



# #DFIRFIT OR BUST

A Forensic Exploration of iOS Health Data

SARAH EDWARDS  
as A SHORT APPLE FANATIC

HEATHER MAHALIK  
as HANK THE MUSTACHIOED BLONDE

# A little DFIR with a touch of motivation

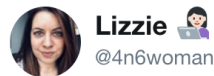
## What is #DFIRFIT?

← Blame High Five @4n6woman

## Health Data

- Acquisition
- Analysis
- Scenarios

## Motivate!



**Lizzie**  
@4n6woman

Following

Y'all, I'm so happy to see #dfirfit take off like it has. We're all in this together. ❤️🧡

1:41 PM - 10 Feb 2018

<https://t.me/learnforensics>



**Sarah Edwards**  
@iamevitwin

Off to a good start at #SANSsecuritywest #DFIRFit with @B1N2H3X and @HeatherMahalik 🍷

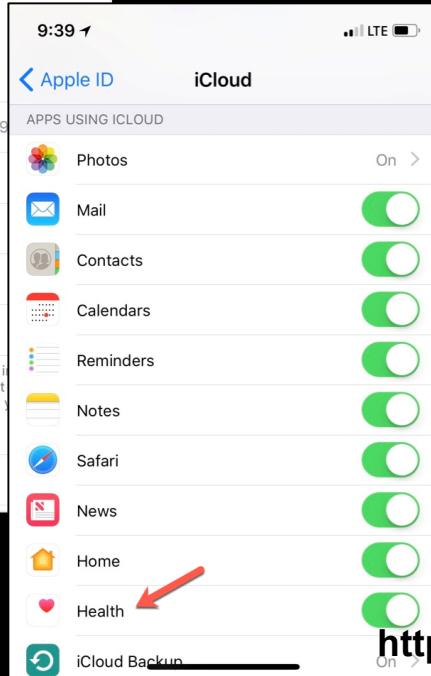
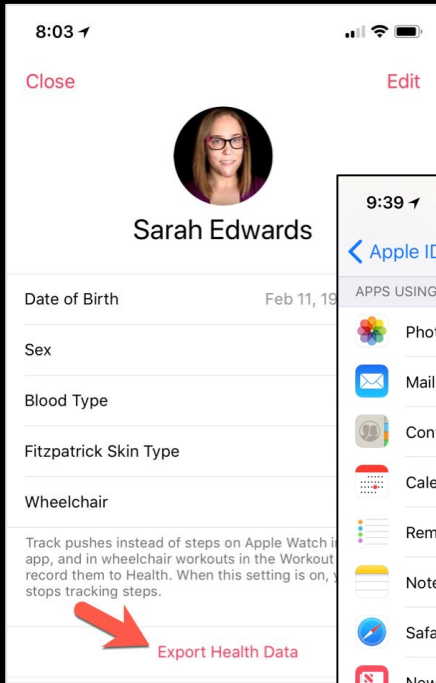


1:41 PM - 10 May 2018

# A bit about us and our goals!



# Acquisition Options



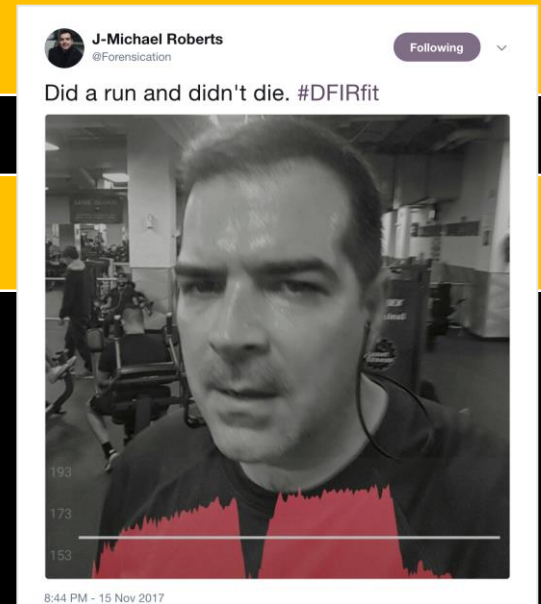
## Encrypted iOS Backups

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

## Health App Export

- XML Files

## iCloud Backups



# XML Output – Big and Messy

- Compressed Zip File (ex: ~52Mb)
  - export.xml (ex: ~940Mb)
  - export\_cda.xml (ex: ~240Mb)



Alissa Torres @sibertor · 6 Dec 2017

This afternoon in #FOR508 Day3 our focus is lateral movement #DFIRfit



```
1134807 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134808 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134809 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134810 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134811 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134812 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134813 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134814 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134815 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134816 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134817 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134818 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134819 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134820 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134821 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134822 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134823 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134824 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134825 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134826 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134827 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134828 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134829 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134830 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134831 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
1134832 <Record type="HKQuantityTypeIdentifierBasalEnergyBurned" sourceName="miWatch" sourceVersion="2.0" device="&lt;&lt;HKDevice: 0
```

# Health App Integration & Sources

## Native

- Health.app – All Health Data
- Activity.app – Workout/Challenge Specific

## 3<sup>rd</sup> Party Apps

- Diet (MyFitnessPal)
- Sleep Monitoring (Sleep++, Pillow)
- Hardware (Scale, Blood Pressure Monitor, Fitbits, etc)
- Workout (Runkeeper, Couch25k)

## Integration with Apple Watch

- May come from other devices too!
- ..or just tracking from iPhone (Steps, Manual workout input)

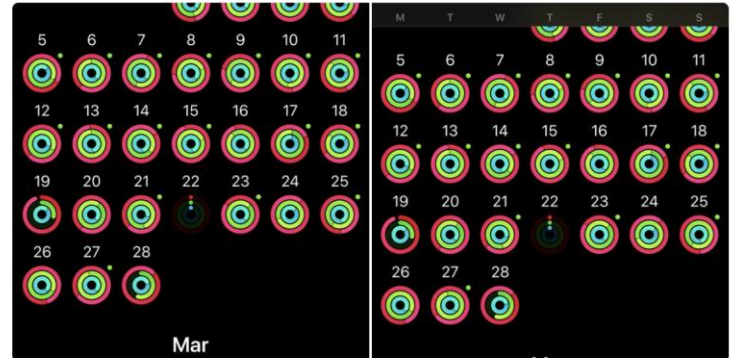


Richie Cyrus

@rrcyrus

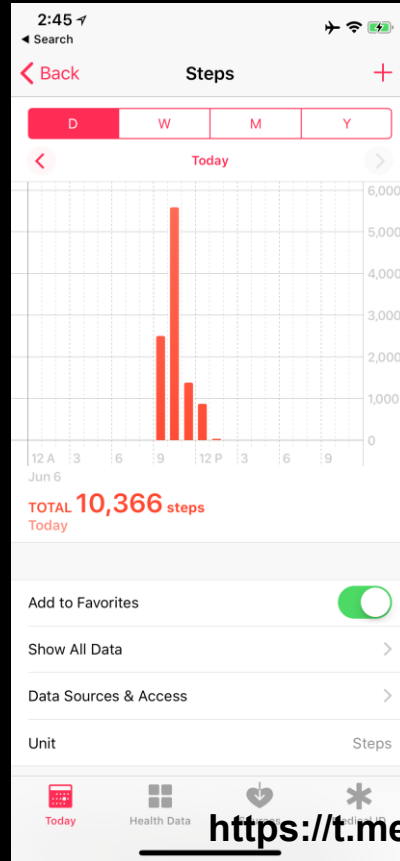
Following

February was about closing rings and getting back to the gym. March is about continuing to put on the 🍌🍌 #DFIRFIT. My wife and I have goals to meet 📈

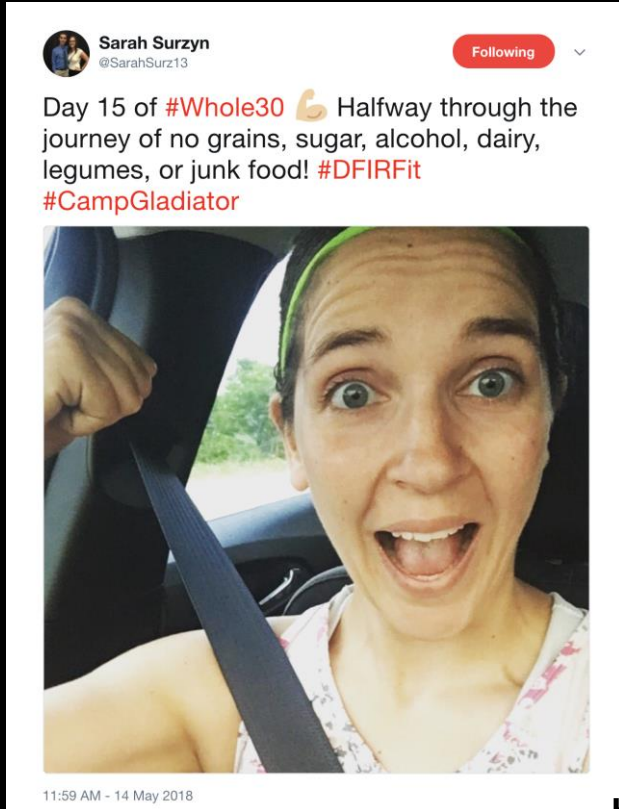


12:00 AM - 14 Mar 2018

# Native Applications – Health & Activity



# Primary Health Databases



healthdb.sqlite

healthdb\_secure.sqlite

Workout & Non-workout Monitoring

Historical Database Contents

Database Path: [/private/var]/mobile/Library/Health/

- healthdb.sqlite & healthdb\_secure.sqlite

Unknown: heathdb\_secure.hfd

- Not SQLite, Appears Encrypted
- Potentially Sensitive Health Data

# Database Contents – healthdb.sqlite

## Sources (Apps and Devices)

- Other apps may provide health data too!

