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

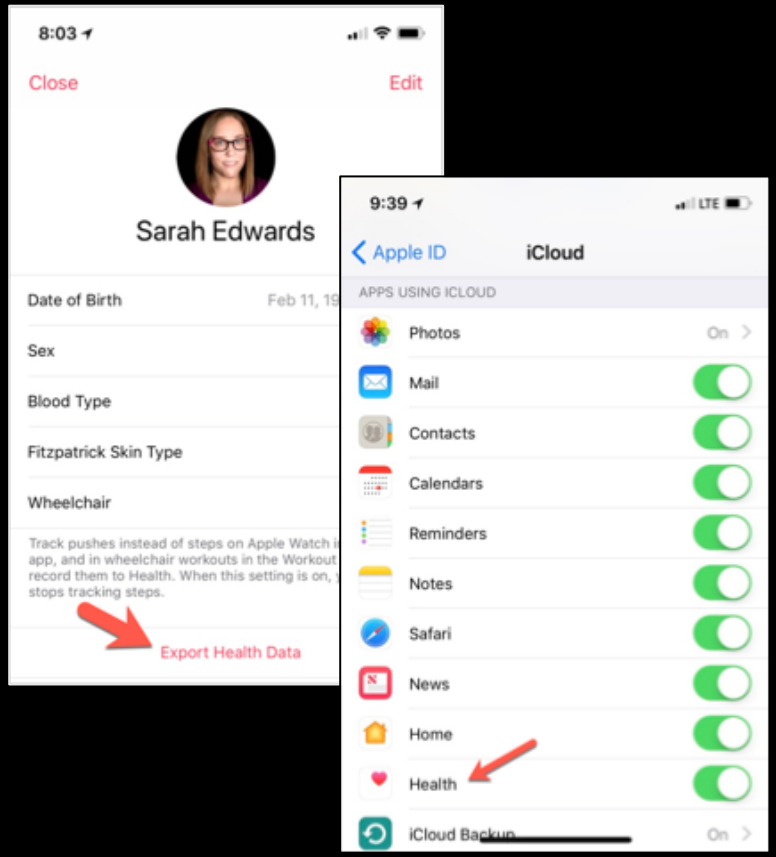
Health Data

- Acquisition
- Analysis
- Scenarios

Motivate!

A bit about us and our goals!

Acquisition Options



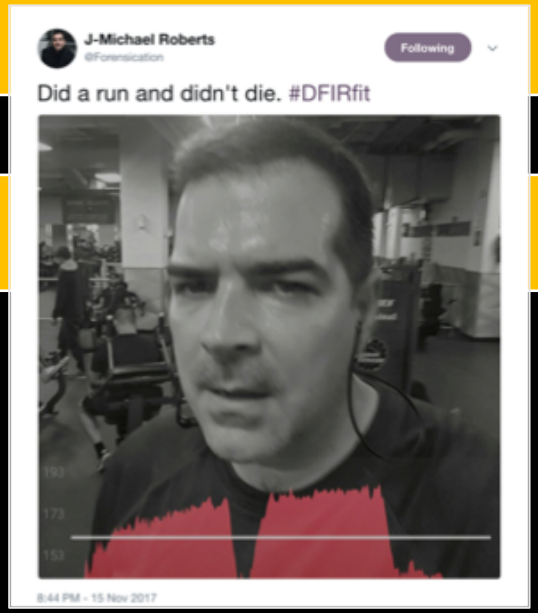
Encrypted iOS Backups

- 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)


```
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 Heath Data
- Activity.app – Workout/Challenge Specific

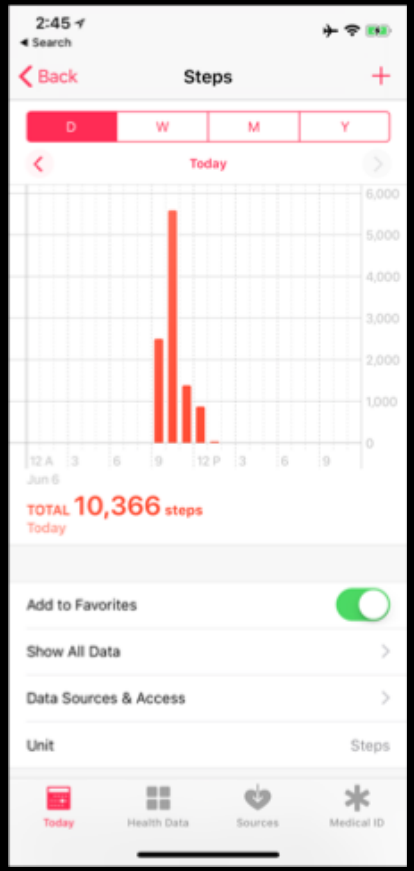
3rd Party Apps

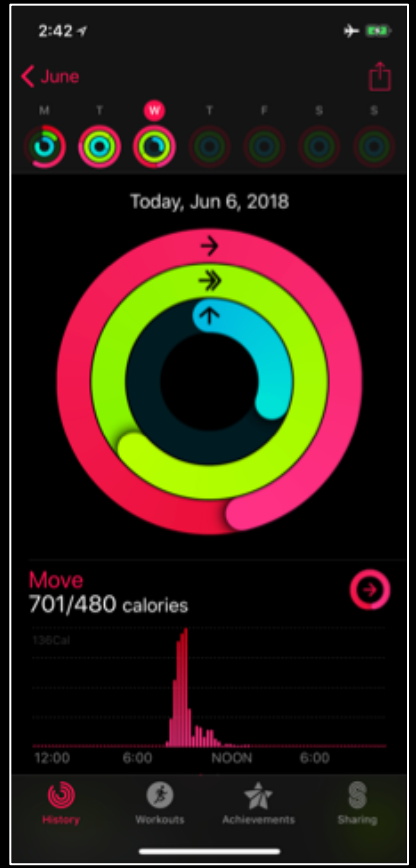
- Diet (MyFitnessPal)
- Sleep Monitoring (Sleep++, Pillow)
- Hardware (Scale, Blood Pressure Monitor, Fitbits, etc)
- Workout (Runkeeper, Couch25k)

Integration with Apple Watch

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

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

Database Contents – healthdb_secure.sqlite

- Achievements
- Historical Health Contents
- Workouts
- Friend Achievements and Workouts
- Records
  - Medical
  - Vaccination
  - Allergy

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

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

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
```

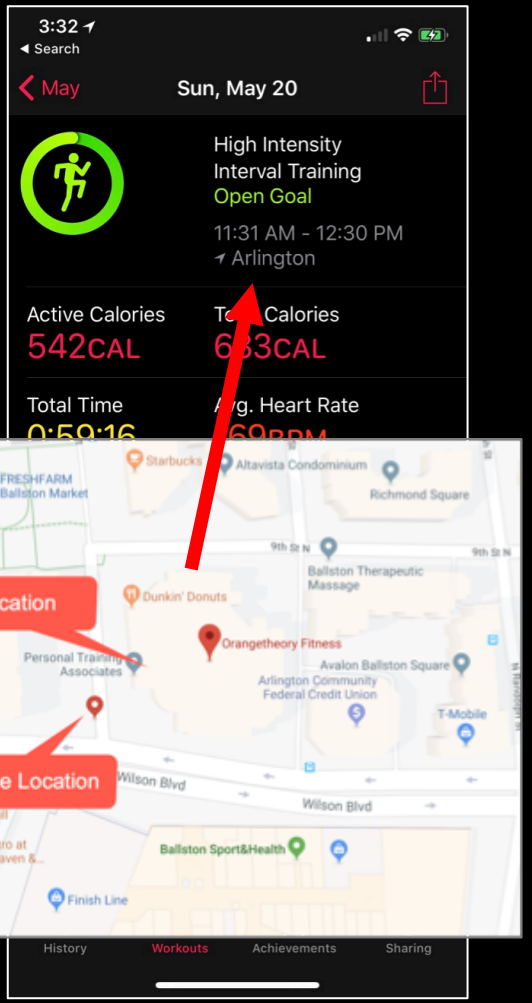
	Start Date	End Date	data_id	numerical_value	key
1	2018-05-20 11:31:18	2018-05-20 12:30:34	3286355	38.880229643481	_HK…
2	2018-05-20 11:31:18	2018-05-20 12:30:34	3286355	-77.111616589084	_HK…
3	2018-05-20 11:20:51	2018-05-20 11:28:12	3282421	38.8819636367535	_HK…
4	2018-05-20 11:20:51	2018-05-20 11:28:12	3282421	-77.1046346898611	_HK…
5	2018-05-15 09:15:00	2018-05-15 10:15:50	3271626	32.733272501983	_HKPrivateWorkoutWeatherLocationCoordinat…
6	2018-05-15 09:15:00	2018-05-15 10:15:50	3271626	-117.160310640047	_HKPrivateWorkoutWeatherLocationCoordinat…
7	2018-05-14 09:11:22	2018-05-14 10:19:39	3267728	32.7332047368432	_HK…
8	2018-05-14 09:11:22	2018-05-14 10:19:39	3267728	-117.160302985525	_HK…
9	2018-05-10 19:34:54	2018-05-10 20:42:37	3257045	32.7332583121942	_HKPrivateWorkoutWeatherLocationCoordinat…
10	2018-05-10 19:34:54	2018-05-10 20:42:37	3257045	-117.16030794439	_HKPrivateWorkoutWeatherLocationCoordinate…
11	2018-05-09 07:04:43	2018-05-09 08:05:39	3244916	38.8802543447835	_HK…
12	2018-05-09 07:04:43	2018-05-09 08:05:39	3244916	-77.1116063044133	_HK…

Arlington (shown)

