

# Bsides Spl22

Innovating in Cyber:  
**I iplocation** for the rest of planet earth  
(Starting with Australia)



**Ugh... My talk got chosen...  
NOW I HAVE TO DO THIS!**

Slides and recording will be made available...

# We are going to look at

- × THE PROBLEM
- × THE THOUGHT PROCESS
- × THE SOLUTION



```
| makeresults count  
| eval randomIP=(random()%254) + "." + (random()%254) + "." + (random()%254) + "." + (random()%254)  
| fields - _time
```

But first... where can we get some data?

So we got lots of src IP's... but we want AU

**FIND THEM... MAKE THEM...**

- who manages the IPs? Who has lots of IP addresses  
TELCOS?...? ISP's!!
- backbone routing tables?
- real data... BIG ISP's

BSplunks\$ whois TELCO.AU Topooooo complicated national POP's...



# Pick a BIG / National ISP...

Get one of their IPs

```
[root@SplunkBSides-2022:~# host bigpond.com
bigpond.com has address 61.9.173.37
bigpond.com mail is handled by 10 extmail.bigpond.com.
root@SplunkBSides-2022:~# ]
```

Get that IP allocation

```
[root@SplunkBSides-2022:~# whois 61.9.173.37|grep 'related to'
% Information related to '61.9.128.0 - 61.9.255.255'
% Information related to '61.9.128.0/17AS1221'
root@SplunkBSides-2022:~# ]
```



@ HOME?

```
curl 'https://api.ipify.org'|xargs
whois|grep 'related to'
```

# Pick a BIG / National ISP...

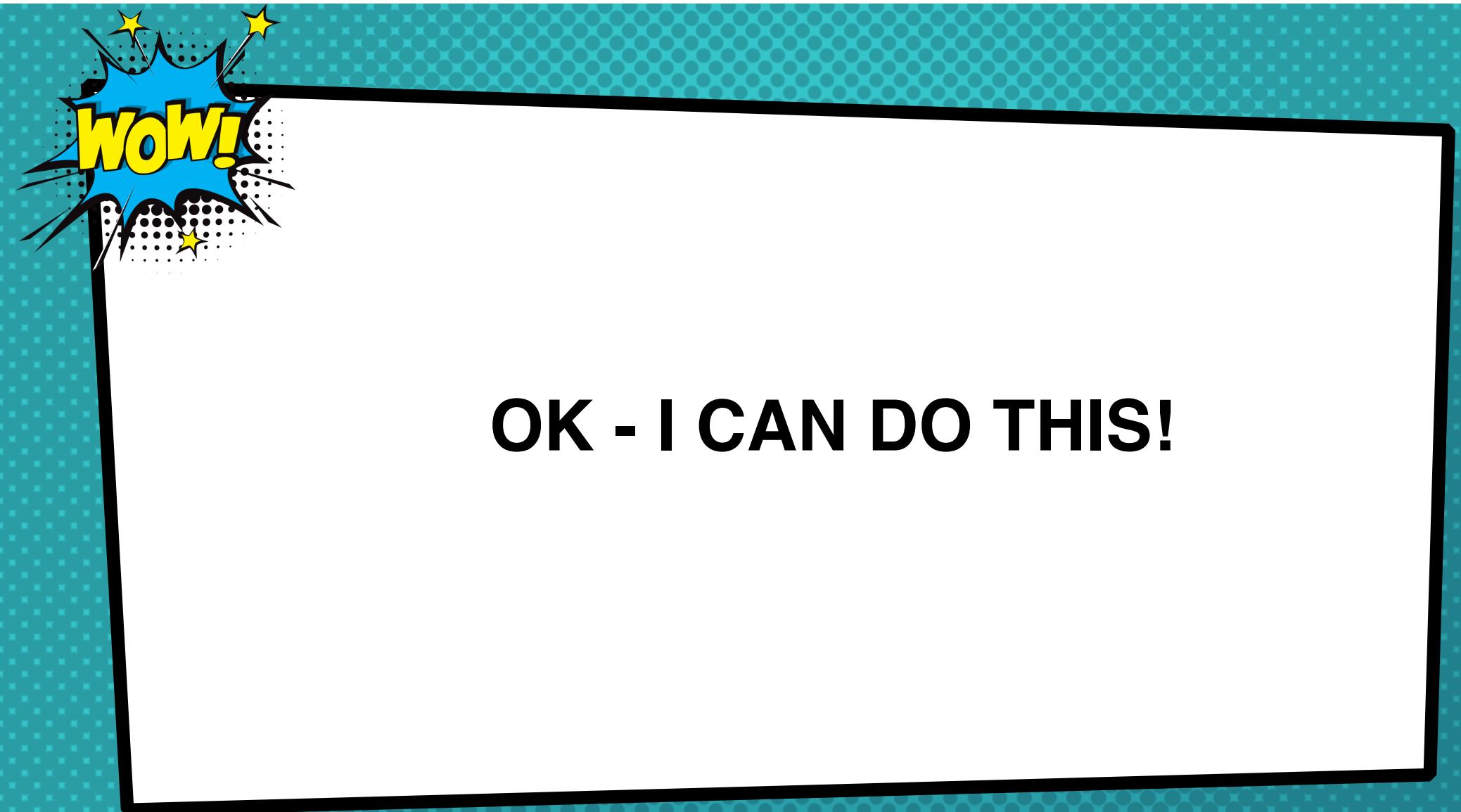
Events Patterns Statistics (5,023) Visualization

