Location Tracking in Splunk

(i)

Remember 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

O 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,"Speed(km/h)":null,"Altitude(ft)":16,"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,"Altitude(ft)":10,"Attitude(ft)":10,"Attitude(ft)":10,"Attitude(ft)":10,"Attitude(ft)":10,"Attitude(ft)":10,"Speed(km/h)":null,"Speed(km/h)":null,"Altitude(ft)":10,"Speed(km/h)":null,"Speed(km/h)":null,"Attitude(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,"Speed(km/h)":null,"Speed(km/h)":null,"Speed(km/h)":null,"Speed(km/h)":null,"Speed(km/h)":null,"Speed(km/h)":null,"Speed(km/h)":null,"Speed(km/h)":null,"Speed(km/h)":null,"Speed(km/h)":null,"Speed(km/h)":null,"Speed(km/h)":10,03377,"Type":"GPS","Speed(mph)":null,"Speed(km/h)":null,"Speed(km/h)":null,"Speed(km/h)":61,"
08T18:20:06+01:00","Latitude":57.01431,"Longitude":10.03389,"Type":"GPS","Speed(mph)":38,"Speed(km/h)":61,"
08T18:20:06+01:00","Latitude":57.01431,"Longitude":10.03389,"Type":"GPS","Speed(mph)":38,"Speed(km/h)":61,"
08T18:20:06+01:00","Latitude(ft)":11,"Dagameerum:10,"[Speed(km/h)":61,"]
08T18:20:06
```

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

 \odot

```
{"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 <u>the simplest way</u>, so I installed the REST API Modular Input Add On, even thought its pretty old. The Add On adds an input possibility:

splunk> Apps V DEVTEST:NPN@NETIC.DK
Data inputs
Local inputs Set up data inputs from files and directories, network ports, and scripted inputs. If you wa Type
Files & directories Index a local file or monitor an entire directory.
HTTP Event Collector Receive data over HTTP or HTTPS.
TCP Listen on a TCP port for incoming data, e.g. syslog.
UDP Listen on a UDP port for incoming data, e.g. syslog.
Scripts Run custom scripts to collect or generate more data.
Splunk Add-on for MySQL Database Collects MySQL logs
REST REST API input for polling data from RESTful endpoints

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

splunk > Apps > (DEVIESTANEN@NETIC.DR) Followmee Data inputs > REST > Followmee Intuit > Followmee Intuit > REST > Followm		
Data inputs > REST > Followmee Endpoint URL http://followmee.com/api/tracks.asps?key= URL to send the HTTP GET request to HTTP Method GET 0	splunk'> Apps v DEVTEST:NPN@NETIC.DK	
http://followmee.com/api/tracka.aspx?hey= URL to send the HTTP GET request to HTTP Method GET •		
Authentication Type none Authentication reporties Authentication reporties Custom HTTP header properties URL Arguments Custom URL arguments : key=value,key2=value2 URL Arguments Custom URL arguments : key=value,key2=value2 Response Type jon Rest Data Response Type, defaults to text Response Handler		http://folowmee.com/api/tracka.aspx?hoy URL to send the HTTP GET request to HTTP Method GET • HTTP method to use Defaults to GET. POST and PUT are not really RESTful for requesting data from the API, but useful to have the option for target APIs that are "REST like" Authentication Type • none • Authentication type • Castom UHTP header properties : key-value,key2-value2 • URL Arguments • Castom URL arguments : key-value,key2-value2 • Response Type • Rest Data Response Type, defaults to text •

And sourcetype and index:

Source type Set sourcetype field for all events from this source. Set sourcetype Manual \$	
Source type followmee-json If this field is left blank, the default value of script will be used for the sour	ce type.
☑ More settings	
Host Host field value splunkserver	
Index Set the destination index for this source. Index followmee	ŧ
Cancel	Save

Notice the polling interval:

Polling Interval		
Polling interval in either seconds or	a CRON time format , defaults to 60 seco	nds.

