Tracking Airplanes and Utilities

Kyle Smith | Integration Developer

October 2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf18

Me

- Integration Developer with Aplura, LLC
- Working with Splunk for ~9 years
- Written many Public Splunk Apps (on splunkbase.splunk.com)
- Current Member of the SplunkTrust
- Wrote the “Splunk Developer’s Guide” - introduction to Splunk App Development
- Active on #splunk on IRC, answers.splunk.com, and Slack
- Co-leader of Baltimore Usergroup
  - My Handle is “alacercogitatus” or just “alacer”

Splunk

- Admin
- User
- Architect
- Evangelist
- Sales Engineer
- Anybody

You

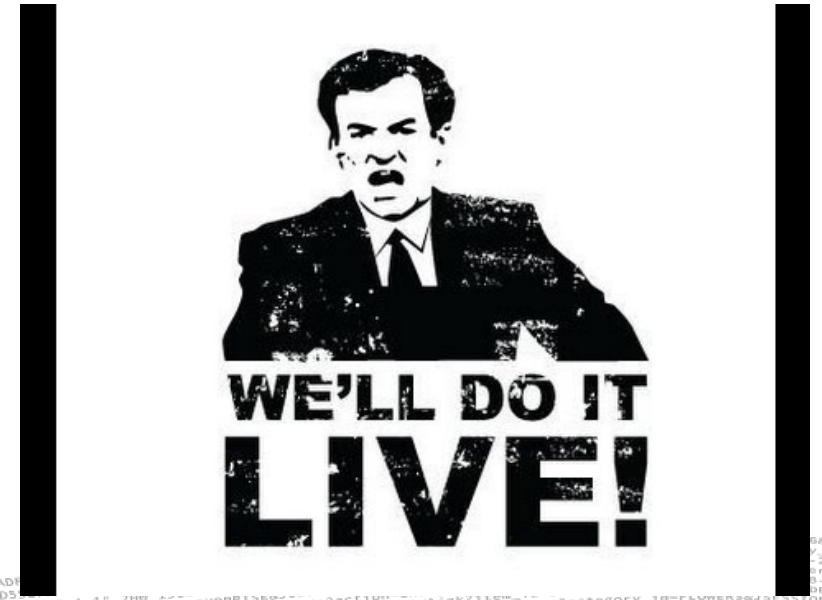
- Want to learn about different ways Splunk can take “non-traditional data”
- Enjoy snarky dry humor, and/or Pina Coladas
- Beginner knowledge of “What is Splunk”

Goals

- High level overview of Radio Frequency
- Show examples of how to integrate with SDR
- DEMO LIVE
- Take actionable items back to your business to “try new things”

Agenda

- What is RTLSDR and Radio Frequency?
- How I got the data
- Trending Analysis and Dashboards
- Demo



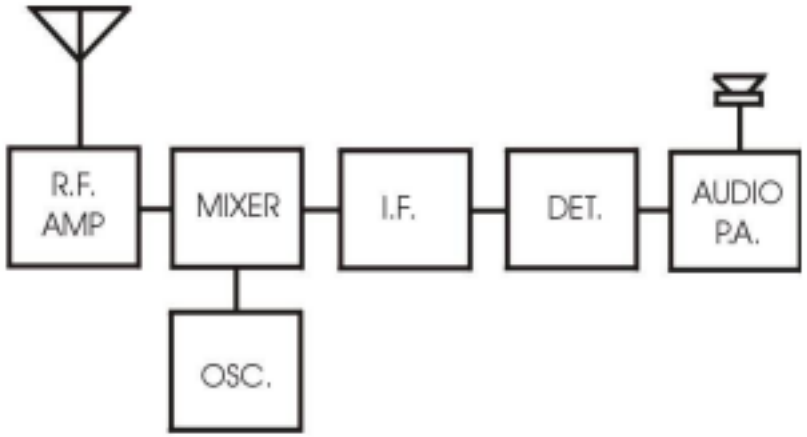
What is SDR?

Two antennas met on a roof, fell in love, and got married.

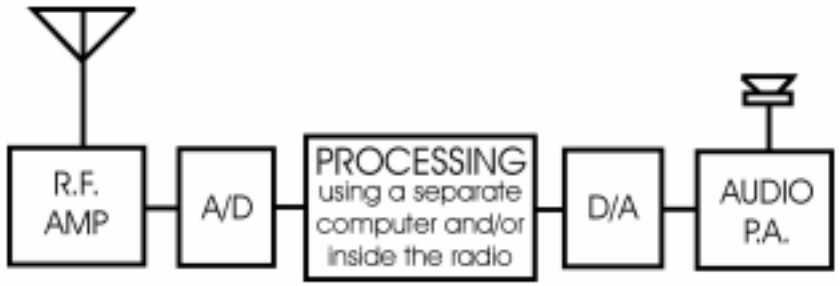
The ceremony wasn't much, but the reception was excellent.

