Location Tracking in Splunk

ⓘ Rememeber to read part 2 later at Location Tracking in Splunk - Drilldown

I wanted to utilize splunk even more (or same) as Edd in Go Splunk Yourself!

First signup for a tracking solution called OpenPaths failed, as the project seems dead and the iOS is not tracking.

Looking into the Apple Store, i found followmee.com and I signed up for an account. Followmee.com has a complete mapping (Tracking) solution, so I could just have stopped it there, but the focus was splunk.

The only interesting App setting on the iPhone is the tracking state and how often the App tracks, read http://followmee.com/Howto.aspx?t=howtoconfigureiphone

✓ **Tracking Power**
It specifies how aggressively the app will track. The default setting is medium, which gives you a new location update every 5 to 10 minutes. If you want more frequent update, choose the high setting, which updates every 1 to 2 minutes. Currently, my setting is High

Getting data out

Next, the data can be extracted to XLS og CVS, but this was to manual, I wanted to utilize and automate, so I signed up for API services, which has 2 primary functions:

Past hours history for a device

Past gives a json like:

```
{"Data":[{"Date":"2017-12-03T15:26:14+01:00","Latitude":57.01060,"Longitude":10.03402,"Type":"GPS","Speed(mph)":
null,"Speed(km/h)":null,"Altitude(ft)":16,"Altitude(m)":5,"Accuracy":124},{"Date":"2017-12-03T15:53:52+01:00","
Latitude":57.01172,"Longitude":10.04380,"Type":"GPS","Speed(mph)":null,"Speed(km/h)":null,"Altitude(ft)":0,"
Altitude(m)":0,"Accuracy":165},{"Date":"2017-12-03T15:57:05+01:00","Latitude":57.01323,"Longitude":10.04936,"
Type":"GPS","Speed(mph)":null,"Speed(km/h)":null,"Altitude(ft)":6,"Altitude(m)":2,"Accuracy":165},{"Date":"2017-
12-03T16:03:25+01:00","Latitude":57.01406,"Longitude":10.04982,"Type":"GPS","Speed(mph)":null,"Speed(km/h)":
null,"Altitude(ft)":3,"Altitude(m)":1,"Accuracy":65},{"Date":"2017-12-03T16:05:50+01:00","Latitude":57.01049,"
Longitude":10.03452,"Type":"GPS","Speed(mph)":null,"Speed(km/h)":null,"Altitude(ft)":16,"Altitude(m)":5,"
Accuracy":67},{"Date":"2017-12-03T16:15:17+01:00","Latitude":57.01063,"Longitude":10.03377,"Type":"GPS","Speed
(mph)":null,"Speed(km/h)":null,"Altitude(ft)":19,"Altitude(m)":6,"Accuracy":65},{"Date":"2017-12-
...
...
08T18:20:06+01:00","Latitude":57.01431,"Longitude":10.03389,"Type":"GPS","Speed(mph)":38,"Speed(km/h)":61,"
Altitude(ft)":36,"Altitude(m)":11,"Accuracy":10},{"Date":"2017-12-08T18:21:58+01:00","Latitude":57.01034,"
Longitude":10.03387,"Type":"GPS","Speed(mph)":4,"Speed(km/h)":6,"Altitude(ft)":29,"Altitude(m)":9,"Accuracy":
5}]}
```

Current location for a device

Current gives a json like

```
{"Data":[{"DeviceName":"Normann P.'s iPhone","DeviceID":"11787783","Date":"2017-12-08T18:21:58+01:00","
Latitude":57.01034,"Longitude":10.03387,"Type":"GPS","Speed(mph)":4,"Speed(km/h)":6,"Altitude(ft)":29,"Altitude
(m)":9,"Accuracy":5}]}
```

In splunk, its a bit complicated to split multivalue json into events, and since this is a POC and I dont really care that much for history, I will go for the current location...