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

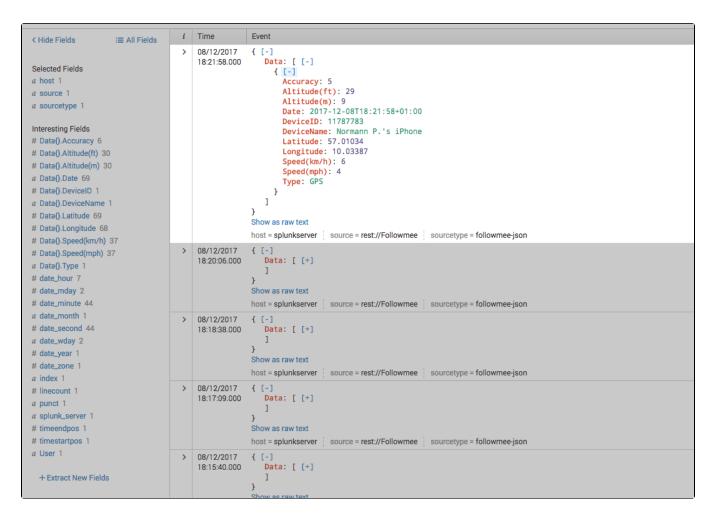
Presenting the data

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 same time as last for same location, the \oslash "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:

ik's App Mos-Eisley Monitoring OEVIESTANAGANETICOX Datasets Reports Alerts Dashboards		Administrator v Messages v Settings v Activity v Help	Mos-Eisley Monitor
ow Mee Location Tracking			Edit Export ~
7 days V Hide Filters			
	Data from Followmee		
Aalborg	_time 0	Data{}.Latitude Data{}.Longitude	0 User 0
	2017-12-08 18:21:58	57.01034 10.033	87 Normann
	2017-12-08 18:20:06	57.01431 10.033	89 Normann
	2017-12-08 18:18:38	57.02047 10.007	66 Normann
	2017-12-08 18:17:09	57.01941 9.981	46 Normann
	2017-12-08 18:15:40	57.02004 9.958	35 Normann
	2017-12-08 18:13:45	57.02401 9.943	23 Normann
	2017-12-08 18:12:16		29 Normann
	2017-12-08 18:10:48	57.02287 9.906	95 Normann
	2017-12-08 18:09:19	57.03321 9.908	44 Normann
	2017-12-08 18:07:45	57.03372 9.904	91 Normann
	2017-12-08 18:06:17	57.02642 9.902	72 Normann
	2017-12-08 18:04:49	57.03129 9.904	11 Normann
Auto Division	2017-12-08 18:03:22		72 Normann
	2017-12-08 18:01:50		10 Normann
	2017-12-08 18:00:21		93 Normann
	2017-12-08 17:58:52		00 Normann
	2017-12-08 17:57:24		56 Normann
Hidsandse	2017-12-08 17:55:55		20 Normann
	2017-12-08 17:54:29		43 Normann
	2017-12-08 17:53:01		05 Normann
	2017 10 08 17 51 02		79 Normann
Q ± 1 O a few second	streetMap		64 Normann
A T I O BIENSEON	2017-12-08 17:48:37		53 Normann
	2017-12-08 17:47:07		35 Normann
	2017-12-08 17:45:39		35 Normann 31 Normann
	2017-12-08 17:44:10		90 Normann
	2017-12-08 16:38:34		75 Normann
	2017-12-08 16:38:34		12 Normann
	2017-12-08 16:29:24		59 Normann
	2017-12-08 16:23:16		18 Normann
	2017-12-08 16:27:48		30 Normann
	2017-12-08 16:13:15		17 Normann
	2017-12-08 16:13:15 2017-12-08 16:11:16		73 Normann
	2017-12-08 16:09:20		44 Normann
	2017-12-08 16:06:34		44 Normann 39 Normann
	2017-12-08 16:05:05		63 Normann
	2017-12-08 16:02:47		60 Normann
	2017-12-08 16:02-47		60 Normann

Compared to followmee.com:

