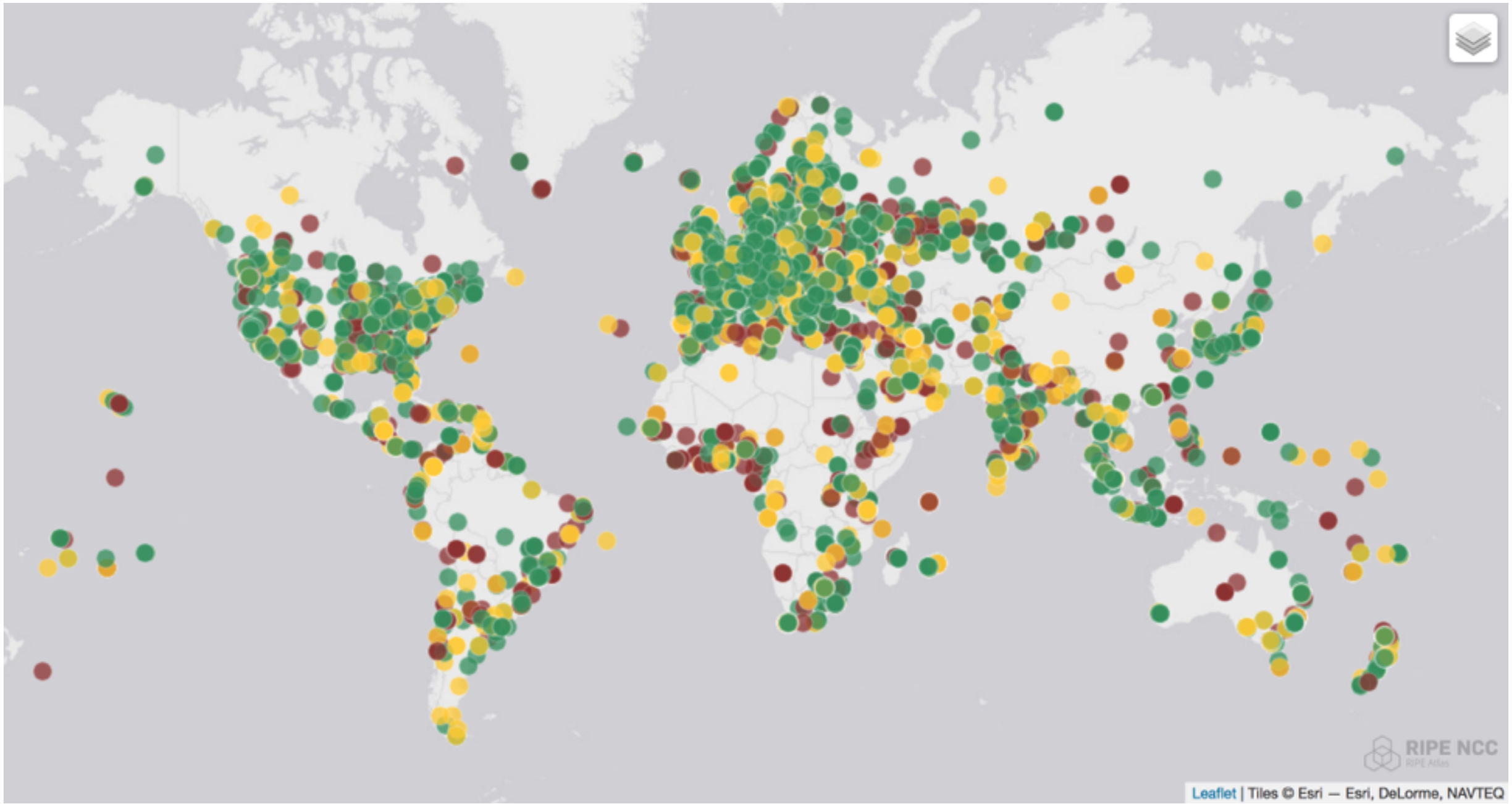
RIPE NCC
RIPE NETWORK COORDINATION CENTRE