Arlington

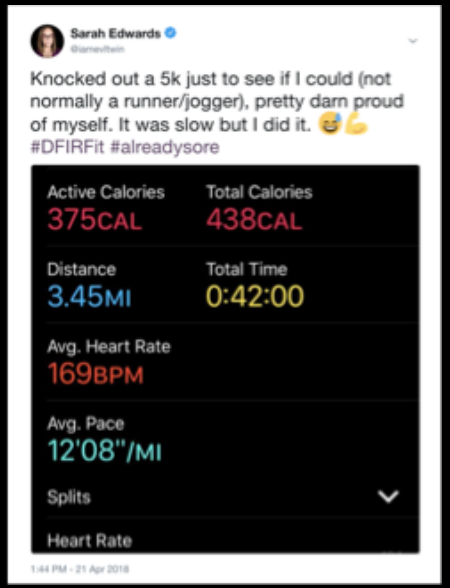
San Diego

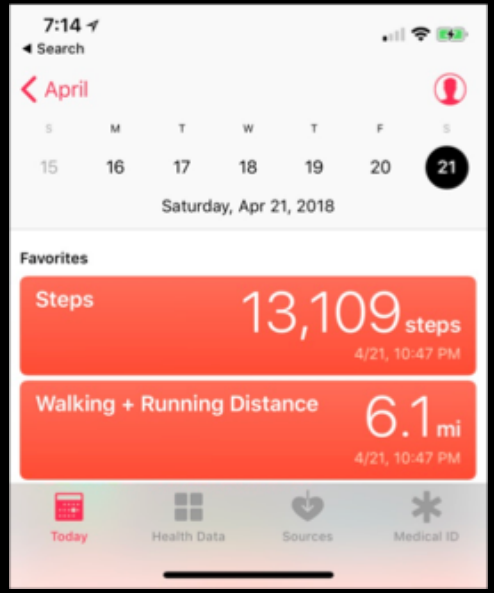
Arlington



Pattern of Life – Steps/Distance Per Day

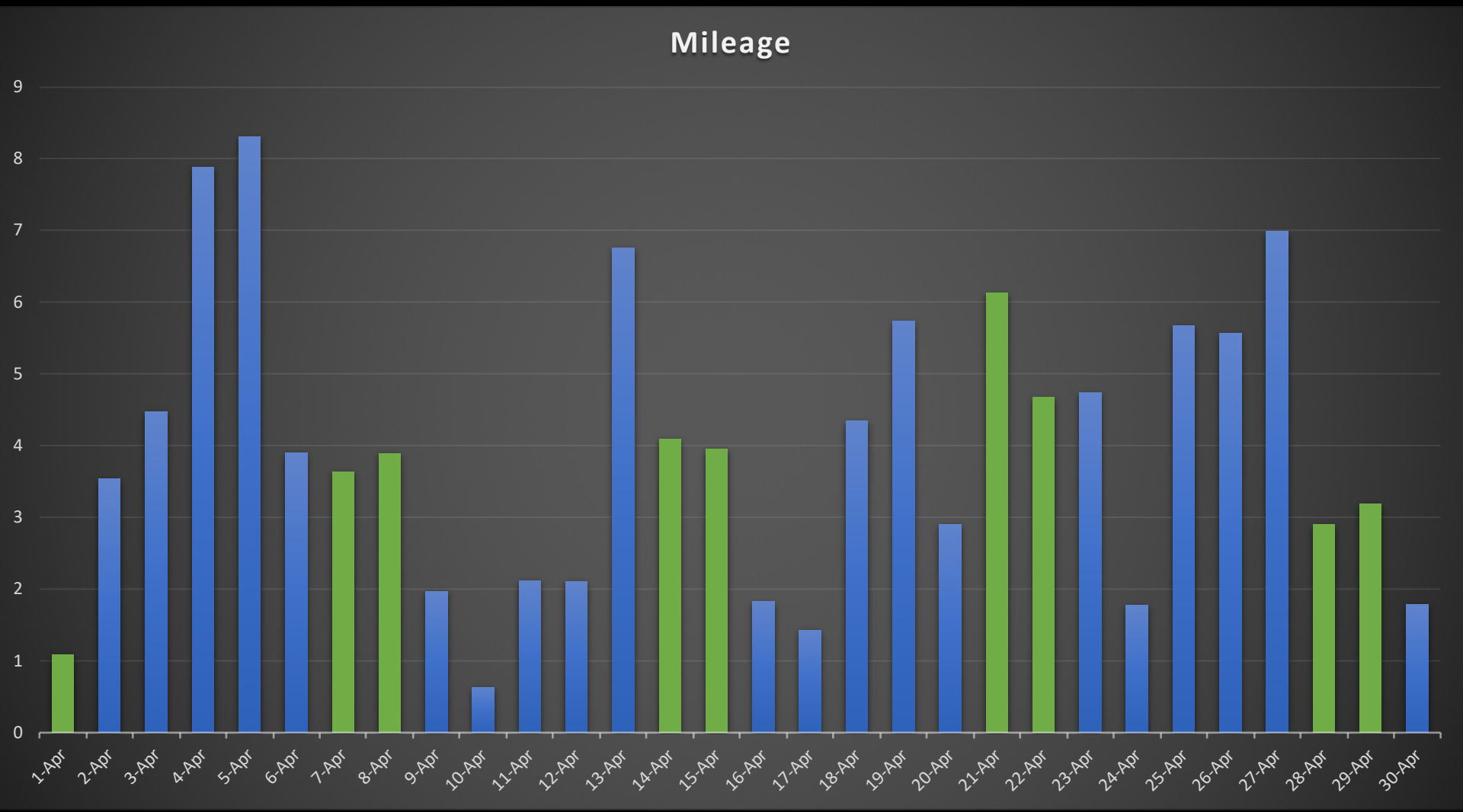
- Potential Issues: Crossing Time Zones, Workouts, Multiple Devices
- Context Required for Interpretation

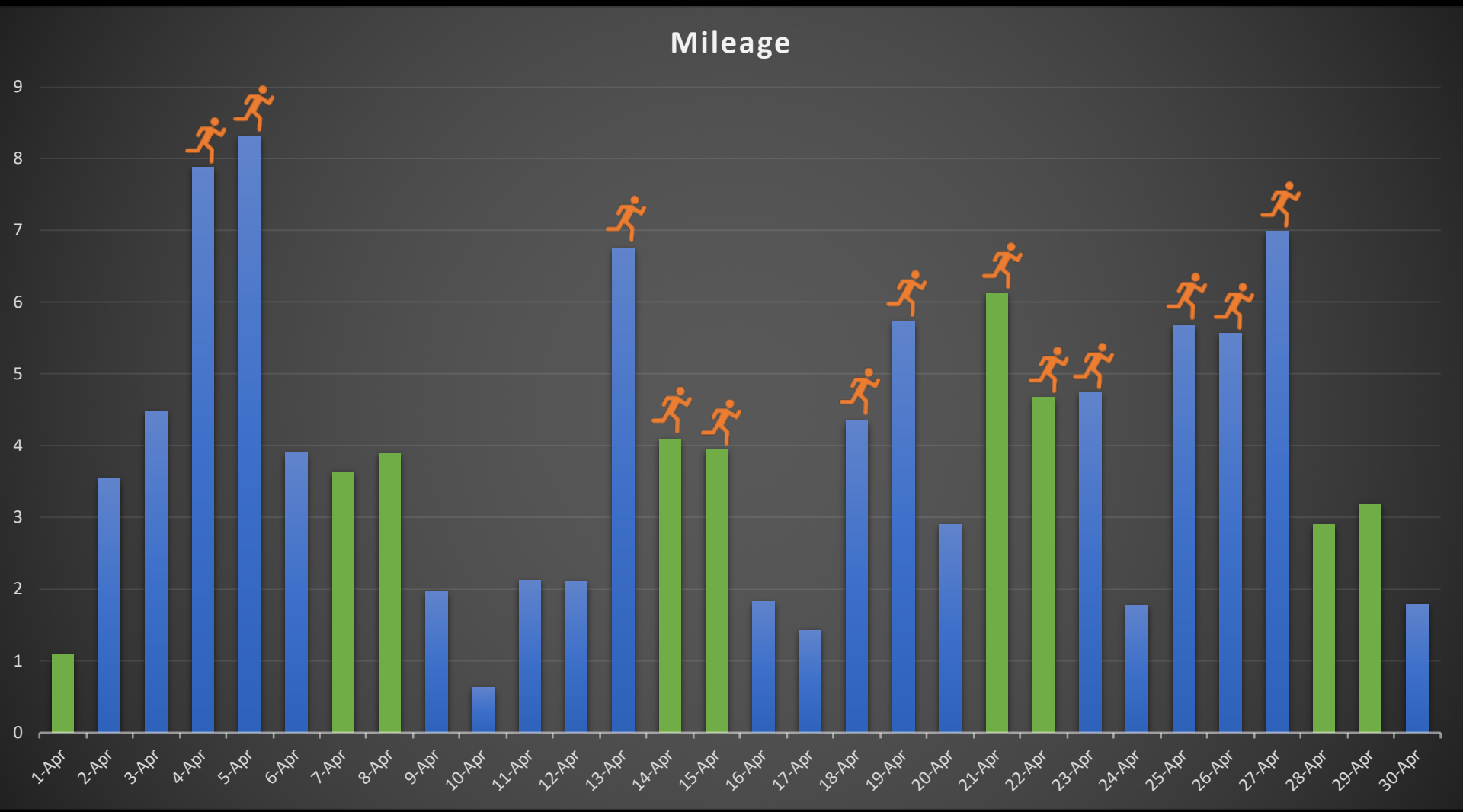


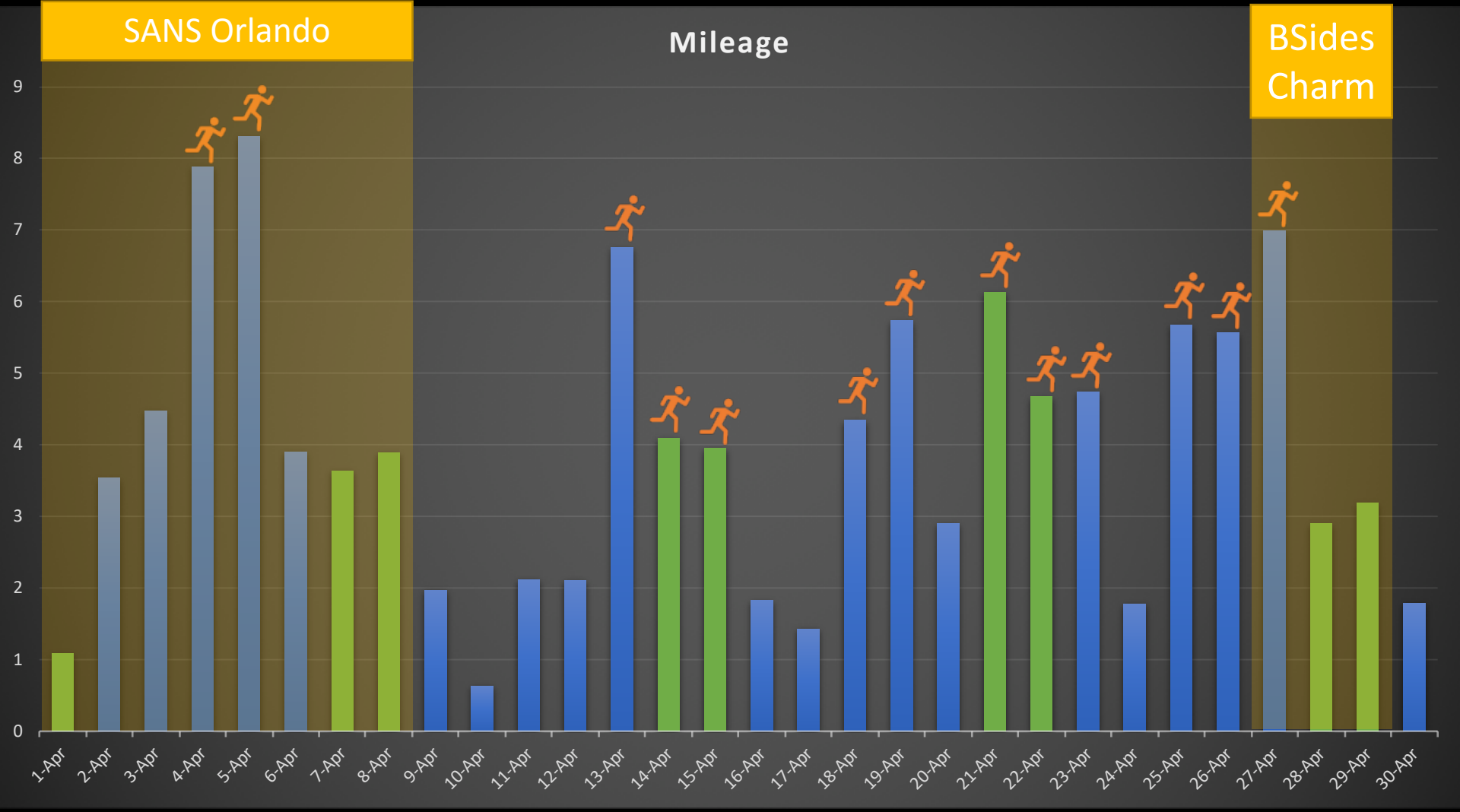


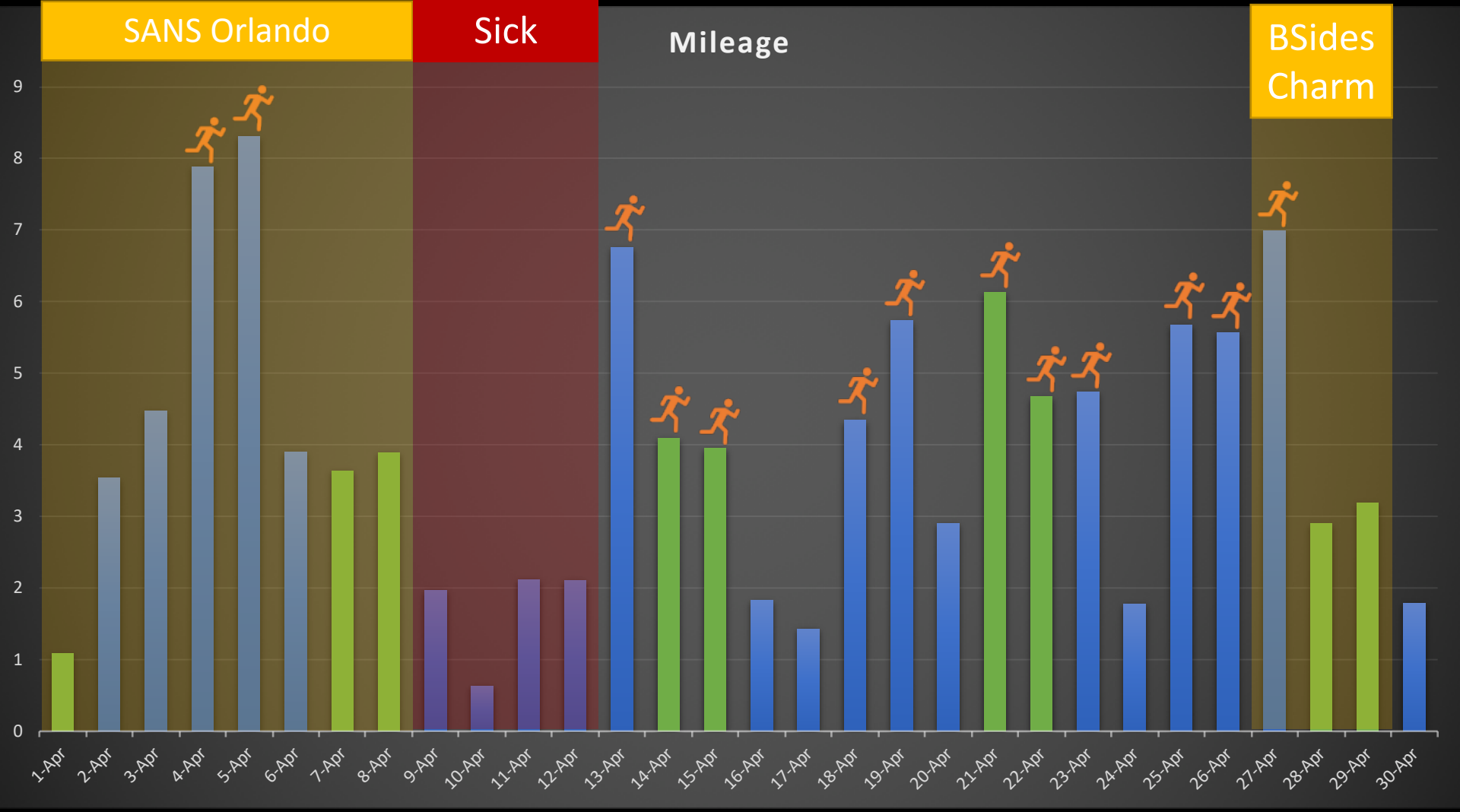

```
1  select datetime(cache_index+978307200,'unixepoch','utc') as "Day",
2  steps, walk_distance*0.000621371 as "Milage"  from activity_caches
3  order by  "Day" desc
```

	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
9
8
7
6
5
4
3
2
1
0
1-Apr
2-Apr
3-Apr
4-Apr
5-Apr
6-Apr
7-Apr
8-Apr
9-Apr
10-Apr
11-Apr
12-Apr
13-Apr
14-Apr
15-Apr
16-Apr
17-Apr
18-Apr
19-Apr
20-Apr
21-Apr
22-Apr
23-Apr
24-Apr
25-Apr
26-Apr
27-Apr
28-Apr
29-Apr
30-Apr


Mileage
9
8
7
6
5
4
3
2
1
0
1-Apr
2-Apr
3-Apr
4-Apr
5-Apr
6-Apr
7-Apr
8-Apr
9-Apr
10-Apr
11-Apr
12-Apr
13-Apr
14-Apr
15-Apr
16-Apr
17-Apr
18-Apr
19-Apr
20-Apr
21-Apr
22-Apr
23-Apr
24-Apr
25-Apr
26-Apr
27-Apr
28-Apr
29-Apr
30-Apr


SANS Orlando
Mileage
BSides Charm
9
8
7
6
5
4
3
2
1
0
1-Apr
2-Apr
3-Apr
4-Apr
5-Apr
6-Apr
7-Apr
8-Apr
9-Apr
10-Apr
11-Apr
12-Apr
13-Apr
14-Apr
15-Apr
16-Apr
17-Apr
18-Apr
19-Apr
20-Apr
21-Apr
22-Apr
23-Apr
24-Apr
25-Apr
26-Apr
27-Apr
28-Apr
29-Apr
30-Apr


SANS Orlando
Sick
Mileage
BSides Charm
9
8
7
6
5
4
3
2
1
0
1-Apr
2-Apr
3-Apr
4-Apr
5-Apr
6-Apr
7-Apr
8-Apr
9-Apr
10-Apr
11-Apr
12-Apr
13-Apr
14-Apr
15-Apr
16-Apr
17-Apr
18-Apr
19-Apr
20-Apr
21-Apr
22-Apr
23-Apr
24-Apr
25-Apr
26-Apr
27-Apr
28-Apr
29-Apr
30-Apr