## Key Values

- Activity Sharing Account, Settings and More

## iOS Versions Used

## Dates of Interest

- Cloud Sync
- Pairing Date



**Brian Moran (Not Brain Morgan)**  
@brianjmoran

Following



Swolemander Shoulder day.

Whether your motivation is [#DFIRFit](#) or [#TrainLikeYouAreLeeWhitfieldsStuntDouble](#) try your best to get a workout in today!



11:26 AM - 9 Mar 2018

# Database Contents – healthdb\_secure.sqlite

Achievements

Historical Health Contents

Workouts

Friend Achievements and Workouts

Records

- Medical
- Vaccination
- Allergy



Rob Lee  
@robtle

Following



Finished #DarkSideHalf today for my first marathon finish. With @KelliTarala @jamestarala #DFIRFit



# 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

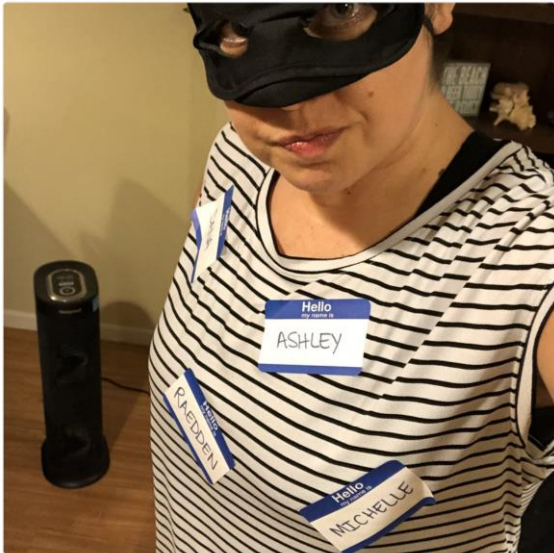
# Forensic Scenarios – Pattern of Life



Lizzie  
@4n6woman

Following

23 splat points. 545 calories. 52:40 time.  
Halloween workout @orangetheory getting  
#DFIRFIT in costume.  
#CoachesAndStaffNames #IdentityThief



10:02 PM - 31 Oct 2017

## Workouts

- Locations & Frequency

## Steps & Distance

## Calories Burned

## Heart Rate

- User has watch on or off

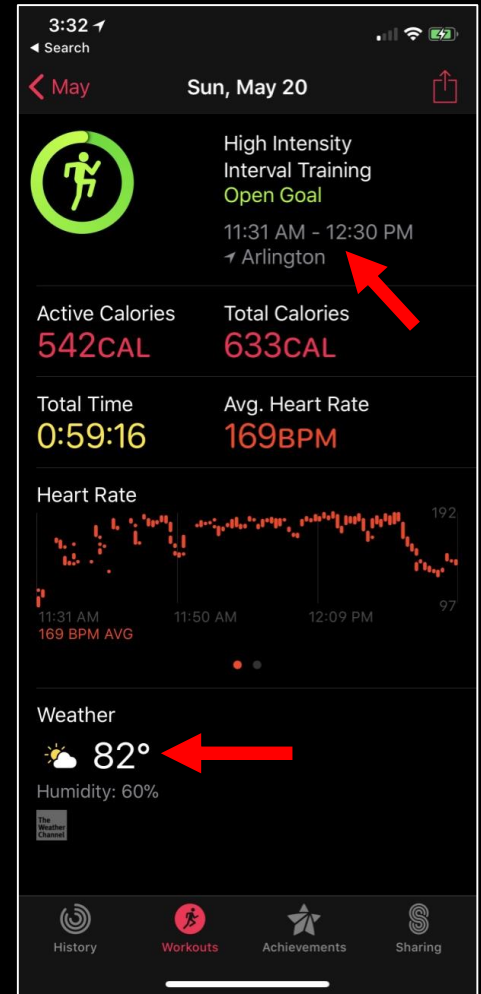
# Pattern of Life – Workout Metadata

- Location, Temperature, Humidity, Weather Conditions
- “Workout” data\_id from Workouts Table

```
1 select datetime(samples.start_date+978307200,'unixepoch','localtime') as "Start Date",
2 datetime(samples.end_date+978307200,'unixepoch','localtime') as "End Date", samples.
3 data_id, metadata_values.numerical_value,metadata_keys.key
4 from samples
5 left outer join quantity_samples on samples.data_id = quantity_samples.data_id
6 left outer join unit_strings on quantity_samples.original_unit = unit_strings.RowID
7 left outer join correlations on samples.data_id = correlations.object
8 left outer join metadata_values on metadata_values.object_id = samples.data_id
9 left outer join metadata_keys on metadata_keys.ROWID = metadata_values.key_id
10 where samples.data_id = 3286355
```

	Start Date	End Date	data_id	numerical_value	key
1	2018-05-20 11:31:18	2018-05-20 12:30:34	3286355	3.0	_HKPrivateWeatherCondition
2	2018-05-20 11:31:18	2018-05-20 12:30:34	3286355	NULL	HKTimeZone
3	2018-05-20 11:31:18	2018-05-20 12:30:34	3286355	38.880229643481	_HKPrivateWorkoutWeatherLocationCoordinatesLatitude
4	2018-05-20 11:31:18	2018-05-20 12:30:34	3286355	82.0	HKWeatherTemperature
5	2018-05-20 11:31:18	2018-05-20 12:30:34	3286355	1.0	_HKPrivateWorkoutWasInDaytime
6	2018-05-20 11:31:18	2018-05-20 12:30:34	3286355	60.0	HKWeatherHumidity
7	2018-05-20 11:31:18	2018-05-20 12:30:34	3286355	-77.111616589084	_HKPrivateWorkoutWeatherLocationCoordinatesLongitude

<https://t.me/learningnets>



# Pattern of Life – Location & Frequency

```

1 select datetime(samples.start_date+978307200,'unixepoch','localtime') as "Start Date",
2 datetime(samples.end_date+978307200,'unixepoch','localtime') as "End Date",
3 samples.data_id, metadata_values.numerical_value,metadata_keys.key
4 from samples
5 left outer join quantity_samples on samples.data_id = quantity_samples.data_id
6 left outer join unit_strings on quantity_samples.original_unit = unit_strings.RowID
7 left outer join correlations on samples.data_id = correlations.object
8 left outer join metadata_values on metadata_values.object_id = samples.data_id
9 left outer join metadata_keys on metadata_keys.ROWID = metadata_values.key_id
10 where metadata_keys.key like "%Coordinates%"
11 order by "Start Date" desc
    
```

	Start Date	End Date	data_id	numerical_value	key
1	2018-05-20 11:31:18	2018-05-20 12:30:34	3286355	38.880229643481	_HKPrivateWorkoutWeatherLocationCoordinates
2	2018-05-20 11:31:18	2018-05-20 12:30:34	3286355	-77.111616589084	_HKPrivateWorkoutWeatherLocationCoordinates
3	2018-05-20 11:20:51	2018-05-20 11:28:12	3282421	38.8819636367535	_HKPrivateWorkoutWeatherLocationCoordinates
4	2018-05-20 11:20:51	2018-05-20 11:28:12	3282421	-77.1046346898611	_HKPrivateWorkoutWeatherLocationCoordinates
5	2018-05-15 09:15:00	2018-05-15 10:15:50	3271626	32.733272501983	_HKPrivateWorkoutWeatherLocationCoordinates
6	2018-05-15 09:15:00	2018-05-15 10:15:50	3271626	-117.160310640047	_HKPrivateWorkoutWeatherLocationCoordinates
7	2018-05-14 09:11:22	2018-05-14 10:19:39	3267728	32.7332047368432	_HKPrivateWorkoutWeatherLocationCoordinates
8	2018-05-14 09:11:22	2018-05-14 10:19:39	3267728	-117.160302985525	_HKPrivateWorkoutWeatherLocationCoordinates
9	2018-05-10 19:34:54	2018-05-10 20:42:37	3257045	32.7332583121942	_HKPrivateWorkoutWeatherLocationCoordinates
10	2018-05-10 19:34:54	2018-05-10 20:42:37	3257045	-117.16030794439	_HKPrivateWorkoutWeatherLocationCoordinates
11	2018-05-09 07:04:43	2018-05-09 08:05:39	3244916	38.88025434478354	_HKPrivateWorkoutWeatherLocationCoordinates
12	2018-05-09 07:04:43	2018-05-09 08:05:39	3244916	-77.1116063044133	_HKPrivateWorkoutWeatherLocationCoordinates

Arlington (shown)

Arlington

San Diego

Arlington

<https://t.me/learningnets>

# Pattern of Life – Steps/Distance Per Day

- Potential Issues: Crossing Time Zones, Workouts, Multiple Devices
- Context Required for Interpretation