SDR 101

Radio Frequency and you



Old Fashioned Superheterodyne Radio



Newfangled SDR (Software Defined Radio)

- SDR
  - Software Defined Radio
  - Modern Computing allows digital processing of analogue signals
  - Cheaper and faster than separate hardware components

http://www.noars.net/miscfiles/SDR101-7.pdf

SDR Ethics

Do not use this for malicious purposes.

I am not and will not be responsible for your actions.

http://www.noars.net/miscfiles/SDR101-7.pdf

RTL SDR

- Based on RTL2832U chipsets
  - Mass produced TV tuner dongles.
  - Antti Palosaari, Eric Fry and Osmocom (in particular Steve M)
    - Wrote custom drivers to implement SDR capabilities
- Cheap
  - RX only models can $20
  - RX/TX models can be $300
- Limited Frequencies
  - Generally in the 25-1700MHz Range

https://www.rtl-sdr.com/about-rtl-sdr/

What can you do with SDR?

- Use as a police radio scanner.
- Listening to EMS/Ambulance/Fire communications.
- Listening to aircraft traffic control conversations.
- Tracking aircraft positions like a radar with ADSB decoding.
- Decoding aircraft ACARS short messages.
- Use rtl-sdr as a high quality entropy source for random number generation.
- Decoding unencrypted digital voice transmissions such as P25/DMR/D-STAR. Decoding POCSAG/FLEX pager traffic.
- Scanning for cordless phones and baby monitors.
- Tracking and receiving meteorological agency launched weather balloon data.
- Tracking your own self launched high altitude balloon for payload recovery.
- Receiving wireless temperature sensors and wireless power meter sensors.
- ……..AND MORE

How I got the Data

RTL SDR

Thanks to the good folks at osmocom.org

- RTL TCP
  - Required to collect Smart Meter data packets
  - Means of controlling and sampling rtl-sdr dongles

- http://osmocom.org/projects/sdr/wiki/rtl-sdr
  - Download via git
  - Build the package
  - Install the package

- Gives you “rtl_tcp” to run
  - Enables a TCP listener for other programs to interact with the SDR dongle

RTL AMR - Utilities

- https://github.com/bemasher/rtlamr
- Requires “go” language
  - Brew install go
- go get github.com/bemasher/rtlamr
  - /Users/<user>/go/bin/rtlamr
- Interacts with ERT Smart Meters
  - Only specific models are supported
  - Not all meters will broadcast

RTL AMR - Utilities

Message Types

- **scm**: Standard Consumption Message. Simple packet that reports total consumption.
- **scm+**: Similar to SCM, allows greater precision and longer meter ID's.
- **idm**: Interval Data Message. Provides differential consumption data for previous 47 intervals at 5 minutes per interval.
- **netidm**: Similar to IDM, except net meters (type 8) have different internal packet structure, number of intervals and precision. Also reports total power production.
- **r900**: Message type used by Neptune R900 transmitters, provides total consumption and leak flags.
- **r900bcd**: Some Neptune R900 meters report consumption as a binary-coded digits.

Running At Home

- **~/go/bin/rtlamr -duration=2m55s -unique=true -filterid=1481111148 -single=true -format=json -msgtype=r900 >> /data/rtl_sdr/utilities/water_meter.log**
  - {"Time":"2018-05-30T09:06:24.168277013-04:00","Offset":0, "Length":0, "Message": **{"ID":1481111148,"Unkn1":161,"NoUse":0,"BackFlow":0, "Consumption":223312,"Unkn3":0,"Leak":15,"LeakNow":3}** }

- **~/go/bin/rtlamr -duration=2m55s -unique=true -filterid=41282045 -single=true -format=json -msgtype=scm >> /data/rtl_sdr/utilities/gas_meter.log**
  - {"Time":"2018-05-30T09:06:40.665886255-04:00", "Offset":0, "Length":0, "Message": **{"ID":41282045,"Type":12,"TamperPhy":3,"TamperEnc":0, "Consumption":238942,"ChecksumVal":26547}** }

splunk> .conf18

Running At Home - HEC

- **Using bash tricks, push into a metrics store via HEC**

- JSONP=$(tail -1 /data/rtl_sdr/utilities/gas_meter.log | awk -F'[",:]' '{print "{\"time\":"systime()",\"event\":\"metric\",\"source\":\"rtlsdr\",\"host\":\"utilities\",\"fields\": {\"metric_name\":\"consumption\",\"_value\":\""$40"\", \"utility_type\":\"natural_gas\", \"meter_id\":\""$24"\" } }"}')
- curl http://localhost:8088/services/collector -H "Authorization: Splunk <auth_token>" -d "$JSONP”

- The actual JSON looks then like:

```
{ "time": "1234567890", "event": "metric", "source": "rtlsdr", "host": "utilities", "fields":
{"metric_name": "consumption", "_value": "494300", "utility_type": "natural_gas", "meter_id": "19238343" } }
```

splunk> .conf18

Running At Home

- [monitor:///data/utilities/gas_meter.log]
- disabled = false
- index = iot
- sourcetype = rtl_sdr:utilities:gas

- [monitor:///data/utilities/water_meter.log]
- disabled = false
- index = iot
- sourcetype = rtl_sdr:utilities:water

splunk> .conf18

dump1090 - Airplanes

- https://github.com/mutability/dump1090
  - There are many dump1090 forks
  - This one has a “write json” feature
- Build
  - Debian based, but can work on OS X
- Running
  - Dump1090
  - Supports write json files, as well as interactive web server

dump1090

- `./dump1090 --write-json ./data --max-range 1000`
  - Writes a JSON file with updated data
  - Consumed via monitor stanza, essentially re-consuming entire file every time

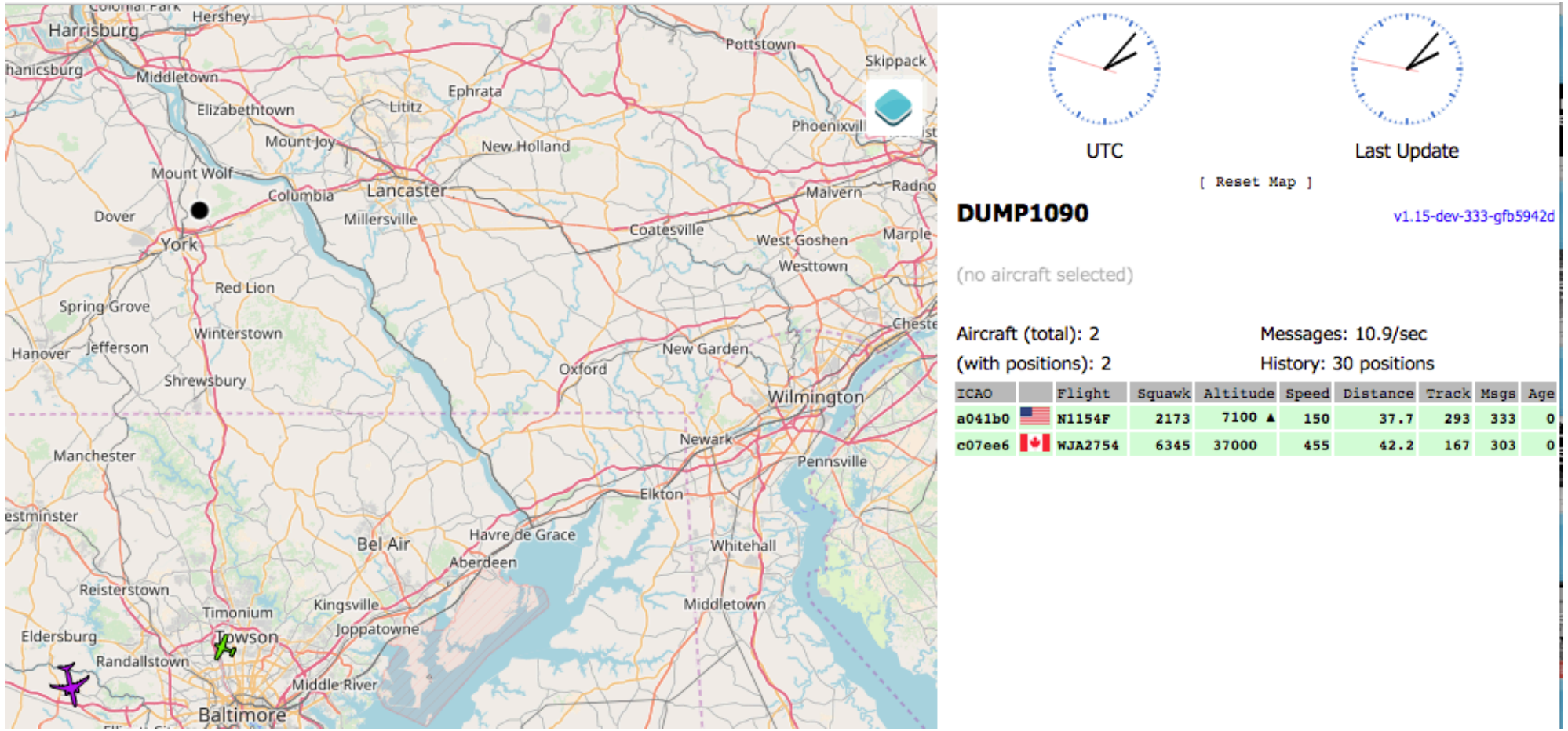
- { "now" : 1527686991.8, "messages" : 6848, "aircraft" : [
{"hex":"acc1ef","squawk":"6257","lat":39.320161,"lon":-76.602356,"nucp":7,"seen_pos":58.8,"altitude":7300,"vert_rate":2368,"track":258,"speed":281,"mlat":[],"tisb":[],"messages":41,"seen":25.5,"rssi":-18.1},
{"hex":"abba6b","mlat":[],"tisb":[],"messages":977,"seen":241.5,"rssi":-21.7},
{"hex":"a32e86","mlat":[],"tisb":[],"messages":1559,"seen":70.7,"rssi":-20.6}]}

splunk> .conf18

dump1090

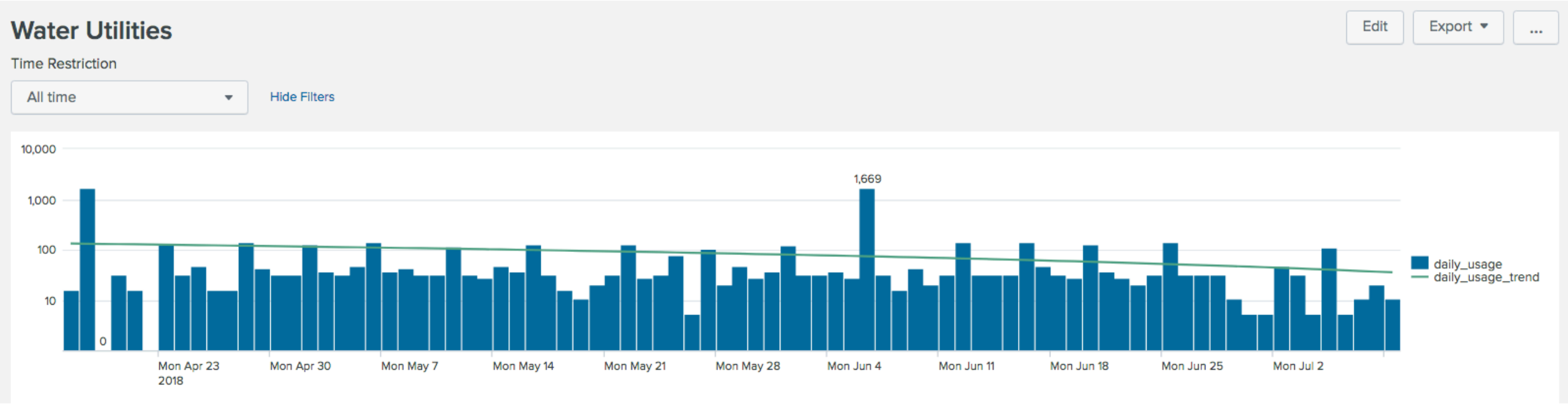
Built in webserver

- python -m SimpleHTTPServer 8090



Splunk Dashboards

Water Utility



- Trendline calculated on the fly
- Shows daily usage verses the trend over the data.

splunk> .conf18

Natural Gas Overview

Natural Gas Utilities

Edit | Export | ...