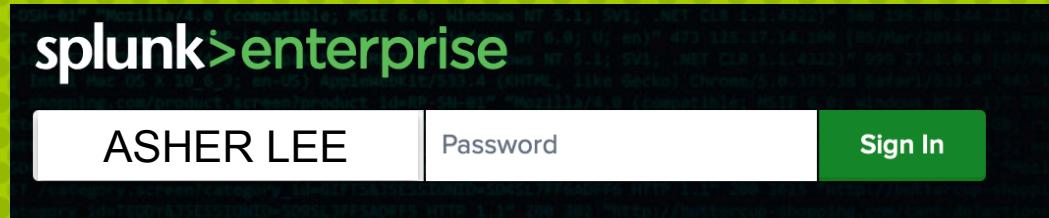
20 Per Page ▾ Format Preview ▾

< Prev 1 2 3 4 5 6 7 8 ... Next >

City	Country	Region	lat	lon	src
Southport	Australia	Queensland	-27.96870	153.41600	61.9.194.171
Southport	Australia	Queensland	-27.96870	153.41600	61.9.227.92
Hobart	Australia	Tasmania	-42.88210	147.32700	61.9.185.54
Melbourne	Australia	Victoria	-37.81360	144.96300	61.9.171.205
Sydney	Australia	New South Wales	-33.86880	151.20900	61.9.161.207
Gold Coast	Australia	Queensland	-28.01670	153.40000	61.9.212.83
Melbourne	Australia	Victoria	-37.81360	144.96300	61.9.133.71
Gold Coast	Australia	Queensland	-28.01670	153.40000	61.9.223.124
Melbourne	Australia	Victoria	-37.81360	144.96300	61.9.147.192
Melbourne	Australia	Victoria	-37.81360	144.96300	61.9.156.105







WOOF



TweetOfAsh



/asherlee/

What  
Problem  
Are  
You  
Solving?