Sarah Edwards @sameditwin

Knocked out a 5k just to see if I could (not normally a runner/jogger), pretty darn proud of myself. It was slow but I did it. 🥳👊  
#DFIRFit #alreadysore

Active Calories	Total Calories
375CAL	438CAL
Distance	Total Time
3.45MI	0:42:00
Avg. Heart Rate	
169BPM	
Avg. Pace	
12'08"/MI	
Splits	
Heart Rate	

1:44 PM · 21 Apr 2018

7:14

◀ Search

◀ April

S M T W T F S

15 16 17 18 19 20 21

Saturday, Apr 21, 2018

Favorites

Steps **13,109** steps  
4/21, 10:47 PM

Walking + Running Distance **6.1** mi  
4/21, 10:47 PM

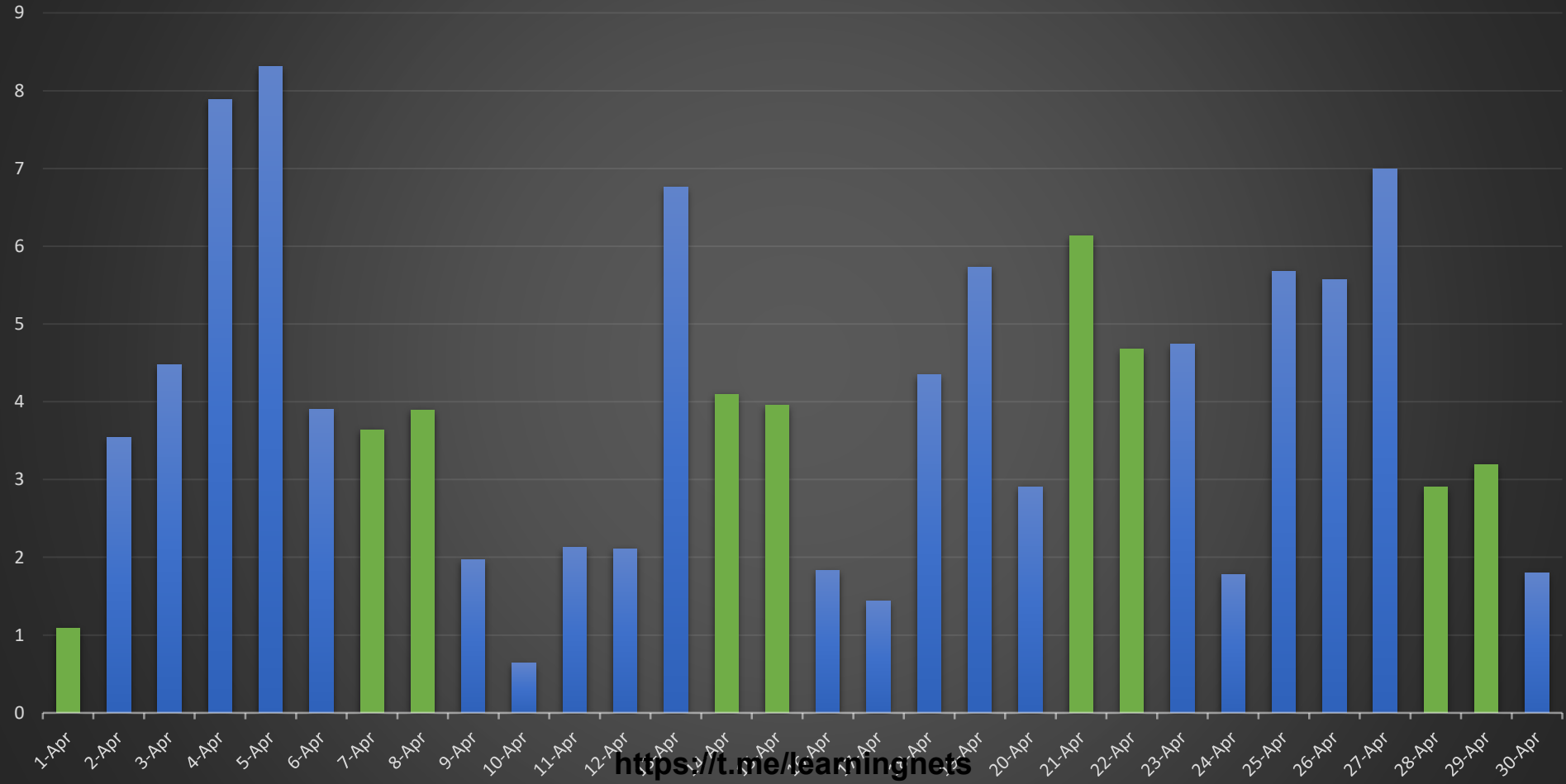
Today Health Data Sources Medical ID

<https://t.me/learn-gnats>

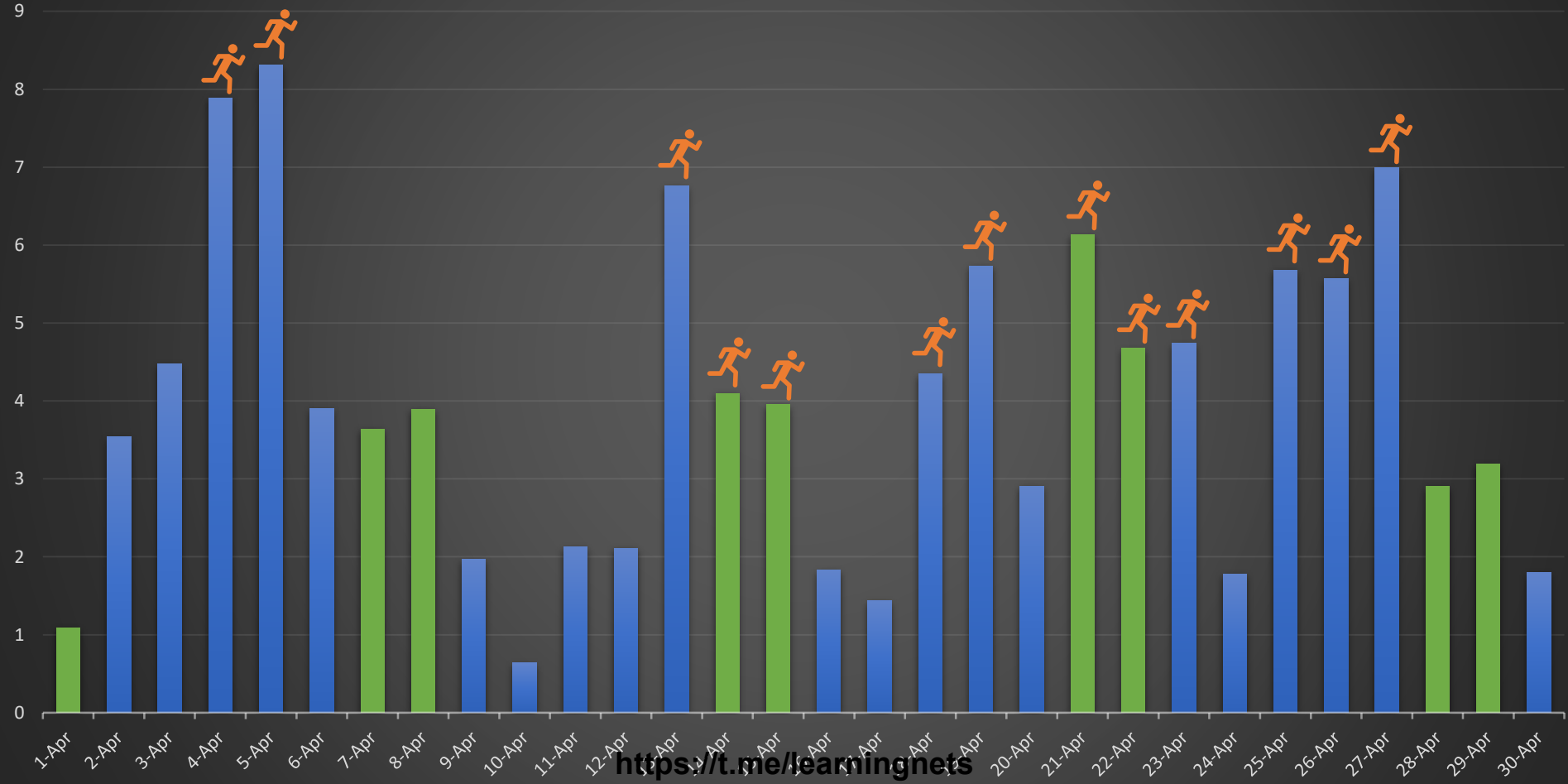
```
1 select datetime(cache_index+978307200,'unixepoch','utc') as "Day",
2 steps, walk_distance*0.000621371 as "Milage" from activity_caches
3 order by "Day" desc
4
```

