IP GeoLocation

- To deal with country regulations
- To provide localized content
- Troubleshooting
- Research
Who is Doing It?

MaxMind: https://support.maxmind.com/geoip-data-correction-request/

dbip: https://db-ip.com/report/?addr=___YOUR_IP___

IP Info: https://ipinfo.io/contact?s=correction

RIPE IPmap:
   https://ipmap.ripe.net/api/v1/crowdsource/_IP_OR_PREFIX_

IPdata.co: support@ipdata.co

IP2Location: support@ip2location.com

IPhub: https://iphub.info/contact

IPIP: support@ipip.net

IPligence: https://www.ipligence.com/contact

Neustar's IP GeoPoint: N/A - try generic support

NetAcuity: N/A - try generic contact
And if Your Data Are Incorrect You Have to Contact Every one of Them!
There is no There There

- No Central Repository
- No Common Strategy
- No Authoritative Data
- Many companies have their own dataset
- Or enrich datasets of geolocation providers
How Do They Do It?

- **WhoIs Data**
- **DNS**
- **Lots of Strange Magic**
- **And now GeoFeeds (RFC 8805)!**

```plaintext
# Geofeeds File for RGnet IP Address Space
# 2020.11.09

147.28.0.0/20,US,US-WA,Seattle,
192.83.230.0/24,US,US-WA,Seattle,
198.133.206.0/24,MK,,Skopje,
198.180.150.0/24,US,US-VA,Ashburn,
198.180.152.0/24,US,US-TX,Dallas,
```
GeoFeeds

- Format for self-published IP geolocation feeds 
  RFC 8805
- Only if/what operator wants to publish
- Flexible
  - Geolocate single IPs or entire prefixes (longest prefix match)
  - Geolocate at whatever level you wish (from nothing to city)
- Adopted by Google and many geolocation providers
Discussion of the GeoFeeds File Format is in the GeoFeeds WG

(there isn't one)
But How Do You Find the GeoFeed Files?
INETNUM: 147.28.0.0 - 147.28.15.255
NETNAME: RGNET-RSCH-147-0
COUNTRY: EE
ORG: ORG-R047-RIPE
ADMIN-C: RB45695-RIPE
TECH-C: RB45695-RIPE
ABUSE-C: AR52766-RIPE
STATUS: LEGACY
NOTIFY: rw@rg.net
MNT-BY: MAINT-RGNET
REMARKS: Geofeed https://rg.net/geofeed
SOURCE: RIPE
remarks:

You Must Be Kidding!
| **inetnum:**       | 147.28.0.0 - 147.28.15.255 |
| **netname:**       | RGNET-RSCH-147-0          |
| **country:**       | EE                        |
| **org:**           | ORG-R047-RIPE             |
| **admin-c:**       | RB45695-RIPE              |
| **tech-c:**        | RB45695-RIPE              |
| **abuse-c:**       | AR52766-RIPE              |
| **status:**        | LEGACY                    |
| **notify:**        | rw@rg.net                 |
| **mnt-by:**        | MAINT-RGNET               |
| **geofeed:**       | https://rg.net/geofeed    |
| **source:**        | RIPE                      |

In the rpsl WG. Oh, there isn't one 😊
% whois -h whois.ripe.net 147.28.0.62
inetnum: 147.28.0.0 - 147.28.15.255
netname: RGNET-RSCH-147-0
country: EE
org: ORG-R047-RIPE
admin-c: RB45695-RIPE
tech-c: RB45695-RIPE
abuse-c: AR52766-RIPE
status: LEGACY
mnt-by: MAINT-RGNET
remarks: Geofeed https://rg.net/geofeed
source: RIPE # Filtered
Scope!

# Geofeeds File for RGnet IP Address Space
# 2020.11.09
#
147.28.0.0/20,US,US-WA,Seattle,
#
192.83.230.0/24,US,US-WA,Seattle,
#
198.133.206.0/24,MK,,Skopje,
#
198.180.150.0/24,US,US-VA,Ashburn,
198.180.152.0/24,US,US-TX,Dallas,

Covered by Four inetnum:s
Use the Longest Match inetnum:
And only what is covered by it
A Bit of Detail

• inetnum: and inet6num:, of course

• Multiple inet[6]num: can refer to the same geofeed file iff the file is not signed!

• Serve GeoFeed data over HTTPS, please

• An optional authenticator MAY be appended
  • Is the Geofeed data authorized by the 'owner'? The inetnum: which points to the geofeed file provides some assurance
  • Additionally, a digest of the main body of the file signed by the private key of the relevant RPKI certificate for the covering prefix can be added

• ARIN uses NetRange, sigh
# Geofeeds File for RGnet IP Address Space
# 2020.11.09
#
198.180.150.0/24,US,US-VA,Ashburn,
198.180.152.0/24,US,US-TX,Dallas,
#
# RPKI Signature: 198.180.150.0/22
# MIIGlwYJKoZIhvcNAQcCoIIGiDCCBoQCAQMxDTALBglghkgBZQMEAgEwDQYLKoZ
# IhvcNAQkQAS+gggSxMIIErTCCA5WgAwIBAgIUJ605QIPX8rW5m4Zwx3WyuW7hZu
# imwYkXpiMxw44EZqDjl36MiWsRDLdgoijBBcGbibwyAfGeR46k5raZCGvxG+4xa
# 08PDTxTfIYwAnBjRBKAqAZ7yX5xHfm58jUXsZJ7Ileq1S7G6Kk=
# End Signature: 198.180.150.0/22
Automation

• You can parse bulk whois data
• Publicly available over FTP for RIPE, LACNIC, AFRINIC, APNIC
• Partially available for ARIN, or
  • You ask bulk access (geo providers already use such data), or
  • You get the NetRanges from bulk and Comments from whois/rdap
There’s an App for That!

https://github.com/massimocandela/geofeed-finder

Steps

Run the binary ./geofeed-finder-linux-x64

See the final geofeed file in result.csv