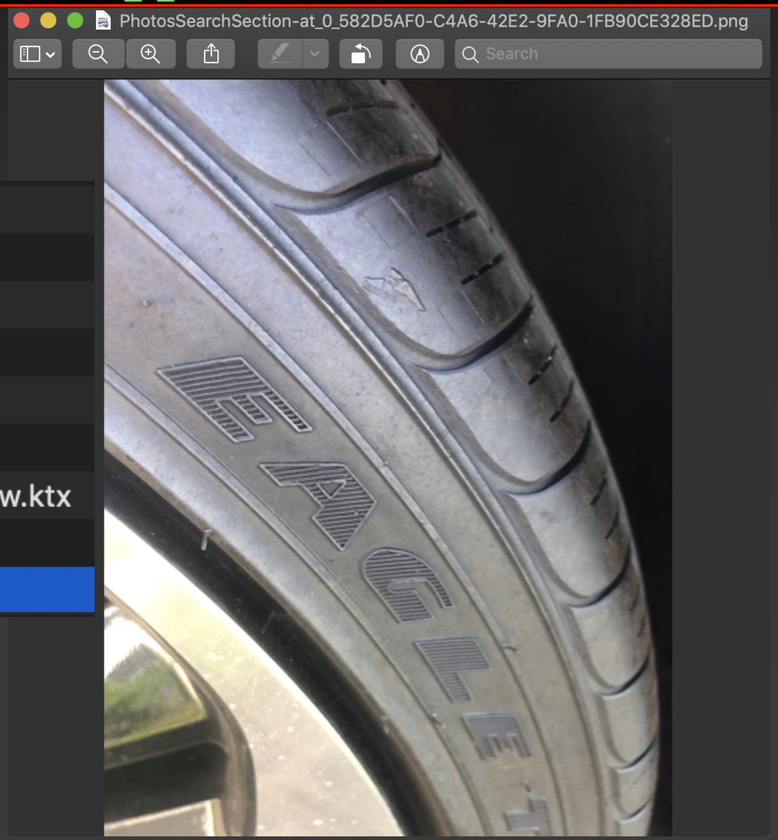
../Previews/Search directory is created!

```
-bash-3.2# /usr/bin/fsmon /private/var/mobile/Library/Caches/com.apple.MobileSMS
FSE_CREATE_DIR  5769    "MobileSMS"     /private/var/mobile/Library/Caches/com.apple.MobileSMS/Previews/Search
```

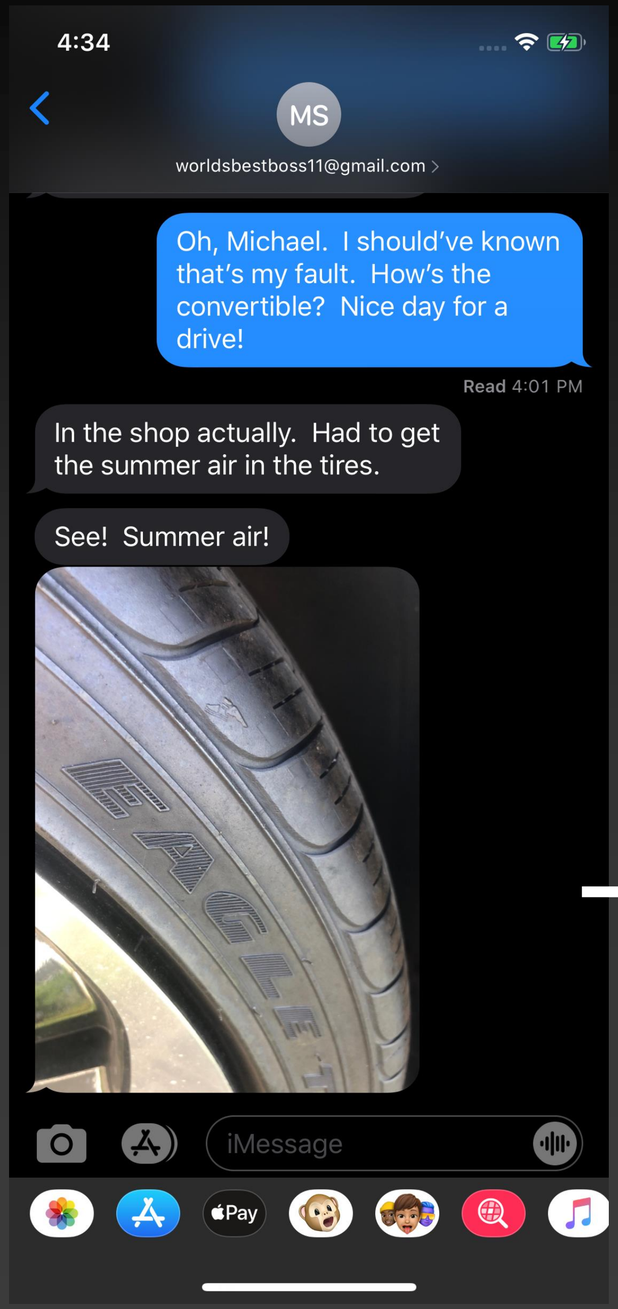
Check of the ../Search directory reveals a .png