	Day	steps	Milage
22	2018-04-29 04:00:00	7888.0	3.19418767527395
23	2018-04-28 04:00:00	7523.0	2.9015358593645
24	2018-04-27 04:00:00	16788.0	6.99464451296289
25	2018-04-26 04:00:00	13328.0	5.57270510257991
26	2018-04-25 04:00:00	13400.0	5.67925951958283
27	2018-04-24 04:00:00	4516.0	1.78107542134273
28	2018-04-23 04:00:00	10840.0	4.74332165001507
29	2018-04-22 04:00:00	11081.0	4.67615928274262
30	2018-04-21 04:00:00	13084.0	6.1348619714447
31	2018-04-20 04:00:00	7427.0	2.90939168371595
32	2018-04-19 04:00:00	13885.0	5.73578631077834
33	2018-04-18 04:00:00	10458.0	4.34843478607333

# Mileage



# Mileage

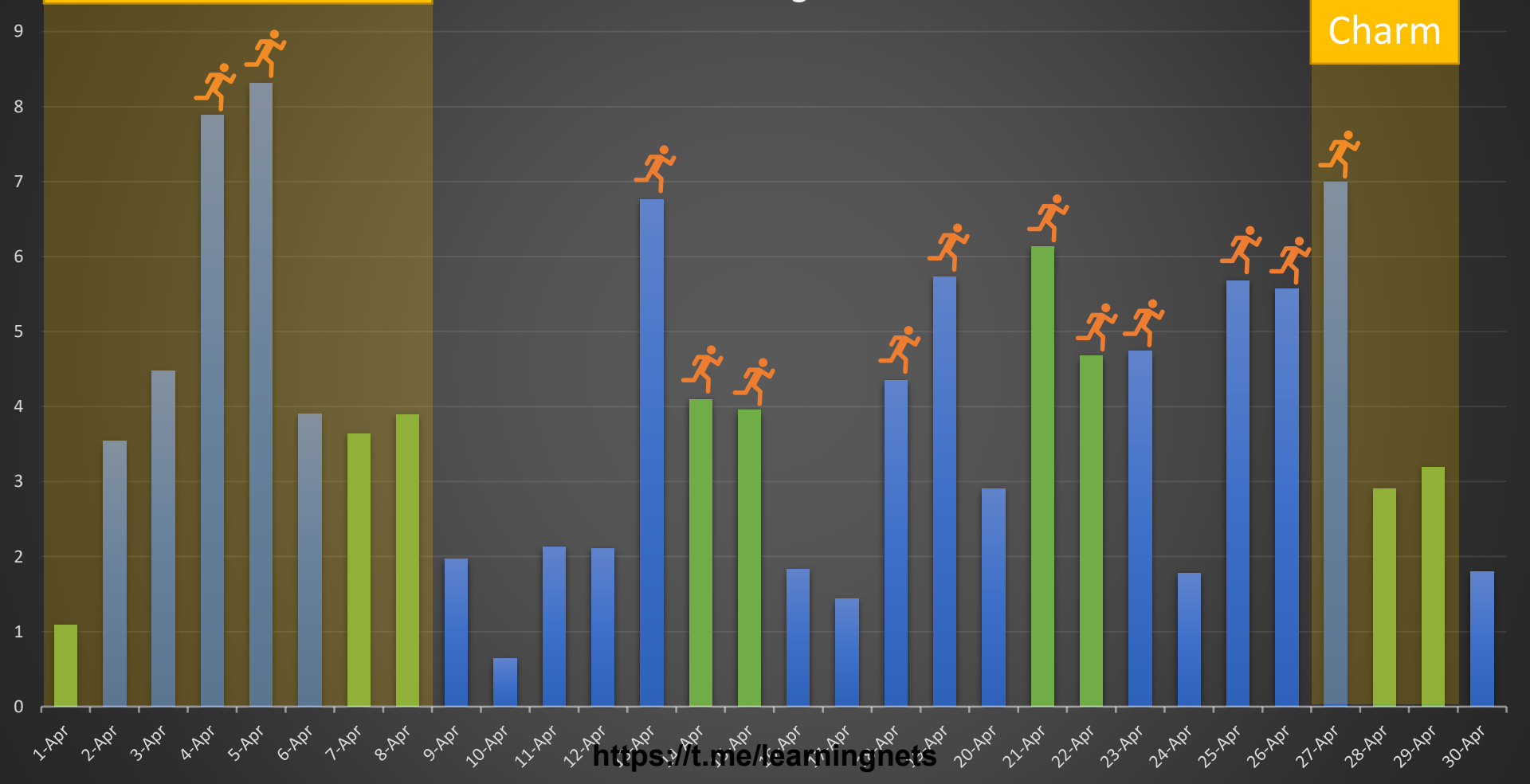


<https://t.me/learningnets>

SANS Orlando

Mileage

BSides Charm



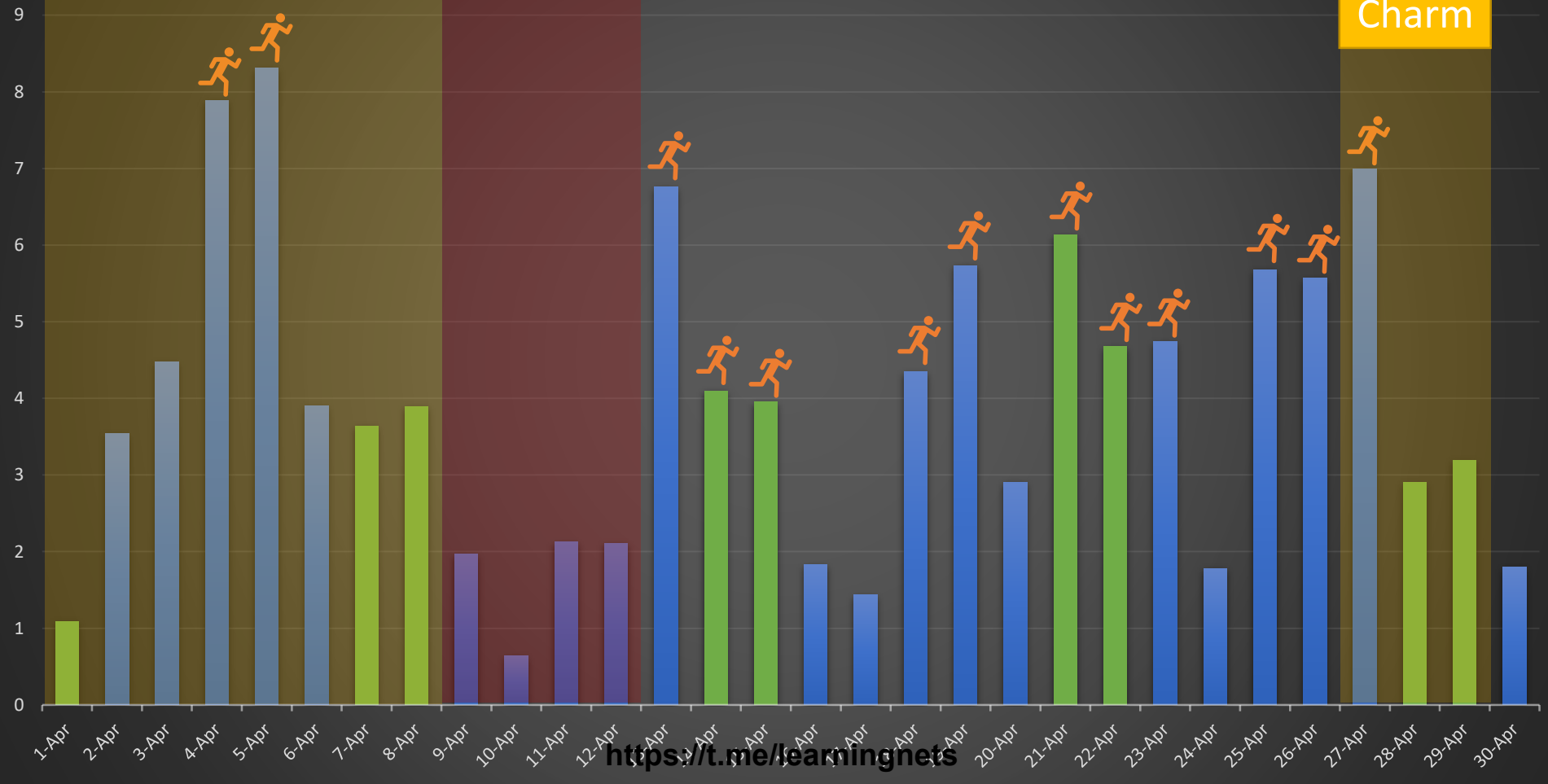
<https://t.me/learningnets>

# SANS Orlando

# Sick

# Mileage

# BSides Charm



<https://t.me/learningnets>

# Forensic Scenarios – Heart Rate - Dragging a Body

## Dragging Down a Hill and Walking Back Up

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

**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, 8:06am

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.

