



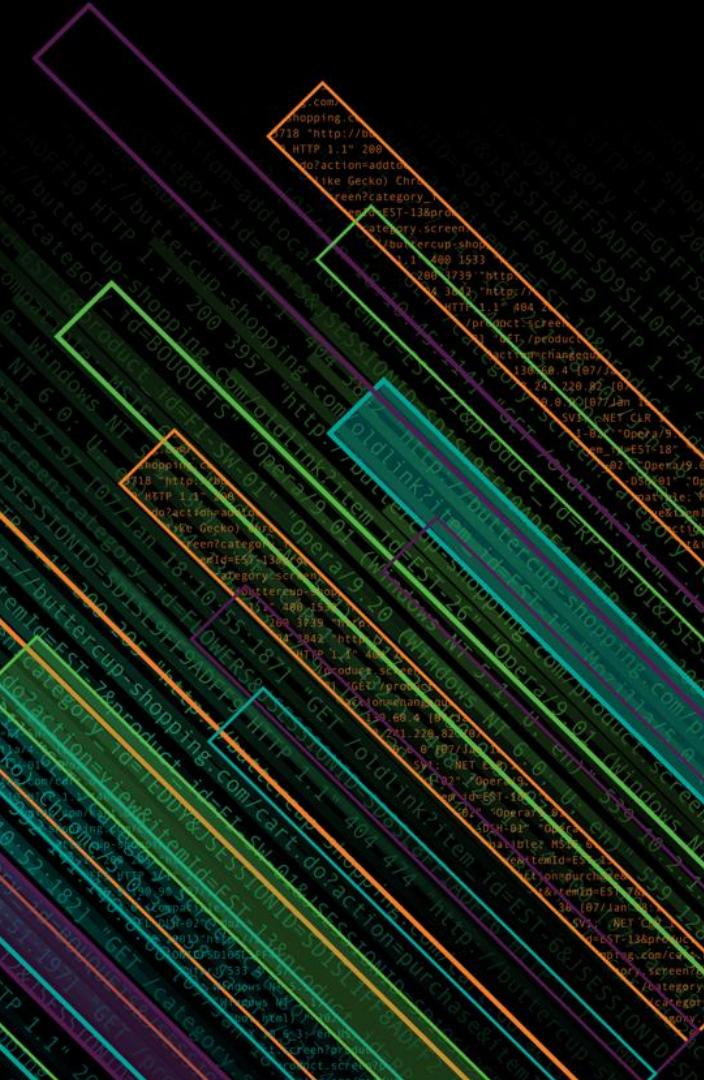
splunk>

Using Splunk to gain insights into airline safety data

FN1252

Cory Syvenky | Sr. Cloud Analyst, WestJet

September 2018 | Version 1.0



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, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.

CORY SYVENKY

Senior Cloud Analyst, WestJet



Who is the speaker?

@spsavvy



- ▶ I'm a Splunk Certified Power User; this is my 3rd .conf.
- ▶ I'm an aspiring Data Scientist.
- ▶ I'm a Licenced Private Pilot.
- ▶ I work in the IT department for a major Canadian airline.
- ▶ We use Splunk for Operational Intelligence.



What is going to be covered?

Safety Data from Transport Canada and the NTSB

- ▶ Insights from plain text.
- ▶ Heatmap by Date.
- ▶ Clustered occurrences by Region.
- ▶ Review the Canadian and American dashboards.
- ▶ Minimal conf needed to process XML.
- ▶ Use of OneDrive for data file storage.

Data captured over-the-air via Raspberry Pi based receiver.

- ▶ Accessing data from IoT hardware.
- ▶ Do commercial aircraft speed?
 - By altitude and proximity to airport.
- ▶ Using GPSBabel and Google Maps for 3D visualization.
- ▶ Stratus app demo of Orlando Airport.

Why do this?

- ▶ Curiosity. Curiosity about flight safety. Curiosity about the challenge.
- ▶ Being able to combine two interests (Aviation, Data Visualizations).
- ▶ An interest in expanding my ability to gain insights from data.
- ▶ Splunk makes it easy.



Incident and accident data from Transport Canada and the NTSB



About these Open Data Sources

- ▶ Transport Canada (TC): Freely available data that I have been processing in my local Splunk environment since January '17.
- ▶ National Transportation Safety Board (NTSB): I have only recently uncovered this data set.
- ▶ Data Ingestion, being a good data steward:
 - receive daily summary email from TC.
 - automating the migration of XML data to Splunk index.

138.60.4 ~ [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F2-SW-09" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.102 ~ [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 332 "http://buttercup-shopping.com/cart.do?action=plus&size=&itemId=EST-26&product_id=F2-SW-09" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.102 ~ [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9F1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=F2-SW-09" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.102 ~ [07/Jan 18:10:56:156] "GET /oldlink?item_id=SURPRISE&JSESSIONID=SD10SLBFF2ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=F2-SW-09" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.102 ~ [07/Jan 18:10:55:187] "GET /oldlink?item_id=EST-6&JSESSIONID=SD10SLBFF2ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&product_id=F2-SW-09" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.102 ~ [07/Jan 18:10:55:187] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-6&product_id=F2-SW-09" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.102

Visualizing Aviation Data

Assistance from Splunkbase add-ons makes this work easy

- ▶ Wordcloud Visualization for narrative

<https://splunkbase.splunk.com/app/3212>

- ▶ Calendar Heat Map Visualization for days with highest incidents

<https://splunkbase.splunk.com/app/3162>

- ▶ Cluster Map for occurrences by region [built-in].

- ▶ Dashboards for easy consumption.

Wordcloud app for narrative field

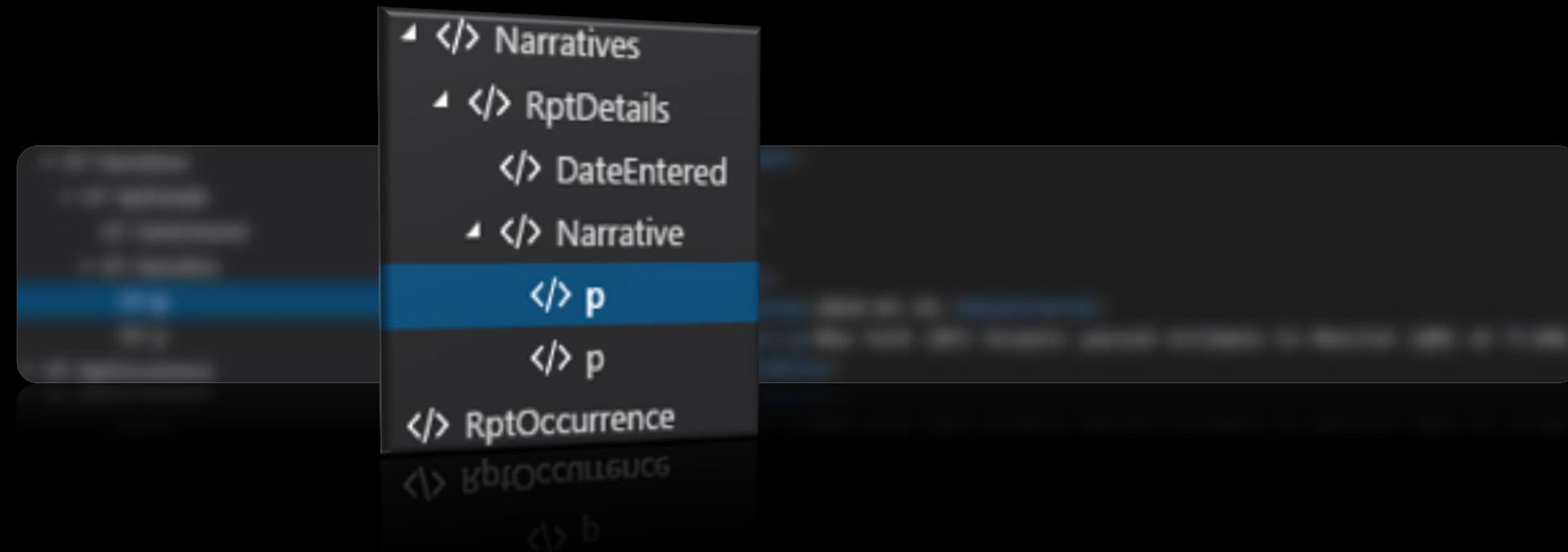
- ▶ The approach phase of flight is the most frequent cause of presence in reports (3.5 times more than the next highest cause, which is take-off).
- ▶ The narrative is in textual paragraph form from the TC investigators.
- ▶ The question:
What words show up most frequently in these reports?
- ▶ The word-cloud represents, in relative size, the frequency of words used as they pertain to the approach phase of flight.

“A Cessna 172K (C-GTXA) on a flight from Nanaimo, BC (CYCD) and landing at Nanaimo, BC (CYCD) was on final for Runway 34. A Jazz de Havilland DHC-8-301 (C-GETA/JZA8271) on a flight from Vancouver Int'l, BC (CYVR) to Nanaimo, BC (CYCD) was number 2 on final and did a go around due to the slower aircraft ahead.”

Source: Transport Canada CADORS

Visual Studio Code

see the structure of the data



KBVS Westjet could vers made Control there 12-30 police WJA349 REPORT 0300Z A320-211 faulty test contacted management went CYXX 01522 After late service sure 1000 nose pour Fault 737-600 roll Aucun continued London uneventfully reli Traffic both WJA114 Yellowknife SAAB second PIKPA fault Beech clear 560XL Abbotsford stab Inspector CHP against locked 737-8CT checklist flap left FLAP exploited Separation caution Cessna SNOW seal snag miles 0335Z K9W While held between KDC413 Pilot fact WJA2215 1955 approximately where equipment never site instructions turbulence York/ l'exploitation ground WJA182 sans passengers National Halifax Incident operator remonté finale TCAS read Edmonton Boeing Runway 737-700 traffic Winnipeg cyyy normal since Terraflaps pont assurred Civil Montré 737-700 traffic Winnipeg cyyy normal since Jamaica roof terrace flap

Ottawa collision ARFF Aprè 23522 avoir Prairie gate medical 17162 operations Havilland Encore deux Fire miles appear Fall r'ea further they DHC-8-400 however Stat priority CYDF half tire Hamilton right back around advised missed Calgary aircraft approach impact 1820 737-7CT minutes Card been Canada control 8975 Report BITE issue wind 2247Z KBUF plan CYZF KLAX bird Fort down when area able board 3228 issued raison drive stop overshoot fuel replaced laid DHC-8-402 landing landed CYYC knots feet sensor Flair Zone 01022 panel Operations Reference departing speed C103 Once turn observed taxi Flap CASI Lake qu'a system 700' 10NW piste rear found their C-GMKG before cyot CAT4 passenger strike conducted looked conducting fast During Unit CYEG light still Vancouver CYYZ City 10NW position while given appropriate high conduct Maintenance cleared occurrence Int'l UPDATE CYVR emergency CYHZ North event There indicator KLGK pieds performed 300A When Universal d'un side loud KFL crew final operational initiated Jazz short passed wake

Grande horizontal maintenance 330° Aviation RNAV reported being first CYUL gear green safety indication received alert Elliott Captain band JZA8368 elected illuminated Quick Tower required 737-800 faiit Toronto/Lester new declared land instructed meet Piper CYLW vertical Canadian KPBI damaged controller hand told CYHM separation arrival sous CYXU laser crossed returned time Taxeway Victoria Airlines CYQB prior MISE STAR 172H CYXE would vehicles pilot cross which overshot Embraer main fluid Airworthiness crew move visual near hydraulic CYXS weather Police 3000' vehicles upon C-GETX deleted reduced Ottawa/MacDonald-Cartier Aircraft call root four CYWG advisory 172M shear alternate came level selected valve Dispatch removal trop TR245 Truck 172S WJA441 noticed during N843MG Minot KMOT George following another hold another 90-around effectuant Lester selected Alors noted planned Sint vicinity pile WJA426 applicable WJA552 inuit cargojet CYXT C-GWWS changed gusts minimum PC0147 TNCM WJA2507 Journey WJA520 WJA845 accordance 0055Z Emergency PA-31-350

Cancun 0900Z manual 10122 11000 east destination Int'l Duplicate CYMM Upon Slow through done clearance avoidance behind Cargojet CYXT C-GWWS poor bulb ambulance message Cana used -reported FSEU message