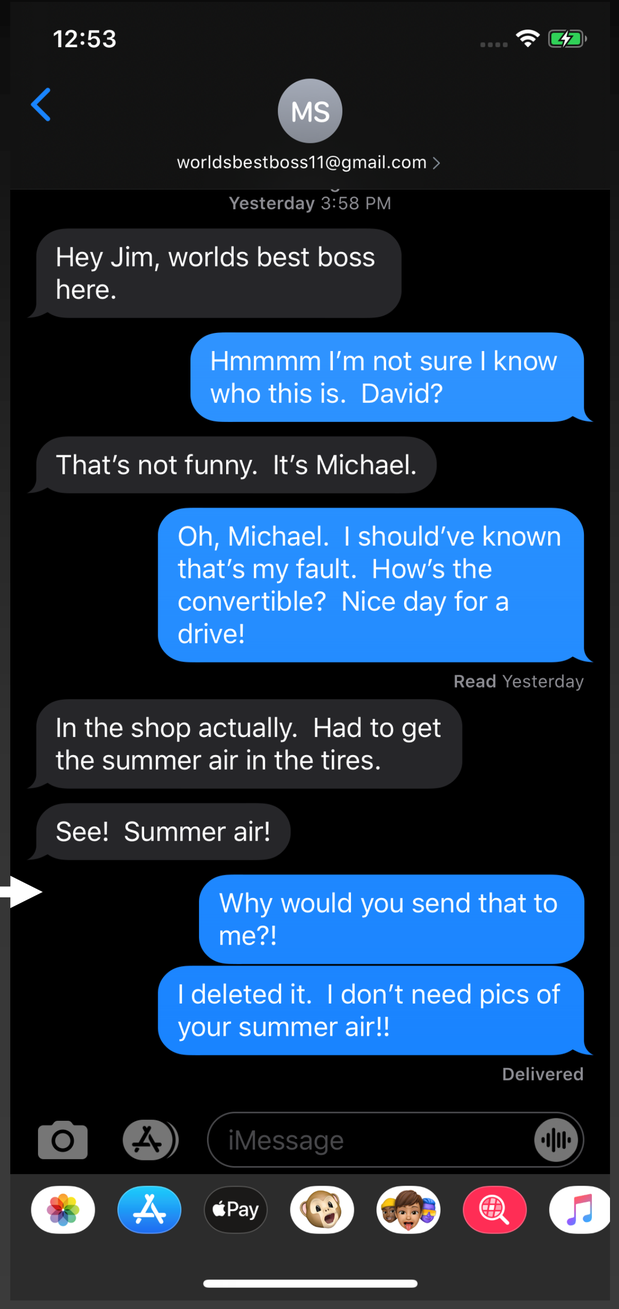
```
[-bash-3.2# /usr/bin/fsmon /private/var/mobile/Library/Caches/com.apple.MobileSMS
 FSE_CREATE_DIR  5769    "MobileSMS"     /private/var/mobile/Library/Caches/com.apple.MobileSMS/Previews/Search
[^C-bash-3.2# ls -la
 total 0
 drwxr-xr-x   4 mobile  mobile   128 Jul  9 16:33 .
 drwx------  93 mobile  mobile  2976 Jul  9 16:40 ..
 drwxr-xr-x   3 mobile  mobile    96 Jul  9 15:56 Plugins
 drwxr-xr-x   4 mobile  mobile   128 Jul  9 16:41 Previews
[-bash-3.2# cd Previews/Search/
[-bash-3.2# ls -la
 total 1008
 drwxr-xr-x  3 mobile  mobile      96 Jul  9 16:41 .
 drwxr-xr-x  4 mobile  mobile     128 Jul  9 16:41 ..
 -rw-r--r--  1 mobile  wheel   514258 Jul  9 16:41 PhotosSearchSection-at_0_582D5AF0-C4A6-42E2-9FA0-1FB90CE328ED.png
```

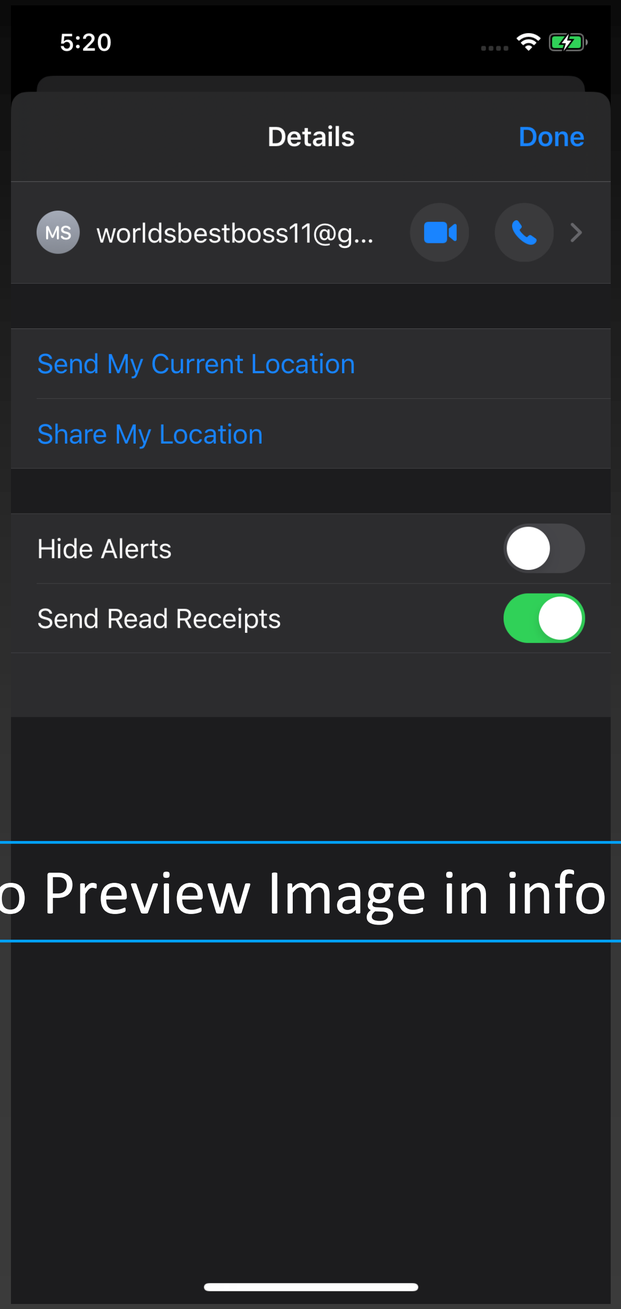




Time to DELETE!!!







