SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Making a Murderer: Health Activity Edition

Heather Mahalik
heather@smarterforensics.com
Twitter @HeatherMahalik

About Me

- Director, Forensic Engineering at ManTech CARD
- SANS Senior Instructor, Course Author and FOR585 Course Lead
- Involved with InfoSec/Forensics for 16+ years
- Co-Author of Practical Mobile Forensics (1st and 2nd Editions)
- Blog at smarterforensics.com
- Wife and a mama
- Dog, horse, wine and bourbon lover ☺

Why Health Data?

MOTHERBOARD

PRIVACY

Apple Health Data Is Being Used as Evidence in a Rape and Murder Investigation

German authorities cracked a man's iPhone and found out what he was up to.

SHARE TWEET

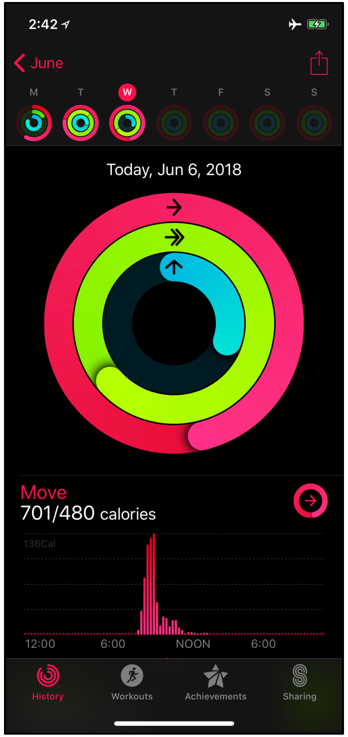
Samantha Cole
Jan 11 2018, 8:00am

Apple health data used in murder trial

12 January 2018

Share

Gaining Access



Today, Jun 6, 2018

Move
701/480 calories

Includes Health and Activity App Data

Encrypted iOS Backups

- Includes tool backup/file system dumps
- NOT in unencrypted backups

Health App Export

- XML Files – very messy dataset

iCloud Backups

SANS DFIR

How to Create The Evidence

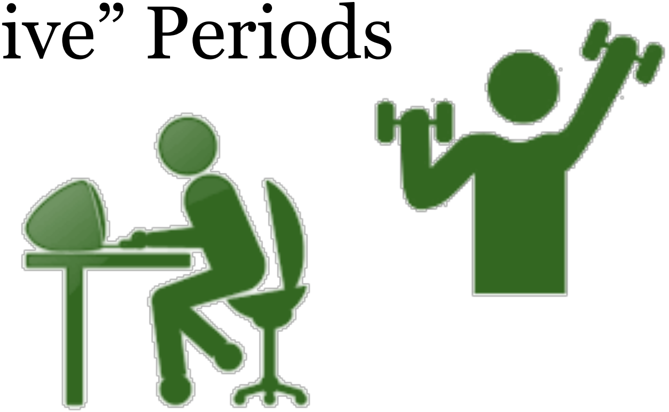
- iTunes – Encryption Selected
- Commercial Tool that Encrypts (Test this)

MAKE SURE YOU KNOW THE PASSWORD!!!!

This will allow account passwords, Health, and HomeKit data to be backed up.

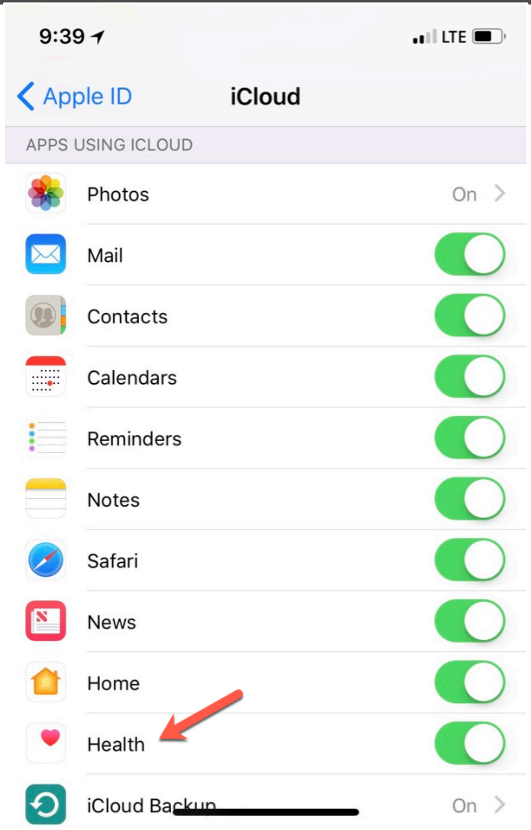
Primary Artifacts

- /private/var/mobile/Library/Health/
  - healthdb.sqlite - Activity Sharing , Settings, Sync, etc.
  - healthdb_secure.sqlite – Achievements, Workouts, Friends, etc.
- Tracks Workout and "Non-Active" Periods
- Historical Database Contents
  - Yep, it seems to never forget!



What You Should Expect

- iPhone Activity
- Apple Watch Activity
- Friends Activity
- 3rd Party Apps Activity
- TONS of data!!!!

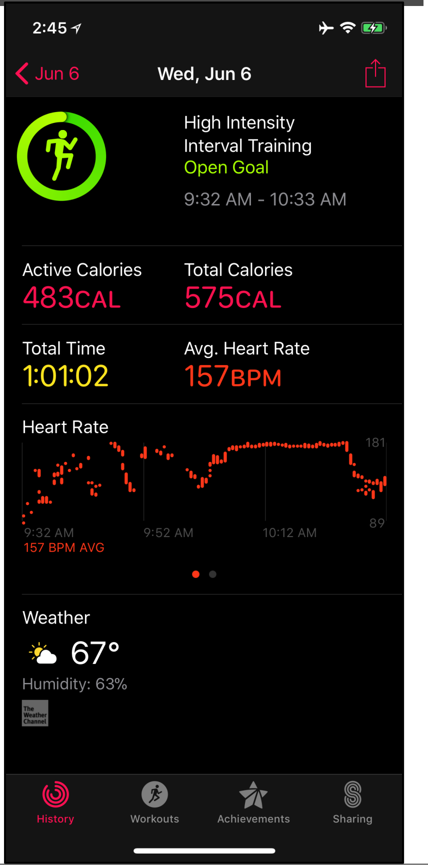


9:39 LTE

< Apple ID iCloud

APPS USING ICLOUD

- Photos: On >
- Mail: On
- Contacts: On
- Calendars: On
- Reminders: On
- Notes: On
- Safari: On
- News: On
- Home: On
- Health: On
- iCloud Backup: On >