KBVS Westjet could very
made Control there 12-30 police JA349 REPORT
0300Z A320-211 fault KLAS decided line authorized CYRF return dme Separation caution Cessna SNOW seal snag miles 0335Z
0320Z 01522 After late service sure 1000 nose pour Fault 737-600 roll Aucun continued London uneventfully relu WJA476 WJA637 vitesse appeared
PIKPA fault telex contacted management CYXX 01522 service checklist Cessna SNOW seal snag miles 0335Z
second passengers Beech clear 560XL Abbotsford stab Inspector against locked 737-8CT checklist KWB While held between kdc413 Pilot WJA114 Yellowknife SAAB
sans operator National Halifax CHP flap left FLAP exploited approximately where equipment KWB fact WJA2215 1955
Incident operator remonté finale TCAS Edmonton read flap left FLAP exploited approximately where equipment KWB fact WJA2215 1955
Ottawa collision ARFF Apré 23522 avoir deux Fire miles Separation caution Cessna SNOW seal snag miles 0335Z
Prairie gate medical operations Havilland Encore CYEG separation caution Cessna SNOW seal snag miles 0335Z
right back around advised missed Calgary CYYC separation caution Cessna SNOW seal snag miles 0335Z
tire Hamilton control been Canada control nautical l'6 Report BITE issue wind plan CYZF KLAX Fall bird Toronto
stop overshoot fuel replaced laid DHC-8-402 landing landed CYYC knots after runway Fall bird Toronto
CJ03 Once turn observed taxi Flap CASI Lake qu'a system 700' Pearson
CAT4 passenger strike conducted looked conducting fast During Unit CYEG light still Vancouver CYYZ 10NW
CYTF conduct Maintenance cleared Occurrence CYVR emergency CYHZ North event There indicator CYF without CYOW Crew risk N503DE 1322
high 300A maintenance loud KFL reported being first CYUL gear crew final operational initiated Jazz occurred short passed wake
When Universal d'un side maintained 330° Aviation RNAV declared land instructed meet green safety indication received alert Elliott Captain band JZA8368
Grande horizontal 2125Z Quick Tower required 737-800 faiat Toronto/Lester new seat 1150Z CYLW vertical Canadian KPBI
elected illuminated hand told CYHM which overshot Embraer main separation arrival sous CYXU laser crossed returned time Taxway Victoria Airlines CYQB prior MISE STAR 172H
damaged controller flex CYUH would vehicles pilot cross deleted reduced Ottawa/MacDonald-Cartier fluid Airworthiness crew move visual near hydraulic CYXS weather Police John
3000' Halifax/Stanfield upon C-GETX hold another 90-around 172M shear alternate came level selected valve Dispatch removal trop TR245 Truck 172S WJA441 noticed
during N843MG Minot KMOT George following destination int Duplicate CYMM Upon Slow through done Alors noted planned snt vicinity pile WJA426 applicable WJA552 Inuit
Cancun 0900Z manual 10122 11000 east Cana used -reported FSEU poor bulb ambulance message clearance Cargojet CYXT C-GWWS changed gusts minimum PC0147 TNCM WJA2507 Journey WJA520 WJA845 accordance 0055Z Emergency PA-31-350

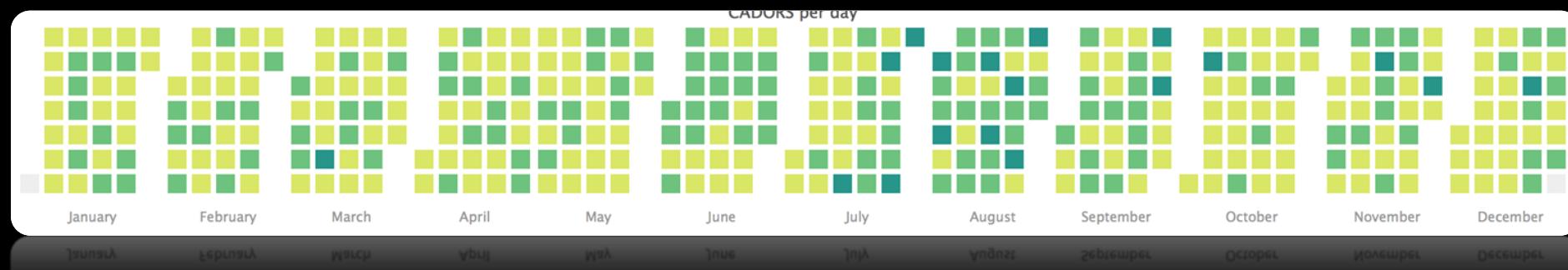
KBVS Westjet could vers
made Control there 12-30 police WJA349 REPORT
0300Z A320-211 faulty test contacted management
RCMP KLAS decided line authorized CYRF return
went CYXX 01522 After late service sure 1000 nose
PIKPA fault 560XL Beech clear 560XL Abbotsford stab
second passengers sans CHP Inspector against locked 737-8CT checklist
operator National Halifax flap left FLAP exploite
Incident remonté finale TCAS Edmonton read
Ottawa collision ARFF Apré 23522 avoir
Prairie gate medical 17162 operations Havilland deux
right back around 8975 advised missed Calgary miles
tire Hamilton control 00202 been Canada Report BITE issue
stop overshoot fuel replaced laid DHC-8-402 landing lander ICYYC
CJ03 Once turn observed taxi Flap 22472 after runway
CAT4 passenger strike conducted looked conducting fast During Unit
CYTT conduct Maintenance Prince about alors call JOUR
high 300A cleared Occurrence Int'l UPDAT CYVR
When Universal d'un side loud KFLL report CYHZ
Grande horizontal 21252 Quick Tower required 737-800 fait
elected illuminated CYHM CYU main separation arrival sous
damaged controller hand told CYUH which overshot Embraer fluid Airworthiness crew
CYXE would vehicles pilot cross deleted reduced Ottawa/MacDonald-Cartier Aircraft call root Four CYWG advisory move
3000' Halifax/Stanfield upon C-GETX hold another 90-around 172M shear alternate came level
during N843MG Minot KMOT George following destination Int'l Duplicate CYMM Upon Slow through done
Cancun 0900Z manual 10122 11000 east Cana used -reported FSEU poor bulb ambulance message
Cargojet CYXT C-GWWS changed gusts minimum PC0147 TNCM
WJA2507 Journey
WJA426
WJA520
WJA845 accordance
00552 Emergency PA-31-350

Calendar Heat Map visualization showing days with highest incidents

- ▶ Transport Canada recorded a total of 17,392 CADORS reports in 2017, that's a national average of 47.6 incident/accidents per day. Thus far in 2018, we are at 10,906.
- ▶ The question:
Which days had the highest amount of reports?
- ▶ We can easily get access to the days that stand out for volume levels.

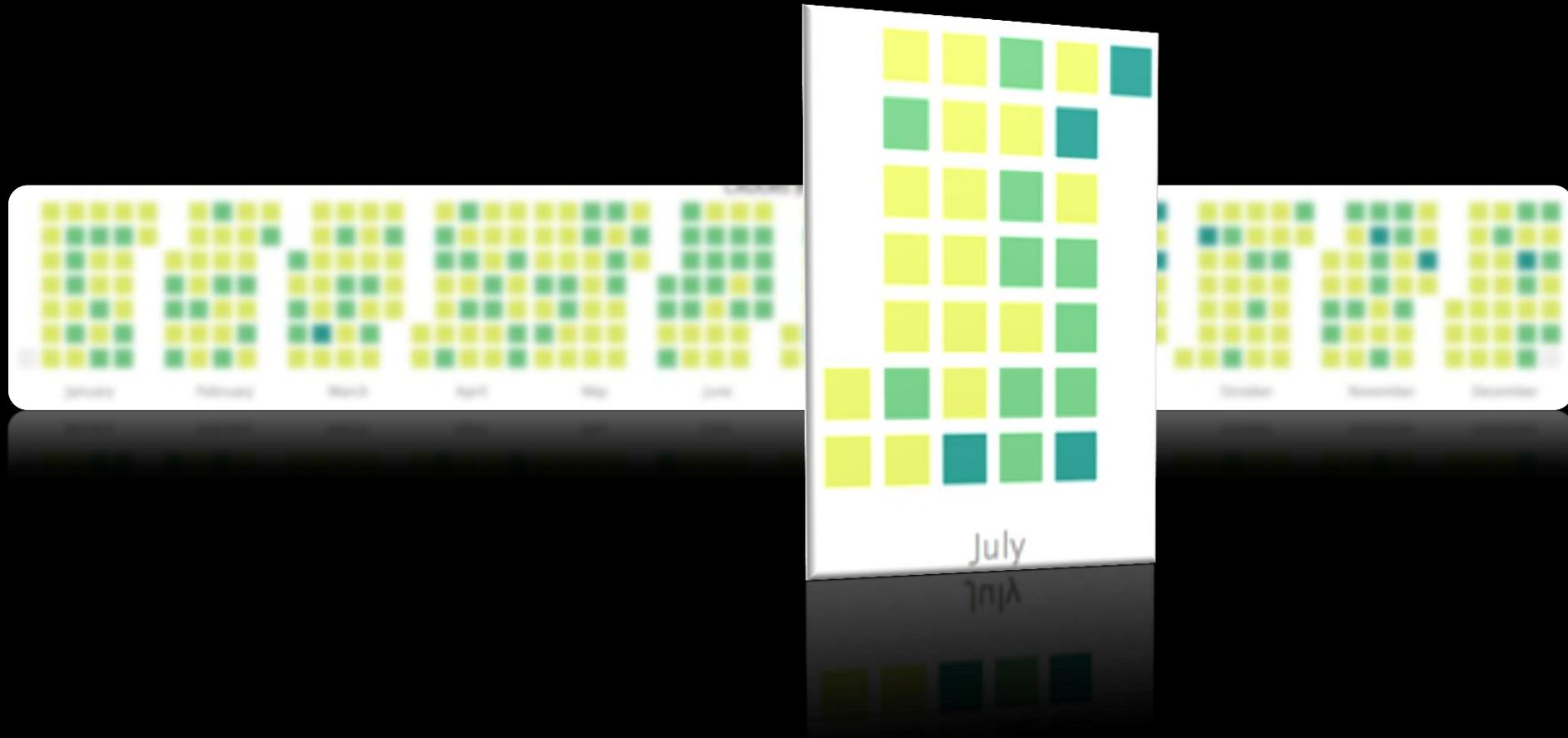
Calendar Heat Map

making it easier to cluster by dates



Calendar Heat Map

making it easier to cluster by dates



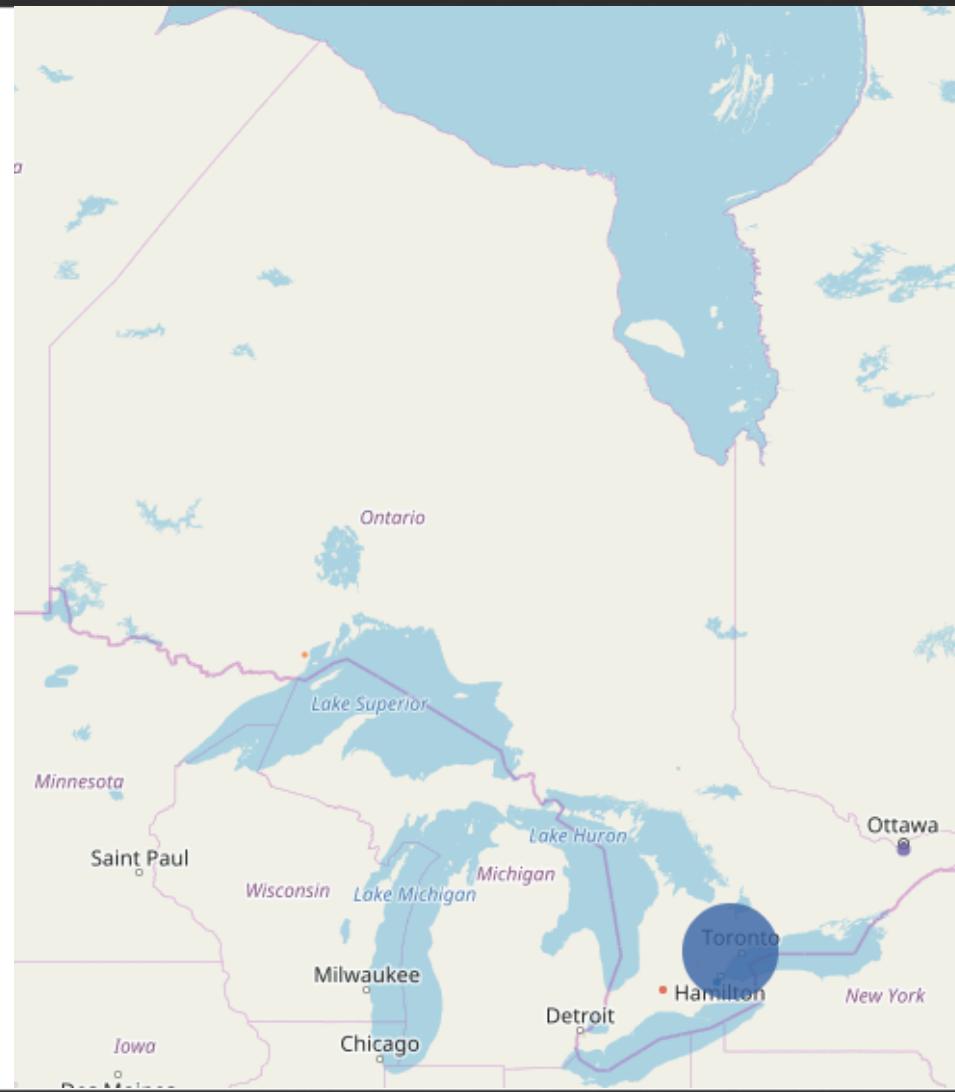
Calendar Heat Map

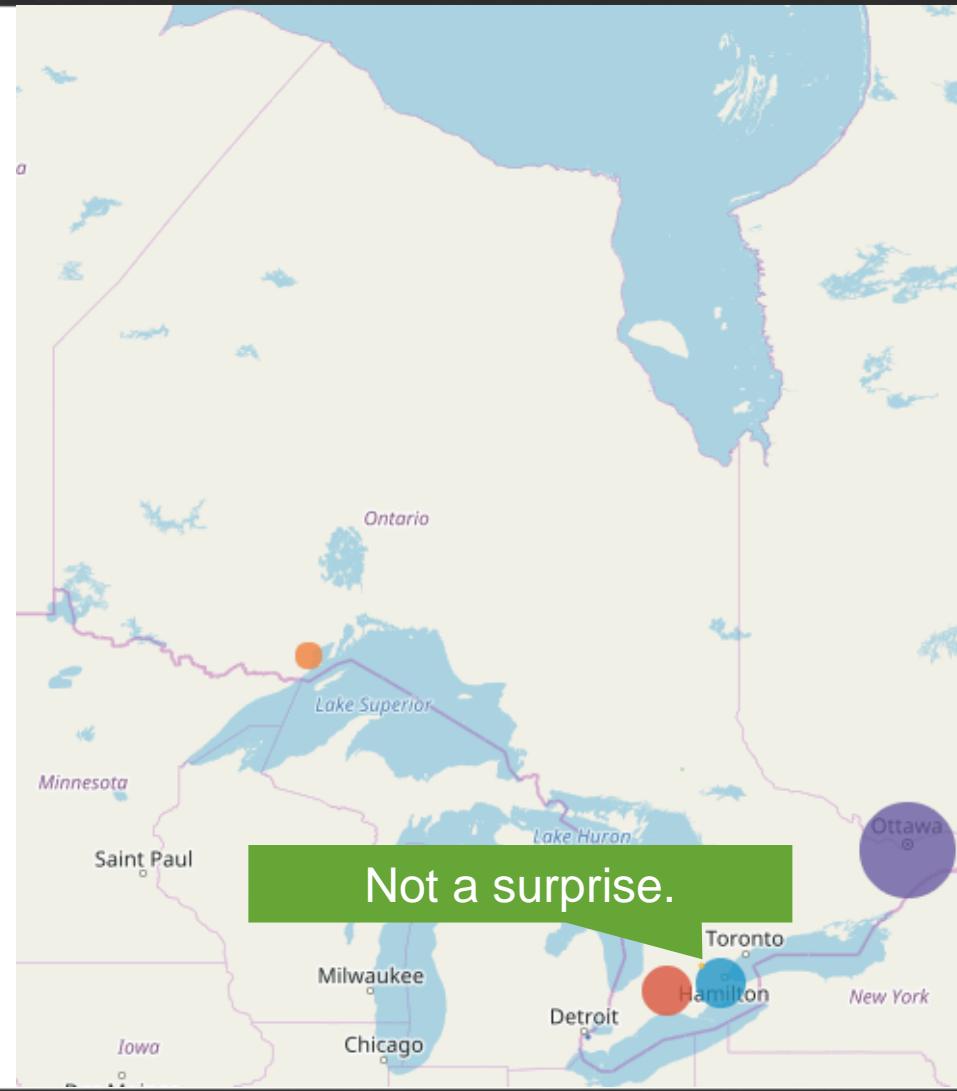
making it easier to cluster by dates

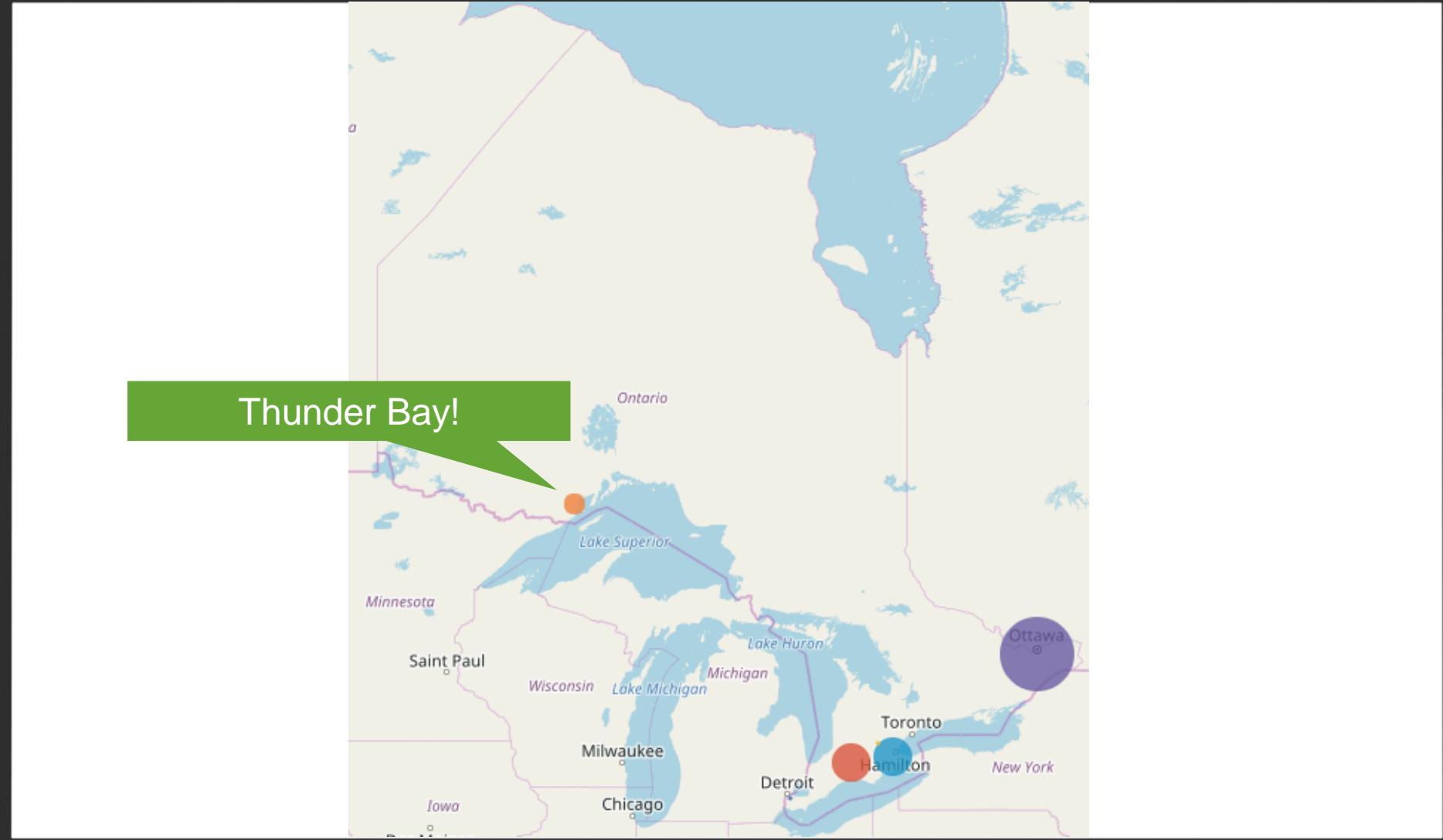


Cluster Map showing occurrences by region

- One of the categorical groupings that Transport Canada has is a data field called "TCRegion".
- The question:
After the heavy hitters were excluded from the data set, which would be the next highest?
- The frequency of occurrences for some airports is easy to guess, due to the size and the frequency of flights arriving and departing.

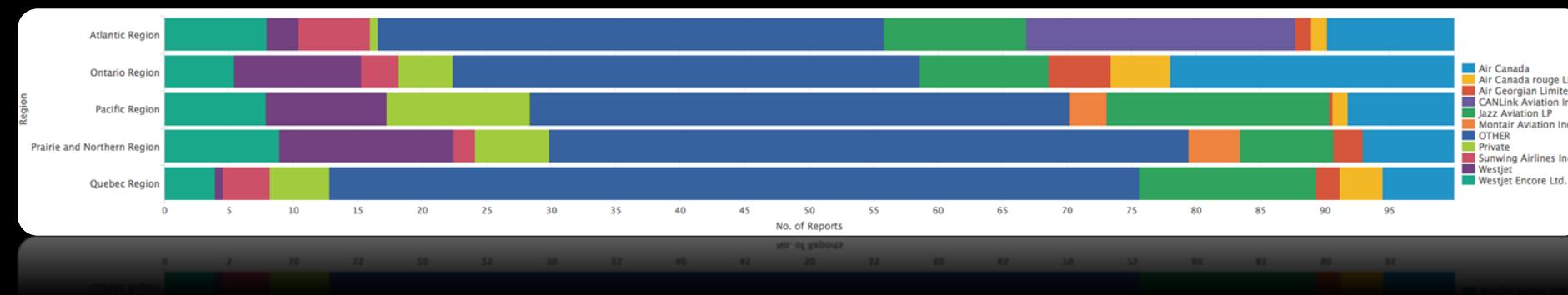






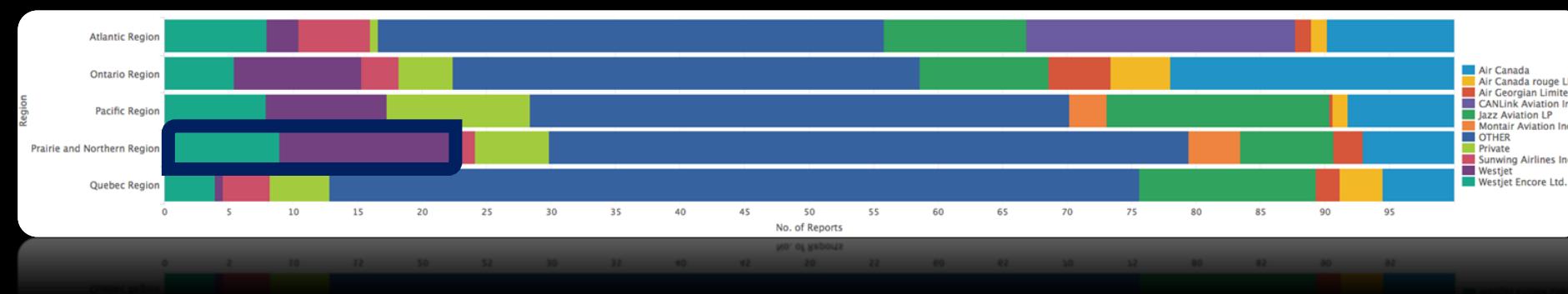
Stacked 100% bar chart

breaking down how each air carrier placed in each national region



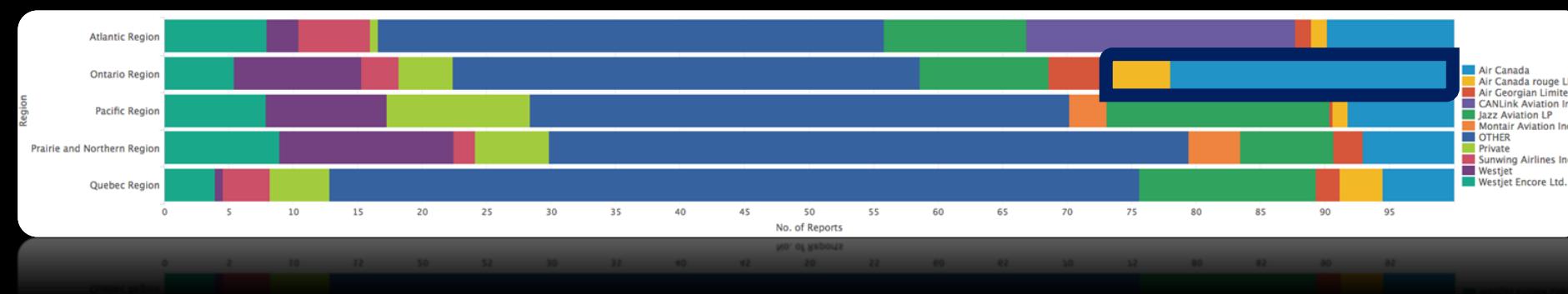
Stacked 100% bar chart

breaking down how each air carrier placed in each national region

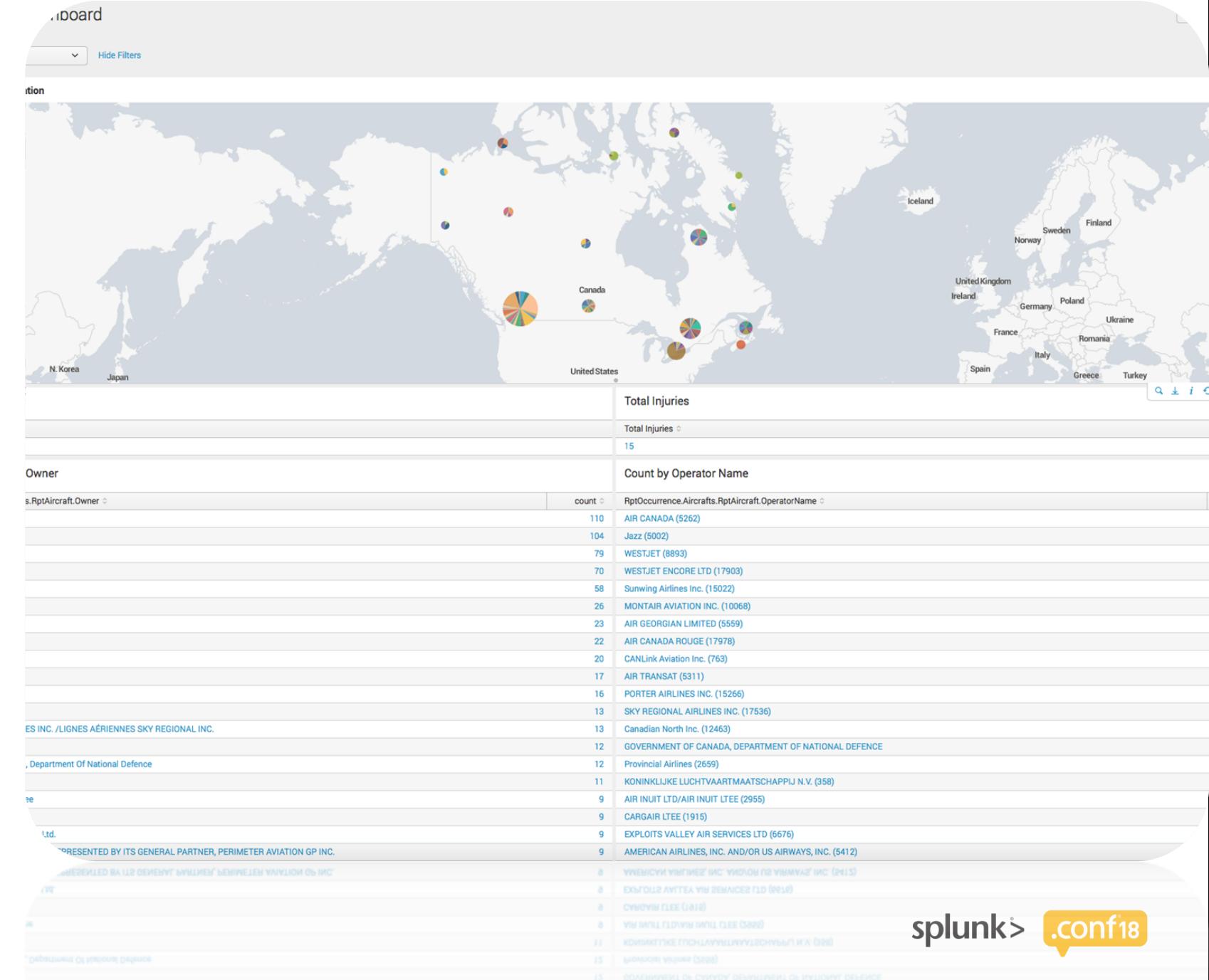


Stacked 100% bar chart

breaking down how each air carrier placed in each national region

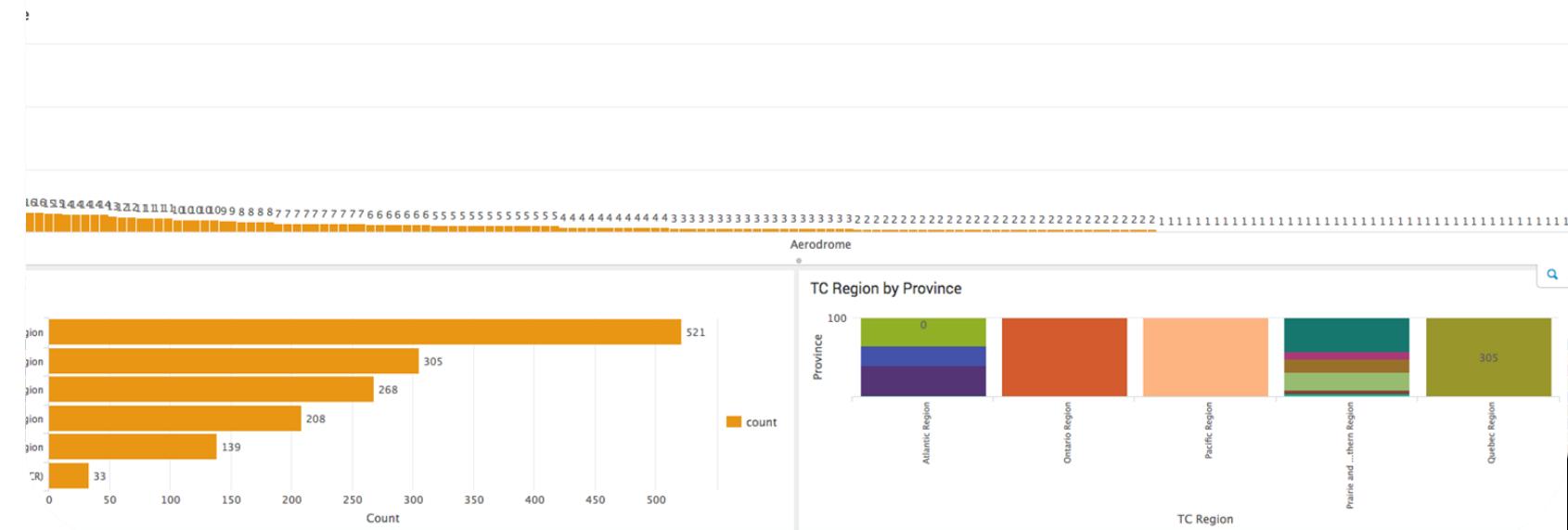


All CADORS Dashboard

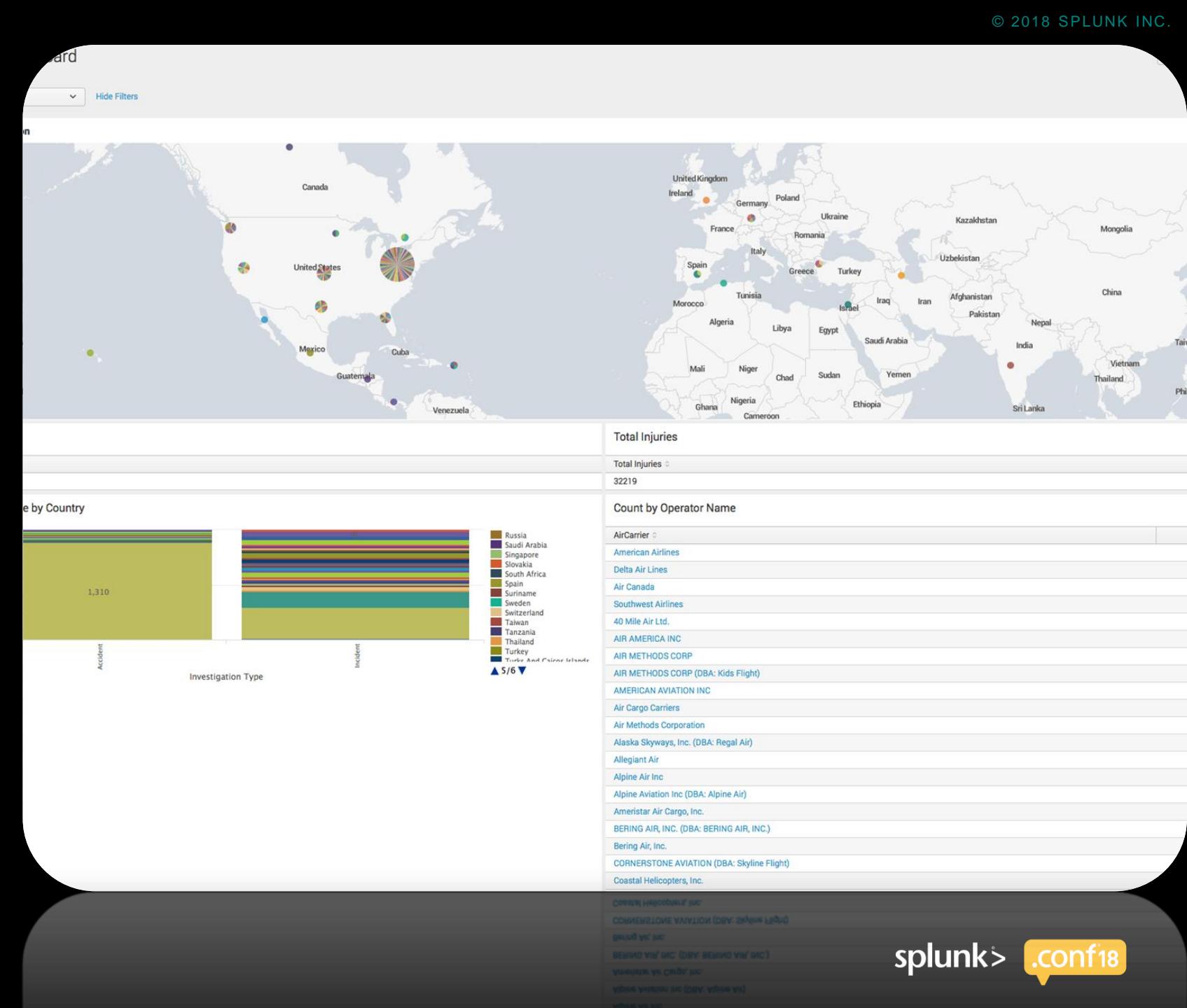


All CADORS Dashboard

Aircraft.AircraftCategory		Count by Aircraft Make	Count by Aircraft Model	Count by Year Built			
Aircraft.AircraftCategory	count	RptOccurrence.Aircrafts.RptAircraft.AircraftMake	count	RptOccurrence.Aircrafts.RptAircraft.AircraftModel	count	RptOccurrence.Aircrafts.RptAircraft.YearBuilt	count
	1119	BOEING	248	DHC-8-402	120		
	43	DEHAVILLAND	198	737-800	35		
	20	CESSNA	150	1900D	28		
	1	AIRBUS	113	DHC-8-102	27		
	1	BEECH	74	172S	22		
		BOMBARDIER	63	ERJ 190-100 IGW	22		
		EMBRAER	52	A320	21		
		PIPER	33	A321-211	20		
		PILATUS	22	CL-600-2D24 (SERIES 900)	20		
		AEROSPATIALE	20	777 300 SERIES	18		
		DIAMOND	11	737 800	15		
		CANADAIR	11	767 300	15		
		UNKNOWN/INCONNU	10	A320-211	15		
		BELL	10	DA 20-C1	15		
		BRITISH AEROSPACE	10	172R	14		
		FAIRCHILD	9	ERJ 170-200 SU	14		
		LOCKHEED	8	PC-12/45	14		
		EUROCOPTER	8	LEARJET	13		
		DAUPHIN	7	172M	13		
		DASSAULT	7	737-700	13		



All NTSB Dashboard



.. can tell Splunk to continuously collect data from a file or directory (keep indexing data as it comes in), or index a static file and then stop.

More settings

Host
Tell Splunk how to set the value of the host field in your events from this source.

Set host

Specify method for getting host field for events coming from this source.

Host field value

Source type
Tell Splunk what kind of data this is so you can group it with other data of the same type when you search. Splunk does this automatically, but you can specify what you want if Splunk gets it wrong.

Set the source type

When this is set to automatic, Splunk classifies and assigns the sourcetype automatically, and gives unknown sourcetypes placeholder names.

Source type *

Index
Set the destination index for this source.

Index

Advanced options

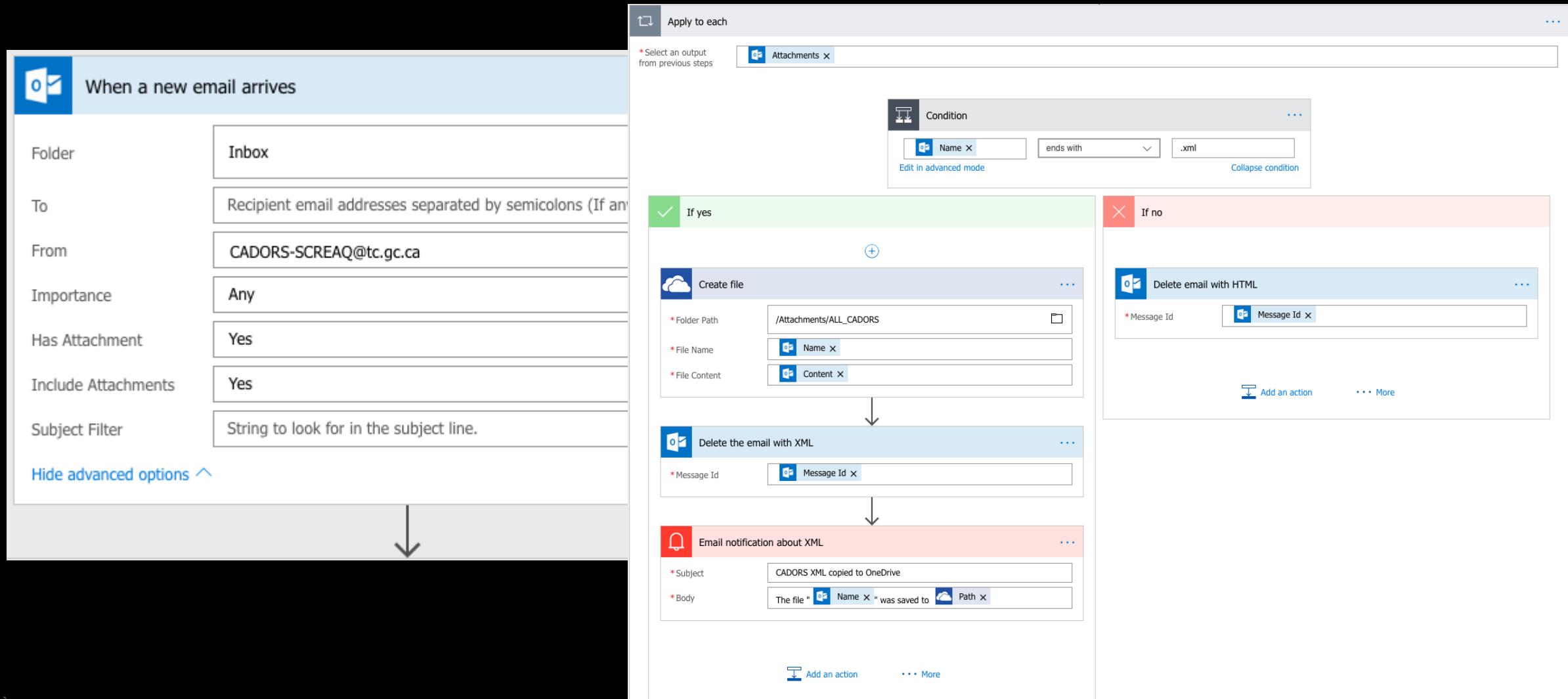
Whitelist

Specify a regex that files from this source must match to be monitored by Splunk.

Blacklist

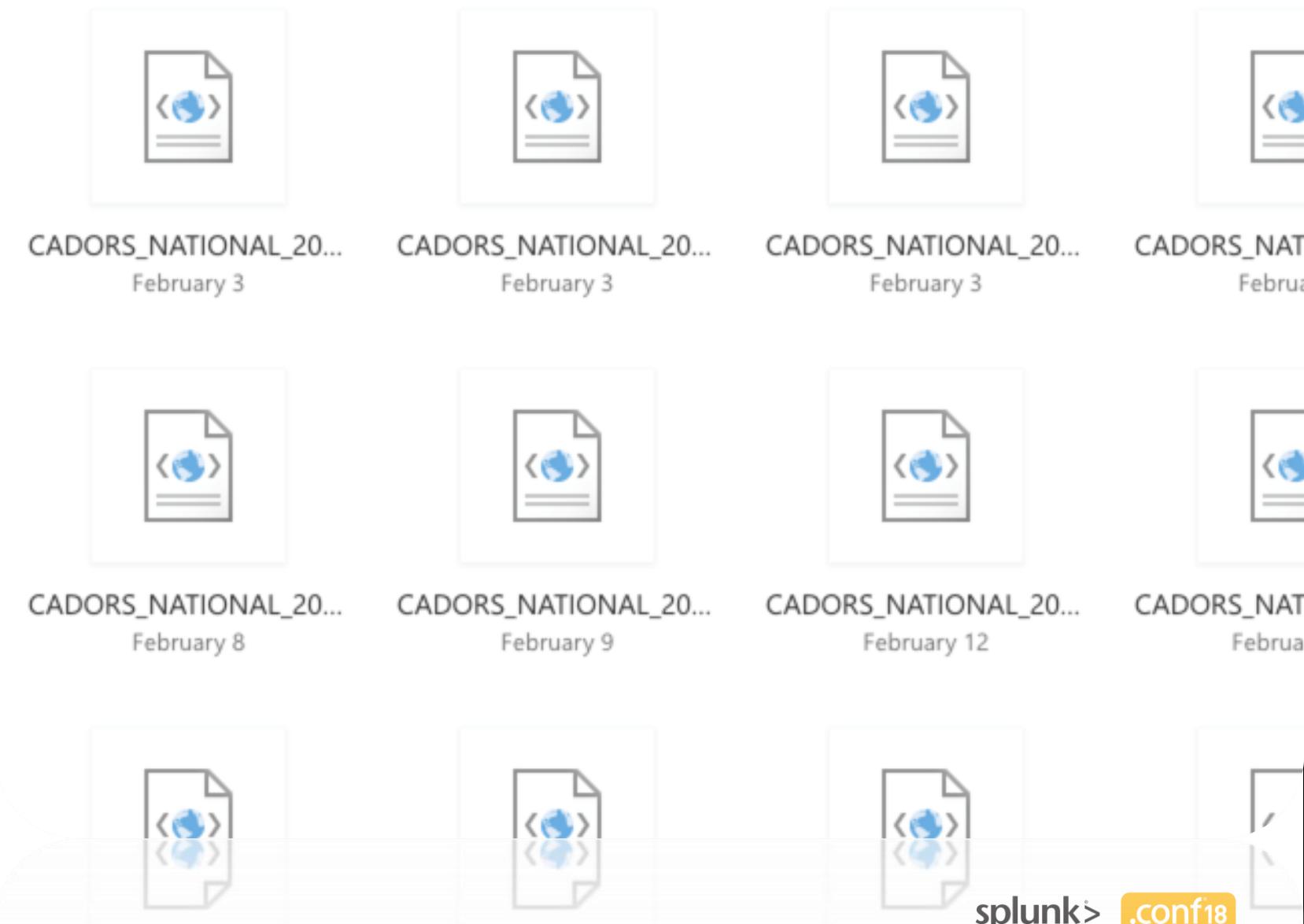
Specify a regex that files from this source must NOT match to be monitored by Splunk.

Automated event ingestion with Microsoft Flow



Long term storage of data files on OneDrive

Files > Attachments > ALL_CADORS





Data captured over-the-air via Raspberry Pi based receiver



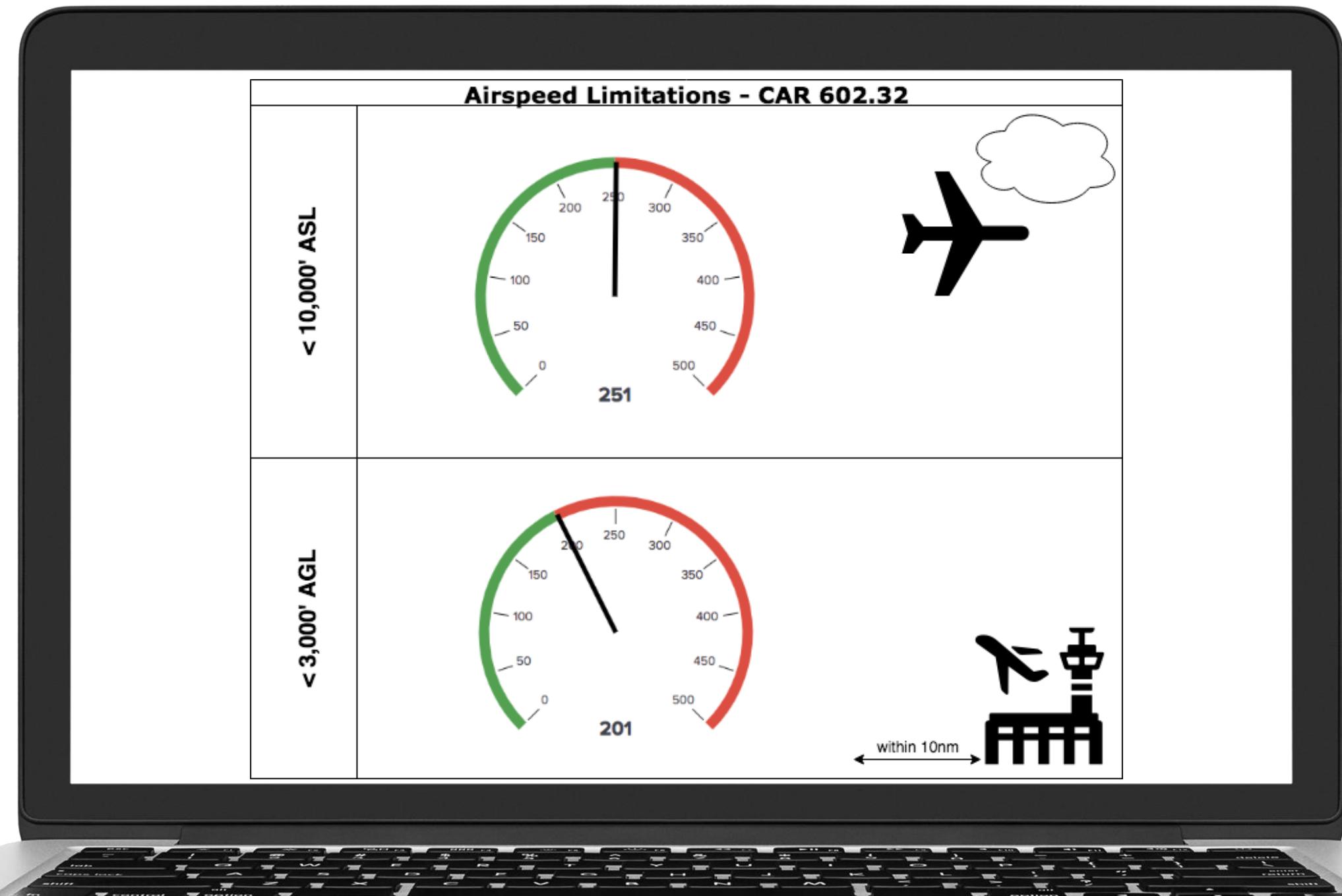
About Over-the-Air Data Sources

- ▶ The Stratus device is an Automatic Dependent Surveillance-Broadcast (ADS-B) receiver made from a Raspberry Pi.
- ▶ The Project
 - What? A weather, traffic, GPS receiver.
 - How? Radio antennae capturing over the air signals and logging to text file.
 - Where? <http://stratus.me>

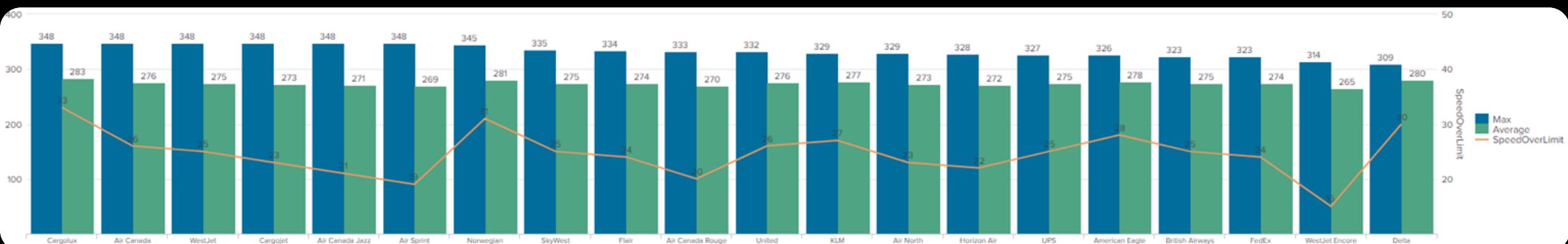


Speed Analysis

- ▶ The data set is 5 months worth of logs in the vicinity of Calgary International (CYYC). The data set has > 22 million events.
- ▶ I have accurate data recorded from aircraft in the vicinity which ranges from altitude and heading to aircraft identifier and speed.
- ▶ The question:
Do commercial aircraft speed?
- ▶ For the first law, the bar chart shows the various carriers that are equipped with ADS-B. For the second law, we'll use a view by Google Earth.
- ▶ Future enhancements could easily include mashups with CADORS data or mashup with for-pay service data such as FlightAware.