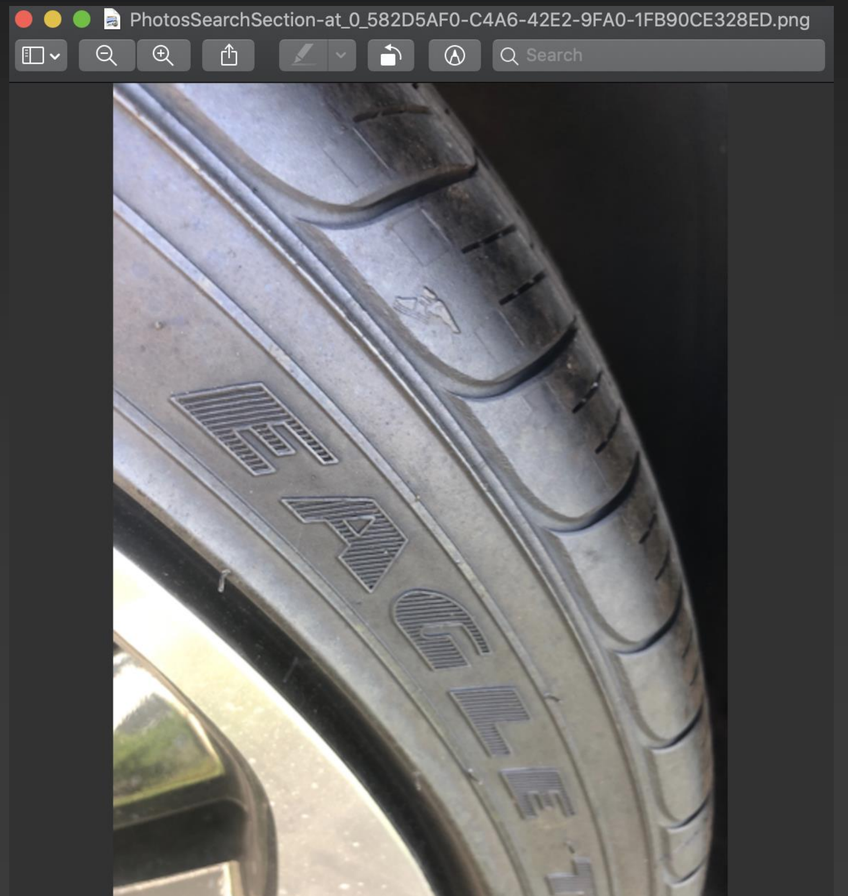
No Preview Image in info

Just Kidding…Not Deleted

Apple kept a copy for you! You're welcome.

4Deleted	Yesterday, 5:19 PM	--	Folder
Plugins	Yesterday, 5:18 PM	--	Folder
Previews	Yesterday, 5:19 PM	--	Folder
Attachments	Today, 12:23 PM	--	Folder
73	Today, 12:23 PM	--	Folder
03	Yesterday, 5:18 PM	--	Folder
Search	Yesterday, 5:18 PM	--	Folder
PhotosSearchSection-at_0_582D5AF0-C4A6-42E2-9FA0-1FB90CE328ED.png	Yesterday, 5:18 PM	514 KB	PNG image

- This photo was never saved anywhere else
- The photo is no longer visible to the user
- Pressing the info small i caused the ../Search directory version of the image to be created
- It IS NOT deleted when the user deletes the image
- It IS NOT deleted when the user deletes the entire thread



Personalization Portrait

PPSQLDatabase.db

Path: /private/var/mobile/Library/PersonalizationPortrait/PPSQLDatabase.db

- Native file first appearing on iOS 13
- iOS 12 had the PersonalizationPortrait directory but no database within it.
- Confirmed in iOS 14 beta via iTunes backup - with even more data!
- Aggregates pieces of data from many different sources including Maps, Mail, Messages, Photos, Safari, News, Notes, and Core Routine data.
- ‘Personalization’ suggests Apple is trying to customize content for the user.
- Data constantly changing as the user performs actions on the device.
- This database is fascinating and frightening at the same time so investigate it, but BE CAREFUL!!

‘loc_records’ table

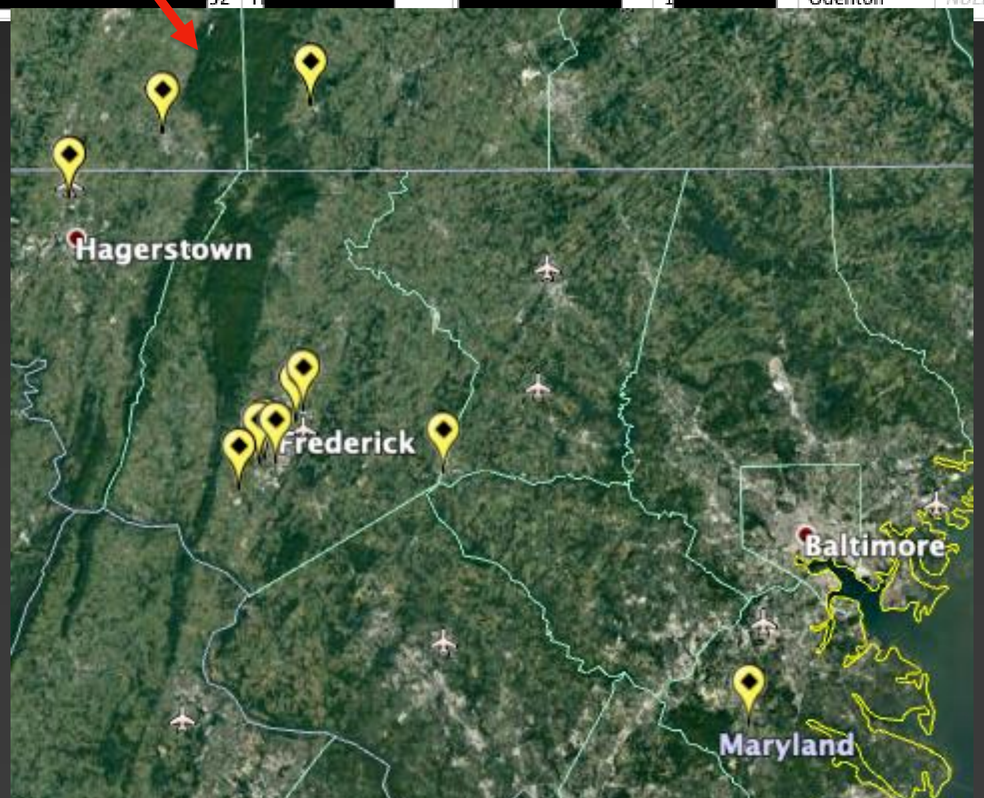
- Can harvest data from 3rd Party Apps, CoreRoutine, Maps, PhotoData, Safari, and more.
- CoreRoutine is duplicative of Local.sqlite, Cloud-V2.sqlite, but this is another source for “Significant Locations” data
- Attribution is difficult! One row from Crew App, next from Apple Maps, then CoreRoutine, and then text from an open Safari tab that included a city, state, or country name.

	id	Bundle ID	Group ID	Source Time	Coordinates	Name	Road	Address #	City	Sub-locality	Admin Area	Sub Admin Area	Postal Code	Country Code	Country
1	129	com.apple.CoreRoutine	*NULL*	2020-07-11 14:06:45	39.	W		6	Frederick	*NULL*	Maryland	Frederick		US	United States
2	130	com.apple.CoreRoutine	*NULL*	2020-07-11 14:06:45	39.	M y		2	Middletown	*NULL*	Maryland	Frederick		US	United States
3	131	com.apple.CoreRoutine	*NULL*	2020-07-11 14:06:45	39.	E		8	Middletown	*NULL*	Maryland	Frederick		US	United States
4	132	com.apple.CoreRoutine	*NULL*	2020-07-11 14:06:45	39.	B Plaza	ke	5	Frederick	*NULL*	Maryland	Frederick		US	United States
5	133	com.apple.CoreRoutine	*NULL*	2020-07-11 14:06:45	39.	F		4	Waynesboro	*NULL*	Pennsylvania	Franklin		US	United States
6	134	com.apple.CoreRoutine	*NULL*	2020-07-11 14:06:45	39. 18	R		1 8	Orchard Hills	*NULL*	Maryland	Washington		US	United States
7	135	com.apple.CoreRoutine	*NULL*	2020-07-11 14:06:45	39.	R		1	Mount Airy	*NULL*	Maryland	Carroll		US	United States
8	136	com.apple.CoreRoutine	*NULL*	2020-07-11 14:06:45	39. 32	H		1	Odenton	*NULL*	Maryland	Anne Arundel		US	United States

com.apple.CoreRoutine

Data selected then placed onto a map, and it's accurate!

	id	Bundle ID	Group ID	Source Time	Coordinates	Name	Road	Address #	City	Sub-locality	Admin Area	Sub Admin Area	Postal Code	Country Code	Country
1	129	com.apple.CoreRoutine	NULL	2020-07-11 14:06:45	39.	W		6	Frederick	NULL	Maryland	Frederick		US	United States
2	130	com.apple.CoreRoutine	NULL	2020-07-11 14:06:45	39.	M y		2	Middletown	NULL	Maryland	Frederick		US	United States
3	131	com.apple.CoreRoutine	NULL	2020-07-11 14:06:45	39.	E		8	Middletown	NULL	Maryland	Frederick		US	United States
4	132	com.apple.CoreRoutine	NULL	2020-07-11 14:06:45	39.	B Plaza	ke	5	Frederick	NULL	Maryland	Frederick		US	United States
5	133	com.apple.CoreRoutine	NULL	2020-07-11 14:06:45	39.	F		4	Waynesboro	NULL	Pennsylvania	Franklin		US	United States
6	134	com.apple.CoreRoutine	NULL	2020-07-11 14:06:45	39. 18	R		1 8	Orchard Hills	NULL	Maryland	Washington		US	United States
7	135	com.apple.CoreRoutine	NULL	2020-07-11 14:06:45	39.	R		1	Mount Airy	NULL	Maryland	Carroll		US	United States
8	136	com.apple.CoreRoutine	NULL	2020-07-11 14:06:45	39. 32	H		1	Odenton	NULL	Maryland	Anne Arundel		US	United States



‘loc_records’ SQL Query

```sql
select
    loc_records.id,
    sources.bundle_id as "Bundle ID",
    sources.group_id as "Group ID",
    datetime(sources.seconds_from_1970, 'unixepoch') as "Source Time",
    loc_records.cll_latitude_degrees || ", "|| loc_records.cll_longitude_degrees as "Coordinates",
    loc_records.clp_name as "CLP Name",
    loc_records_contextual_ne.name as "Context Name",
    loc_records.clp_thoroughfare as "Road",
    loc_records.clp_subThoroughfare as "Address #",
    loc_records.clp_locality as "City",
    loc_records.clp_subLocality as "Sub-locality",
    loc_records.clp_administrativeArea as "Admin Area",
    loc_records.clp_subAdministrativeArea as "Sub Admin Area",
    loc_records.clp_postalCode as "Postal Code",
    loc_records.clp_ISOcountryCode as "Country Code",
    loc_records.clp_country as "Country",
    hex (loc_records.clp_location) as "Location BLOB (hex)",
    loc_records.extraction_os_build as "iOS Build Version",
    loc_records.category as "Category",
    loc_records.algorithm as "Algorithm",
    loc_records.initial_score as "Initial Score"
from loc_records
left join sources on loc_records.source_id=sources.id
left join loc_records_contextual_ne on loc_records_contextual_ne.loc_id=loc_records.id
where sources.bundle_id is not 'com.apple.news'
```

3rd Party App Data

- Possible to find data derived from a 3rd party installed application that otherwise might have been overlooked.
- Below, a location based notification was setup for a workgroup named “Dundee Candidates” in the Crew app to show chat availability only when the device was in a pre-set geofence.