# Forensic Scenarios – Heart Rate - Dragging a Body

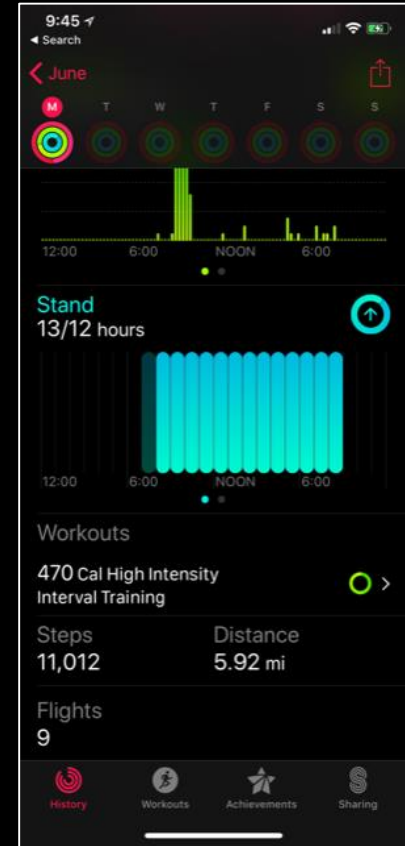
```
1 select datetime(samples.start_date+978307200,'unixepoch','localtime') as "Start Date",
2 datetime(samples.end_date+978307200,'unixepoch','localtime') as "End Date", samples.
3 data_id, data_type, quantity, original_quantity, unit_strings.unit_string, original_unit,
4 correlations.correlation, correlations.object,correlations.provenance
5 string_value, metadata_values.data_value, metadata_values.numerical_value,
6 metadata_values.value_type,metadata_keys.key
7 from samples
8 left outer join quantity_samples on samples.data_id = quantity_samples.data_id
9 left outer join unit_strings on quantity_samples.original_unit = unit_strings.RowID
10 left outer join correlations on samples.data_id = correlations.object
11 left outer join metadata_values on metadata_values.object_id = samples.data_id
12 left outer join metadata_keys on metadata_keys.RowID = metadata_values.key_id
13 where "Start Date" like '%2018-06-04 17:%' and data_type = 5
14 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

<https://t.me>



<https://t.me>



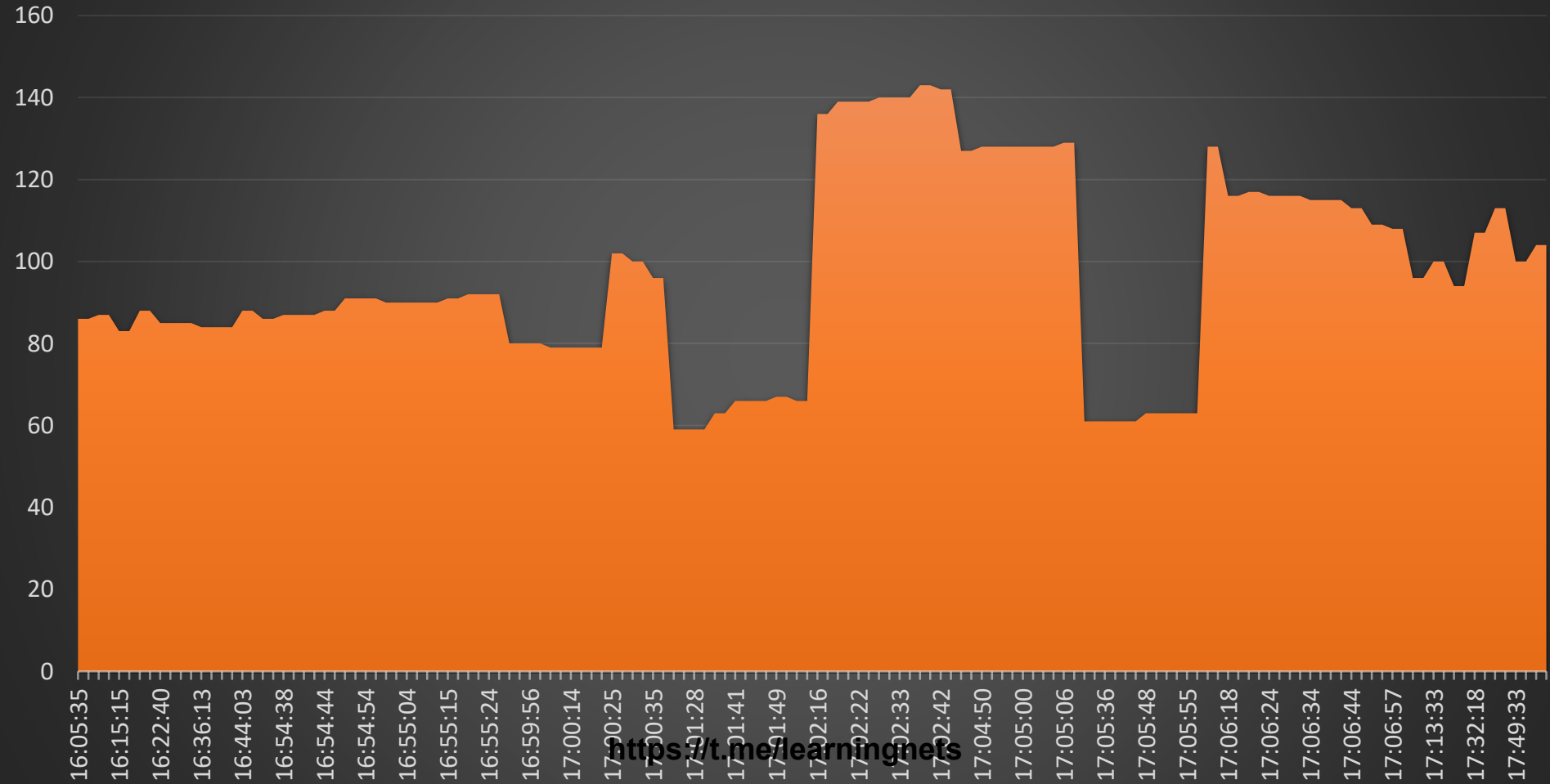
<https://t.me>