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

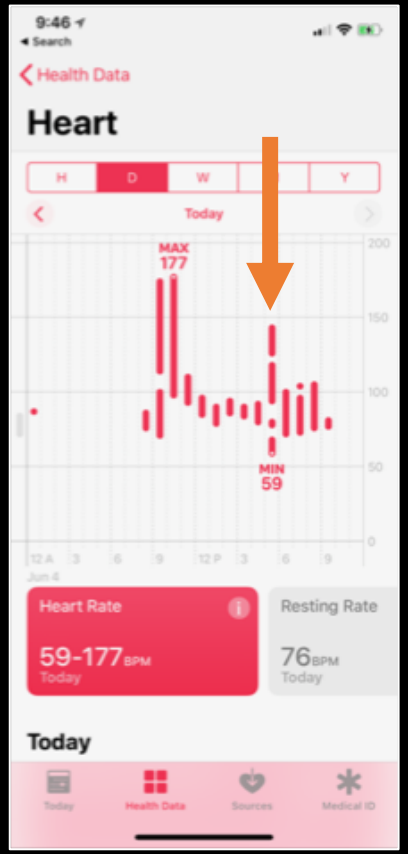
Jan 11 2018, 8:00am

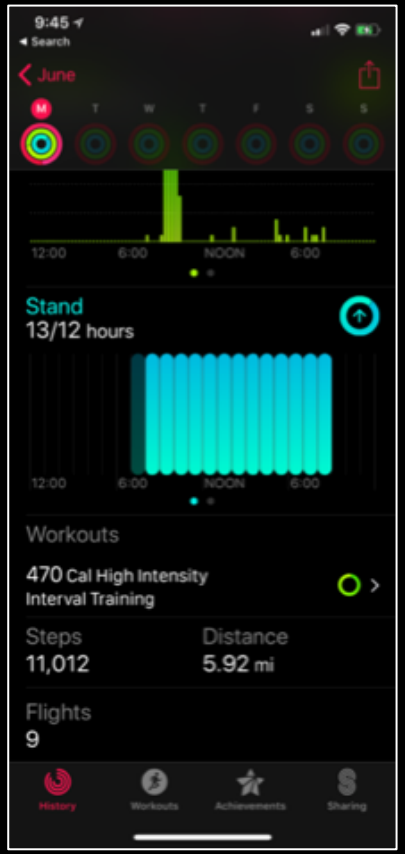
The app recorded a portion of his activity as “climbing stairs,” which authorities were able to correlate with the time he would have dragged his victim down the river embankment, and then climbed back up. Freiburg police sent an investigator to the scene to replicate his movements, and sure enough,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

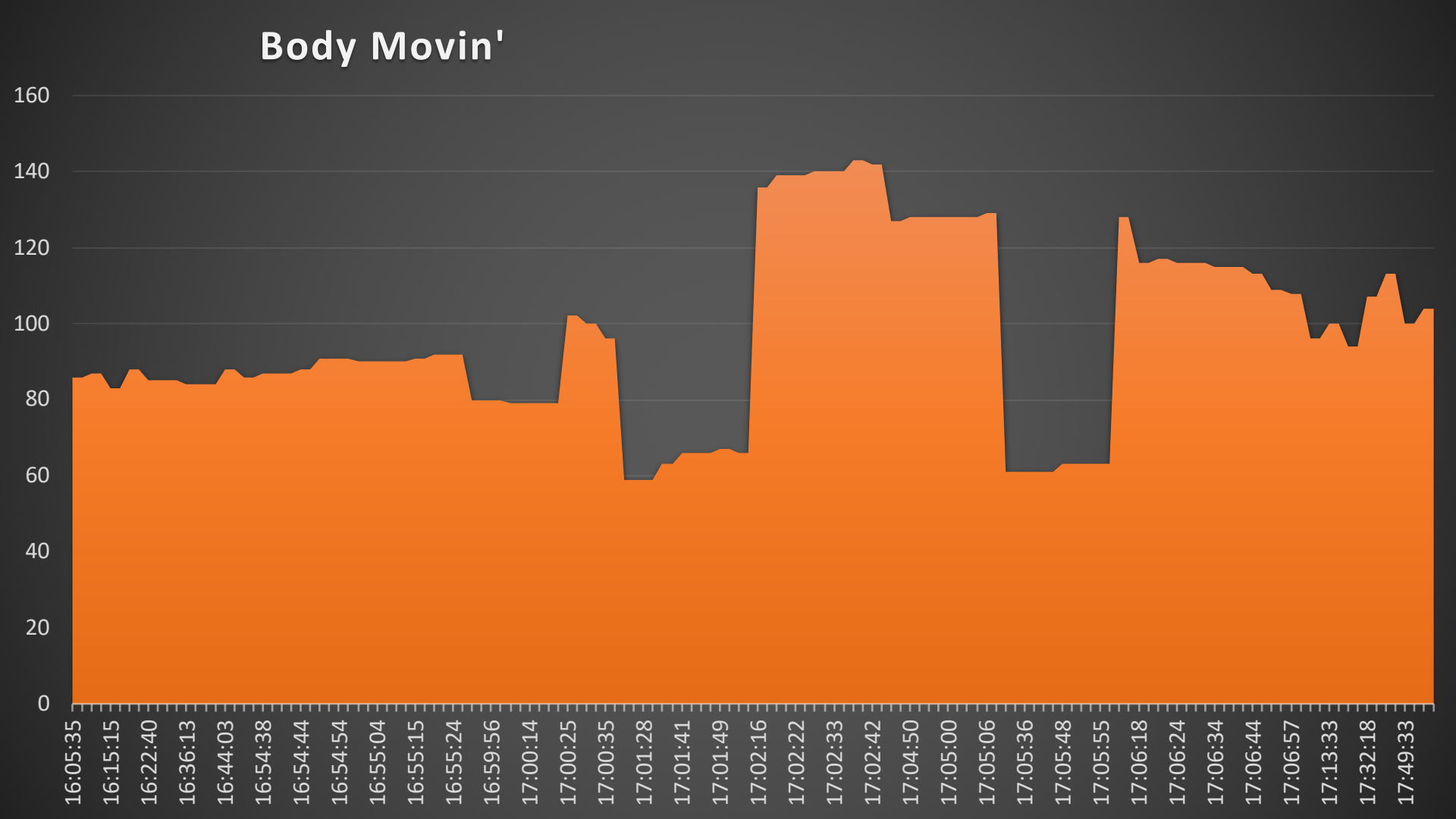
	Start Date	End Date	data_id	data_type	quantity	original_quantity	unit_string	original_u
61	2018-06-04 17:02:37	2018-06-04 17:02:37	1547823	5	2.38333333333333	143.0	count/min	2
62	2018-06-04 17:02:37	2018-06-04 17:02:37	1547823	5	2.38333333333333	143.0	count/min	2
63	2018-06-04 17:02:33	2018-06-04 17:02:33	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