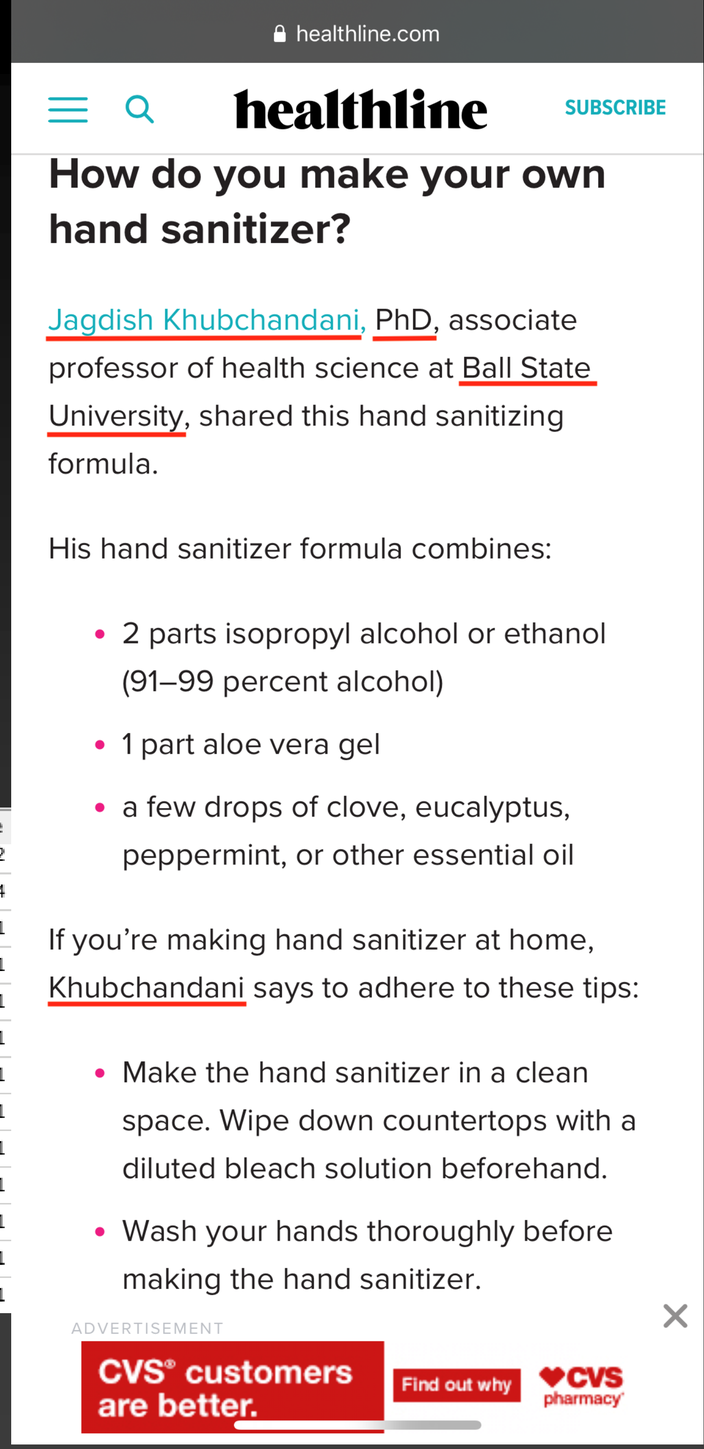
```
1   select
2      loc_records.id,
3      sources.bundle_id as "Bundle ID",
4      loc_records.clp_thoroughfare as "Road",
5      loc_records.clp_locality as "City",
6      loc_records.clp_administrativeArea as "State",
7      loc_records.clp_name,
8      loc_records.cll_latitude_degrees || ", "|| loc_records.cll_longitude_degrees as "Coordinates",
9      sources.group_id as "Group ID"
10  from loc_records
11  left join sources on loc_records.source_id=sources.id
```

	id	Bundle ID	Road	City	State	clp_name	Coordinates
1	1	inc.speramus.ios.crew	[redacted] Dr	Frederick	MD	Dundee Candidates	*NULL*
2	2	inc.speramus.ios.crew	[redacted] Dr	Frederick	MD	Dundee Candidates	*NULL*
3	3	inc.speramus.ios.crew	[redacted] Dr	Frederick	MD	Dundee Candidates	*NULL*
4	4	inc.speramus.ios.crew	[redacted] Dr	Frederick	MD	Dundee Candidates	*NULL*

‘ne_records’ table

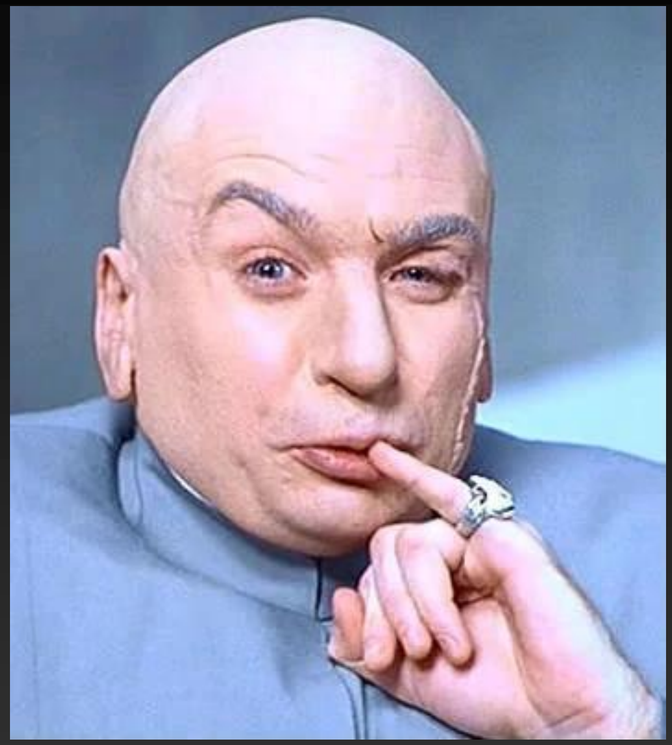
- ‘ne’ believed to mean ‘name’
- Selects ‘name’ data from Safari browser tabs, Apple Maps, CoreRoutine, Contacts, and other sources
- Name can be of a place, person, company, object (such as “Outback Dundee Lounger” as a type of chair)

id	Name	Source Bundle	Source Doc ID	Source Timestamp	Category	Language	Score	Occurrences in Source
546	FDA	com.apple.mobilesafari	22037111E85CF93704C34AB20C30D78BA416C759A23...	2020-07-11 16:15:32	2	en	0.5625	2
547	CDC	com.apple.mobilesafari	22037111E85CF93704C34AB20C30D78BA416C759A23...	2020-07-11 16:15:32	2	en	0.703125	4
548	Food and Drug Administration	com.apple.mobilesafari	22037111E85CF93704C34AB20C30D78BA416C759A23...	2020-07-11 16:15:32	2	en	0.375	1
549	Jagdish Khubchandani	com.apple.mobilesafari	22037111E85CF93704C34AB20C30D78BA416C759A23...	2020-07-11 16:15:32	1	en	0.375	1
550	World Health Organization	com.apple.mobilesafari	22037111E85CF93704C34AB20C30D78BA416C759A23...	2020-07-11 16:15:32	2	en	0.375	1
551	Spray	com.apple.mobilesafari	22037111E85CF93704C34AB20C30D78BA416C759A23...	2020-07-11 16:15:32	1	en	0.375	1
552	CDCTrusted Source	com.apple.mobilesafari	22037111E85CF93704C34AB20C30D78BA416C759A23...	2020-07-11 16:15:32	2	en	0.375	1
553	Pinterest	com.apple.mobilesafari	22037111E85CF93704C34AB20C30D78BA416C759A23...	2020-07-11 16:15:32	2	en	0.375	1
554	Ball State University	com.apple.mobilesafari	22037111E85CF93704C34AB20C30D78BA416C759A23...	2020-07-11 16:15:32	2	en	0.375	1
555	Khubchandani	com.apple.mobilesafari	22037111E85CF93704C34AB20C30D78BA416C759A23...	2020-07-11 16:15:32	1	en	0.375	1
556	Spanish	com.apple.mobilesafari	22037111E85CF93704C34AB20C30D78BA416C759A23...	2020-07-11 16:15:32	3	en	0.375	1
557	Centers for Disease Control and Prevention	com.apple.mobilesafari	22037111E85CF93704C34AB20C30D78BA416C759A23...	2020-07-11 16:15:32	2	en	0.375	1
558	PhD	com.apple.mobilesafari	22037111E85CF93704C34AB20C30D78BA416C759A23...	2020-07-11 16:15:32	1	en	0.375	1