2:45

< Jun 6 Wed, Jun 6

High Intensity Interval Training
Open Goal
9:32 AM - 10:33 AM

Active Calories	Total Calories
483CAL	575CAL

Total Time	Avg. Heart Rate
1:01:02	157BPM

Heart Rate

157 BPM AVG

Weather
67°
Humidity: 63%

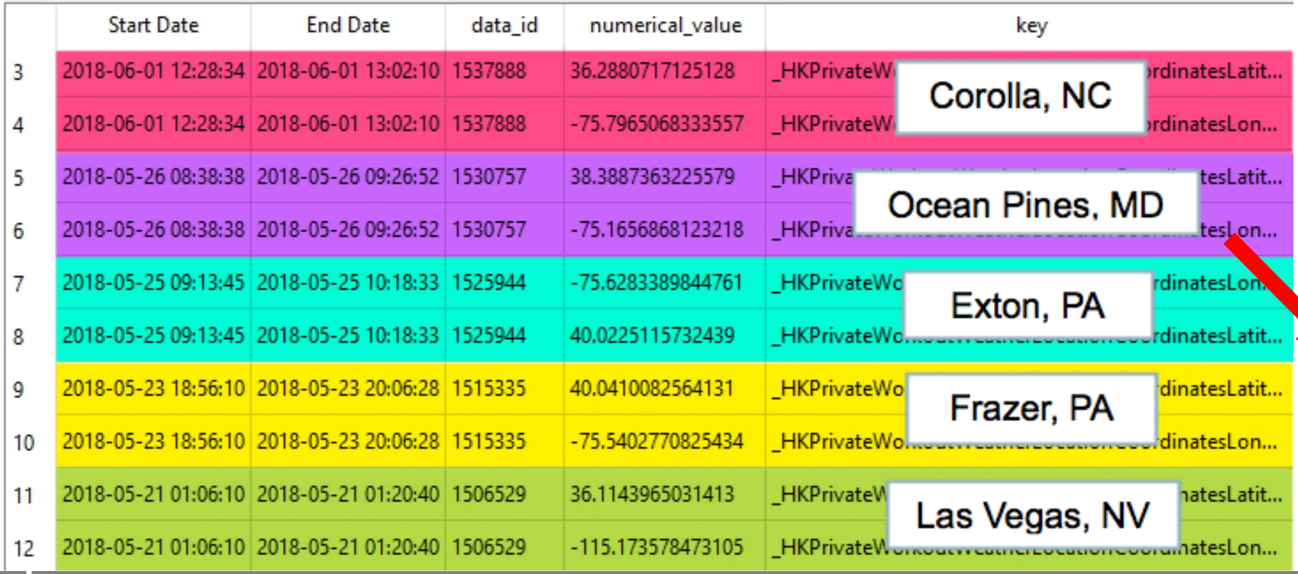
Data Types – What are you looking for?

- 3 = Weight
- 5 = Heart Rate
- 7 = Steps
- 8 = Distance in Meters
- 9 = Resting Energy
- 10 = Active Energy
- 12 = Flights Climbed
- 20’s ~ 30’s = Nutrition
- 67 = Weekly Calorie Goal
- 70= Watch On
- 75 = Stand (Stood)
- 76 = Activity
- 79 = Workout
- 83 = Some Workouts

Forensic Scenarios – Scene of a Crime

Workout Location Map

Associate to Other Applications – Photos, Mapping, Workout, etc.



	Start Date	End Date	data_id	numerical_value	key
3	2018-06-01 12:28:34	2018-06-01 13:02:10	1537888	36.2880717125128	_HKPrivateW rdinatesLatit...
4	2018-06-01 12:28:34	2018-06-01 13:02:10	1537888	-75.7965068333557	_HKPrivateW rdinatesLon...
5	2018-05-26 08:38:38	2018-05-26 09:26:52	1530757	38.3887363225579	_HKPriva tesLatit...
6	2018-05-26 08:38:38	2018-05-26 09:26:52	1530757	-75.1656868123218	_HKPriva tesLon...
7	2018-05-25 09:13:45	2018-05-25 10:18:33	1525944	-75.6283389844761	_HKPrivateWo rdinatesLon...
8	2018-05-25 09:13:45	2018-05-25 10:18:33	1525944	40.0225115732439	_HKPrivateWo rdinatesLatit...
9	2018-05-23 18:56:10	2018-05-23 20:06:28	1515335	40.0410082564131	_HKPrivateWo rdinatesLatit...
10	2018-05-23 18:56:10	2018-05-23 20:06:28	1515335	-75.5402770825434	_HKPrivateWo rdinatesLon...
11	2018-05-21 01:06:10	2018-05-21 01:20:40	1506529	36.1143965031413	_HKPrivateW natesLatit...
12	2018-05-21 01:06:10	2018-05-21 01:20:40	1506529	-115.173578473105	_HKPrivateW natesLon...

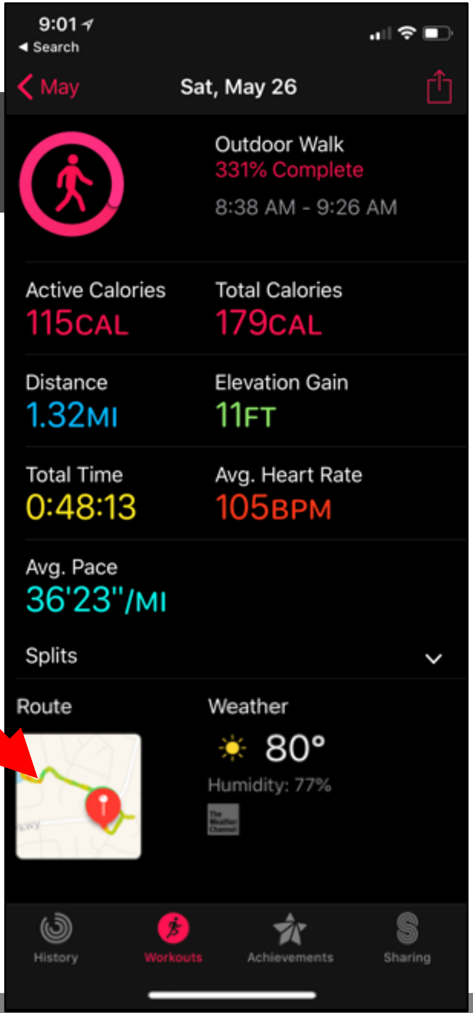
Corolla, NC

Ocean Pines, MD

Exton, PA

Frazer, PA

Las Vegas, NV



9:01

◀ Search

< May Sat, May 26

Outdoor Walk
331% Complete
8:38 AM - 9:26 AM

Active Calories 115CAL	Total Calories 179CAL
Distance 1.32MI	Elevation Gain 11FT
Total Time 0:48:13	Avg. Heart Rate 105BPM
Avg. Pace 36'23"/MI	