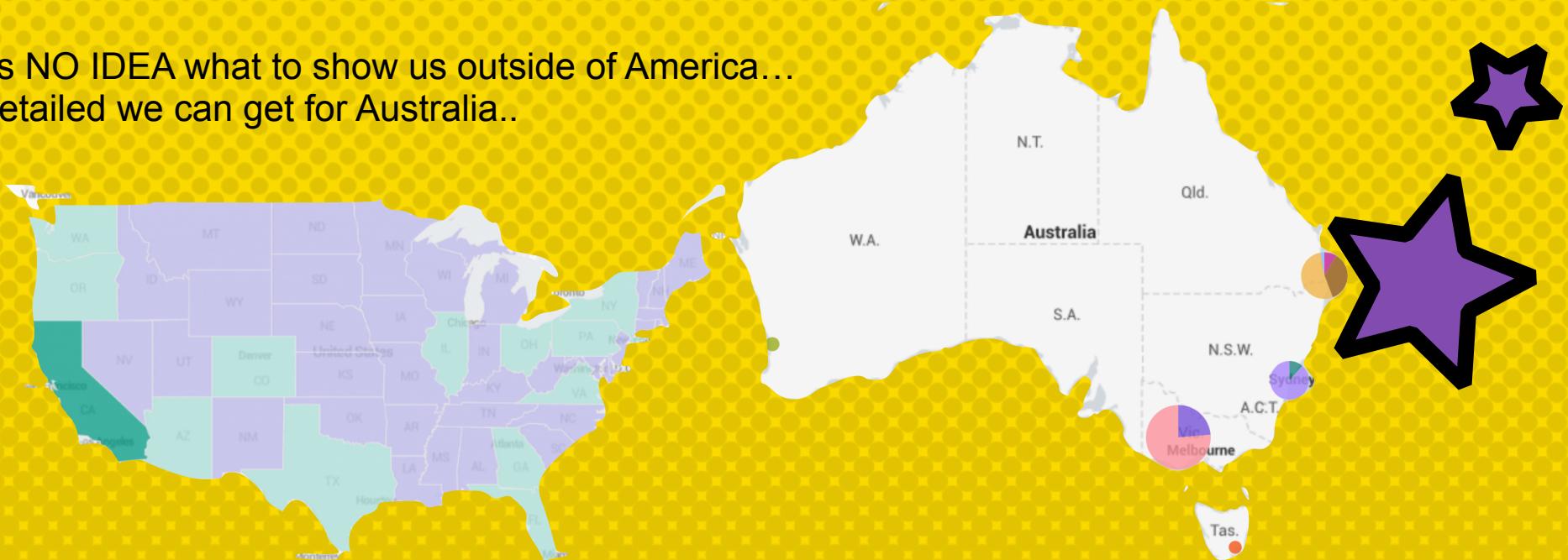


# WHATS WRONG ANYWAY?

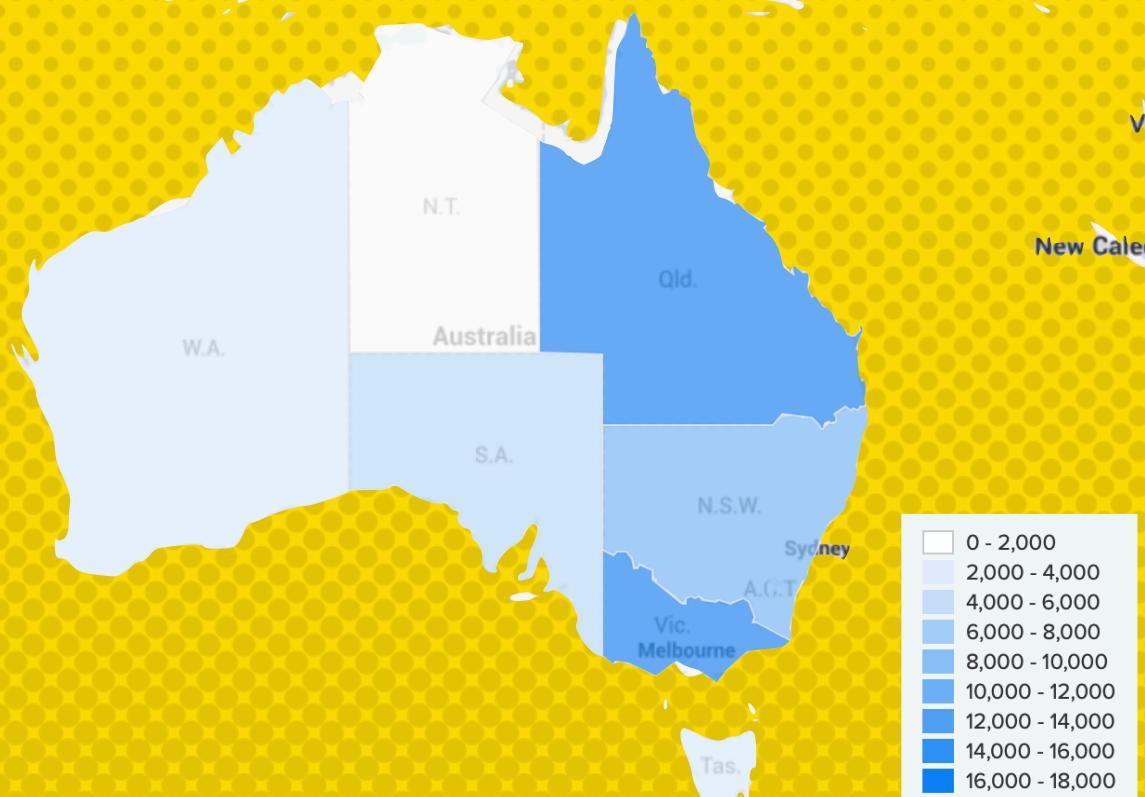


# Choropleth vs Cluster Maps

The System has NO IDEA what to show us outside of America...  
I wonder how detailed we can get for Australia..  
LETS GO



# RESULT...?



# What do we need to know?

## iplocation

Lets go maxmind lets go  
MAPPING the IP with a  
Country / City / LGA / Postcode /  
lat / long

## kmz / kml

The important file for geom ...  
how do we know?

## Documentation?

Yes there is splunk docs.. lets  
search Choropleth & geom

## iplocation

### geom

## Cluster Maps

Used to supply the map  
bounds for Choropleth maps...  
this is helpful if data is  
not found it!

## geom

### Lookups:

## kmz

- Has an option for GeoIP

Lookup file examples:

- geo\_attr\_countries.csv

## Documentation

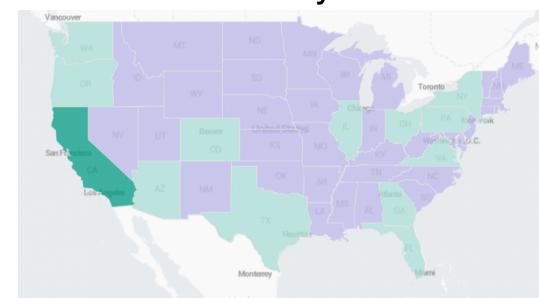
?#^@!

## Cluster Maps

Working...

## Choropleth Maps

DOES NOT WORK FOR  
AUSTRALIA or anywhere  
outside the USA really...



# Some more IP Geolocations ...

- 1. ipstack
- 2. Positionstack
- 3. ipapi
- 4. Abstract API
- 5. ipdata
- 6. Maxmind
- 7. IP Geolocation API by WhoisXML
- 8. IP-API
- 9. ipgeolocation
- 10. Ipify
- 11. IPwhois
- 12. Ipregistry
- 13. IP2Location
- 14. DB-IP
- 15. IPInfo