‘ne_records’ table

Why? Diabolical plan?



Credit: super-villain.fandom.com

- In a recent SMS message with my uncle, I called him “Uncle Rodney” in my reply to him. From that message, the ‘ne_records’ table recorded “Uncle Rodney” and separately his last name which was not said in the SMS message.
- So this table grabbed “Uncle Rodney <Last Name>” and recorded them. WHY?? Is my phone going to use my using “Uncle” to some way associate that contact as a family member?

	id	Name	Source Bundle	Source Doc ID	Source Timestamp	Category	Language	Score	Occurrences in Source	OS Build
14998	269285	Last Name	com.apple.MobileSMS	1B35F270-D4B3-4D27-9322-2C1B57CB6016	2020-07-06 13:29:14	1	en	0.5	1	iOS-17F75
14999	269286	Uncle Rodney	com.apple.MobileSMS	1B35F270-D4B3-4D27-9322-2C1B57CB6016	2020-07-06 13:29:14	1	en	0.5	1	iOS-17F75

‘ne_records’ SQL Query

```sql
select
    ne.id,
    ne.name as "Name",
    s.bundle_id as "Source Bundle",
    s.doc_id as "Source Doc ID",
    datetime(s.seconds_from_1970, 'unixepoch') as "Source Timestamp",
    ne.category as "Category",
    ne.language as "Language",
    ne.initial_score as "Score",
    ne.occurrences_in_source as "Occurrences in Source",
    ne.extraction_os_build as "OS Build"
from ne_records ne
left join sources s where s.id=ne.source_id
```

‘tp_records’ table

- ‘tp’ believed to mean ‘topic’
- Interesting artifact is the ‘extraction_os_build’ column which can contain other Cloud connected devices
- Can be joined to ‘sources’ table to get a rough estimate of the timeframe for the OS upgrades, and also show when the activity came from a secondary device

Table: tp_records

	id	topic_id	algorithm	initial_score	decay_rate	sentiment_score	extraction_os_build
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	39	Q1370	4	1.0	0.0	0.0	iOS-17A577
2	40	Q298594	1	0.909090909090909	0.0	0.0	macOS-18G87
3	41	Q48493	1	0.833333333333333	0.0	0.0	macOS-18G87
4	42	Q2766	1	1.0	0.0	0.0	macOS-18G87

iOS Version History
iOS-17A577 = iOS 13.0
iOS-17A878 = iOS 13.1.3
iOS-17B111 = iOS 13.2.3
iOS-17C54 = iOS 13.3
iOS-17D50 = iOS 13.3.1
iOS-17F75 = iOS 13.5

Credit: theiphonewiki.com

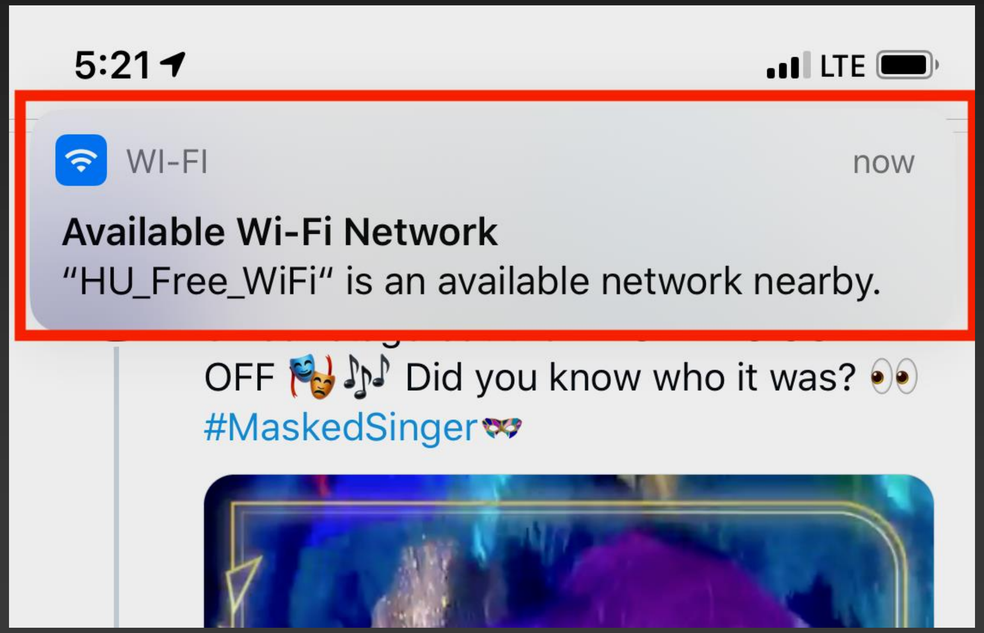
‘tp_records’ SQL Query

```sql
select DISTINCT
    tp.id,
    tp.extraction_os_build as "Extraction OS Build",
    datetime(sources.seconds_from_1970, 'unixepoch') as "Source Time"
from tp_records tp
left join sources on sources.id=tp.source_id
```

	id	Extraction OS Build	Source Time
1	39	iOS-17A577	2019-09-21 16:18:08
2	40	macOS-18G87	2019-09-13 02:56:55

Three Bars

How many bars?



Apparently just three.