Bar chart with speed overlay



max recorded speed
avg recorded speed
delta between the speed limit
and the average speed

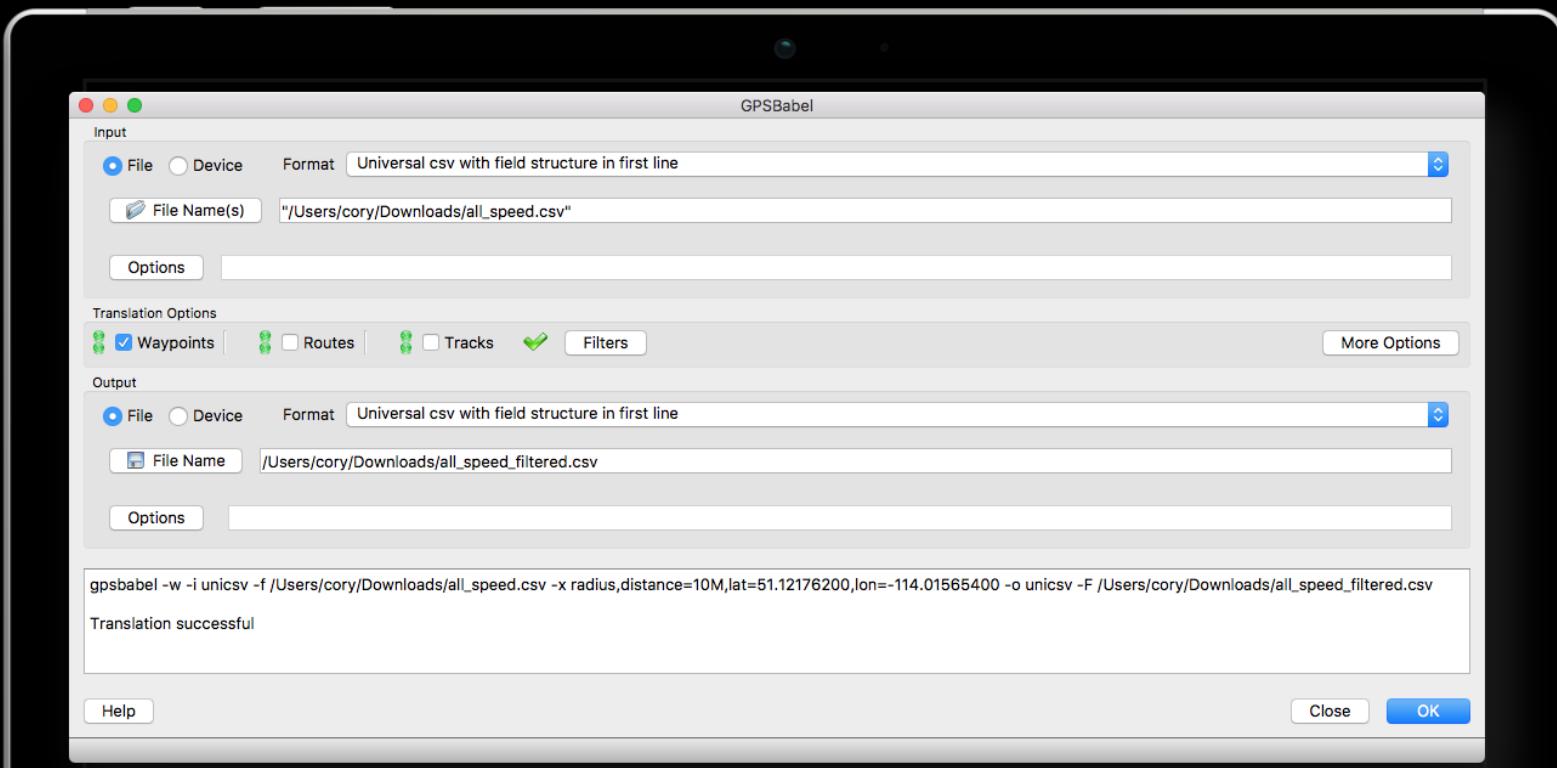
Using GPSBabel to isolate events based on latitude and longitude

The screenshot shows two Microsoft Excel tabs: 'all_speed' and 'all_speed_filtered'. The 'all_speed' tab contains a large dataset of event data with columns for time, tail, airline, registration, longitude, latitude, altitude, speed, and track. The 'all_speed_filtered' tab shows a smaller subset of data, indicating which rows were processed by GPSBabel.

The GPSBabel utility window is also visible, showing the input file 'U:\Users\copy\Downloads\all_speed.csv' and the output file 'U:\Users\copy\Downloads\all_speed_filtered.csv'. The output window displays the command: 'gpsbabel -w -u -cvin -f U:\Users\copy\Downloads\all_speed.csv -x radius,distance=10M,lat=-113.9961200,lon=-14.01668400 -ucin -f U:\Users\copy\Downloads\all_speed_filtered.csv'. The message 'Translation successful' is displayed.

Time	Tail	Airline	Registration	Longitude	Latitude	Altitude	Speed	Track
2018-03-21T15:08:53.000-0600	WIA1541	Westjet	C-GIWS	-113.9036	51.10089	3900	343	1031
2018-03-21T15:08:38.000-0600	WIA1541	Westjet	C-GIWS	-113.904	51.09878	4050	493	1031
2018-03-14T23:21:46.000-0600	WIA1465	Westjet	C-GWSZ	-113.9056	51.566483	6250	2693	469
2018-03-08T15:35:00.000-0700	WIA1268	Westjet	C-GWVU	-113.9593	51.572205	5925	2368	436
2018-03-19T02:41:00.000-0600	WIA1464	Westjet	C-GIWF	-113.973	50.924386	5975	2418	373
2018-03-17T02:11:34.000-0600	WIA146H	Westjet	C-GIWI	-113.973	50.924386	5975	2418	373
2018-03-08T18:29:02.000-0700	WEH3229	WestJet Encore	C-GENV	-114.0419	51.82805	4725	1168	353
2018-03-10T08:28:47.000-0700	WEH3229	WestJet Encore	C-GENV	-114.0419	51.82805	4725	1168	353
2018-03-19T06:28:56.000-0600	WIA230	Westjet	C-GWVJ	-113.4895	51.06059	3475	-82	345
2018-03-19T06:28:41.000-0600	WIA230	Westjet	C-GWVJ	-113.4895	51.06059	3475	-82	345
2018-03-19T06:28:26.000-0600	WIA230	Westjet	C-GWVJ	-113.4895	51.06059	3475	-82	345
2018-03-19T06:28:11.000-0600	WIA456	Westjet	C-GWVJ	-113.675	51.050574	6375	2813	399
2018-03-19T10:56:54.000-0600	AC4322	Academy	C-GFQH	-113.838944	51.134124	4820	1425	321
2018-03-22T15:06:29.000-0600	AC4222	Air Canada	C-FGII	-113.838844	51.45724	6500	2943	313
2018-03-22T15:06:14.000-0600	AC4222	Air Canada	C-FGII	-113.838844	51.45724	6500	2943	313
2018-03-28T08:21:40.000-0600	WIA653	Westjet	C-GQWY	-113.4887	51.02884	6500	2943	303
2018-03-28T08:21:25.000-0600	WIA653	Westjet	C-GQWY	-113.4887	51.02884	6500	2943	303
2018-03-28T08:21:10.000-0600	WIA653	Westjet	C-GQWY	-113.4887	51.02884	6500	2943	303
2018-03-28T08:20:55.000-0600	WIA653	Westjet	C-GQWY	-113.4887	51.02884	6500	2943	303
2018-03-22T09:14:25.000-0600	N200IN	National	C-GQWY	-113.2831	51.182405	6375	2765	297
2018-03-22T09:14:24.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:14:23.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:14:22.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:14:21.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:14:20.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:14:19.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:14:18.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:14:17.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:14:16.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:14:15.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:14:14.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:14:13.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:14:12.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:14:11.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:14:10.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:14:09.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:14:08.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:14:07.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:14:06.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:14:05.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:14:04.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:14:03.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:14:02.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:14:01.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:14:00.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:59.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:58.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:57.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:56.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:55.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:54.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:53.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:52.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:51.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:50.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:49.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:48.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:47.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:46.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:45.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:44.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:43.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:42.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:41.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:40.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:39.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:38.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:37.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:36.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:35.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:34.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:33.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:32.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:31.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:30.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:29.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:28.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:27.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:26.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:25.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:24.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:23.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:22.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:21.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:20.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:19.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:18.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:17.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:16.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	6500	2869	297
2018-03-22T09:13:15.000-0600	WIA5625	Westjet	C-GQDQ	-113.847374	51.032548	6500	2869	297
2018-03-22T09:13:14.000-0600	WIA5625	Westjet	C-GQWY	-114.1645	51.082489	65		

What is GPSBabel?



- ▶ “GPSBabel converts waypoints, tracks, and routes between popular GPS receivers such as Garmin or Magellan and mapping programs like Google Earth or Basecamp.”
- ▶ “It also has powerful manipulation tools for such data.”
- ▶ “It has been downloaded and used tens of millions of times since it was first created in 2001, so it's stable and trusted.”

Integrating Google Earth

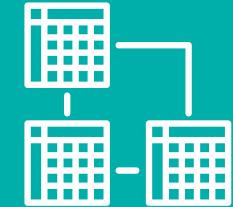
The 3-step data import process



Import from CSV



Select fields with
coordinates



Cast to correct data type

A vertical column of extremely long and complex log entries from a Splunk search results page, showing numerous HTTP requests, session IDs, and product details, illustrating the volume and complexity of data being integrated.

Data Import Wizard

Specify Delimiter

This step allows you to specify the field delimiter in your text file

Field Type

Delimited Fixed width

Delimited

Select the delimiter that separates each field. If there can be more than one delimiter between two fields (such as spaces), check the "treat consecutive delimiters as one" option. You can also provide your own custom delimiter by checking the "other" option

Space Treat consecutive delimiters as one
 Tab
 Comma
 Other

Fixed Width

Column width

Text Encoding

Supported encodings

This is a preview of the data in your dataset.

No	Latitude	Longitude	Name	Altitude	Speed
1 \$	51.100890	-113.990360	WPT001	343.0	1031.00
2 2	51.152298	-114.016420	WPT113	2893.0	268.00

Data Import Wizard

Select Latitude/Longitude Fields

This dataset does not contain latitude/longitude information, but street addresses

Latitude field

Longitude field

This is a preview of the data in your dataset.

No	Latitude	Longitude	Name	Altitude	Speed	Date
1 \$	51.100890	-113.990360	WPT001	343.0	1031.00	2018/04/15
2 2	51.152298	-114.016420	WPT113	2893.0	268.00	2018/04/07
3 3	51.089780	-113.990400	WPT002	493.0	1031.00	2018/04/15
4 4	51.074230	-114.024124	WPT414	2668.0	250.00	2018/04/07

Data Import Wizard

Specify Field Types (optional)

This step allows you to specify the type of each field in your dataset. This is optional.

Field	Type
No	integer
Latitude	floating point
Longitude	floating point
Name	string
Altitude	floating point
Speed	floating point
Date	string
Time	string

This is a preview of the data in your dataset.