How RIPE NCC tools can help with online investigations

Ivo Dijkhuis & Mirjam Kühne | TF-CSIRT 50 | 24-01-2017

The Internet Registry System

RIPE Atlas Coverage

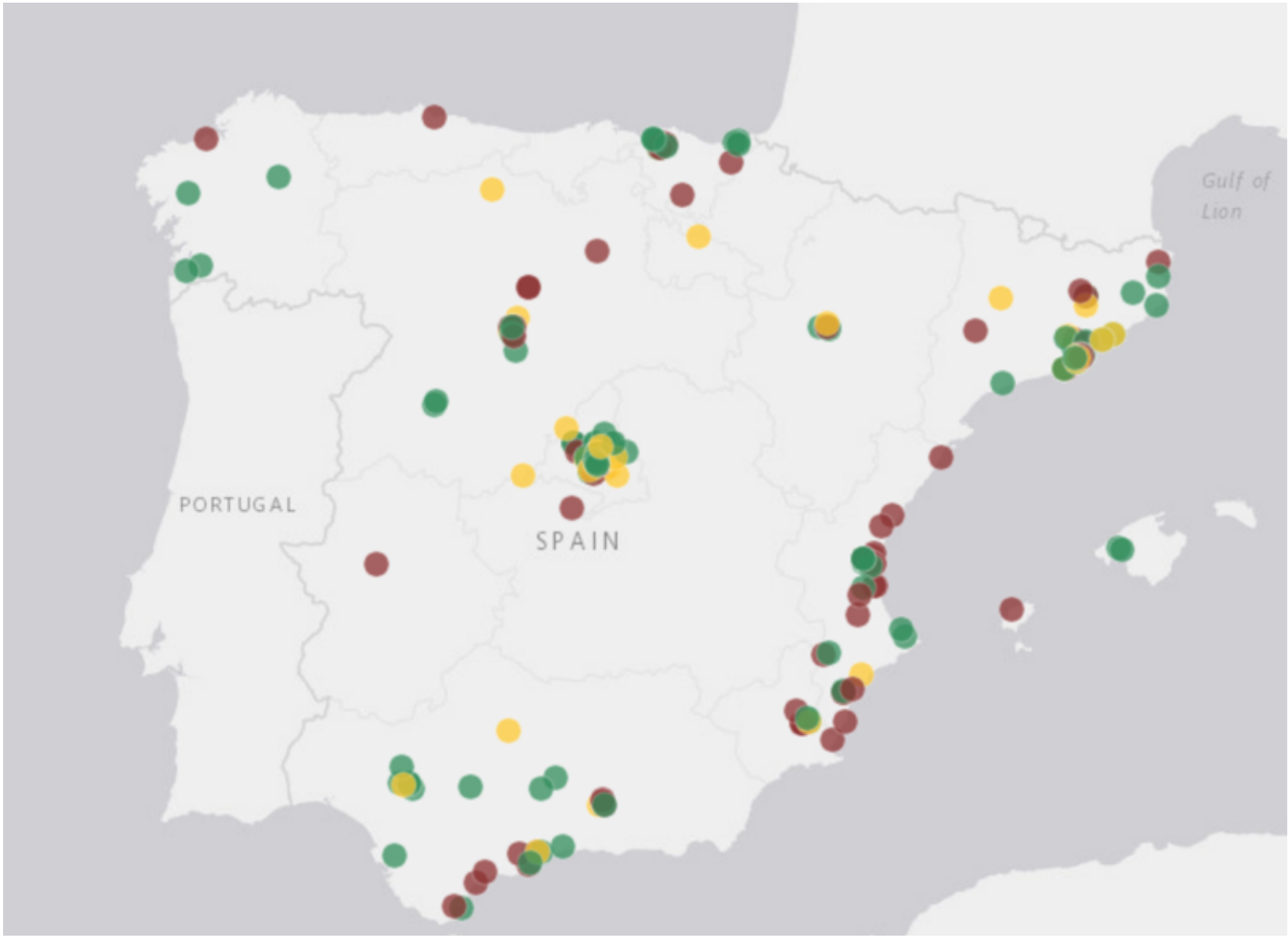


RIPE Atlas - atlas.ripe.net

- RIPE Atlas is a global active measurements platform
- Probes hosted by volunteers
- Data publicly available

"RIPE Atlas: A Global Internet Measurement Network" (PDF). Internet Protocol Journal 18. September 2015. ISSN 1944-1134.

Zoom in to Spain



RIPE Atlas Numbers

- 9,400 RIPE Atlas probes connected worldwide
- 4,100 Measurements collected per second
- 35,000 user-defined measurements per week

RIPE Atlas Measurements

- **Built-in** Global measurements towards root name servers
  - Visualised as Internet traffic maps
- **Built-in** Regional measurements towards RIPE Atlas anchors
- **Users** can run customised measurements
  - ping, traceroute, DNS, SSL/TLS, NTP and HTTP (only towards RIPE Atlas anchors)

Some Features

Most Popular Features

- Powerful and informative visualisations
- APIs to start measurements and get results
- Command line interface
- Streaming data for real-time results
- “Time Travel”