ThreeBars.sqlite

Path: /private/var/root/Library/Caches/com.apple.wifid/ThreeBars.sqlite

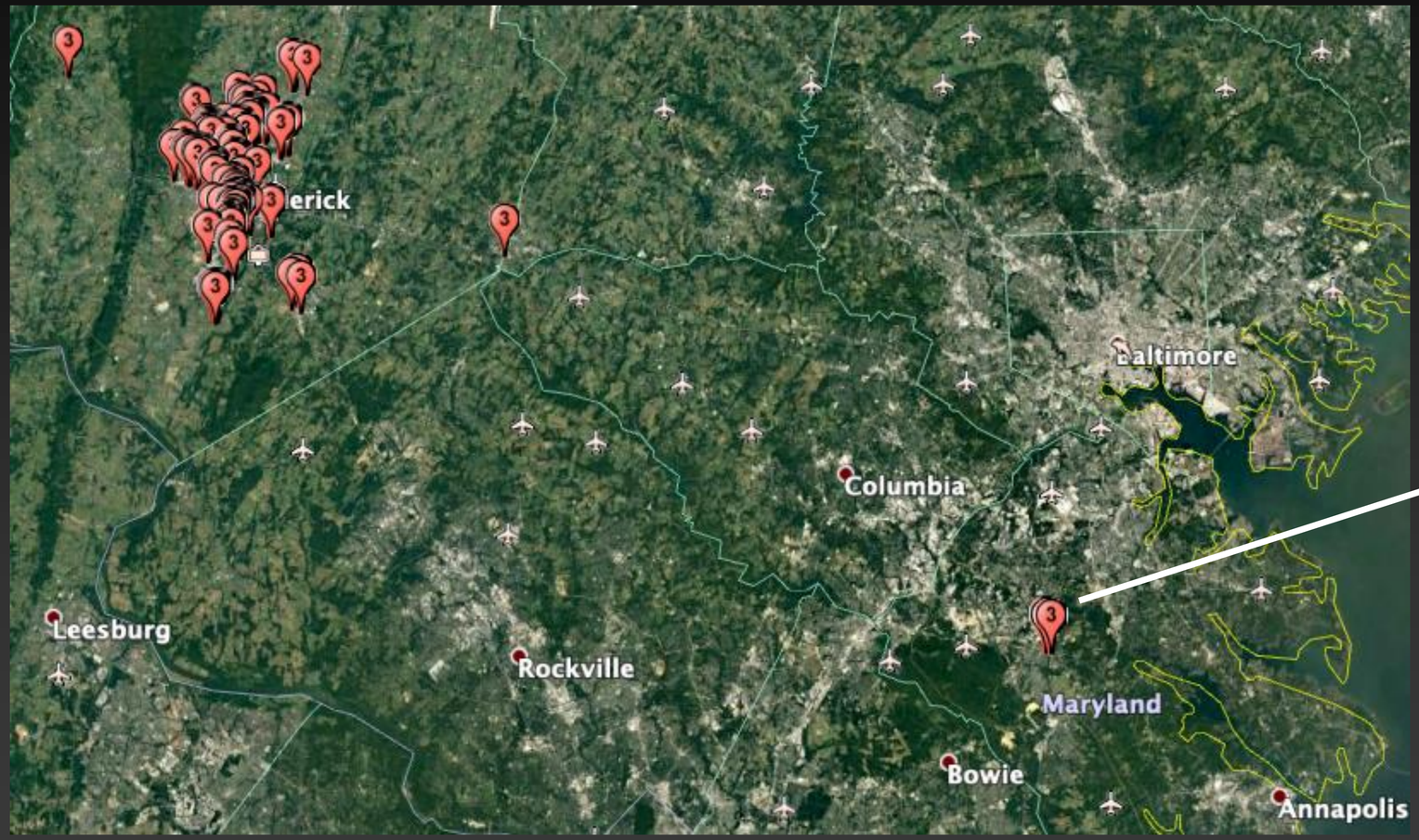
- Believed to be Apple offering publicly available WiFi access points to iDevices
- Tends to be commercial buildings, not residential homes
- Coarse location tracking made possible by this file recording Latitude, Longitude and WiFi BSSID's (Basic Service Set Identifiers) of nearby access points
- Relies on an internet connection (WiFi or cellular) to estimate the location of the device as it relates to nearby WiFi access points.
  - Tested device with no internet connection using navigation app, and no data was populated to this file
- ~6 days of stored data
- How are these networks populated?
  - If a hotel's open WiFi constantly has iPhones connected to it…does Apple give that network a higher popularity score?

ThreeBars.sqlite SQL Query

```
3   select
4       datetime(zap.ZCREATED+978307200, 'unixepoch') as "Created Time",
5       zap.ZLAT as "Latitude",
6       zap.ZLNG as "Longitude",
7       zap.ZBSSID as "BSSID",
8       zn.ZPOPULARITYSCOREVALUE as "Popularity Score",
9       zn.ZPUBLIC as "Public",
10      zn.ZNAME as "Name",
11      zn.ZAUTHMASK as "AuthMask",
12      zn.ZCAPTIVE as "Captive",
13      zn.ZMOVING as "Moving"
14  from ZACCESSPOINT zap
15  left join ZNETWORK zn on zn.Z_PK=zap.ZNETWORK
```

	Created Time	Latitude	Longitude	BSSID	Popularity Score	Public	AuthMask	Captive	Name	Moving
1	2020-07-04 08:10:59	39.[redacted]	-77.[redacted]	04:da:d[redacted]	588	1	1	1		0
2	2020-07-04 08:10:59	39.[redacted]	-77.[redacted]	0c:27:2[redacted]	588	1	1	1		0
3	2020-07-04 08:10:59	39.[redacted]	-77.[redacted]	68:86:a[redacted]	588	1	1	1		0
4	2020-07-04 08:10:59	39.[redacted]	-77.[redacted]	34:bd:c[redacted]	588	1	1	1		0
5	2020-07-04 08:10:59	39.[redacted]	-77.[redacted]	04:da:d[redacted]	588	1	1	1		0
6	2020-07-04 08:10:59	39.[redacted]	-77.[redacted]	34:bd:c[redacted]	588	1	1	1		0
7	2020-07-04 08:10:59	39.[redacted]	-77.[redacted]	58:97:1[redacted]	588	1	1	1		0
8	2020-07-04 08:10:59	39.[redacted]	-77.[redacted]	04:da:d[redacted]	588	1	1	1		0
9	2020-07-04 08:10:59	39.[redacted]	-7[redacted]	34:bd:c[redacted]	588	1	1	1		0
10	2020-07-04 08:10:59	39.[redacted]	-77.[redacted]	04:da:d[redacted]	588	1	1	1		0
11	2020-07-04 08:10:59	39.[redacted]	-77.[redacted]	34:bd:c[redacted]	588	1	1	1		0
12	2020-07-04 08:10:59	39.[redacted]	-77.[redacted]	04:da:d[redacted]	588	1	1	1		0