No	Latitude	Longitude	Name	Altitude	Speed	Date
1 \$	51.100890	-113.990360	WPT001	343.0	1031.00	2018/04/15
2 2	51.152298	-114.016420	WPT113	2893.0	268.00	2018/04/07
3 3	51.089780	-113.990400	WPT002	493.0	1031.00	2018/04/15
4 4	51.074230	-114.024124	WPT414	2668.0	250.00	2018/04/07

Integrating Google Earth

The 4-step style template creation



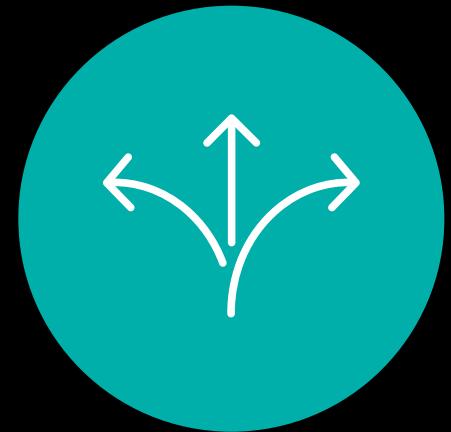
Name



Color

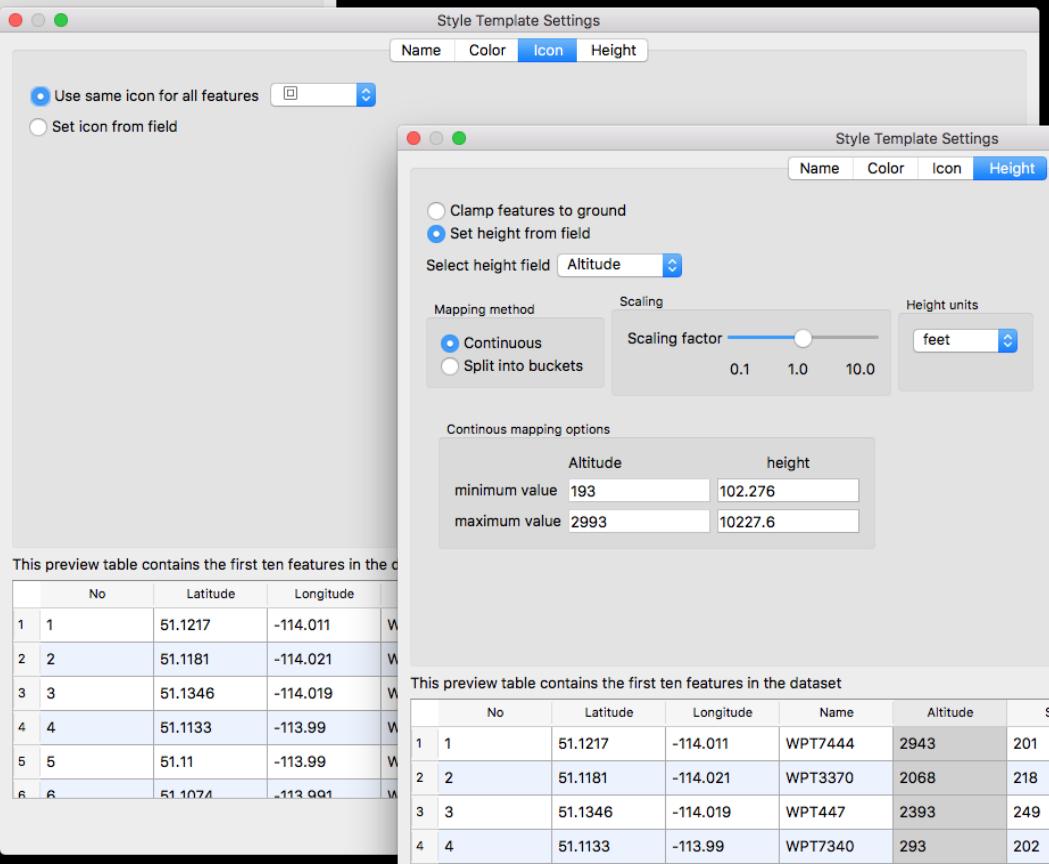
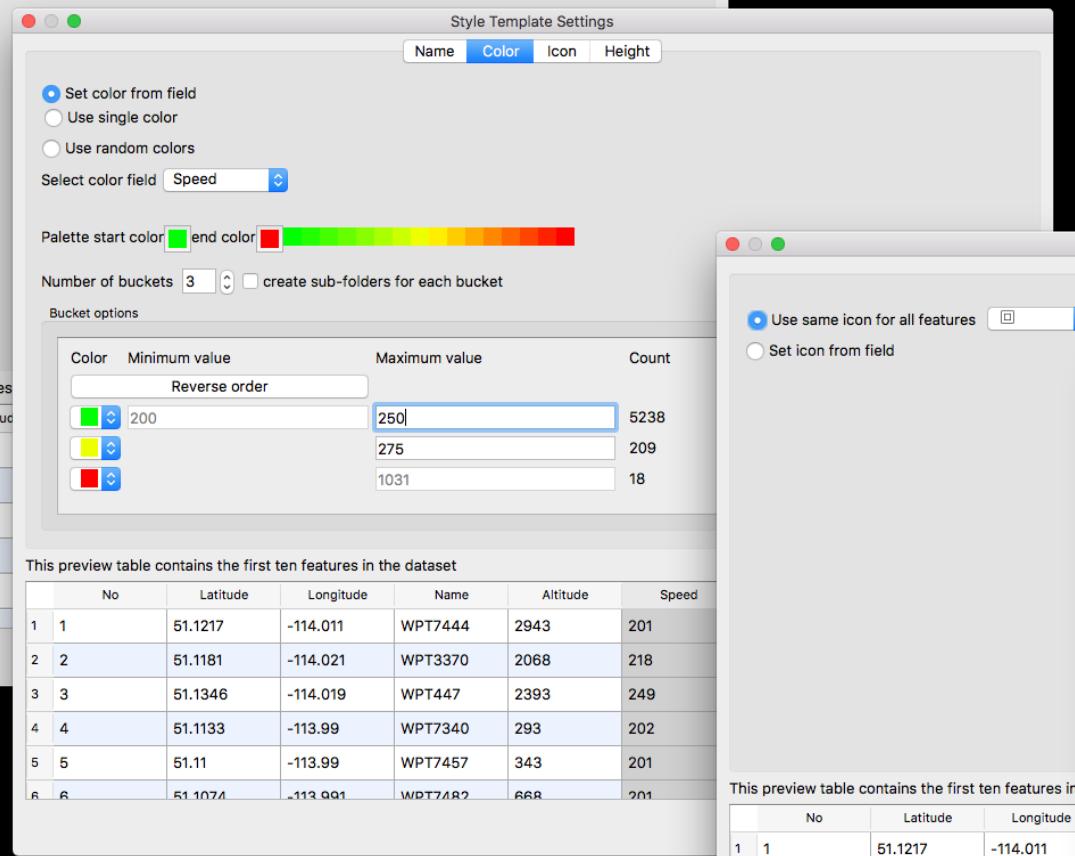
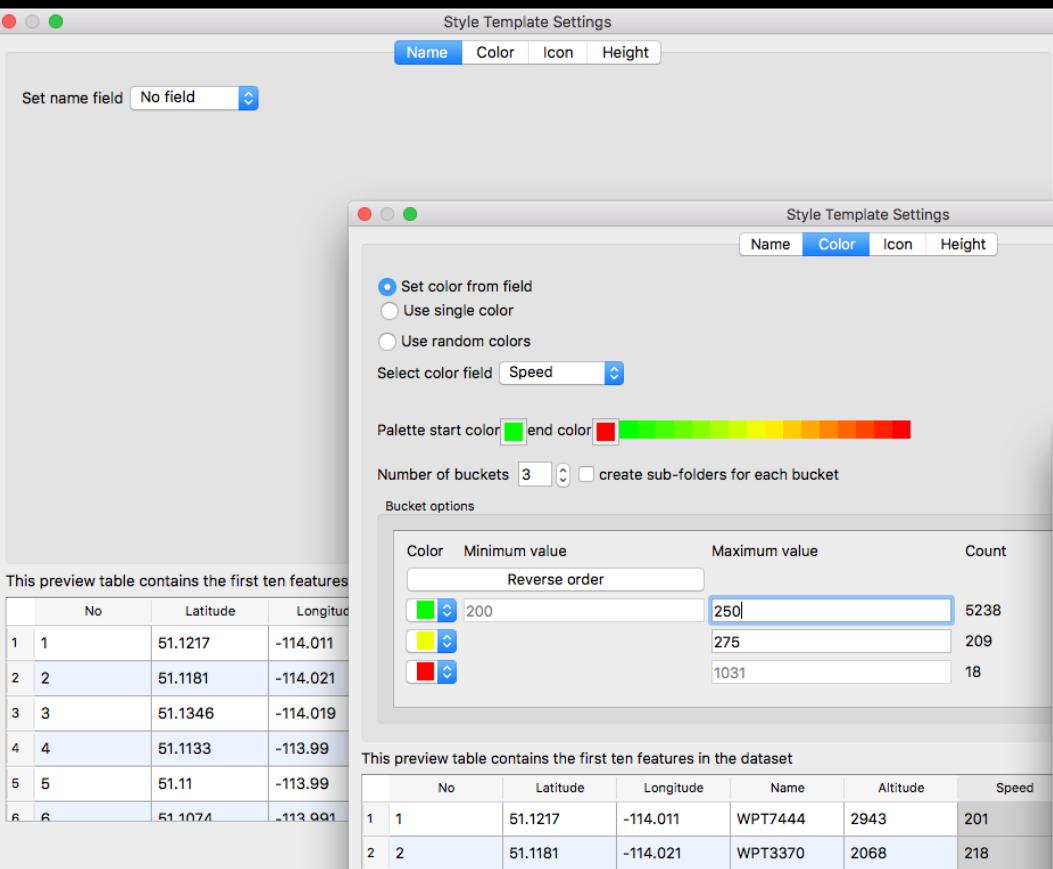


Icon

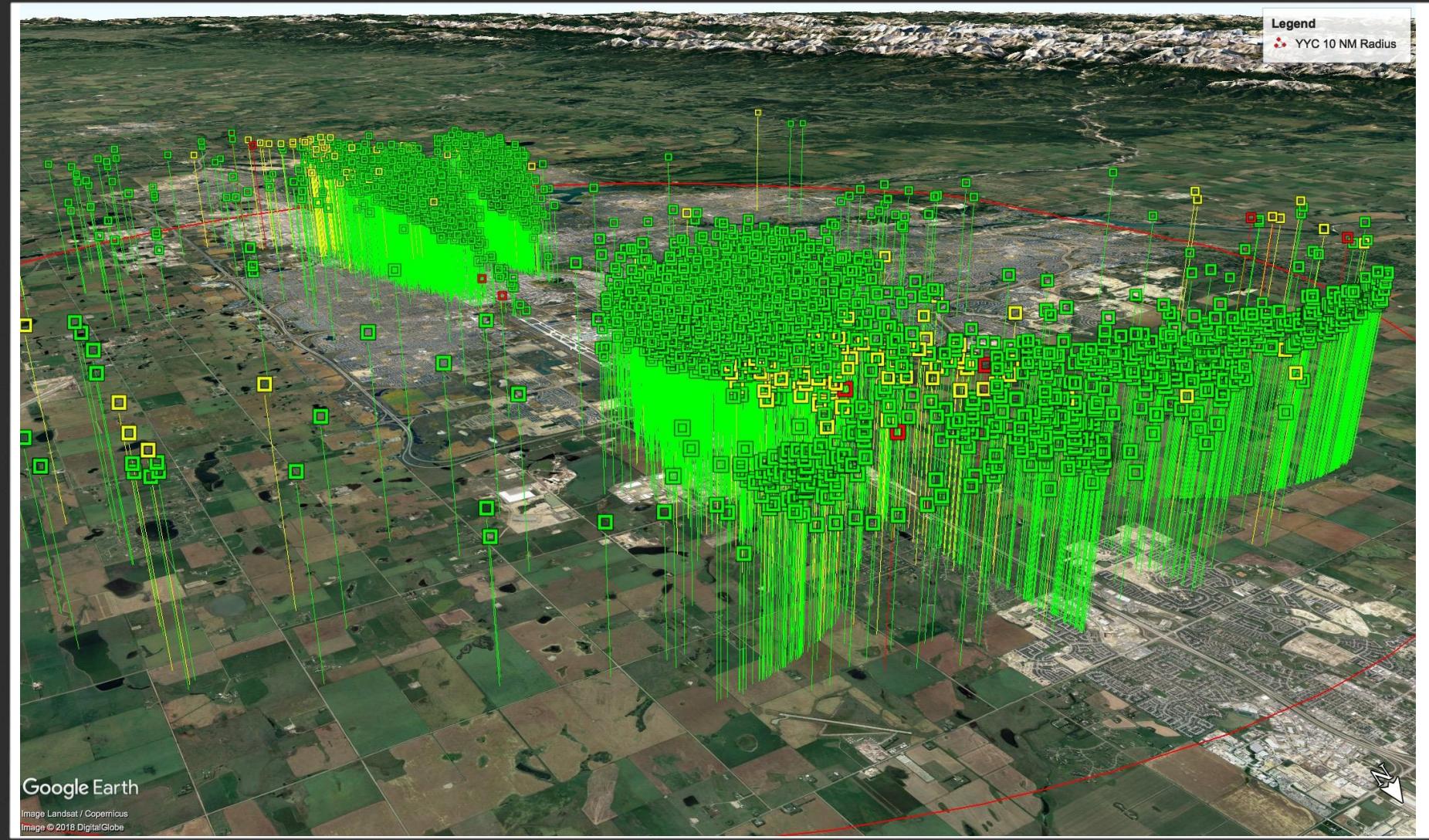


Height

A large block of log data from Splunk, including timestamps, URLs, and various log entries related to a shopping cart and product purchases.