<https://geekflare.com/geolocation-ip-api/>

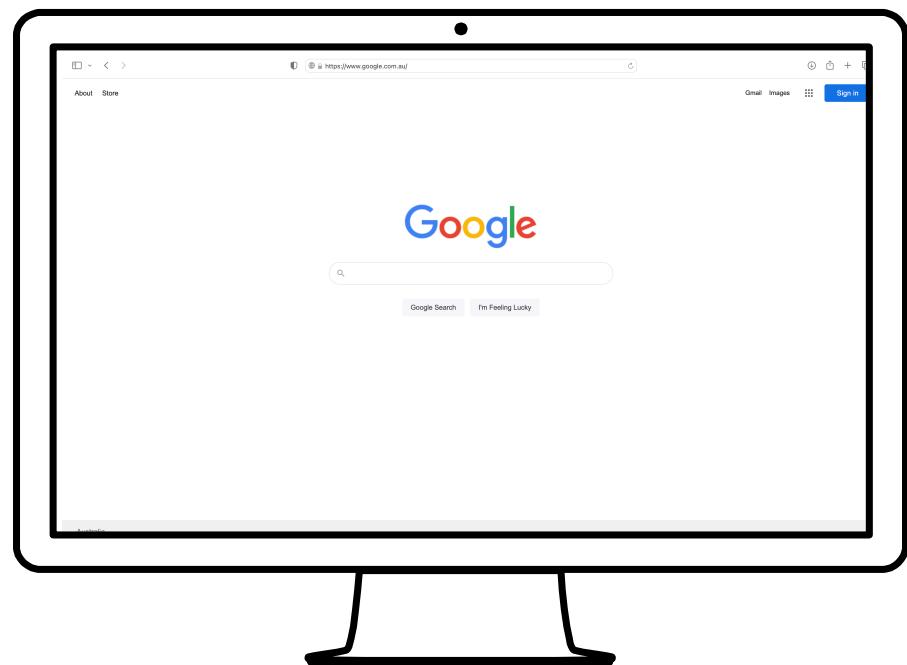
# Lets go geom, lets go!

What kind of problem is this?

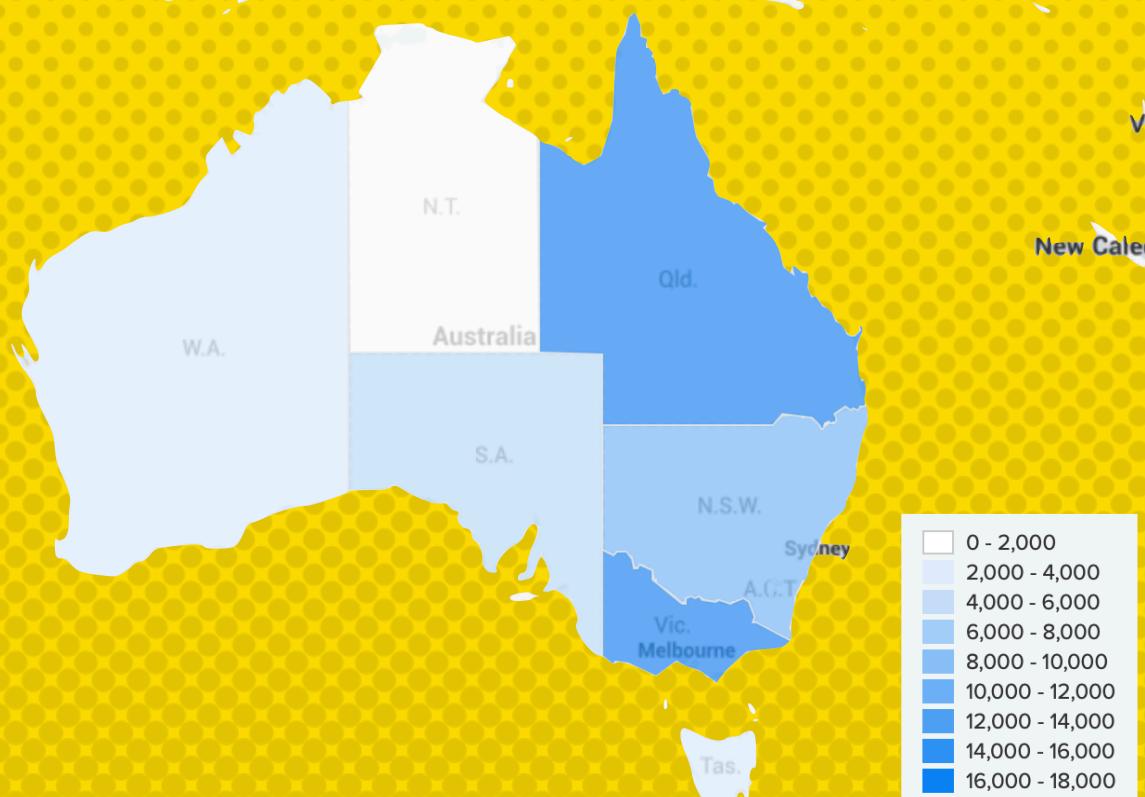
Why doesn't it populate?

What kind of data is missing?

What is geom?



★ That's our AU State Borders...



# GEOM Maxmind extra

Continent

Country (Inc EU Country)

Country of Registration

Subdivisions (regions)

City Name

Postal Code (Outside USA)

Latitude / Longitude

Accuracy Radius (km)

Metro Code (USA only)

Time zone

GeoNames IDs



The screenshot shows a web browser displaying the Maxmind GeoIP2 Databases Demo page. The URL in the address bar is [www.maxmind.com/en/geolp2-demo](http://www.maxmind.com/en/geolp2-demo). The page has a header with the Maxmind logo and navigation links for Products, Support, Developers, Company, Blog, and Contact. A search bar is also present. The main content area is titled "GeoIP2 Databases Demo". It features a text input field labeled "IP Addresses" containing the entries "61.9.255.235,61.9.229.251,61.9.131.101". Below this is a note: "Enter up to 25 IP addresses separated by spaces or commas. You can also test your own IP address." A "Submit" button is located below the input field. The results are displayed in a table titled "GeoIP2 City Plus Database Results". The table has columns for IP Address, Country Code, Location, Network, Postal Code, Approximate Coordinates\*, Accuracy Radius (km), ISP, Organization, Domain, and Metro Code. The data for the three IP addresses is as follows:

IP Address	Country Code	Location	Network	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
61.9.255.235	AU	Port Lincoln, South Australia, Australia, Oceania	61.9.255.0/24	5606	-34.7256, 135.8969	1000	Telstra Internet	Telstra Internet		
61.9.229.251	AU	Port Lincoln, South Australia, Australia, Oceania	61.9.228.0/22	5606	-34.7256, 135.8869	1000	Telstra Internet	Telstra Internet	bigpond.net.au	
61.9.131.101	AU	Melbourne, Victoria, Australia, Oceania	61.9.130.0/23	3003	-37.8159, 144.9669	200	Telstra Internet	Telstra Internet		

At the bottom of the results table, there is a note: "Is this data incorrect? Please submit correction requests [here](#). You may also be interested in [reading more about geolocation accuracy](#) on our knowledge base." A "Help" link is located in the bottom right corner of the page.

# ZOOM ZOOM ... (Not the chat kind)



Zoom only goes so deep...



What are Map Tiles?



How do I get some?



# ZOOM ZOOM ZOOM (EVEN MORE ZOOM...)



More detail than google?