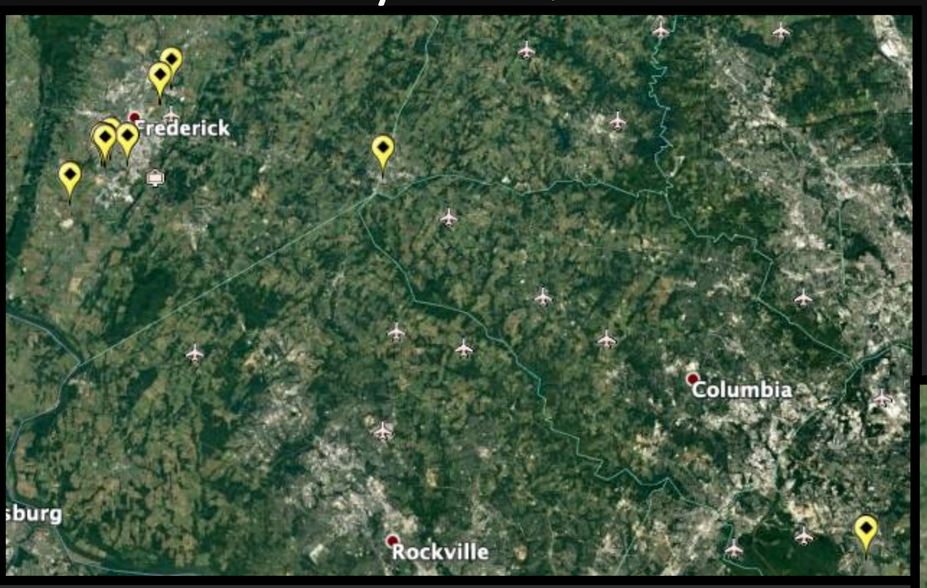
Rough Locations



Location Tracking

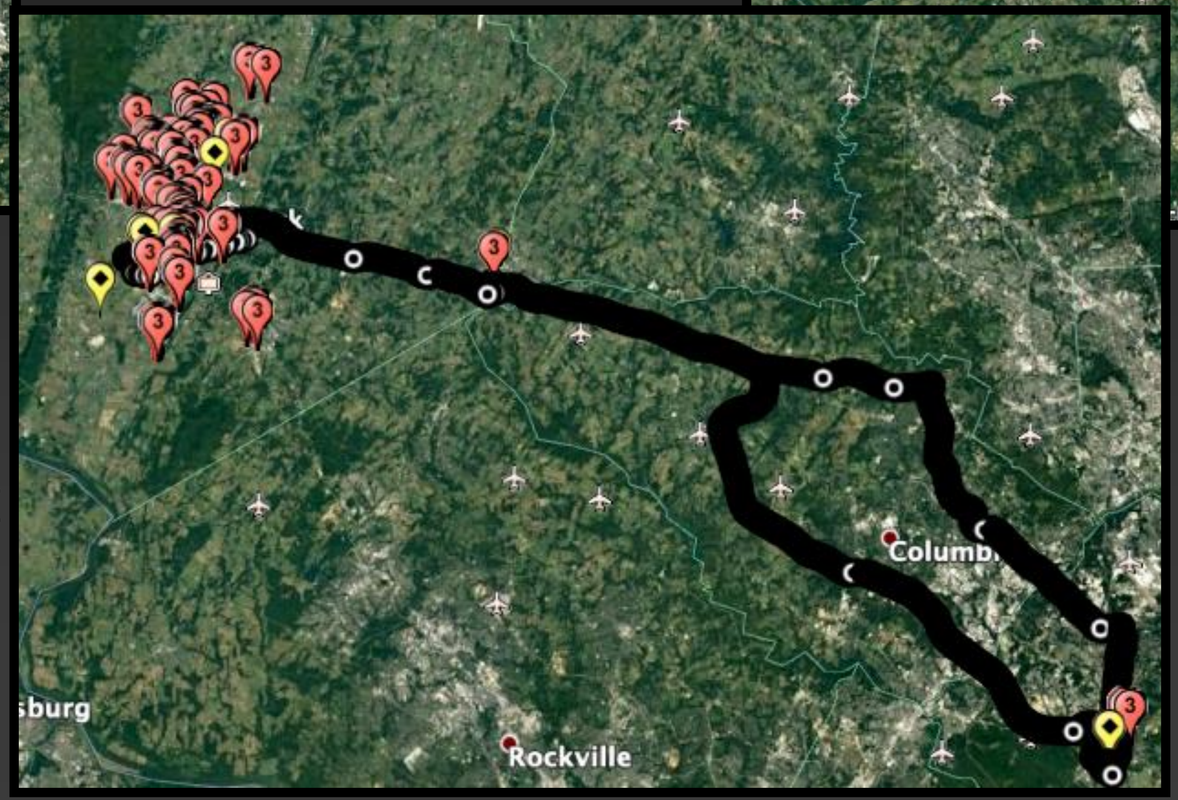
Ehh..sort of.

Only PPSQL



Only ThreeBars

PPSQL+ThreeBars+Cache.sqlite



Do you care?

- Every iPhone on iOS 13+ is constantly checking in with Apple on where it is when it is internet connected, and this file populates nearby wireless access points.
- Fences and gates do not stop the access point data from being shared to nearby iDevices.
- Is your corporate / government access point making this list?
- Does this mean Apple knows how many iPhones are connected to a WiFi network? Are they recording it and then using the data to suggest that network to others nearby?

All My Thanks!

- Sarah Edwards @iamevltwin
- Heather Mahalik @HeatherMahalik
- Brigs @AlexisBrignoni
- Josh Hickman @josh_hickman1
- checkra1n
- unc0ver
- DB Browser for SQLite
- HexFiend

Feeling lucky? Go All In!

Additional details soon on mac4n6.com

Jared Barnhart @bizzybarney

Parsons Corporation Test Engineer, Principal