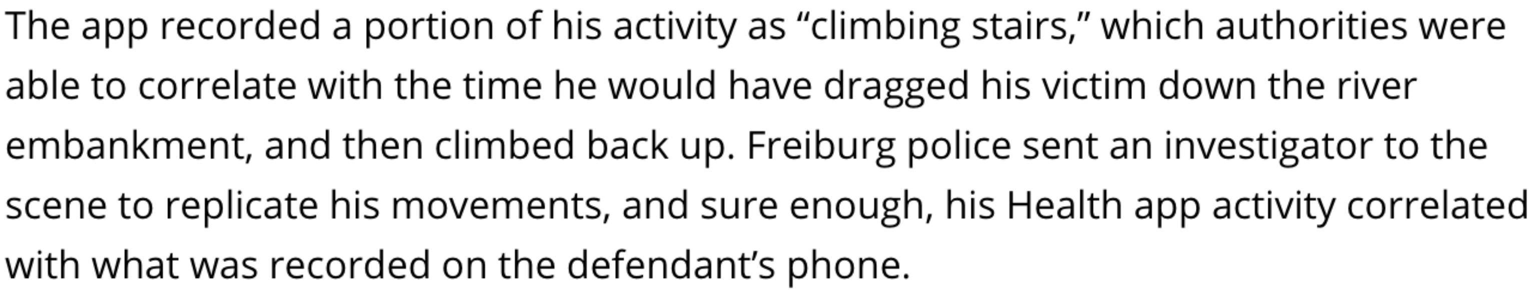
Splits

Route

Weather
80°
Humidity: 77%

Forensic Scenarios – Heart Rate - Dragging a Body

- Changes in Heart Rate Pattern
- Flights Climbed
- Testing by Investigators…

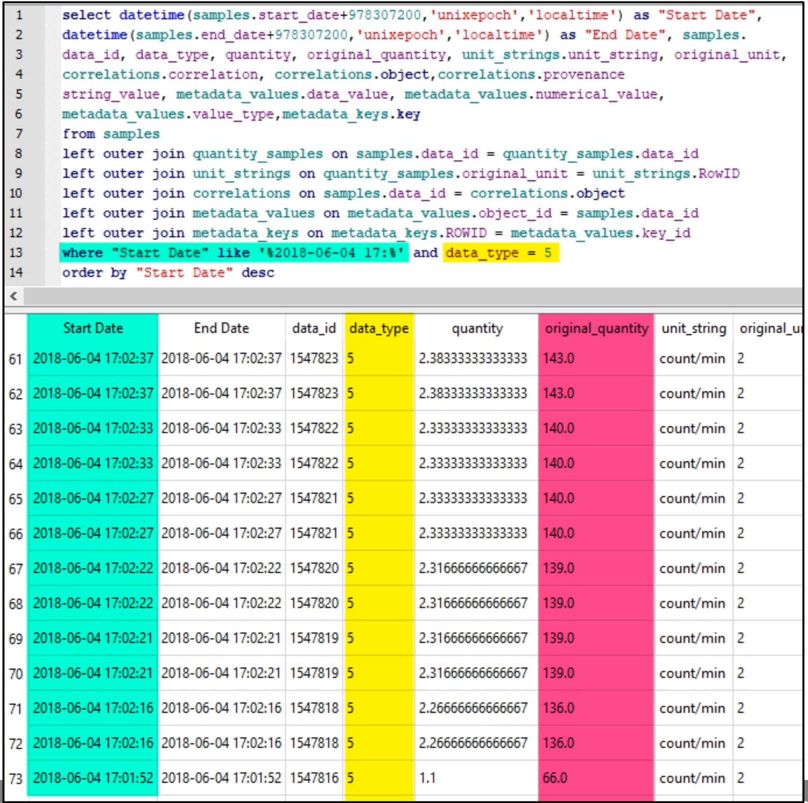


The app recorded a portion of his activity as “climbing stairs,” which authorities were able to correlate with the time he would have dragged his victim down the river embankment, and then climbed back up. Freiburg police sent an investigator to the scene to replicate his movements, and sure enough, his Health app activity correlated with what was recorded on the defendant’s phone.

And Now My Lawn is Dead

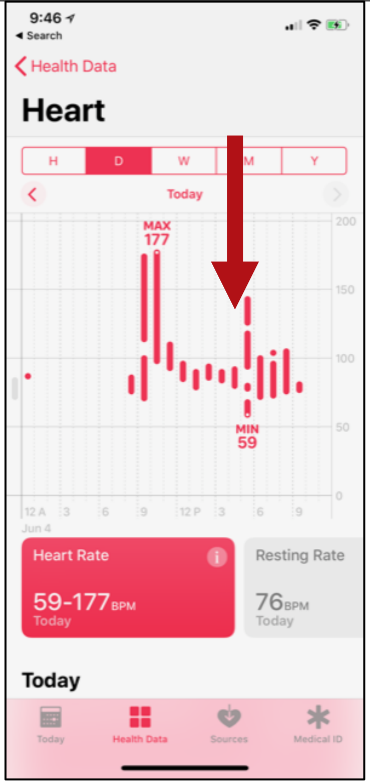
- What This Looked Like

Forensic Scenarios – Heart Rate - Dragging a Body



```sql
select datetime(samples.start_date+978307200,'unixepoch','localtime') as "Start Date",
datetime(samples.end_date+978307200,'unixepoch','localtime') as "End Date", samples.
data_id, data_type, quantity, original_quantity, unit_strings.unit_string, original_unit,
correlations.correlation, correlations.object,correlations.provenance
string_value, metadata_values.data_value, metadata_values.numerical_value,
metadata_values.value_type,metadata_keys.key
from samples
left outer join quantity_samples on samples.data_id = quantity_samples.data_id
left outer join unit_strings on quantity_samples.original_unit = unit_strings.RowID
left outer join correlations on samples.data_id = correlations.object
left outer join metadata_values on metadata_values.object_id = samples.data_id
left outer join metadata_keys on metadata_keys.ROWID = metadata_values.key_id
where "Start Date" like '%2018-06-04 17:%' and data_type = 5
order by "Start Date" desc
```

	Start Date	End Date	data_id	data_type	quantity	original_quantity	unit_string	original_u
61	2018-06-04 17:02:37	2018-06-04 17:02:37	1547823	5	2.38333333333333	143.0	count/min	2
62	2018-06-04 17:02:37	2018-06-04 17:02:37	1547823	5	2.38333333333333	143.0	count/min	2
63	2018-06-04 17:02:33	2018-06-04 17:02:33	1547822	5	2.33333333333333	140.0	count/min	2
64	2018-06-04 17:02:33	2018-06-04 17:02:33	1547822	5	2.33333333333333	140.0	count/min	2
65	2018-06-04 17:02:27	2018-06-04 17:02:27	1547821	5	2.33333333333333	140.0	count/min	2
66	2018-06-04 17:02:27	2018-06-04 17:02:27	1547821	5	2.33333333333333	140.0	count/min	2
67	2018-06-04 17:02:22	2018-06-04 17:02:22	1547820	5	2.31666666666667	139.0	count/min	2
68	2018-06-04 17:02:22	2018-06-04 17:02:22	1547820	5	2.31666666666667	139.0	count/min	2
69	2018-06-04 17:02:21	2018-06-04 17:02:21	1547819	5	2.31666666666667	139.0	count/min	2
70	2018-06-04 17:02:21	2018-06-04 17:02:21	1547819	5	2.31666666666667	139.0	count/min	2
71	2018-06-04 17:02:16	2018-06-04 17:02:16	1547818	5	2.26666666666667	136.0	count/min	2
72	2018-06-04 17:02:16	2018-06-04 17:02:16	1547818	5	2.26666666666667	136.0	count/min	2
73	2018-06-04 17:01:52	2018-06-04 17:01:52	1547816	5	1.1	66.0	count/min	2