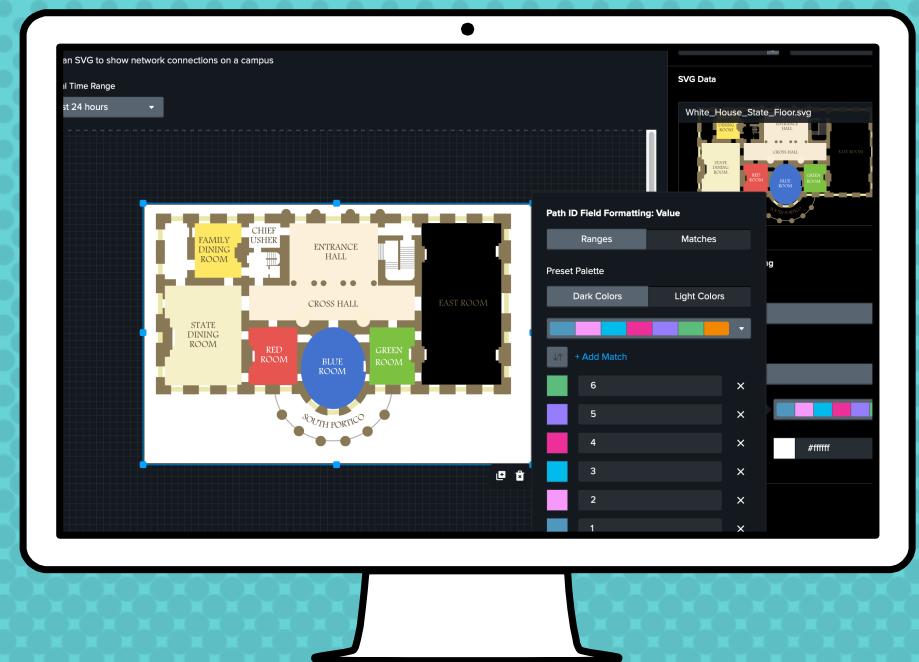
Lets consider...



SVG - An office layout?



WiFi Usage / Density ?



# ZOOM ZOOM ZOOM (EVEN MORE ZOOM...)



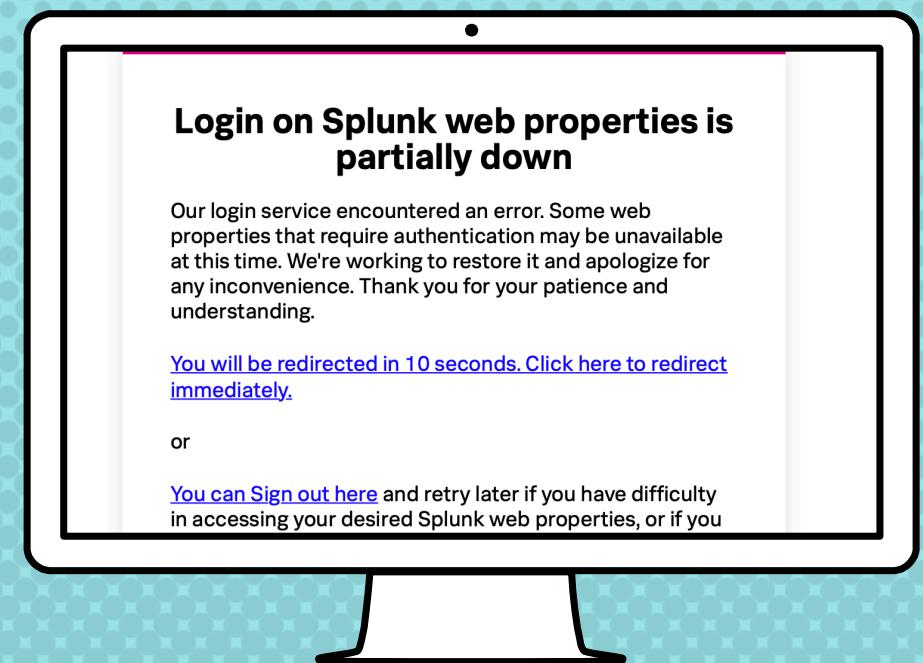
More detail than google?



Lets consider...



SVG - People Finder?



# Management...

Your data can come from a lot of places...

GEOIP & Shipping Address are popular

Chloropleth Maps make data visual.

Visualisation make a story.

Managers like visual stories.

Good story telling can increase budgets

Better budgets mean more toys for us!

Be-ware the toxic workplace and the toxic manager

# QUESTIONS?

# THANKS!