Time Restriction

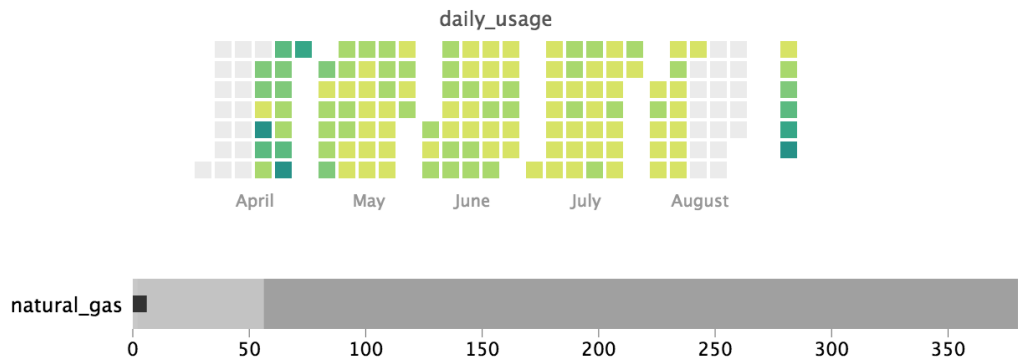
All time | Hide Filters

Meter ID

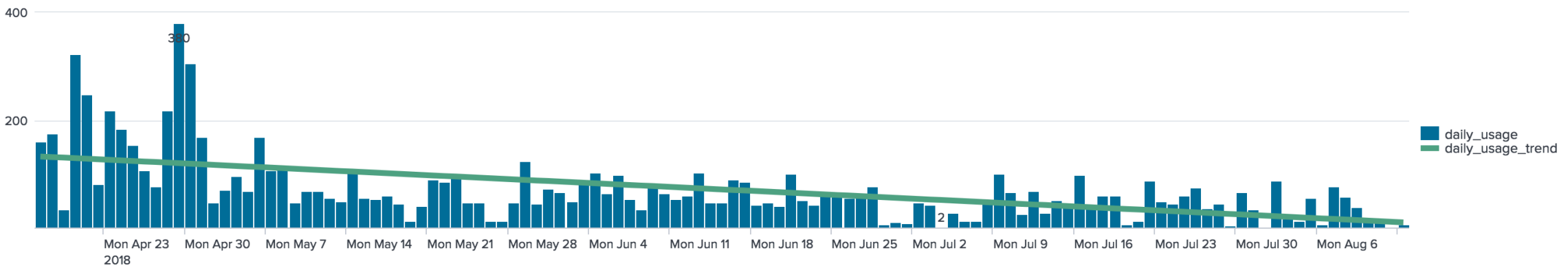
41282045

30m ago

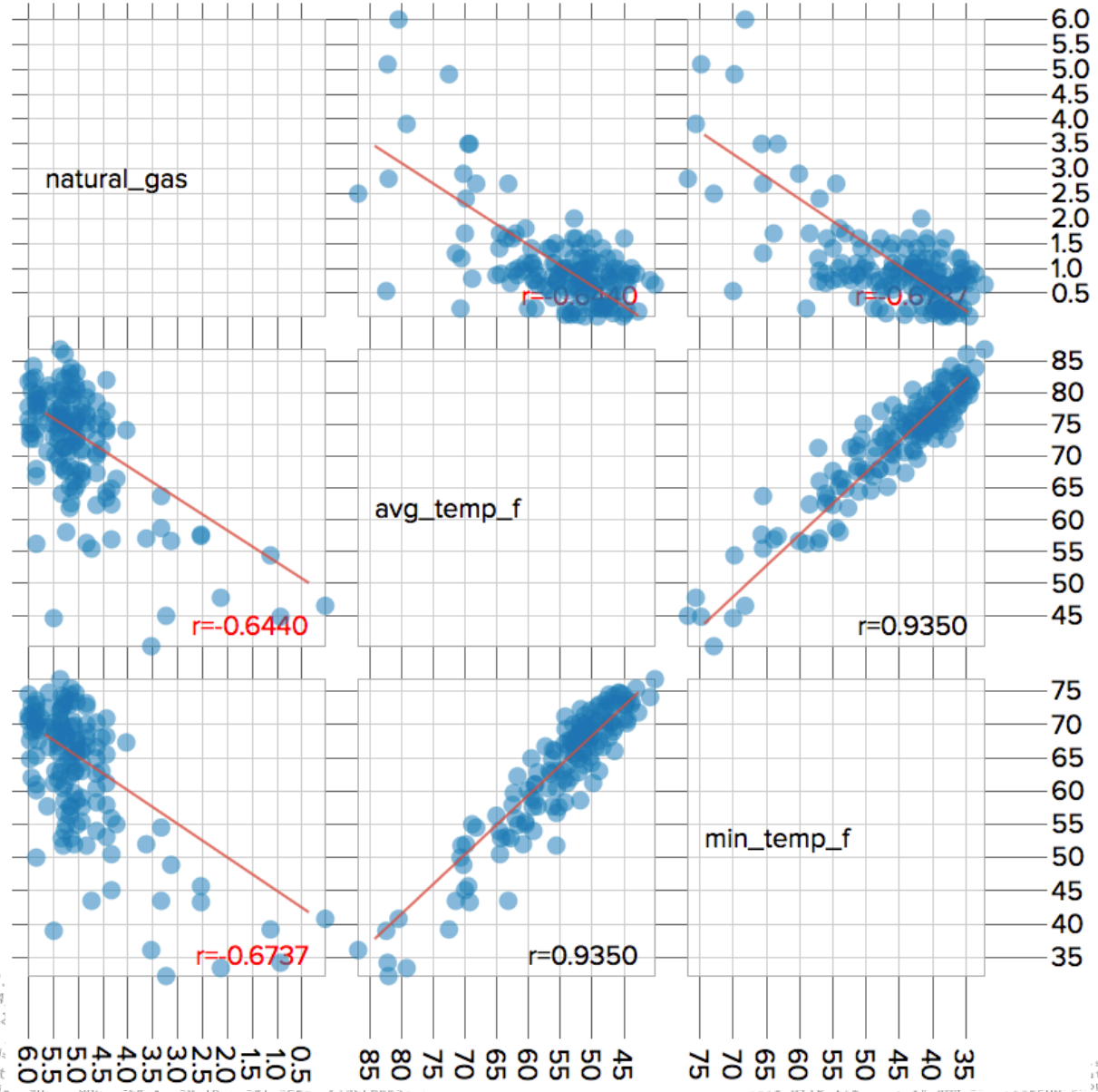
Avg Usage over Days



Daily Usage with Trend over Time Period



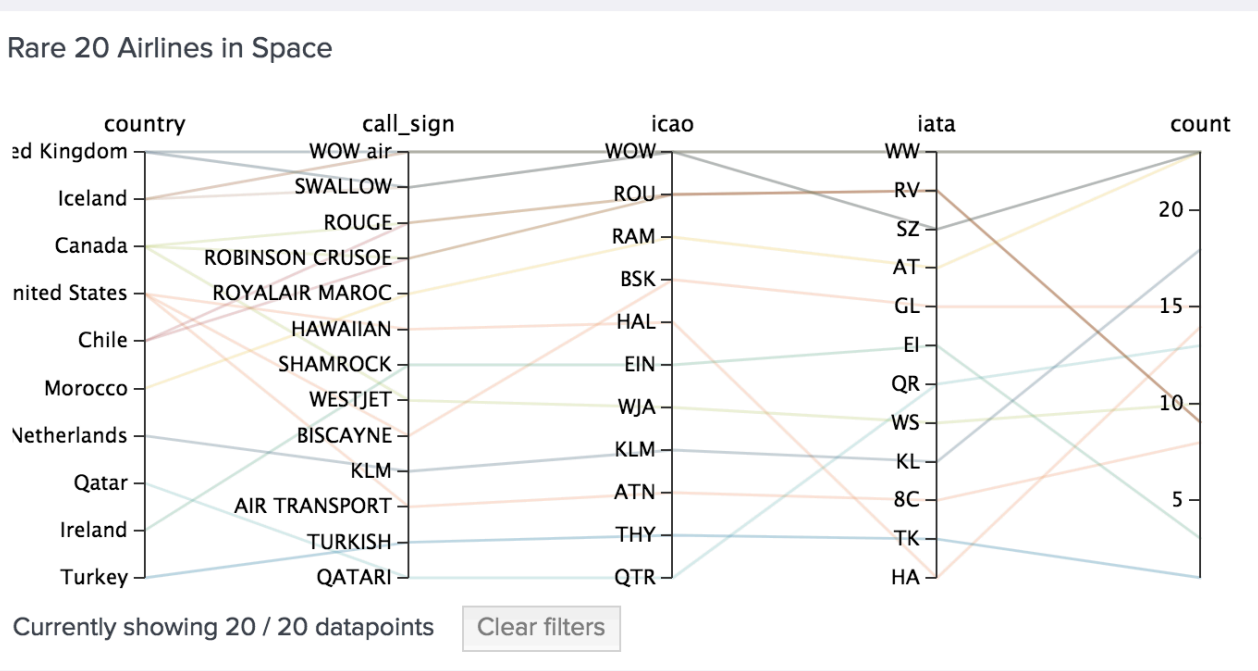
Scatterplot Matrix of Natural Gas Information



Compares usage and average temp
Time-restricted for the data, but visualization not time-bound
Each data point is a different day
R=1.000 indicates direct relationship,
R=0.000 indicates no relationship

More usage, when it's colder.