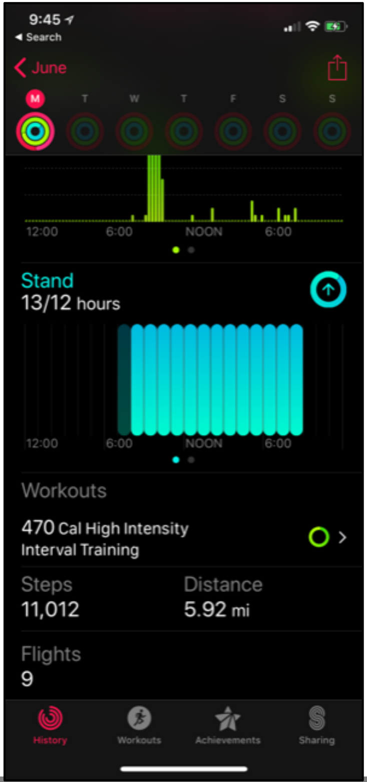


Heart

Heart Rate 59-177 BPM Today

Resting Rate 76 BPM Today

Today



Stand 13/12 hours

Workouts

470 Cal High Intensity Interval Training

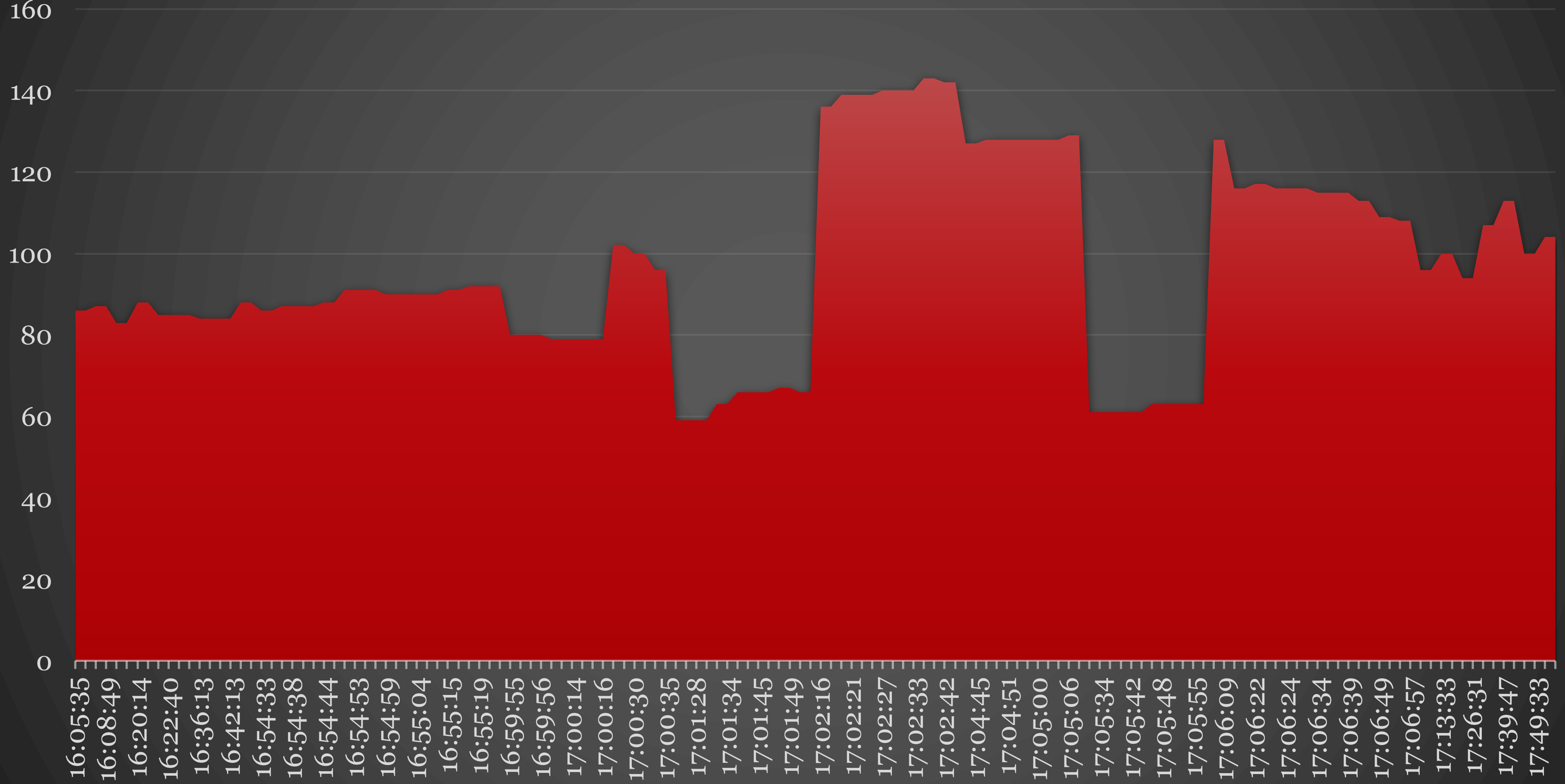
Steps 11,012

Distance 5.92 mi

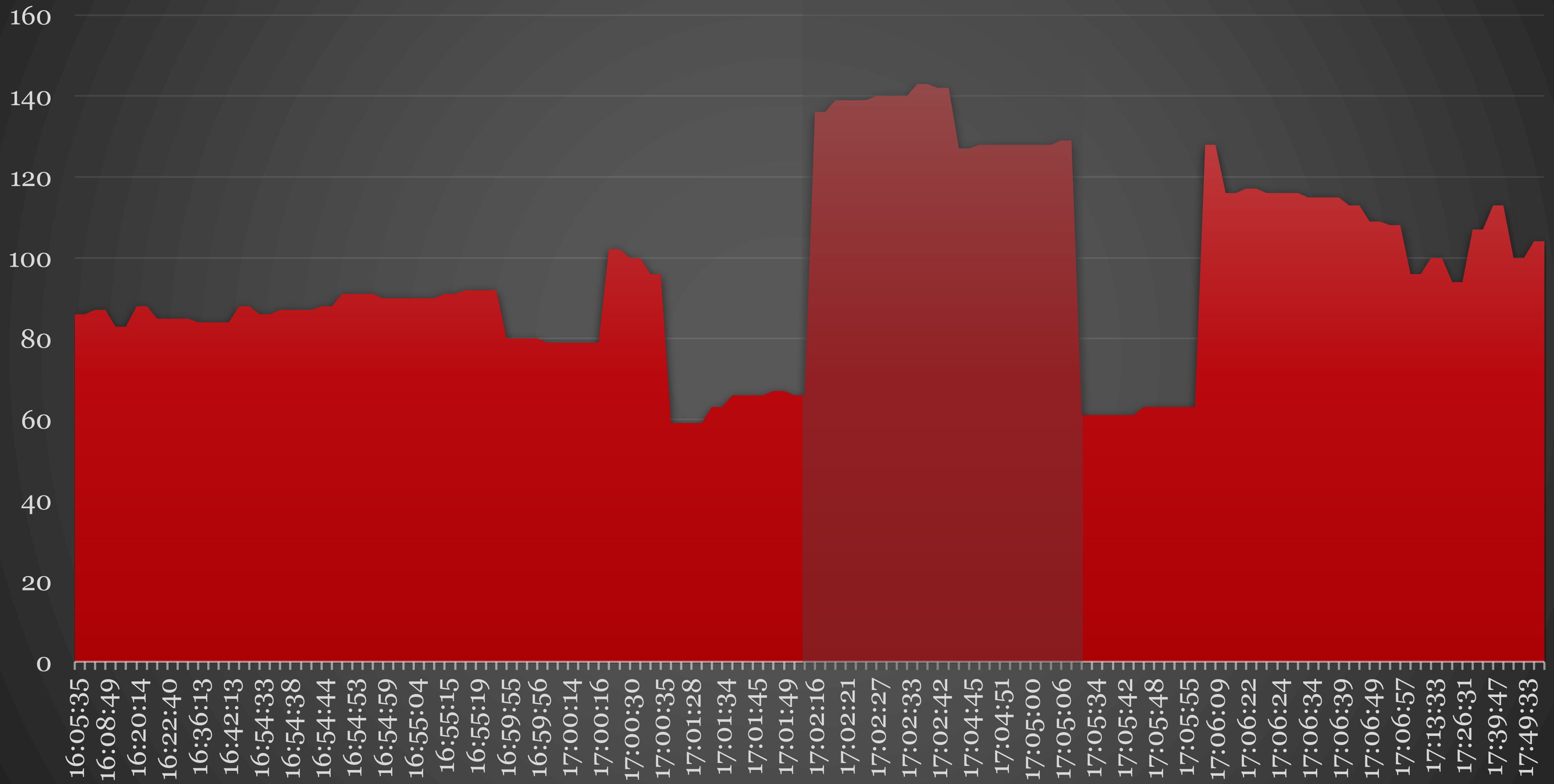
Flights 9

SANS | DFIR

Body Movin'

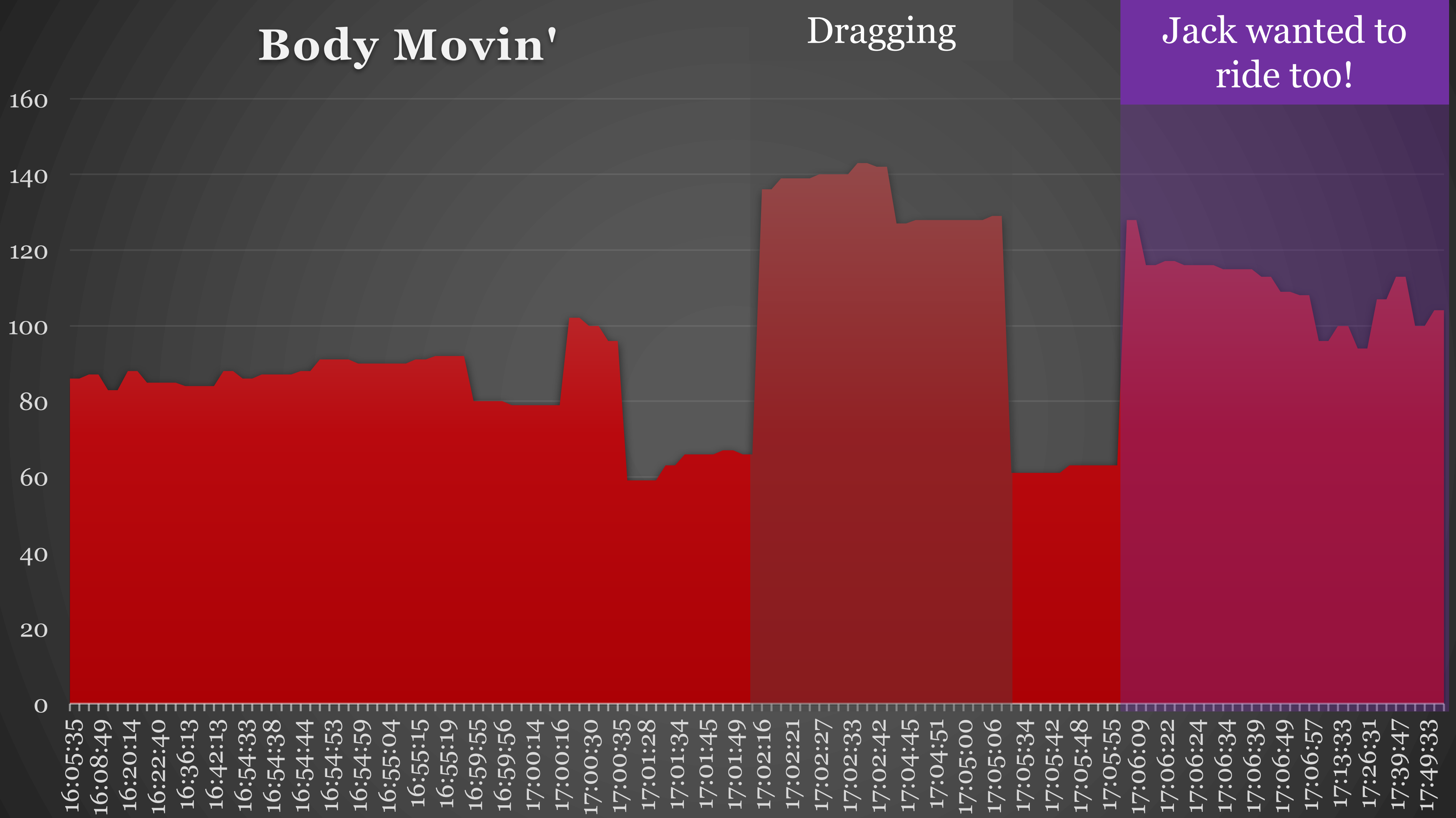

160
140
120
100
80
60
40
20
0
16:05:35
16:08:49
16:20:14
16:22:40
16:36:13
16:42:13
16:54:33
16:54:38
16:54:44
16:54:53
16:54:59
16:55:04
16:55:15
16:55:19
16:59:55
16:59:56
17:00:14
17:00:16
17:00:30
17:00:35
17:01:28
17:01:34
17:01:45
17:01:49
17:02:16
17:02:21
17:02:27
17:02:33
17:02:42
17:04:45
17:04:51
17:05:00
17:05:06
17:05:34
17:05:42
17:05:48
17:05:55
17:06:09
17:06:22
17:06:24
17:06:34
17:06:39
17:06:49
17:06:57
17:13:33
17:26:31
17:39:47
17:49:33

Body Movin'



Dragging

Body Movin'



Dragging

Jack wanted to ride too!

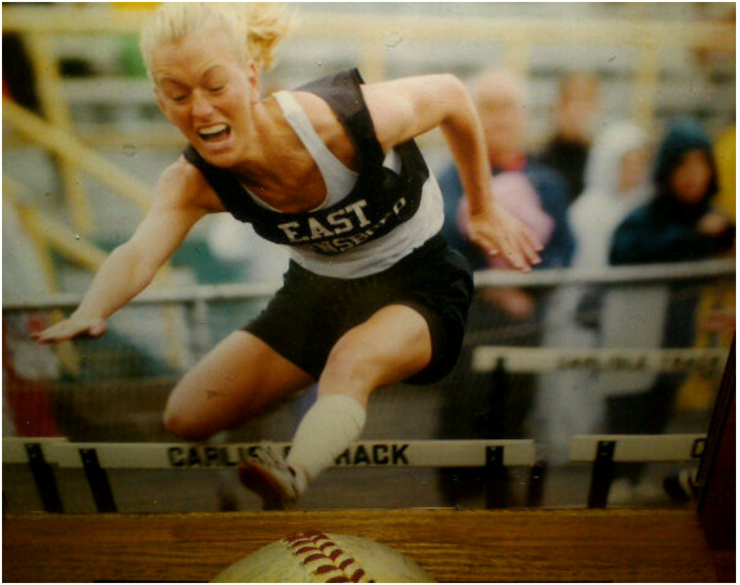
Forensic Scenario: Heart Rate – Dead or Alive?

Death

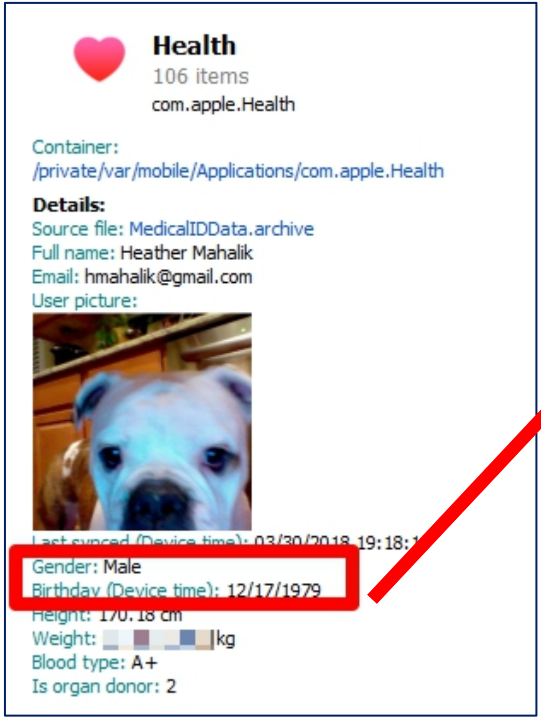
- Drop in Heart Rate
- Correlate with iOS Application Usage
  - CurrentPowerlog.PLSQL
    - No Longer backed up in iOS 11 or iOS 12
  - Physical/Jailbroken Access?
- Really difficult to test
  - Volunteers?

Alive

- Active time during day
  - Assumes user always wears Apple Watch or has Phone on their person
- Periods of activity versus rest
- Correlate with iOS Activity
  - Assumes same user on iOS device (via passcode)



Validate Tool Findings

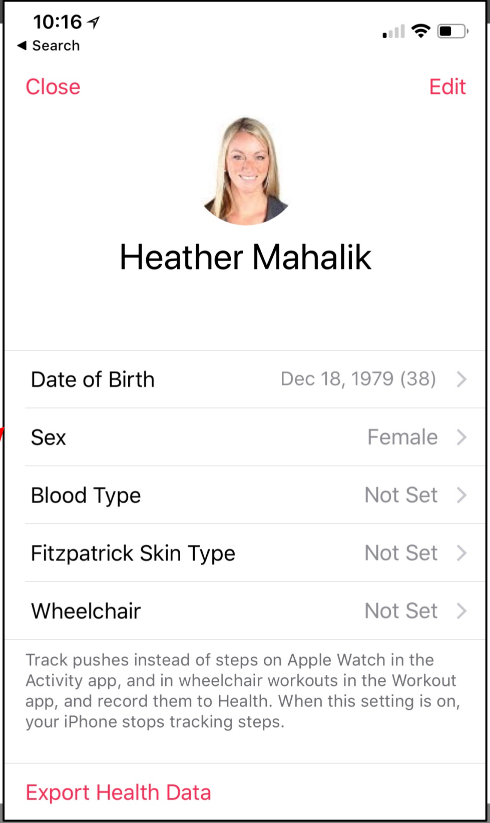


Health
106 items
com.apple.Health

Container:
/private/var/mobile/Applications/com.apple.Health

Details:
Source file: MedicalIDData.archive
Full name: Heather Mahalik
Email: hmahalik@gmail.com
User picture:

Last synced (Device time): 03/30/2018 19:18:1
Gender: Male
Birthday (Device time): 12/17/1979
Height: 170.18 cm
Weight: [redacted] kg
Blood type: A+
Is organ donor: 2



10:16
◀ Search

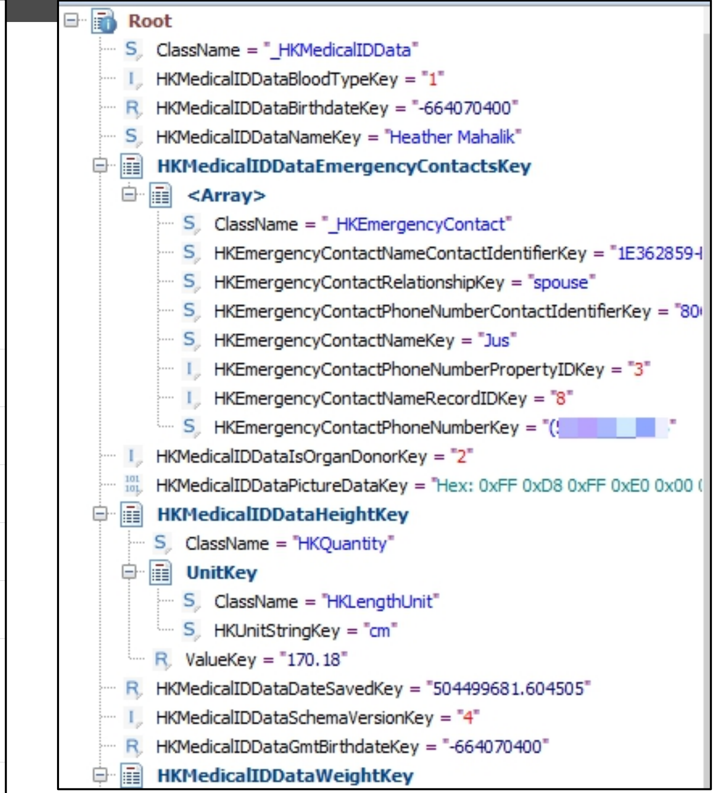
Close
Edit

Heather Mahalik

Date of Birth	Dec 18, 1979 (38)
Sex	Female
Blood Type	Not Set
Fitzpatrick Skin Type	Not Set
Wheelchair	Not Set

Track pushes instead of steps on Apple Watch in the Activity app, and in wheelchair workouts in the Workout app, and record them to Health. When this setting is on, your iPhone stops tracking steps.

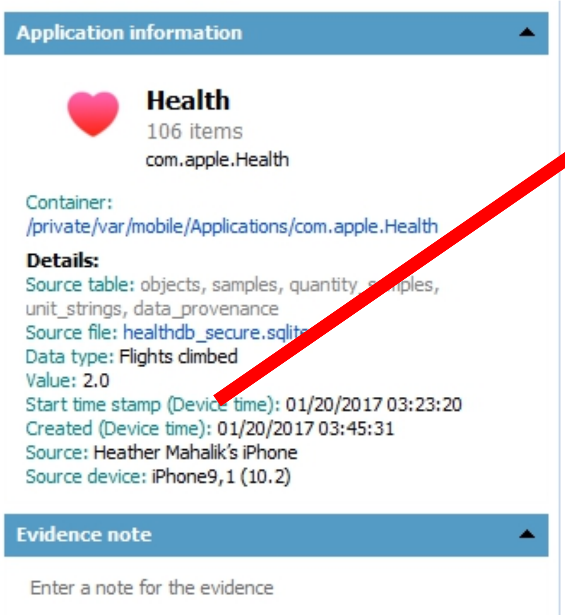
Export Health Data



```
Root
    S  ClassName = "_HKMedicalIDData"
    I  HKMedicalIDDataBloodTypeKey = "1"
    R  HKMedicalIDDataBirthdateKey = "-664070400"
    S  HKMedicalIDDataNameKey = "Heather Mahalik"
    HKMedicalIDDataEmergencyContactsKey
        <Array>
            S  ClassName = "_HKEmergencyContact"
            S  HKEmergencyContactNameContactIdentifierKey = "1E362859-
            S  HKEmergencyContactRelationshipKey = "spouse"
            S  HKEmergencyContactPhoneNumberContactIdentifierKey = "80
            S  HKEmergencyContactNameKey = "Jus"
            I  HKEmergencyContactPhoneNumberPropertyIDKey = "3"
            I  HKEmergencyContactNameRecordIDKey = "8"
            S  HKEmergencyContactPhoneNumberKey = "([redacted]"
    I  HKMedicalIDDataIsOrganDonorKey = "2"
    101 HKMedicalIDDataPictureDataKey = "Hex: 0xFF 0xD8 0xFF 0xE0 0x00 
    HKMedicalIDDataHeightKey
        S  ClassName = "HKQuantity"
        UnitKey
            S  ClassName = "HKLengthUnit"
            S  HKUnitStringKey = "cm"
        R  ValueKey = "170.18"
    R  HKMedicalIDDataDateSavedKey = "504499681.604505"
    I  HKMedicalIDDataSchemaVersionKey = "4"
    R  HKMedicalIDDataGmtBirthdateKey = "-664070400"
    HKMedicalIDDataWeightKey
```

Some Tools May Parse Bits of Health Data

- Verify Time Zone



Application information

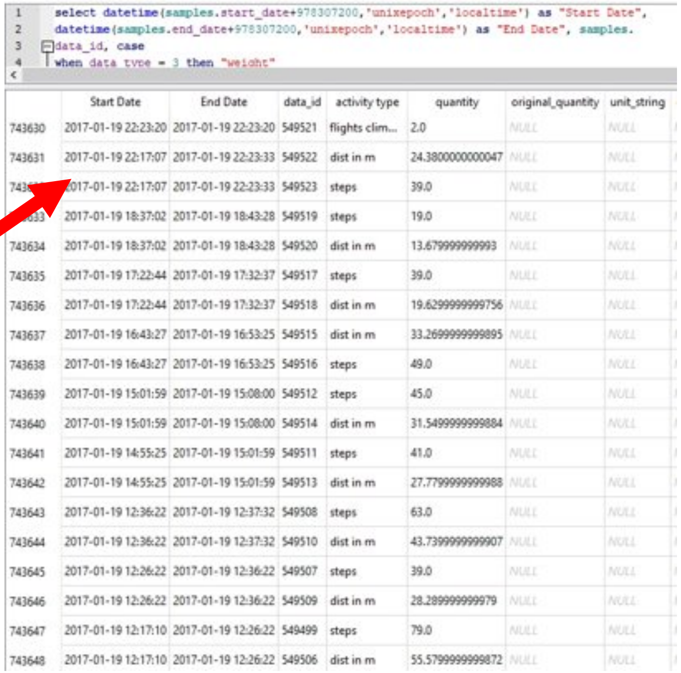
Health
106 items
com.apple.Health

Container:
/private/var/mobile/Applications/com.apple.Health

Details:
Source table: objects, samples, quantity_samples, unit_strings, data_provenance
Source file: healthdb_secure.sqlite
Data type: Flights climbed
Value: 2.0
Start time stamp (Device time): 01/20/2017 03:23:20
Created (Device time): 01/20/2017 03:45:31
Source: Heather Mahalik's iPhone
Source device: iPhone9,1 (10.2)