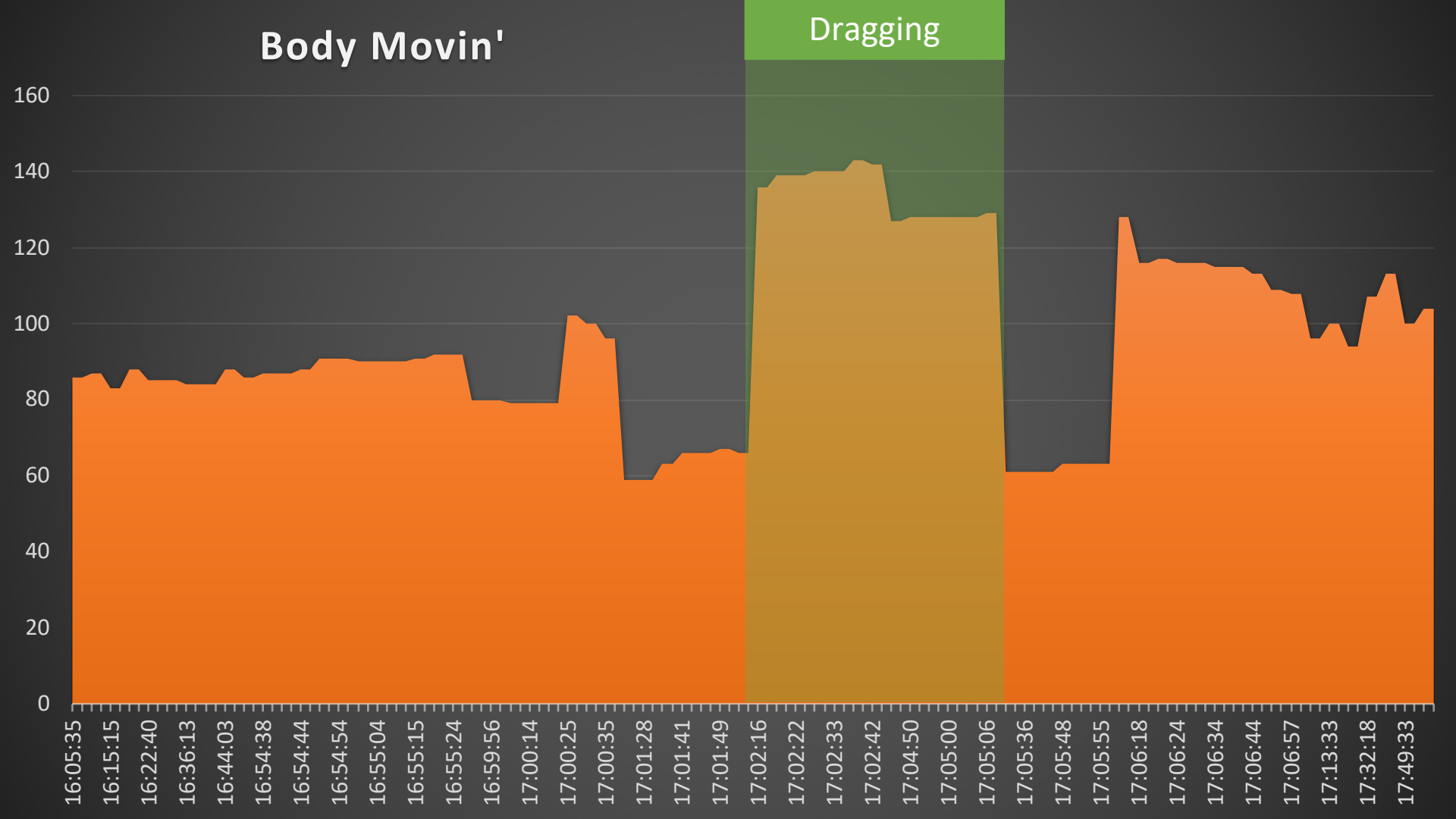


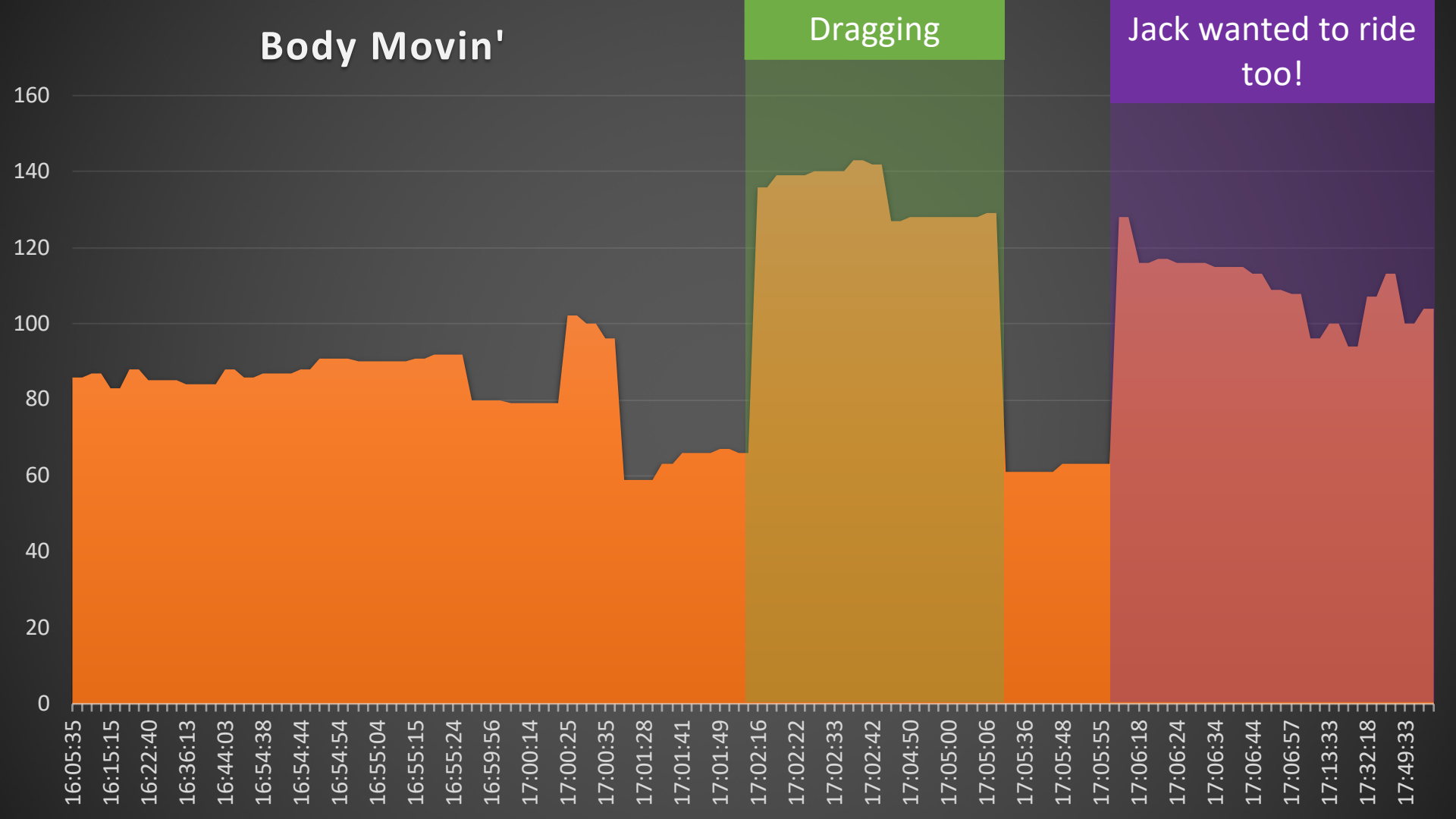


And Now My Lawn is Dead

- What This Looked Like


Body Movin'
160
140
120
100
80
60
40
20
0
16:05:35
16:15:15
16:22:40
16:36:13
16:44:03
16:54:38
16:54:44
16:54:54
16:55:04
16:55:15
16:55:24
16:59:56
17:00:14
17:00:25
17:00:35
17:01:28
17:01:41
17:01:49
17:02:16
17:02:22
17:02:33
17:02:42
17:04:50
17:05:00
17:05:06
17:05:36
17:05:48
17:05:55
17:06:18
17:06:24
17:06:34
17:06:44
17:06:57
17:13:33
17:32:18
17:49:33


Body Movin'
Dragging
160
140
120
100
80
60
40
20
0
16:05:35
16:15:15
16:22:40
16:36:13
16:44:03
16:54:38
16:54:44
16:54:54
16:55:04
16:55:15
16:55:24
16:59:56
17:00:14
17:00:25
17:00:35
17:01:28
17:01:41
17:01:49
17:02:16
17:02:22
17:02:33
17:02:42
17:04:50
17:05:00
17:05:06
17:05:36
17:05:48
17:05:55
17:06:18
17:06:24
17:06:34
17:06:44
17:06:57
17:13:33
17:32:18
17:49:33


Body Movin'
Dragging
Jack wanted to ride too!
160
140
120
100
80
60
40
20
0
16:05:35
16:15:15
16:22:40
16:36:13
16:44:03
16:54:38
16:54:44
16:54:54
16:55:04
16:55:15
16:55:24
16:59:56
17:00:14
17:00:25
17:00:35
17:01:28
17:01:41
17:01:49
17:02:16
17:02:22
17:02:33
17:02:42
17:04:50
17:05:00
17:05:06
17:05:36
17:05:48
17:05:55
17:06:18
17:06:24
17:06:34
17:06:44
17:06:57
17:13:33
17:32:18
17:49:33

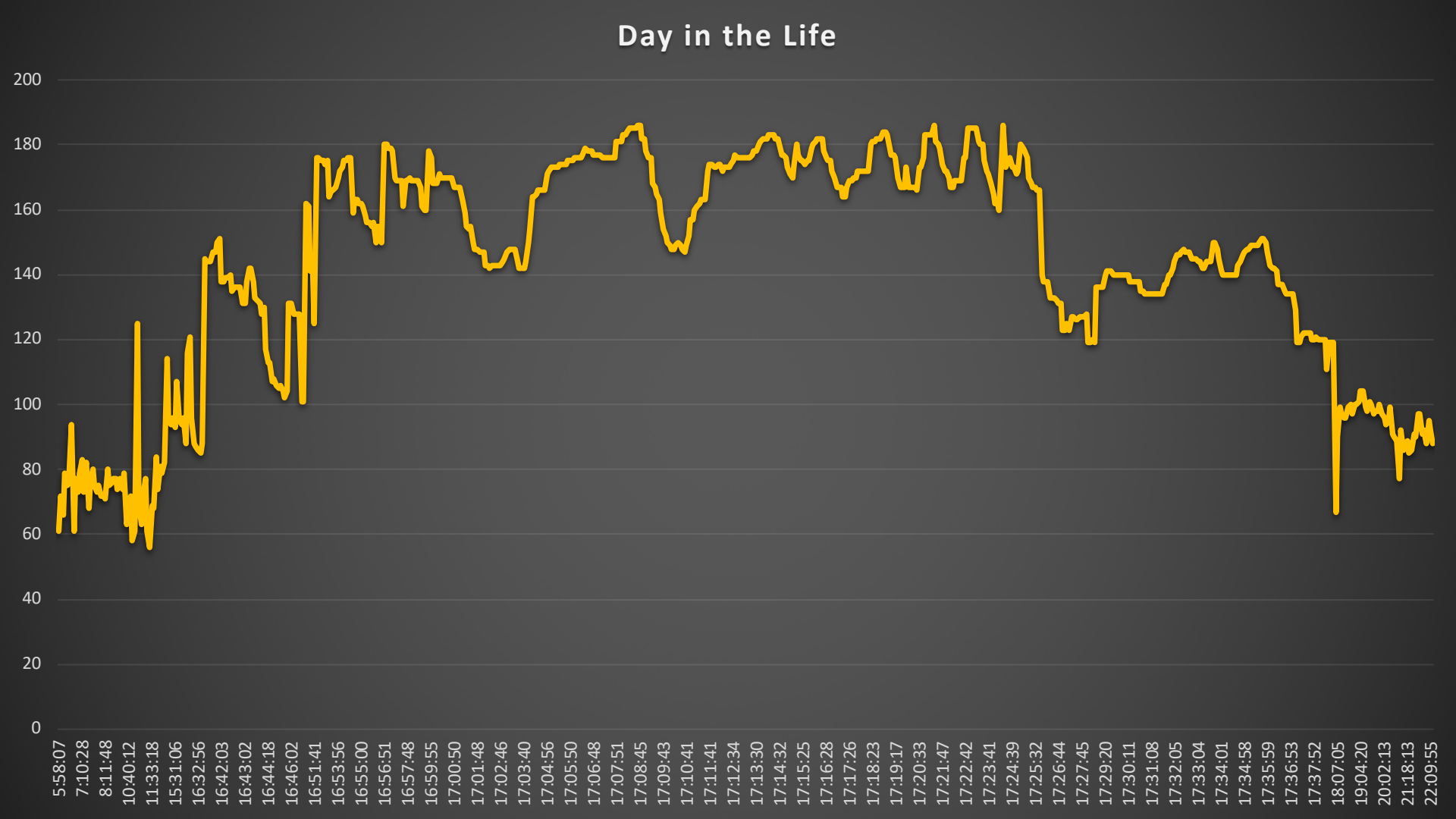
Forensic Scenarios – Heart Rate – Dead or Alive?

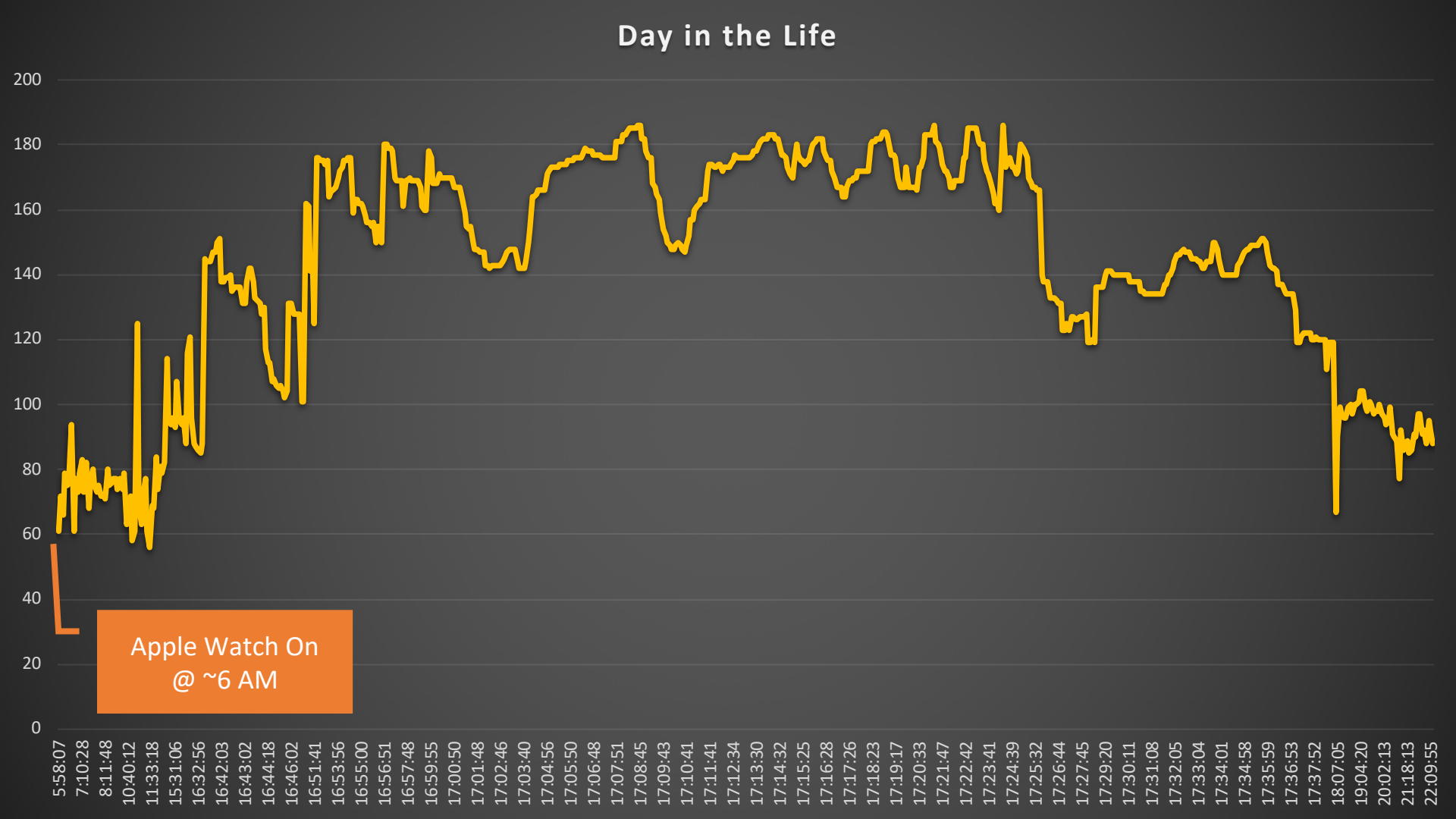
Death

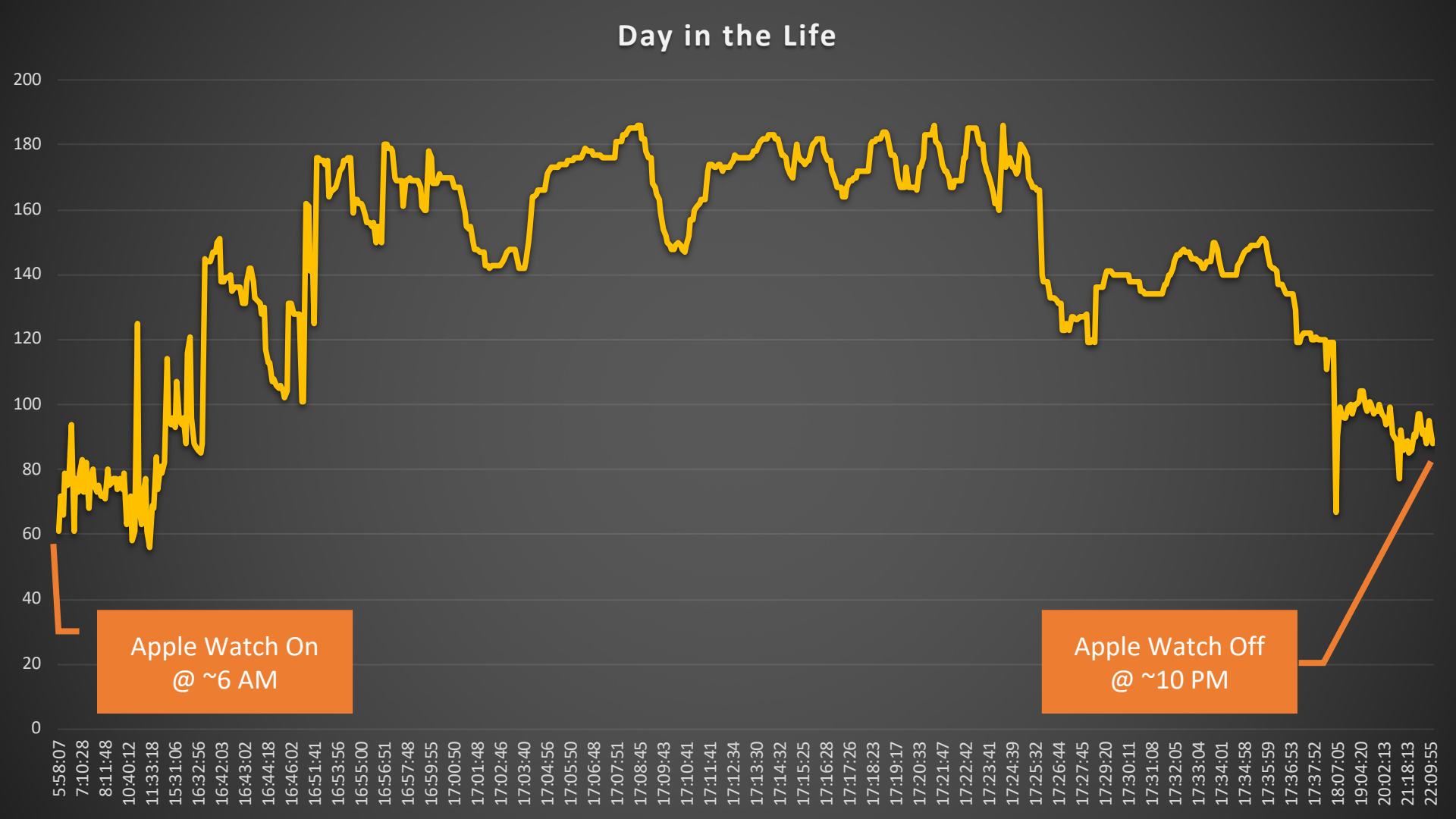
- Drop in Heart Rate
- Correlate with iOS Application Usage
  - CurrentPowerlog.PLSQL
  - No Longer backed up in iOS 11
  - Physical/Jailbroken Access
- Really difficult to test
  - Volunteers?

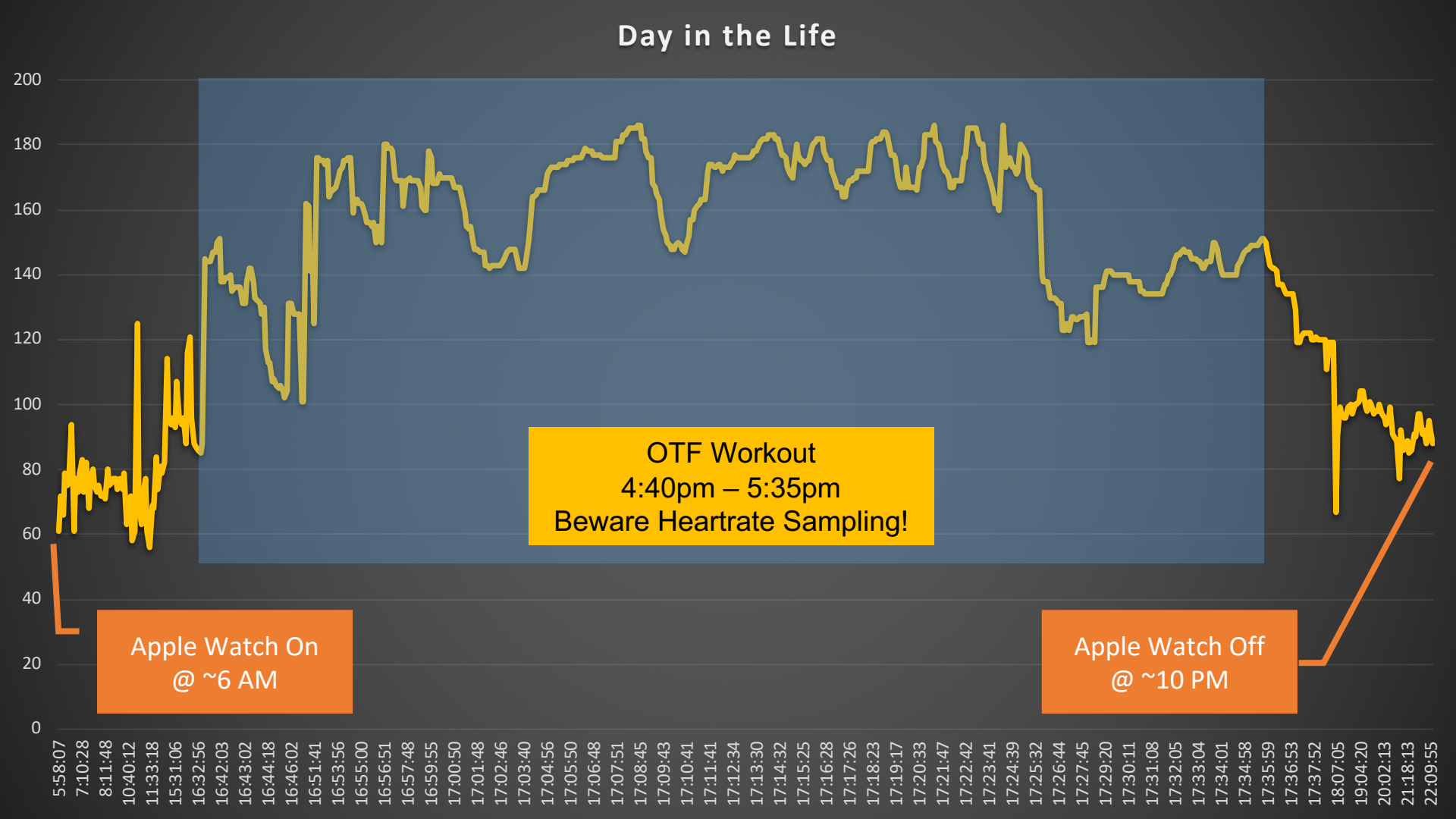
Alive

- 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)


Day in the Life
200
180
160
140
120
100
80
60
40
20
0
5:58:07
7:10:28
8:11:48
10:40:12
11:33:18
15:31:06
16:32:56
16:42:03
16:43:02
16:44:18
16:46:02
16:51:41
16:53:56
16:55:00
16:56:51
16:57:48
16:59:55
17:00:50
17:01:48
17:02:46
17:03:40
17:04:56
17:05:50
17:06:48
17:07:51
17:08:45
17:09:43
17:10:41
17:11:41
17:12:34
17:13:30
17:14:32
17:15:25
17:16:28
17:17:26
17:18:23
17:19:17
17:20:33
17:21:47
17:22:42
17:23:41
17:24:39
17:25:32
17:26:44
17:27:45
17:29:20
17:30:11
17:31:08
17:32:05
17:33:04
17:34:01
17:34:58
17:35:59
17:36:53
17:37:52
18:07:05
19:04:20
20:02:13
21:18:13
22:09:55


Day in the Life
200
180
160
140
120
100
80
60
40
20
0
Apple Watch On
@ ~6 AM
5:58:07
7:10:28
8:11:48
10:40:12
11:33:18
15:31:06
16:32:56
16:42:03
16:43:02
16:44:18
16:46:02
16:51:41
16:53:56
16:55:00
16:56:51
16:57:48
16:59:55
17:00:50
17:01:48
17:02:46
17:03:40
17:04:56
17:05:50
17:06:48
17:07:51
17:08:45
17:09:43
17:10:41
17:11:41
17:12:34
17:13:30
17:14:32
17:15:25
17:16:28
17:17:26
17:18:23
17:19:17
17:20:33
17:21:47
17:22:42
17:23:41
17:24:39
17:25:32
17:26:44
17:27:45
17:29:20
17:30:11
17:31:08
17:32:05
17:33:04
17:34:01
17:34:58
17:35:59
17:36:53
17:37:52
18:07:05
19:04:20
20:02:13
21:18:13
22:09:55

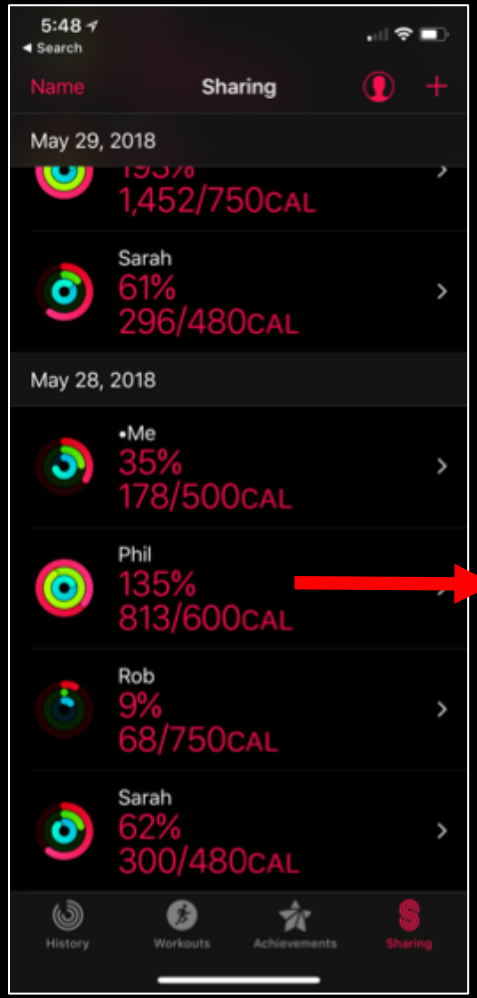

Day in the Life
200
180
160
140
120
100
80
60
40
20
0
5:58:07
7:10:28
8:11:48
10:40:12
11:33:18
15:31:06
16:32:56
16:42:03
16:43:02
16:44:18
16:46:02
16:51:41
16:53:56
16:55:00
16:56:51
16:57:48
16:59:55
17:00:50
17:01:48
17:02:46
17:03:40
17:04:56
17:05:50
17:06:48
17:07:51
17:08:45
17:09:43
17:10:41
17:11:41
17:12:34
17:13:30
17:14:32
17:15:25
17:16:28
17:17:26
17:18:23
17:19:17
17:20:33
17:21:47
17:22:42
17:23:41
17:24:39
17:25:32
17:26:44
17:27:45
17:29:20
17:30:11
17:31:08
17:32:05
17:33:04
17:34:01
17:34:58
17:35:59
17:36:53
17:37:52
18:07:05
19:04:20
20:02:13
21:18:13
22:09:55
Apple Watch On
@ ~6 AM
Apple Watch Off
@ ~10 PM

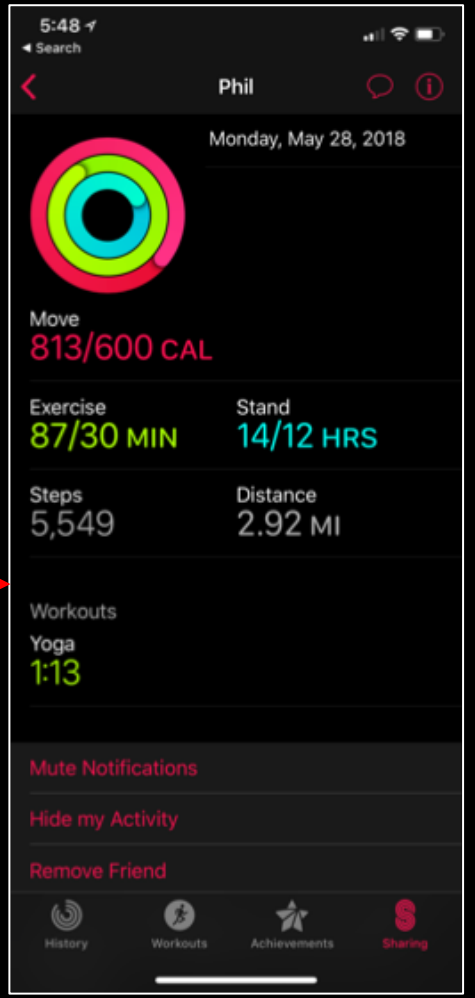

Day in the Life
200
180
160
140
120
100
80
60
40
20
0
OTF Workout
4:40pm – 5:35pm
Beware Heartrate Sampling!
Apple Watch On
@ ~6 AM
Apple Watch Off
@ ~10 PM
5:58:07
7:10:28
8:11:48
10:40:12
11:33:18
15:31:06
16:32:56
16:42:03
16:43:02
16:44:18
16:46:02
16:51:41
16:53:56
16:55:00
16:56:51
16:57:48
16:59:55
17:00:50
17:01:48
17:02:46
17:03:40
17:04:56
17:05:50
17:06:48
17:07:51
17:08:45
17:09:43
17:10:41
17:11:41
17:12:34
17:13:30
17:14:32
17:15:25
17:16:28
17:17:26
17:18:23
17:19:17
17:20:33
17:21:47
17:22:42
17:23:41
17:24:39
17:25:32
17:26:44
17:27:45
17:29:20
17:30:11
17:31:08
17:32:05
17:33:04
17:34:01
17:34:58
17:35:59
17:36:53
17:37:52
18:07:05
19:04:20
20:02:13
21:18:13
22:09:55