# And Now My Lawn is Dead

- What This Looked Like

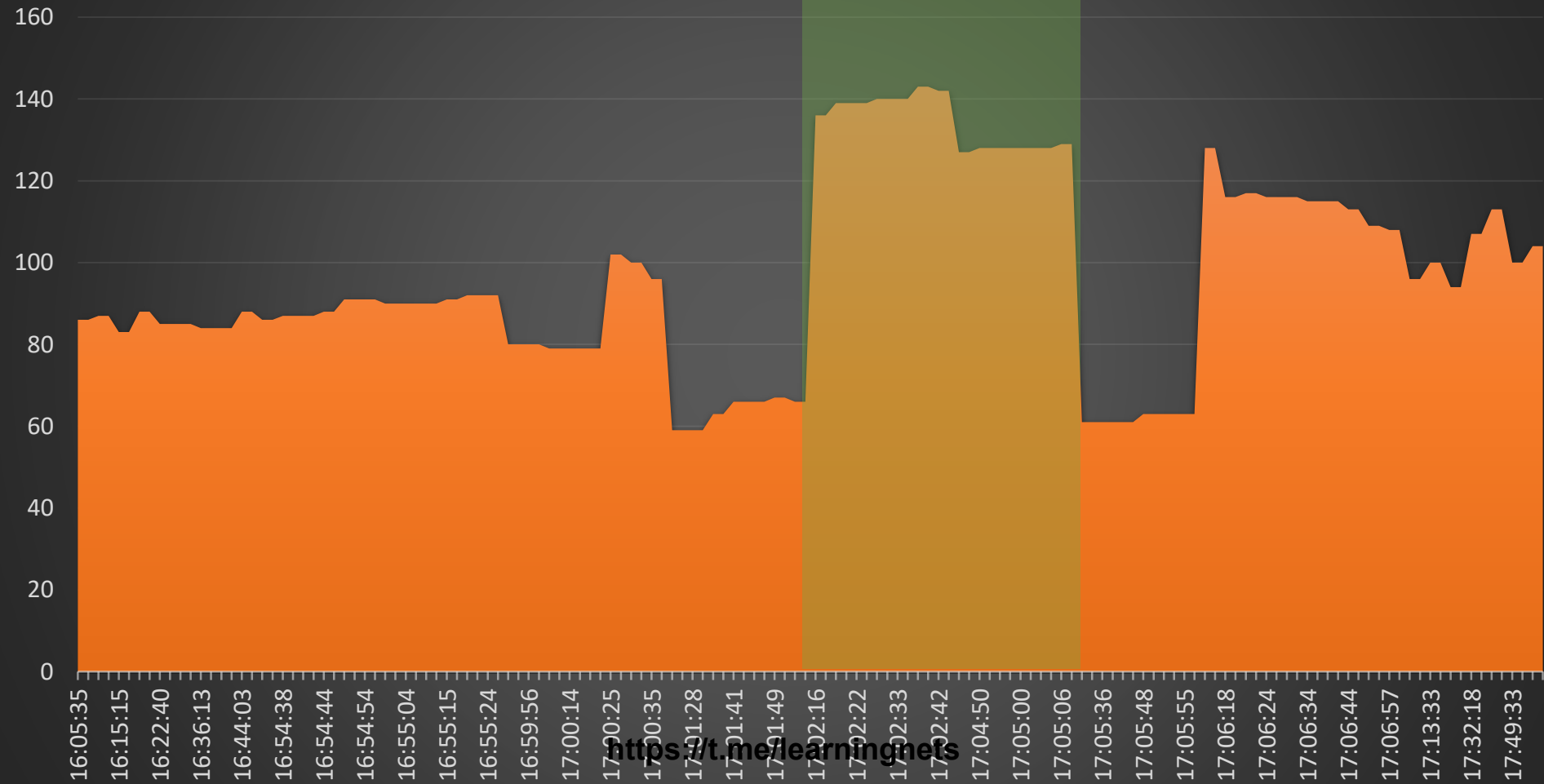


# Body Movin'



# Body Movin'

## Dragging

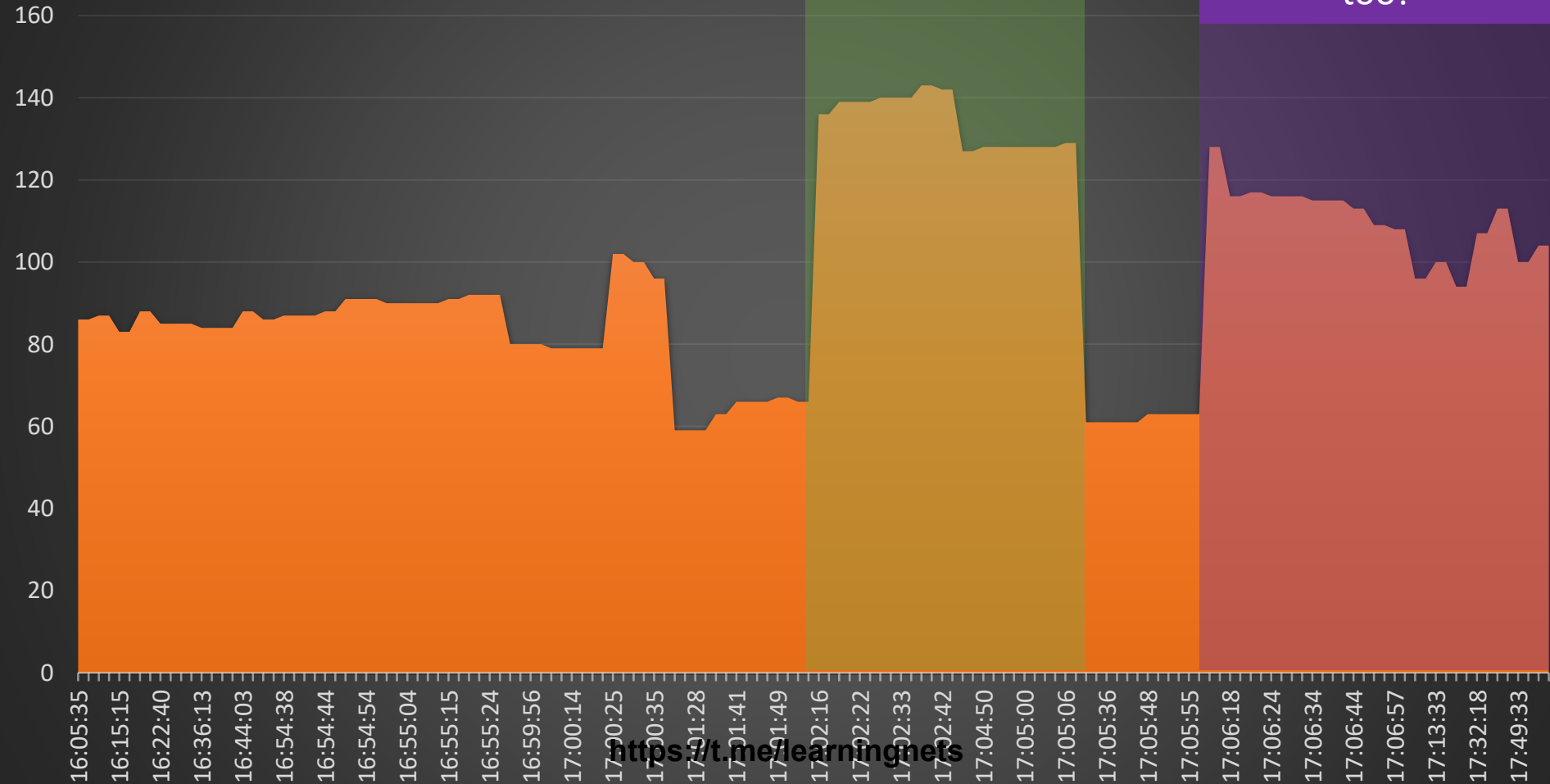


<https://t.me/learningnets>

# Body Movin'

## Dragging

Jack wanted to ride too!



<https://t.me/learningnets>

# Forensic Scenarios – Heart Rate – Dead or Alive?

## Death

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

## Alive

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



Phill Moore  
@phillmoore

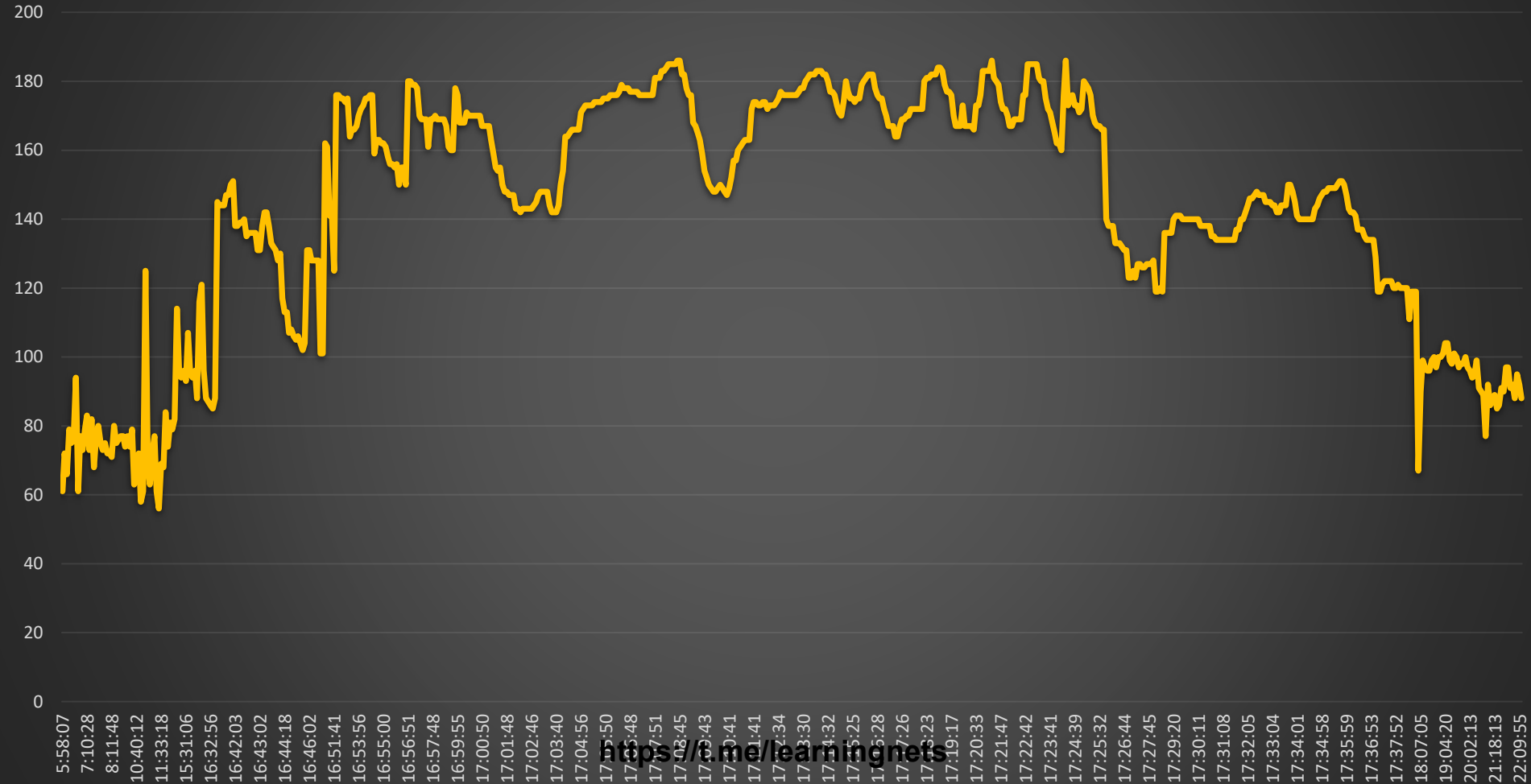
Following

Last #DFIRFIT for the year i think. Been a good one. Relaxing day planned tomorrow (3-4 blog posts :D)



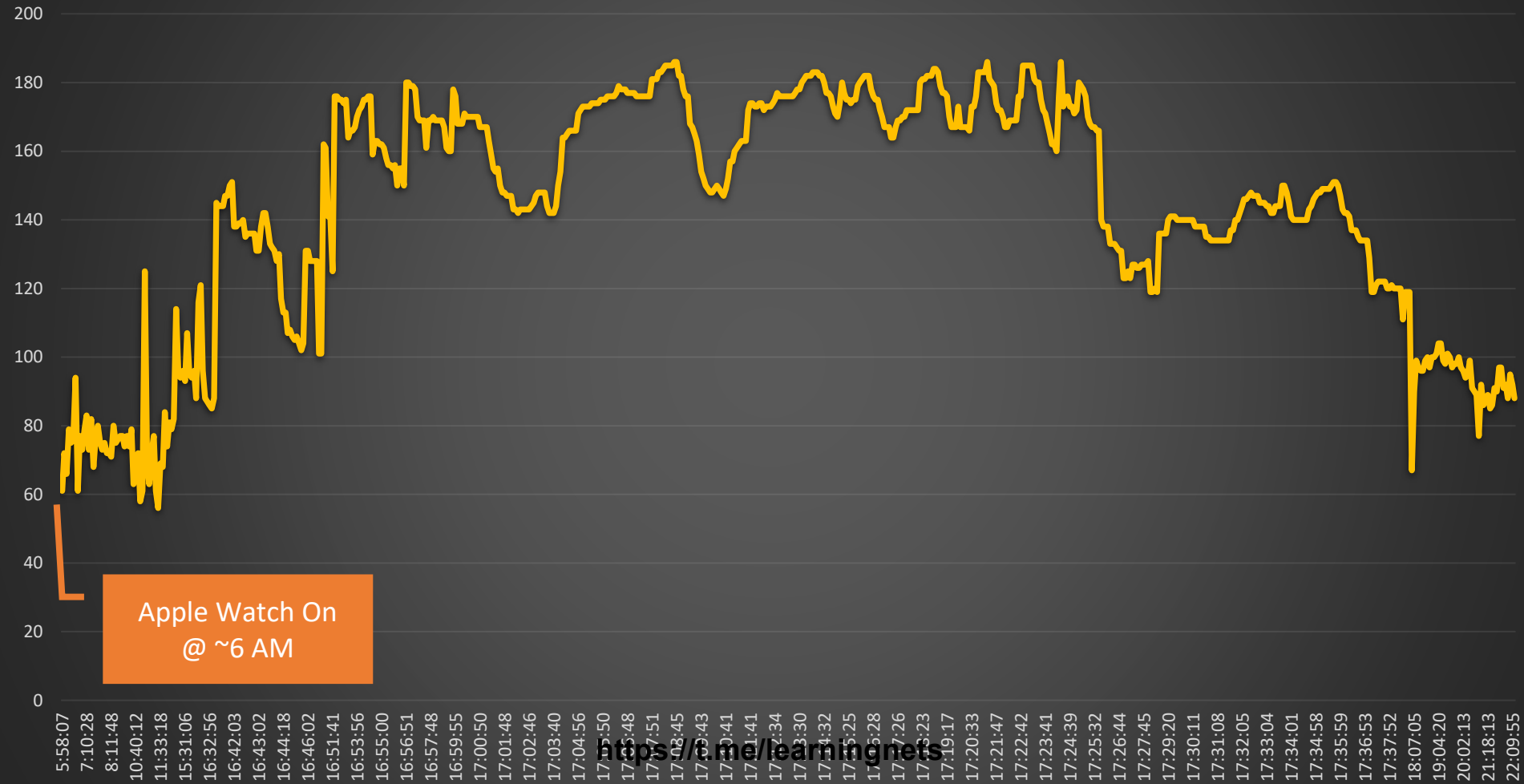
11:03 PM - 29 Dec 2017

# Day in the Life

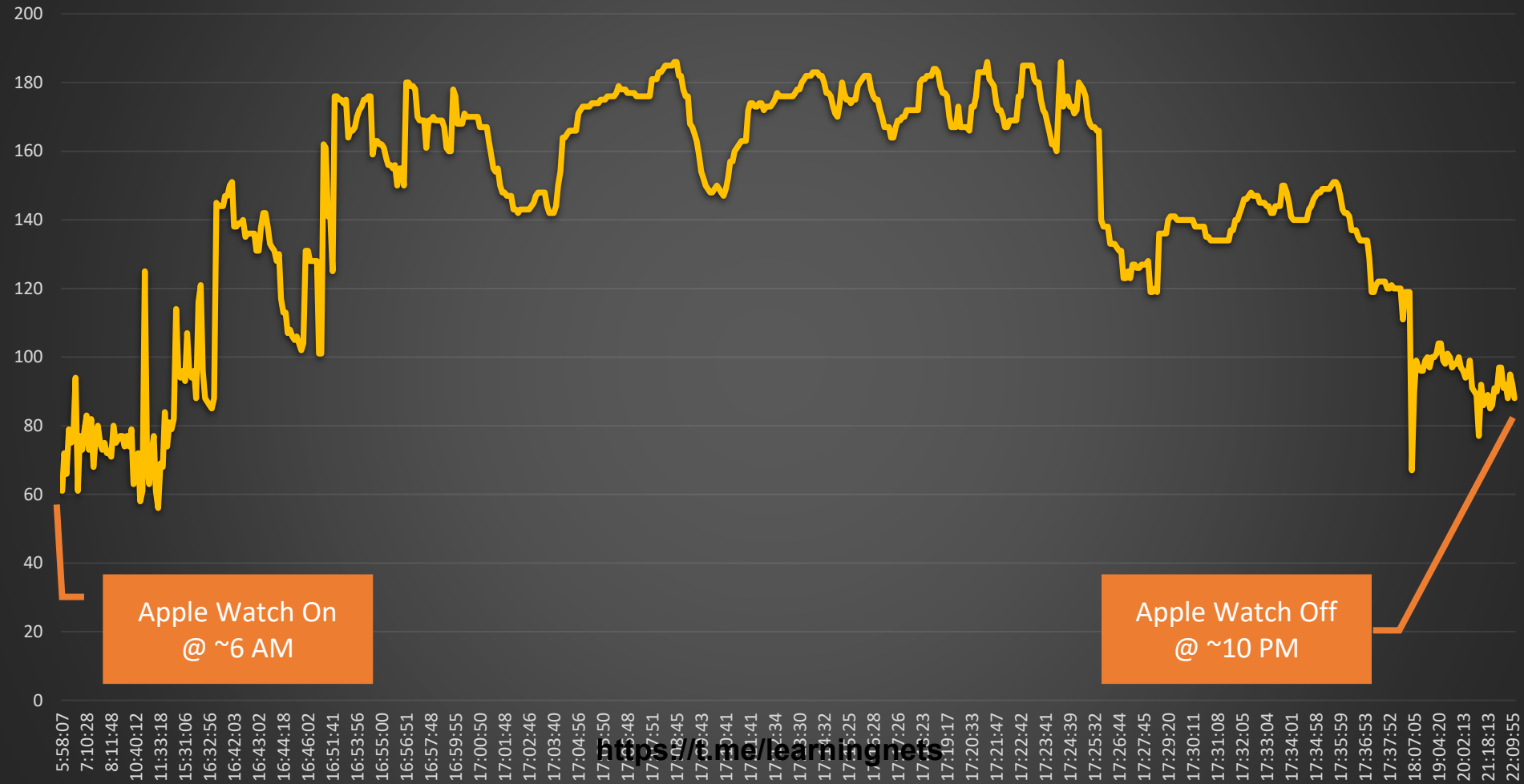


<https://t.me/learningnets>

# Day in the Life



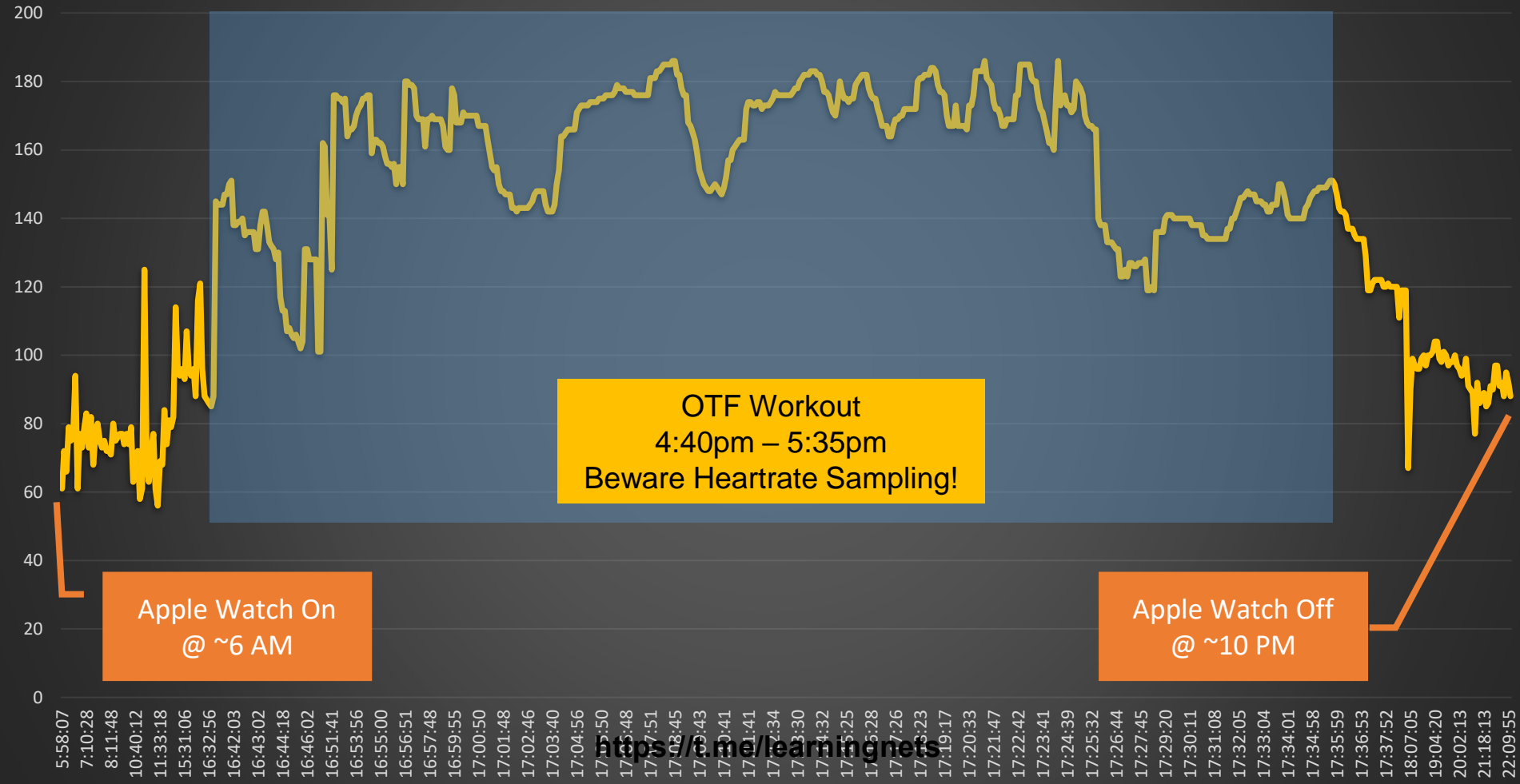
# Day in the Life



Apple Watch On  
@ ~6 AM

Apple Watch Off  
@ ~10 PM

# Day in the Life

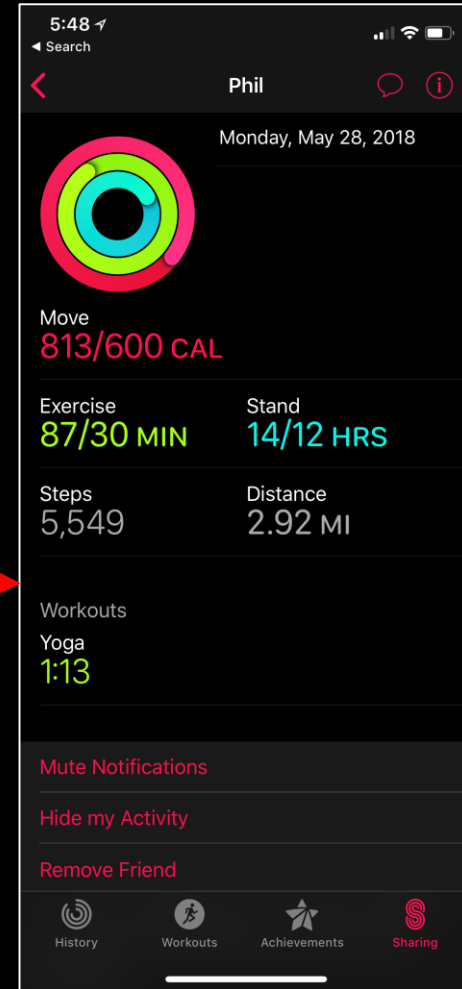
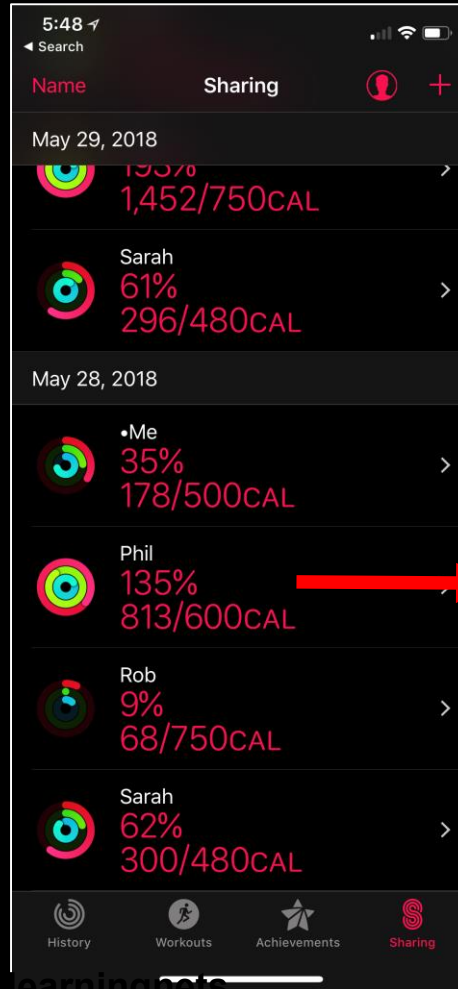


# Narc on your Homies

- Friends Workout Stats & Activities
- [/private/var]/mobile/Library/Health/ActivitySharing/contacts.dat
- Ugly BLOB data with embedded binary plists.