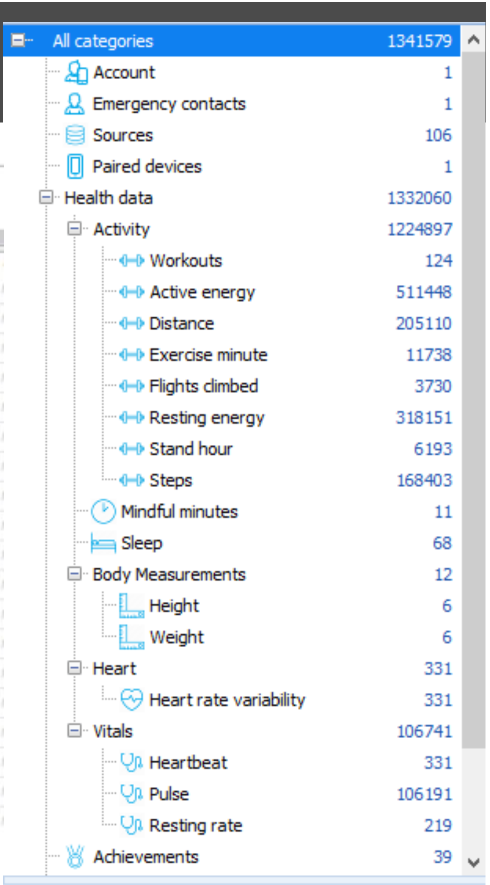
Evidence note

Enter a note for the evidence



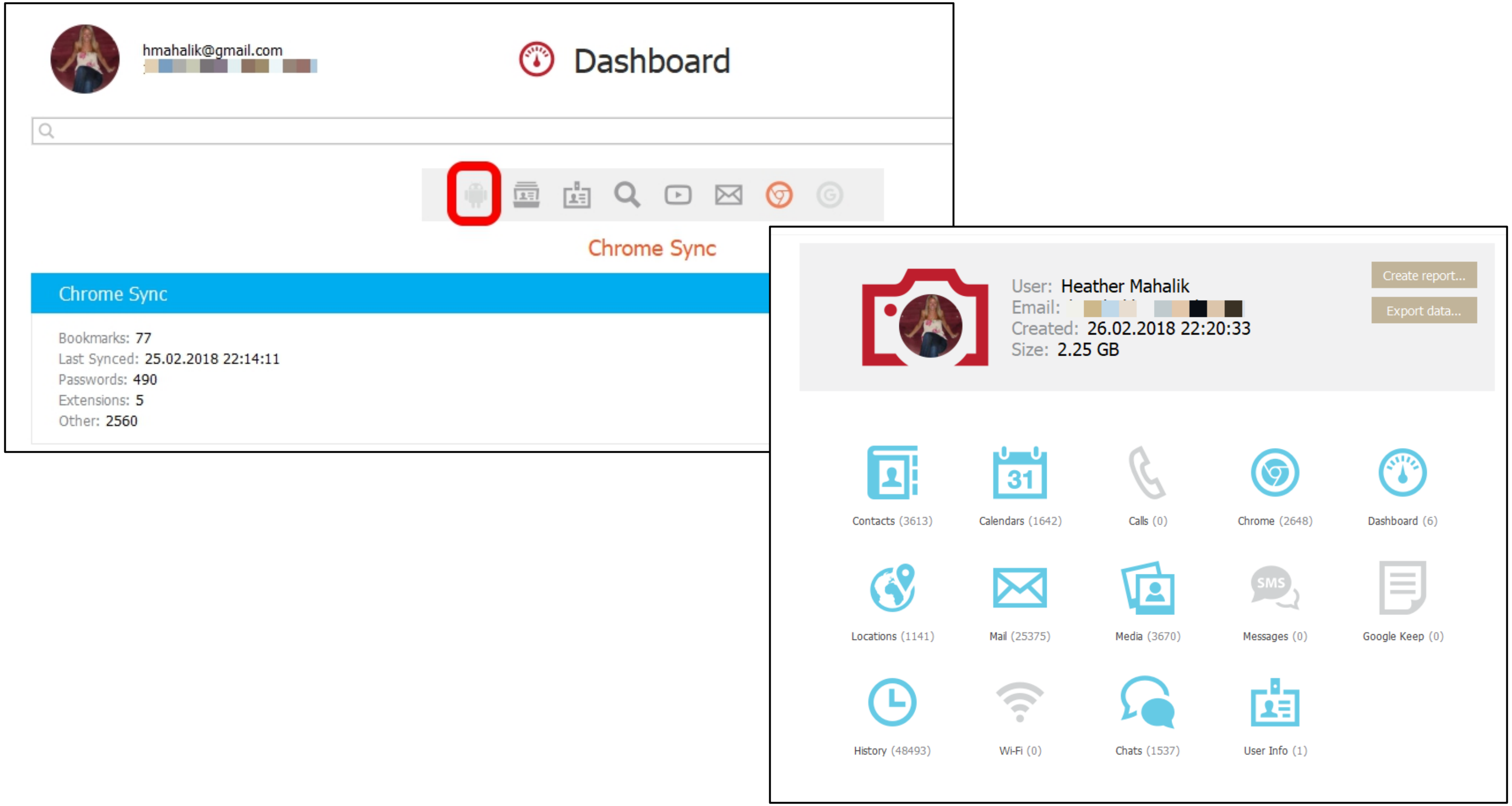
```
select datetime(samples.start_date+978307200,'unixepoch','localtime') as "Start Date",
datetime(samples.end_date+978307200,'unixepoch','localtime') as "End Date", samples.
data_id, case
when data type = 3 then "weight"
```

	Start Date	End Date	data_id	activity type	quantity	original_quantity	unit_string
743630	2017-01-19 22:23:20	2017-01-19 22:23:20	549521	flights clim...	2.0	NULL	NULL
743631	2017-01-19 22:17:07	2017-01-19 22:23:33	549522	dist in m	24.3800000000047	NULL	NULL
743[illegible]	2017-01-19 22:17:07	2017-01-19 22:23:33	549523	steps	39.0	NULL	NULL
[illegible]633	2017-01-19 18:37:02	2017-01-19 18:43:28	549519	steps	19.0	NULL	NULL
743634	2017-01-19 18:37:02	2017-01-19 18:43:28	549520	dist in m	13.6799999999993	NULL	NULL
743635	2017-01-19 17:22:44	2017-01-19 17:32:37	549517	steps	39.0	NULL	NULL
743636	2017-01-19 17:22:44	2017-01-19 17:32:37	549518	dist in m	19.6299999999756	NULL	NULL
743637	2017-01-19 16:43:27	2017-01-19 16:53:25	549515	dist in m	33.2699999999895	NULL	NULL
743638	2017-01-19 16:43:27	2017-01-19 16:53:25	549516	steps	49.0	NULL	NULL
743639	2017-01-19 15:01:59	2017-01-19 15:08:00	549512	steps	45.0	NULL	NULL
743640	2017-01-19 15:01:59	2017-01-19 15:08:00	549514	dist in m	31.5499999999884	NULL	NULL
743641	2017-01-19 14:55:25	2017-01-19 15:01:59	549511	steps	41.0	NULL	NULL
743642	2017-01-19 14:55:25	2017-01-19 15:01:59	549513	dist in m	27.7799999999988	NULL	NULL
743643	2017-01-19 12:36:22	2017-01-19 12:37:32	549508	steps	63.0	NULL	NULL
743644	2017-01-19 12:36:22	2017-01-19 12:37:32	549510	dist in m	43.7399999999907	NULL	NULL
743645	2017-01-19 12:26:22	2017-01-19 12:36:22	549507	steps	39.0	NULL	NULL
743646	2017-01-19 12:26:22	2017-01-19 12:36:22	549509	dist in m	28.289999999979	NULL	NULL
743647	2017-01-19 12:17:10	2017-01-19 12:26:22	549499	steps	79.0	NULL	NULL
743648	2017-01-19 12:17:10	2017-01-19 12:26:22	549506	dist in m	55.5799999999872	NULL	NULL



All categories	1341579
Account	1
Emergency contacts	1
Sources	106
Paired devices	1
Health data	1332060
Activity	1224897
Workouts	124
Active energy	511448
Distance	205110
Exercise minute	11738
Flights climbed	3730
Resting energy	318151
Stand hour	6193
Steps	168403
Mindful minutes	11
Sleep	68
Body Measurements	12
Height	6
Weight	6
Heart	331
Heart rate variability	331
Vitals	106741
Heartbeat	331
Pulse	106191
Resting rate	219
Achievements	39