Top and Rare Airlines

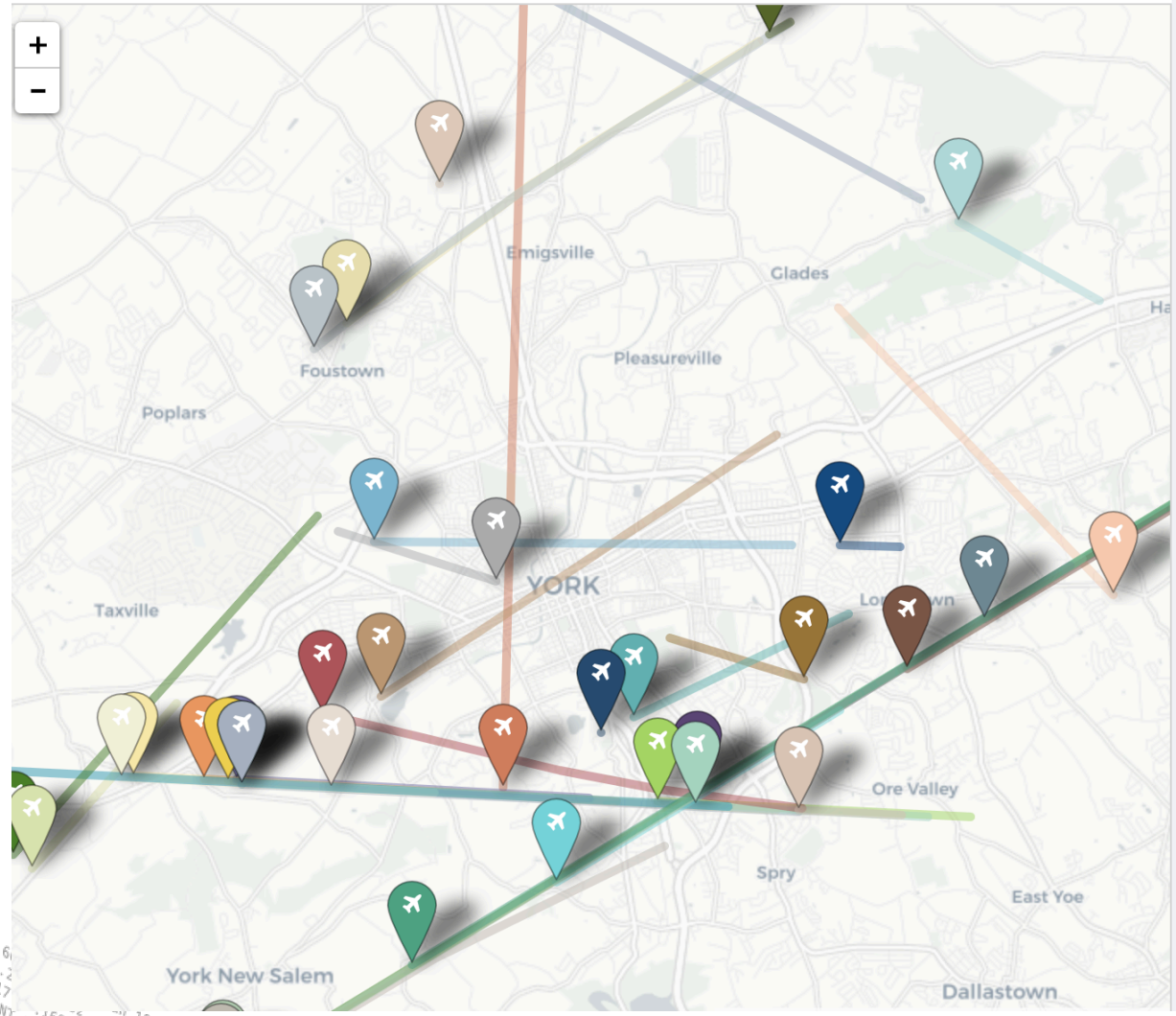


- Uses the Parallel Coordinates visualization
- Sample taken over 7 days

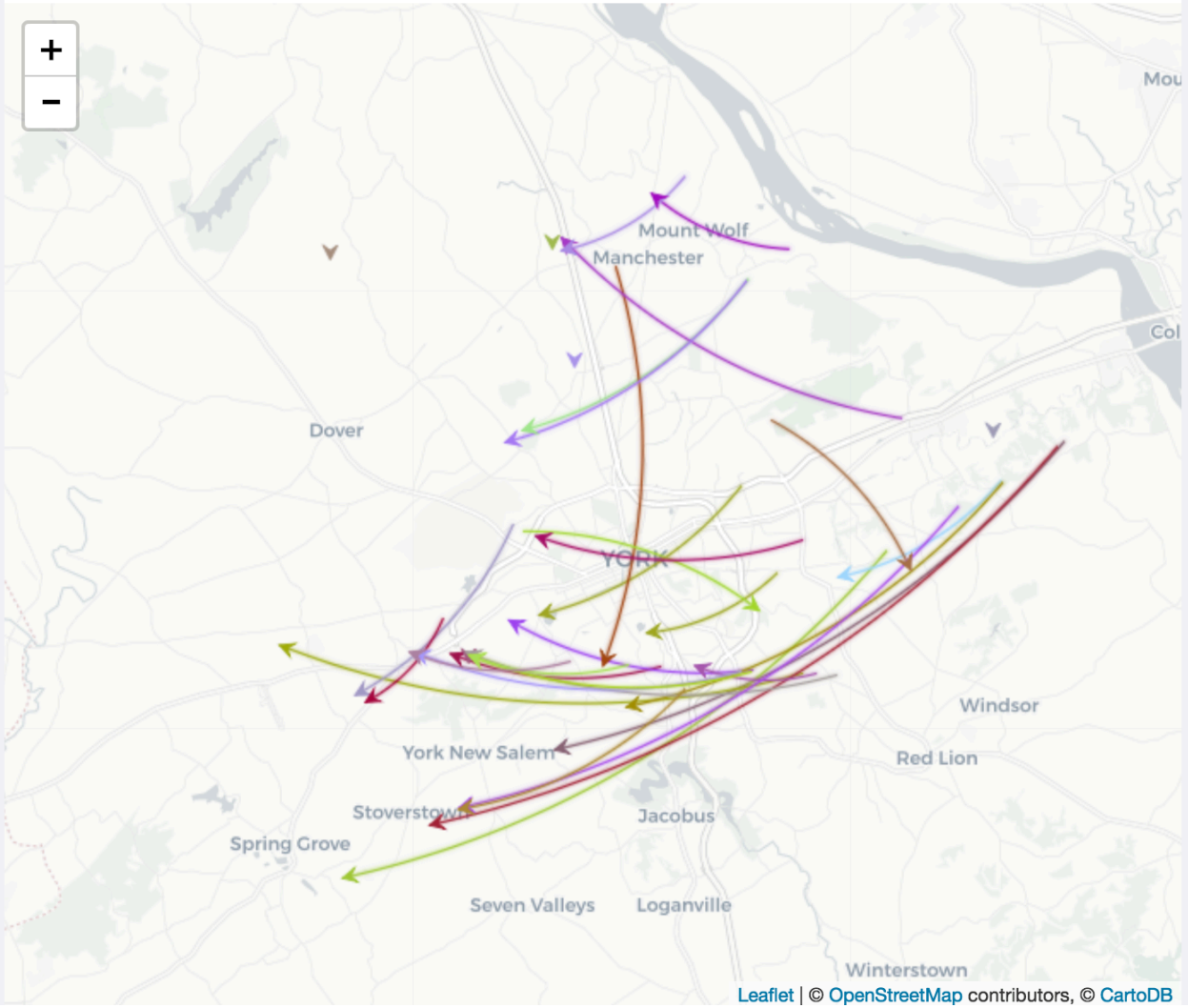
splunk> .conf18

Aircraft Positions

Current Aircraft positions - last 4 hours



Directional Map Positions - Last 4 hours



splunk> .conf18

DEMO!

More Information

Why does SDR Matter?

- https://www.rtl-sdr.com/tutorial-replay-attacks-with-an-rtl-sdr-raspberry-pi-and-rpitx/
  - Open car doors with HackRF.
  - Open a garage door
- http://www.keplercommunications.com/blog/item/all-about-software-defined-radios
  - Enable much faster communications with satellites
  - Could be up to 500Mbps
- https://www.crisis-response.com/comment/blogpost.php?post=181
  - Could bridge communication gaps between crisis centers during times of humanitarian needs

Where to next?

- FN1470 – The Way to Build the Largest Splunk User Group and Engage Splunk Fans
  - Yutaka Yamada, et al. Today, 1:00pm
- DEV2043 – Exciting, To Be Announced Developer Session
  - Manu Jose, et al. Today, 1:30pm
- FN1784 – Master Joining Datasets Without Using Join: How to Build Amazing Reports Across Multiple Datasets Without Sacrificing Performance
  - Nick Mealy, Today, 1:30pm

Resources and Questions

- IRC #splunk on efnet.org (look for alacer)
- docs.splunk.com
- answers.splunk.com (I'm alacercogitatus)
- wiki.splunk.com
- Slack! Join a User Group! (https://splk.it/slack)
- The Splunk Trust - We are here to help! (find us by our fez!)
- forums.splunk.community

Thank You

Don't forget to rate this session in the .conf18 mobile app

And JOIN the Community!

splunk>