✓ Use the website http://json.parser.online.fr/ to text and exanime Your json

Getting data in

To get data in splunk, several approaches can be made - and typically I would choose a on-disk script to pull data from the API to a file to be parsed (via cron), but this time I wanted to play with getting the json in splunk the simplest way, so I installed the REST API Modular Input Add On, even thought its pretty old. The Add On adds an input possibility:
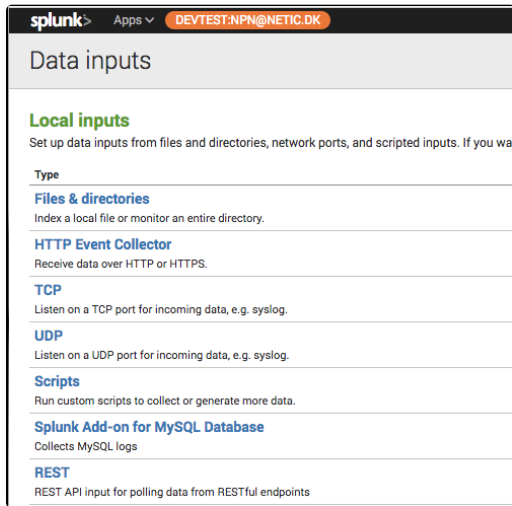
So, after adding a new index for the data, and getting the API Key from the followmee.com website, we add an input for the REST Url

```
http://followmee.com/api/tracks.aspx?
key=***************************&username=moseisleydk&output=json&function=currentfordevice&deviceid=11787783
```
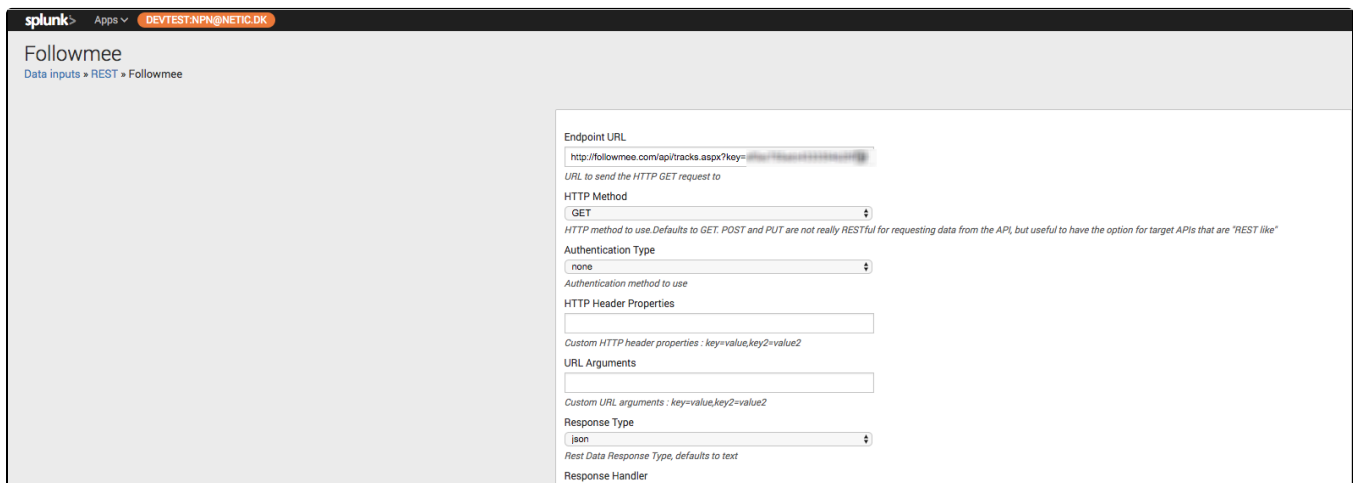

And sourcetype and index:

Notice the polling interval:

I leave it blank, so the REST Url will be called every 60 secs. Also refer to "**Tracking Power"** above.

Presenting the data

Looking at possible visualisations, I first went for the map/geostats visualisation, but the density and zoomlevel is more world event like than street/block level needed, so I installed the Location Tracker - Custom Visualization.

And created the needed search:

```
index="followmee" | dedup _time | eval User="Normann" | table _time "Data{}.Latitude" "Data{}.Longitude" User
```

> ⊘ As follow me reports a lot of the same data on the API when the phone is not moving by reporting <u>same time as last for same location</u>, the "dedup" command removes these. The current search is not time important, only location specific. For Time importance, I would problably make another Dashboard

after looking at what the REST Add On fetches from the followmee.com API:

And then build a Dashboard:

Compared to followmee.com:

Map marker list (top map):

- 2017-12-07 07:15:58 AM
- 2017-12-07 07:17:37 AM
- 2017-12-07 07:19:05 AM
- 2017-12-07 07:20:40 AM
- 2017-12-07 07:22:13 AM
- 2017-12-07 07:23:42 AM
- 2017-12-07 07:25:47 AM
- 2017-12-07 07:27:42 AM
- 2017-12-07 07:29:10 AM
- 2017-12-07 07:30:41 AM
- 2017-12-07 07:32:10 AM
- 2017-12-07 07:34:23 AM
- 2017-12-07 07:35:51 AM
- 2017-12-07 07:37:23 AM
- 2017-12-07 07:39:03 AM
- 2017-12-07 07:40:36 AM
- 2017-12-07 07:42:31 AM
- 2017-12-07 07:45:09 AM
- 2017-12-07 07:46:40 AM
- 2017-12-07 07:48:08 AM
- 2017-12-07 07:49:37 AM
- 2017-12-07 07:51:05 AM
- 2017-12-07 07:52:34 AM
- 2017-12-07 07:54:03 AM
- 2017-12-07 07:55:32 AM

Map marker list (bottom map):

- 2017-12-06 05:50:48 PM
- 2017-12-07 07:15:58 AM
- 2017-12-07 07:17:37 AM
- 2017-12-07 07:19:05 AM
- 2017-12-07 07:20:40 AM
- 2017-12-07 07:22:13 AM
- 2017-12-07 07:23:42 AM
- 2017-12-07 07:25:47 AM
- 2017-12-07 07:27:42 AM
- 2017-12-07 07:29:10 AM
- 2017-12-07 07:30:41 AM
- 2017-12-07 07:32:10 AM
- 2017-12-07 07:34:23 AM
- 2017-12-07 07:35:51 AM
- 2017-12-07 07:37:23 AM
- 2017-12-07 07:39:03 AM
- 2017-12-07 07:40:36 AM
- 2017-12-07 07:42:31 AM
- 2017-12-07 07:45:09 AM
- 2017-12-07 07:46:40 AM
- 2017-12-07 07:48:08 AM
- 2017-12-07 07:49:37 AM
- 2017-12-07 07:51:05 AM
- 2017-12-07 07:52:34 AM
- 2017-12-07 07:54:03 AM
- 2017-12-07 07:55:32 AM
- 2017-12-07 07:57:01 AM
- 2017-12-07 07:58:30 AM