```
Complex = {  
  1: = [  
    LengthValue = A080C50F-17EA-4112-B809-DDA45A097689  
  ]  
  2: = [  
    LengthValue = Sarah Edwards  
  ]  
  3: = [  
    LengthValue = Sarah  
  ]  
  4: = [  
    LengthValue = oompa@  
    LengthValue = +1  
    LengthValue = iamevltwin@  
  ]  
}
```

<https://t.me/terminator16>



# Some Tools May Parse Bits of Health Data

- Oxygen Parses
- 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

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

	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	24.38000000000047	NULL	NULL
743632	2017-01-19 22:17:07	2017-01-19 22:23:33	549523	steps	39.0	NULL	NULL
743633	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	19.62999999999756	NULL	NULL
743637	2017-01-19 16:43:27	2017-01-19 16:53:25	549515	dist in m	33.26999999999895	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	31.54999999999884	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	27.77999999999968	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	43.73999999999907	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	28.28999999999979	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	55.57999999999872	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


# Validate Tool Findings

- Verify Accuracy

**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 19:18:10

**Gender: Male**  
**Birthday (Device time): 12/17/1979**  
Height: 170.18 cm  
Weight:  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 = "1E3628594"
│       │   │   ├── S, HKEmergencyContactRelationshipKey = "spouse"
│       │   │   ├── S, HKEmergencyContactPhoneNumberContactIdentifierKey = "80"
│       │   │   ├── S, HKEmergencyContactNameKey = "Jus"
│       │   │   ├── I, HKEmergencyContactPhoneNumberPropertyIDKey = "3"
│       │   │   ├── I, HKEmergencyContactNameRecordIDKey = "8"
│       │   │   └── S, HKEmergencyContactPhoneNumberKey = "(?)"
│       └── I, HKMedicalIDDataIsOrganDonorKey = "2"
├── 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
```