This preview table contains the first ten features in the dataset								
	No	Latitude	Longitude	Name	Altitude	Speed	Date	Time
1	1	51.1217	-114.011	WPT7444	2943	201	2018/04/22	07:38:17
2	2	51.1181	-114.021	WPT3370	2068	218	2018/04/07	13:26:10
3	3	51.1346	-114.019	WPT447	2393	249	2018/04/07	13:26:25
4	4	51.1133	-113.99	WPT7340	293	202	2018/04/10	19:18:55
5	5	51.11	-113.99	WPT7457	343	201	2018/04/23	13:04:28
6	6	51.1074	-113.991	WPT7482	668	201	2018/04/16	19:32:49



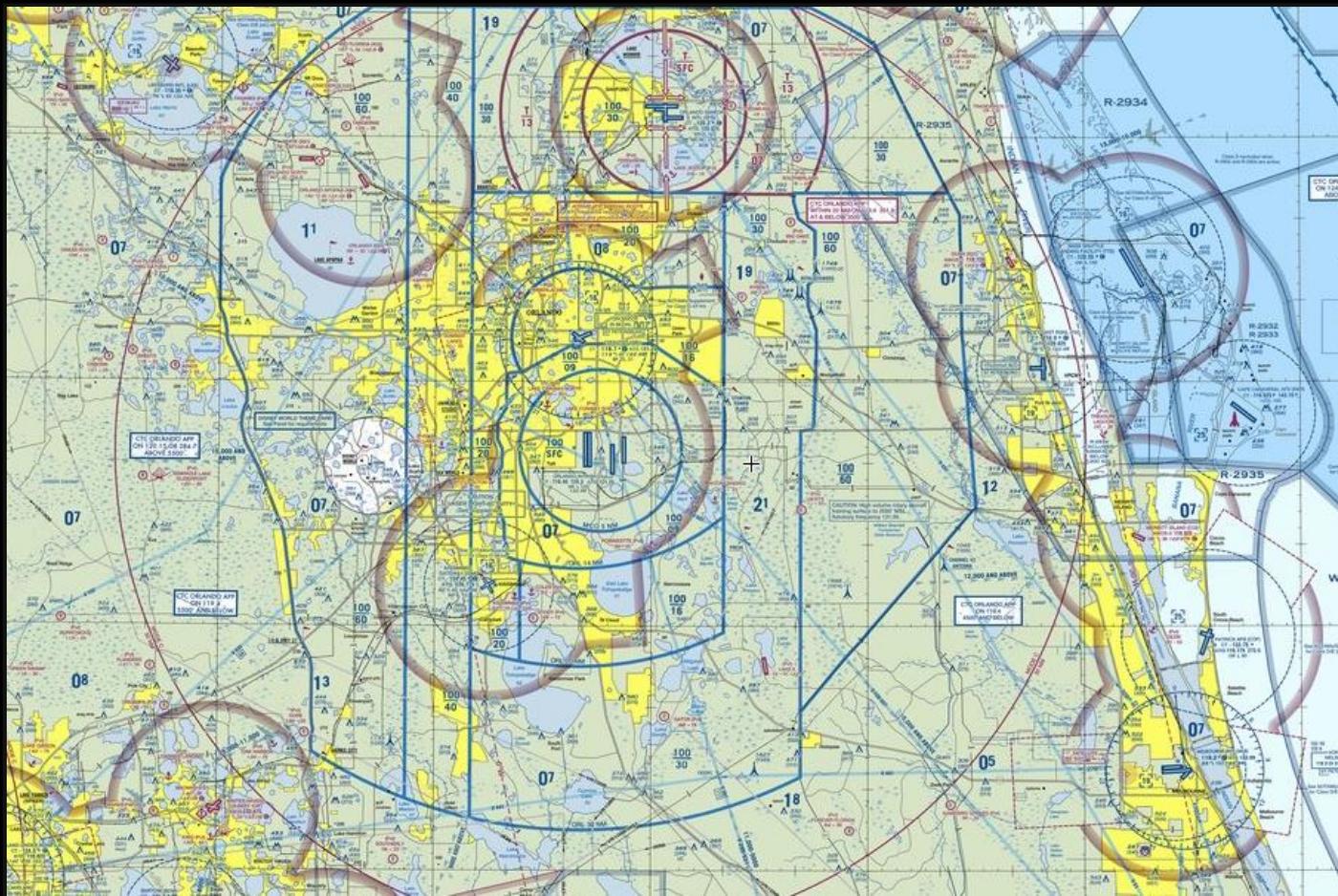
Stratux Demo

Take a peek at the Stratux App



Orlando (MCO) Airspace

Terminal Area Chart

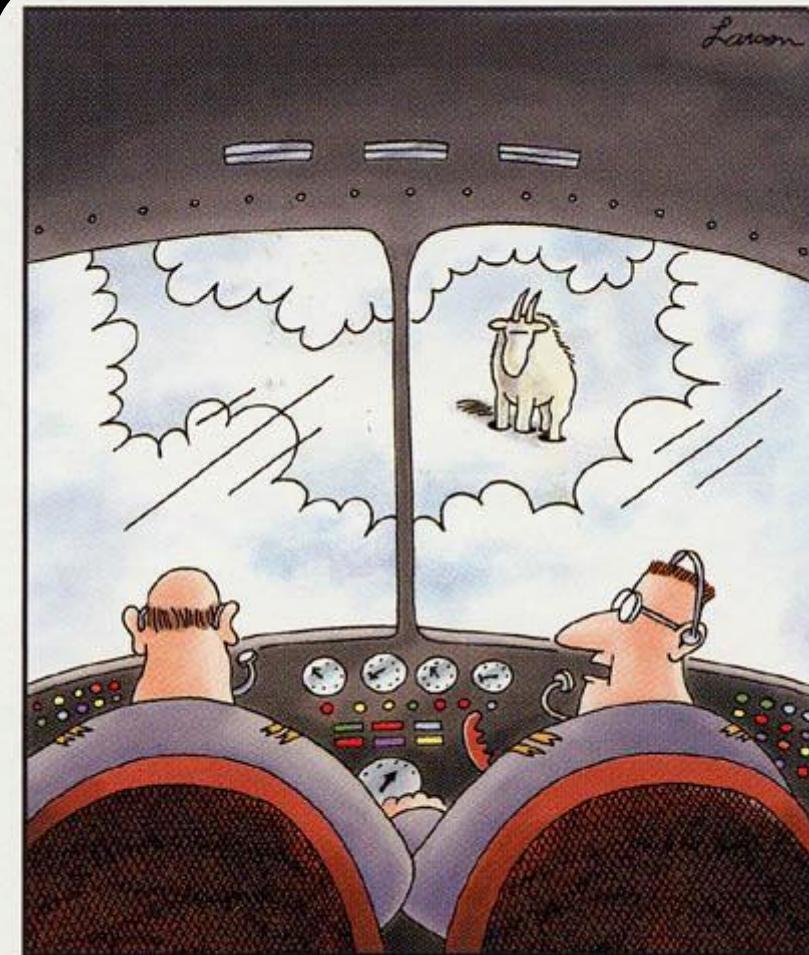


- There are 4 significantly sized airports and 8 smaller within 30 nm of MCO.
- Very busy airspace; Tampa (west), Miami (south), and Kennedy Space Center (east).

The things that make it go

- ▶ Splunk app
 - ▶ SPL:
 - eventtype
 - eval with case
 - outlier
 - table
 - ▶ props.conf to parse fields from JSON
 - ▶ Simple XML Dashboard
 - ▶ Google Earth
 - ▶ GPSBabel

```
props.conf x
1 [Stratux]
2 DATETIME_CONFIG =
3 NO_BINARY_CHECK = true
4 category = Custom
5 description = ADS-B Receiver Logs
6 disabled = false
7 pulldown_type = true
8 EXTRACT-icao_addr = Icao_addr\":(?<icao_addr>\d{1,})
9 EXTRACT-registration = Reg\":(?<registration>[\w-]{1,})
10 EXTRACT-emitter = Emitter_category\":(?<emitter>\d{1,})
11 EXTRACT-onground = OnGround\":(?<onground>\w*)
12 EXTRACT-tail = Tail\":(?<tail>[\w\s-]{1,})
13 EXTRACT-signal = SignalLevel\\":(?<signal>[-\d.\d]*)
14 EXTRACT-squawk = Squawk\\":(?<squawk>\d*)
15 EXTRACT-targettype = TargetType\\":(?<targettype>\d*)
16 EXTRACT-positionvalid = Position_valid\\":(?<positionvalid>\w*)
17 EXTRACT-altitude = \Alt\\":(?<altitude>\d*)
18 EXTRACT-latitude = Lat\\":(?<latitude>[-\d.\d]*)
19 EXTRACT-longitude = Lng\\":(?<longitude>[-\d.\d]*)
20 EXTRACT-gnssdifffrombaroalt = GnssDiffFromBaroAlt\\":(?<gnssdifffrombaroalt>\d*)
21 EXTRACT-altisgnss = AltIsGNSS\\":(?<altisgnss>\w*)
22 EXTRACT-speed = Speed\\":(?<speed>\d*)
23 EXTRACT-track = Track\\":(?<track>\d*)
24 EXTRACT-speedvalid = Speed_valid\\":(?<speedvalid>\w*)
25 EXTRACT-vvel = Vvel\\":(?<vvel>[\d-]*)
26 EXTRACT-prioritystatus = PriorityStatus\\":(?<prioritystatus>\d*)
27 EXTRACT-lastgnssdiffalt = Last_GnssDiffAlt\\":(?<lastgnssdiffalt>\d*)
28 EXTRACT-age = Age\\":(?<age>[\d.]*)
29 EXTRACT-agelastalt = AgeLastAlt\\":(?<agelastalt>[\d.]*)
30 EXTRACT-bearing = Bearing\\":(?<bearing>\d*)
31 EXTRACT-distance = Distance\\":(?<distance>\d*)
32 EXTRACT-extrapolatedposition = ExtrapolatedPosition\\":(?<extrapolatedposition>\w*)
```



"Say ... what's a mountain goat doing
way up here in a cloud bank?"



1. All CADORS App

http://github.com/csvenky/all_cadors

2. All NTSB App

https://github.com/csvenky/all_ntsb

3. Stratus App

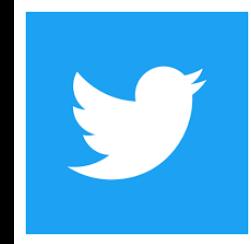
<http://github.com/csvenky/stratus>

Takeaways

My Contact Info and Links

- ▶ Stratus
 - <https://github.com/cyoung/stratus>
 - <http://stratus.me>
- ▶ Splunk Addons
 - <https://splunkbase.splunk.com>
- ▶ GPSBabel
 - <https://www.gpsbabel.org>
- ▶ Visual Studio Code
 - <https://code.visualstudio.com>
- ▶ Microsoft Flow
 - <https://flow.microsoft.com>

@spsavvy



- ▶ CADORS
 - <http://wwwapps.tc.gc.ca/saf-sec-sur/2/cadors-screaq/m.aspx>
- ▶ National Transport Safety Board Data
 - https://www.ntsb.gov/_layouts/ntsb.aviation/Index.aspx
- ▶ Federal Aviation Administration Data
 - https://www.faa.gov/data_research/aviation_data_statistics

Thank You

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