Google Cloud Data – NOT just for Android Users



hmahalik@gmail.com
[redacted]

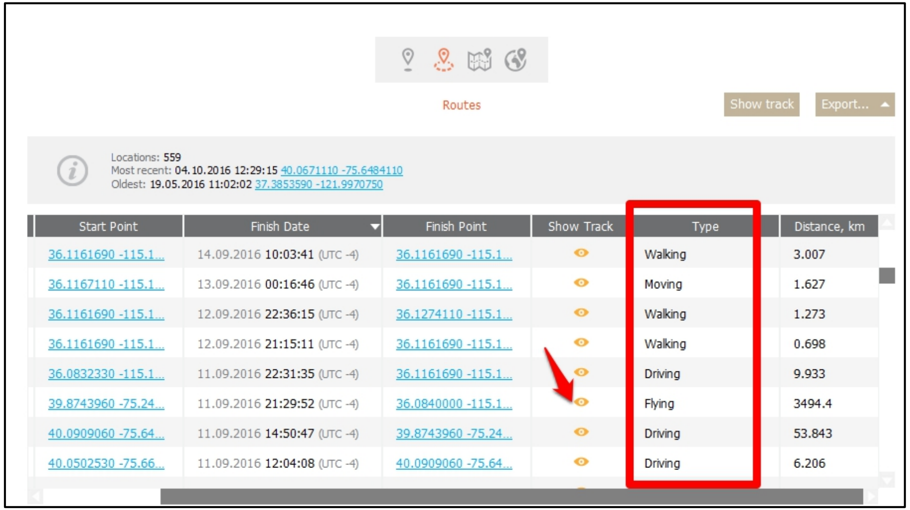
Chrome Sync

Bookmarks: 77
Last Synced: 25.02.2018 22:14:11
Passwords: 490
Extensions: 5
Other: 2560

User: Heather Mahalik
Email: [redacted]
Created: 26.02.2018 22:20:33
Size: 2.25 GB

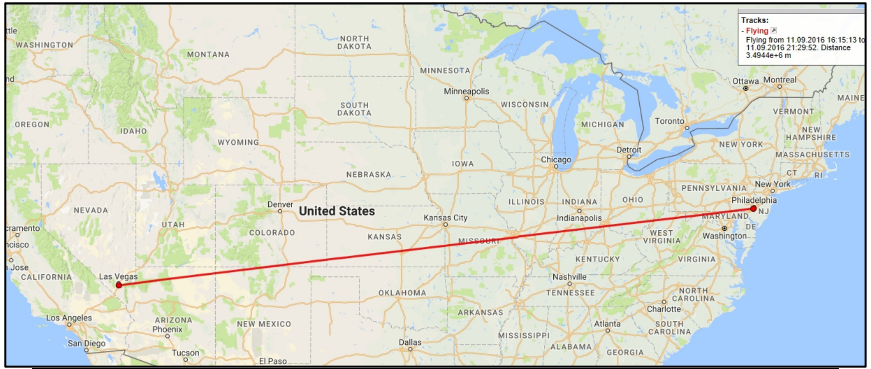
Contacts (3613)	Calendars (1642)	Calls (0)	Chrome (2648)	Dashboard (6)
Locations (1141)	Mail (25375)	Media (3670)	Messages (0)	Google Keep (0)
History (48493)	Wi-Fi (0)	Chats (1537)	User Info (1)	

Think You Can Delete Your Traces?

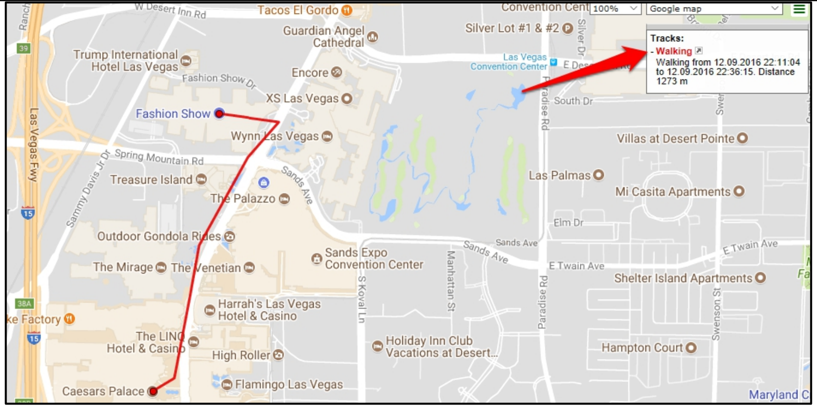


Locations: 559
Most recent: 04.10.2016 12:29:15 40.0671110 -75.6484110
Oldest: 19.05.2016 11:02:02 37.3853590 -121.9970750

Start Point	Finish Date	Finish Point	Show Track	Type	Distance, km
36.1161690 -115.1...	14.09.2016 10:03:41 (UTC -4)	36.1161690 -115.1...	👁	Walking	3.007
36.1167110 -115.1...	13.09.2016 00:16:46 (UTC -4)	36.1161690 -115.1...	👁	Moving	1.627
36.1161690 -115.1...	12.09.2016 22:36:15 (UTC -4)	36.1274110 -115.1...	👁	Walking	1.273
36.1161690 -115.1...	12.09.2016 21:15:11 (UTC -4)	36.1161690 -115.1...	👁	Walking	0.698
36.0832330 -115.1...	11.09.2016 22:31:35 (UTC -4)	36.1161690 -115.1...	👁	Driving	9.933
39.8743960 -75.24...	11.09.2016 21:29:52 (UTC -4)	36.0840000 -115.1...	👁	Flying	3494.4
40.0909060 -75.64...	11.09.2016 14:50:47 (UTC -4)	39.8743960 -75.24...	👁	Driving	53.843
40.0502530 -75.66...	11.09.2016 12:04:08 (UTC -4)	40.0909060 -75.64...	👁	Driving	6.206



Tracks:
- Flying
  Flying from 11.09.2016 16:15:13 to 11.09.2016 21:29:52. Distance 3.4944e+6 m



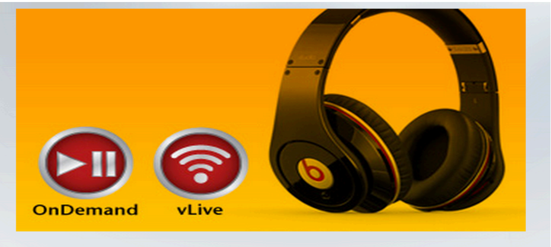
Tracks:
- Walking
  Walking from 12.09.2016 22:11:04 to 12.09.2016 22:36:15. Distance 1273 m

Next Steps

- Set expectations on what is possible
- Allocate time to test what you believe occurred
- Don’t forget about cloud
  - iCloud
  - Google
- Don’t reinvent the wheel
  - https://www.youtube.com/watch?v=tLyjP6rRdyI
  - smarterforensics.com/blog
  - smarterforensics.com/presentations

About 585…

- Course launched in 2014
- GASF Cert – Vendor neutral available to everyone
- Addresses the hard to tackle topics (Encryption, Parsing, Query drafting, decompiling malware, etc.)
- Covers iOS, Android, 3rd Party Apps, Malware, BlackBerry 10, Data Destruction and more
- Includes 24 hands-on labs + 1 capstone challenge of current smart devices (bonus take home case + 6 bonus labs)
- Is vendor NEUTRAL – We teach you the best methods, not how to use commercial tools



FOR585 Advanced Smartphone Forensics Course Available At:

FOR585.com/course

Dec: CDI – SIM available

Jan: Amsterdam

Feb: New Orleans (SIM), Tokyo, VA and TX

Apr: Orlando, FL and Boston, MA

May: San Diego, CA

OnDemand ANYTIME!

Heather Mahalik
heather@smarterforensics.com
@HeatherMahalik
Blog: for585.com/blog

QUESTIONS?