**Joshua A. Dellinger**  
@hooopen

Follow

I live/work in SF, and park on the street. It takes 45-90 minutes to find parking, so I tend to walk more to do my errands. On Nob Hill it ends up being uphill both way. #DFIRFit

Tuesday, May 8, 2018

Activity

Walking + Running Distance **7.4** mi  
Today at 5:48 PM

Steps **15,044** steps  
Today at 5:48 PM

Flights Climbed **64** floors  
Today at 5:46 PM

11:05 PM - 8 May 2018

# #DFIRFIT or BUST!

We Assume Cloud Pulls are on the Horizon

We Need to Test Medical Records

Tool Support is Lacking

So much tracking we couldn't cover. Got a theory? Do some active research!

Get MOTIVATED and Get ACTIVE People!

**Keith**  
@Tazdrumm3r

Follow

Rings closed. Therapy completed. #DFIRFit #hackerfitness

**HOW I FEEL**

**AFTER I LEAVE THE GYM**

7:22 PM - 23 Apr 2018

**Keith**  
@Tazdrumm3r

Follow

Fun fact: I have at least 15 conference shirts, size 2XL.

Today, two accomplishments.

1. Wore a size Small Brides Detroit Kids shirt to Converge
2. Acquired my first size Medium conference shirt.

#DFIRFit #hackerfitness

9:46 PM - 10 May 2018

**EZ**  
@Forensicator

Follow

Couch2 5k app no longer needed. Got to week befining of week 5 and said screw dat. Went for it. Success! 10k, u next... #DFIRFit

6:12 AM - 16 May 2018

# Want to See More of Us?

We LOVE RESEARCH! Look out for more talks & come to our classes!

585 - Advanced Smartphone Forensics - FOR585.com

- DC (Jul), NYC (Aug), Vegas (Sept), Denver (Oct) , Prague, CZ (Oct), Miami (Nov)

518 – Mac & iOS Forensic Analysis and Incident Response - FOR518.com

- Vegas (Sep), Prague, CZ (Oct), Sydney (Nov)

Both available On Demand



**Jean-Philippe** @Jipe\_ · 4h

#DFIRFIT is such a great idea! 😊👍 You'll do 50 pushups for every missed artifacts! 😊

<https://t.me/learningnets>



**Brad Garnett**  
@brgarnett

Following

Best way to stay warm and visible during cold, outdoor December morning cardio!  
#DFIRFIT



10:05 AM - 8 Dec 2017



**matthew seyer**  
@forensic\_matt

Following

Getting #DFIRFit in the back country.  
Sporting my @MagnetForensics swag.



8:43 PM - 24 Feb 2018



**Brian Moran (Not Brain Morgan)**  
@brianjmoran

Following

Happy Workout Wednesday!! Get a #DFIRFit workout in today and exercise!

In the event that you are totally unmotivated, imagine you are being chased by a giant T-Rex!!



10:37 AM - 25 Apr 2018