Narc on your Homies

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

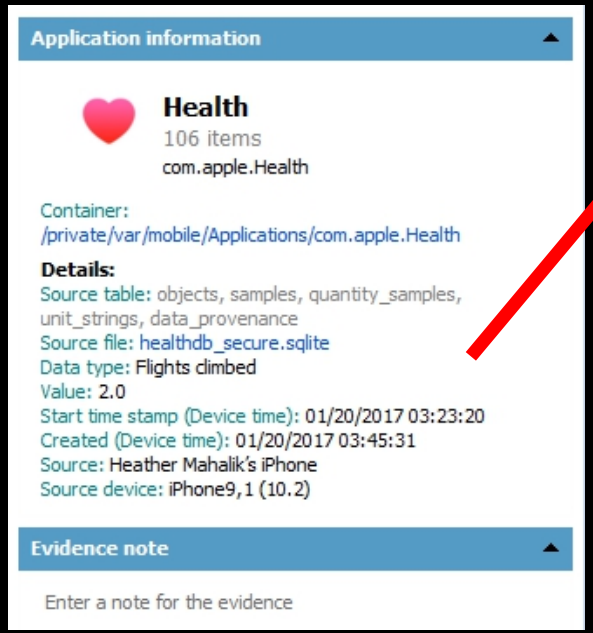
```
Complex = {
    1 : = [
        LengthValue = A080C50F-17EA-4112-B809-DDA45A097689
    2 : = [
        LengthValue = Sarah Edwards
    3 : = [
        LengthValue = Sarah
    4 : = [
        LengthValue = oompa@
        LengthValue = +1
        LengthValue = iamevltwin@
```

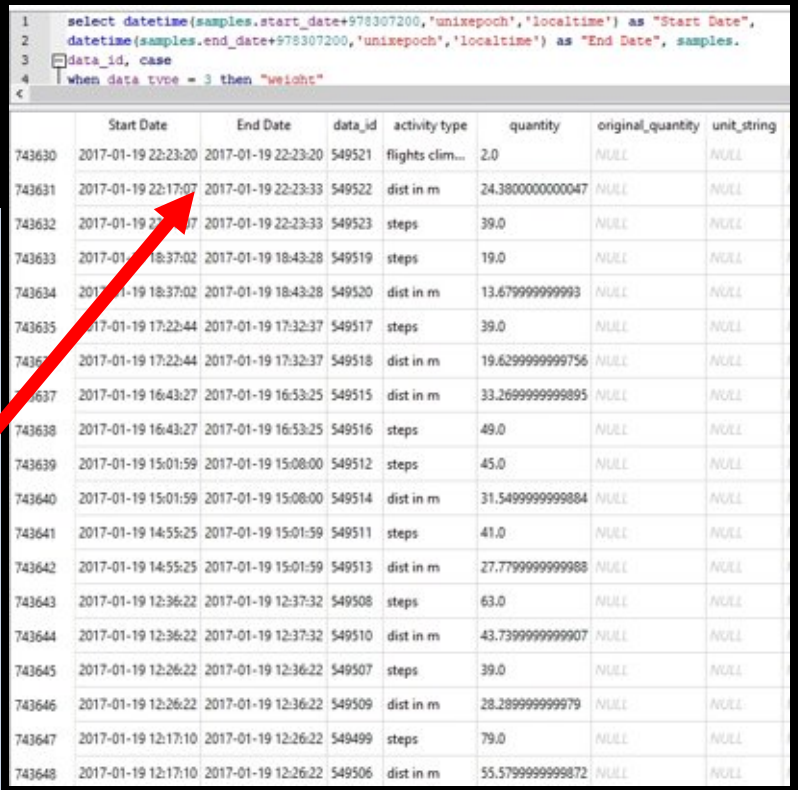




Some Tools May Parse Bits of Health Data

- Oxygen Parses
- Verify Time Zone



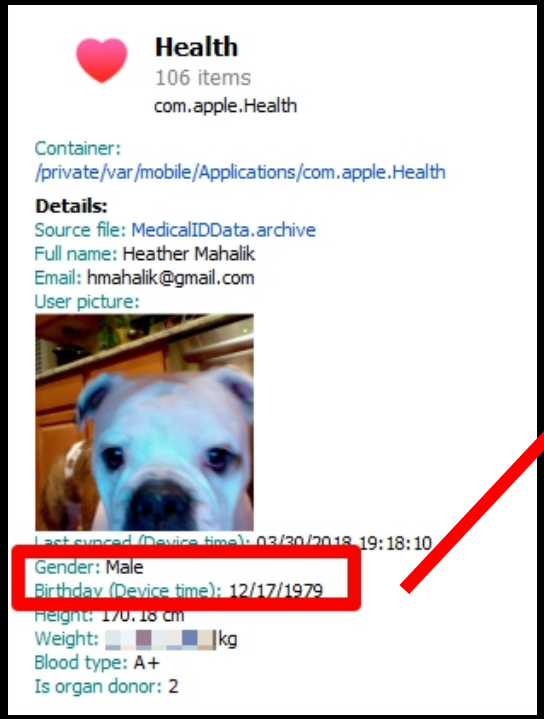


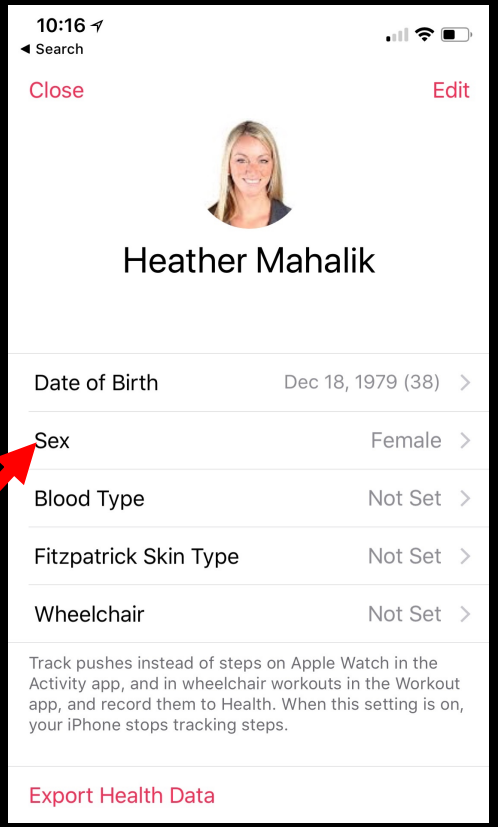
```
select datetime(samples.start_date+978307200,'unixepoch','localtime') as "Start Date",
datetime(samples.end_date+978307200,'unixepoch','localtime') as "End Date", samples.
data_id, case
when data_type = 3 then "weight"
```

	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
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	13.679999999993	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

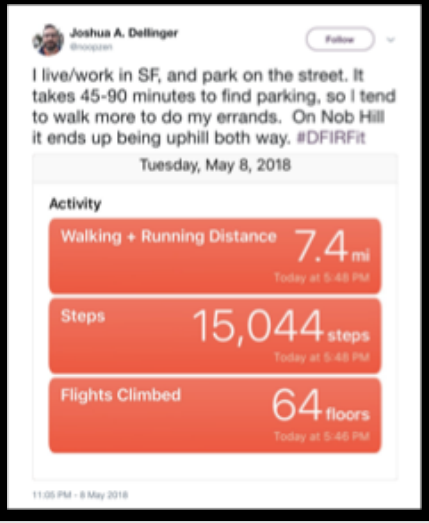
Validate Tool Findings

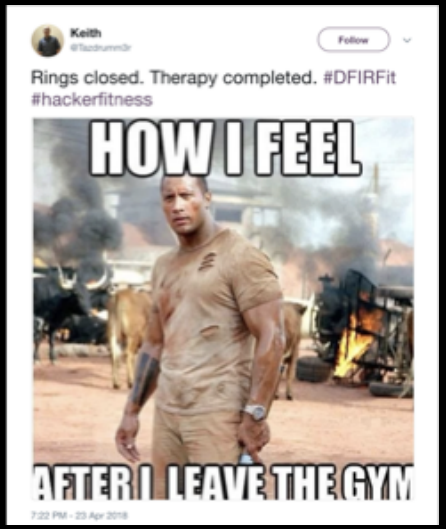
- Verify Accuracy



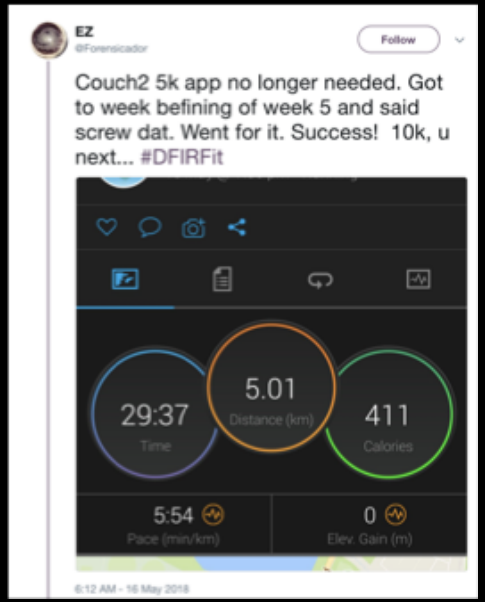


#DFIRFIT or BUST!





- 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!



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

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