Monitoring using RIPE Atlas

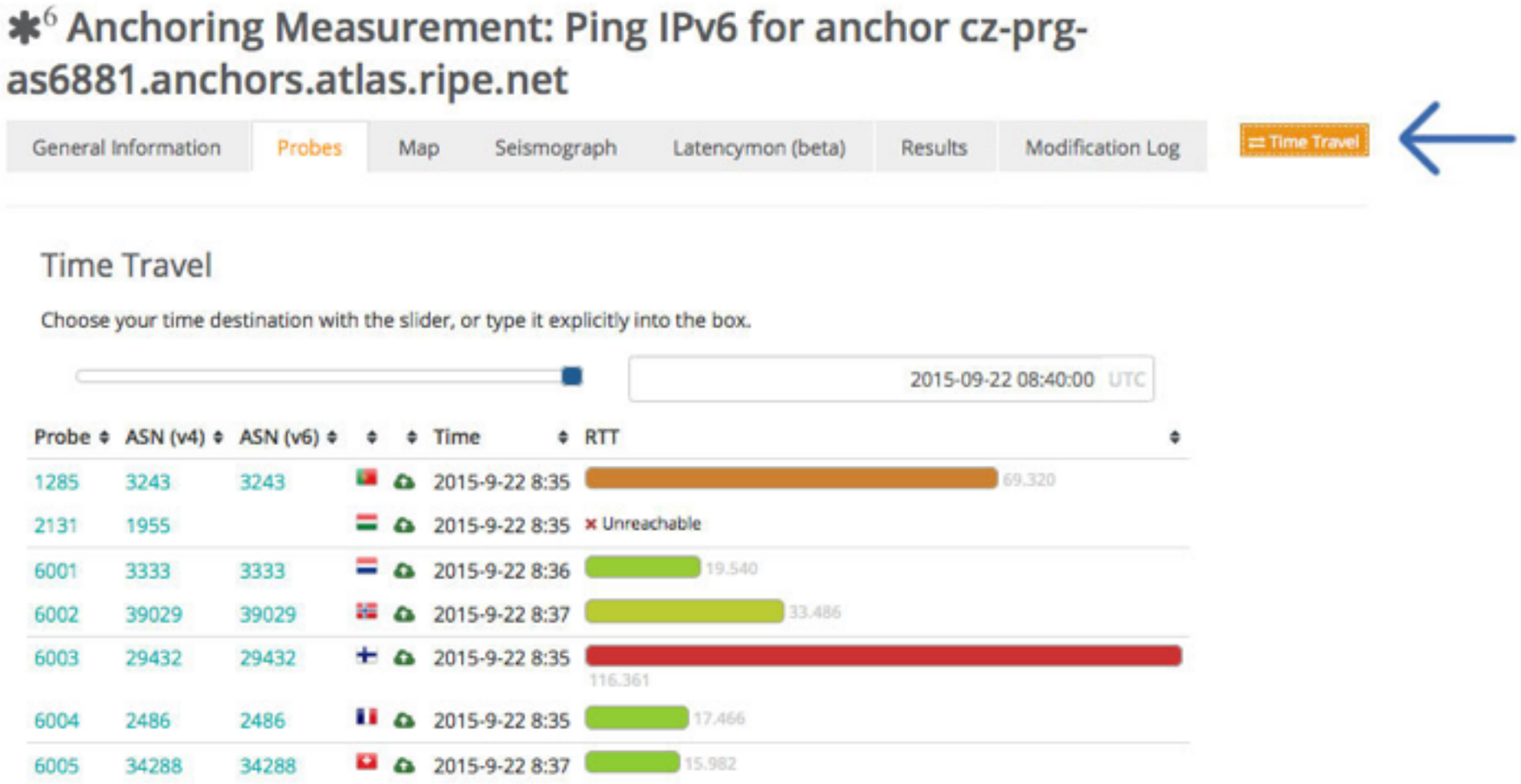
- Integrate “status checks” with existing monitoring tools (such as Icinga, Nagios)

- Using real-time data streaming
  - Server monitoring
  - Detecting and visualising outages

- Developed by community: “RIPE Atlas Monitor”

Time Travel

- Allows you to look at historical data
- For Internet maps and measurement results



Use Cases on RIPE Labs

- Measuring Internet Access Disruptions
  - https://labs.ripe.net/Members/emileaben/internet-access-disruption-in-turkey
  - https://labs.ripe.net/Members/emileaben/internet-access-disruption-in-the-gambia-2016

- Measuring DNS Censorship and Hijacking
  - https://labs.ripe.net/Members/babak_farrokhi/operator-level-dns-redirection
  - https://labs.ripe.net/Members/stephane_bortzmeyer/dns-censorship-dns-lies-seen-by-atlas-probes

Use Cases on RIPE Labs

- Monitoring connectivity and connectivity problems
  - https://labs.ripe.net/Members/annika_wickert/using-ripe-atlas-to-monitor-game-service-connectivity
  - https://labs.ripe.net/Members/jason_read/using-ripe-atlas-to-measure-cloud-connectivity
  - https://labs.ripe.net/Members/stephane_bortzmeyer/using-ripe-atlas-to-debug-network-connectivity-problems

More Information

- https://atlas.ripe.net/
- https://labs.ripe.net/atlas
- Webinars, Training Courses
- Targeted workshops

RIPE WHOIS Database

RIPE Database

- Public Internet resource and routing registry database

- Answers:
  - Who is using an address block?
  - How can I contact them?

- All 5 RIRs have their own database
  - http://www.iana.org/whois

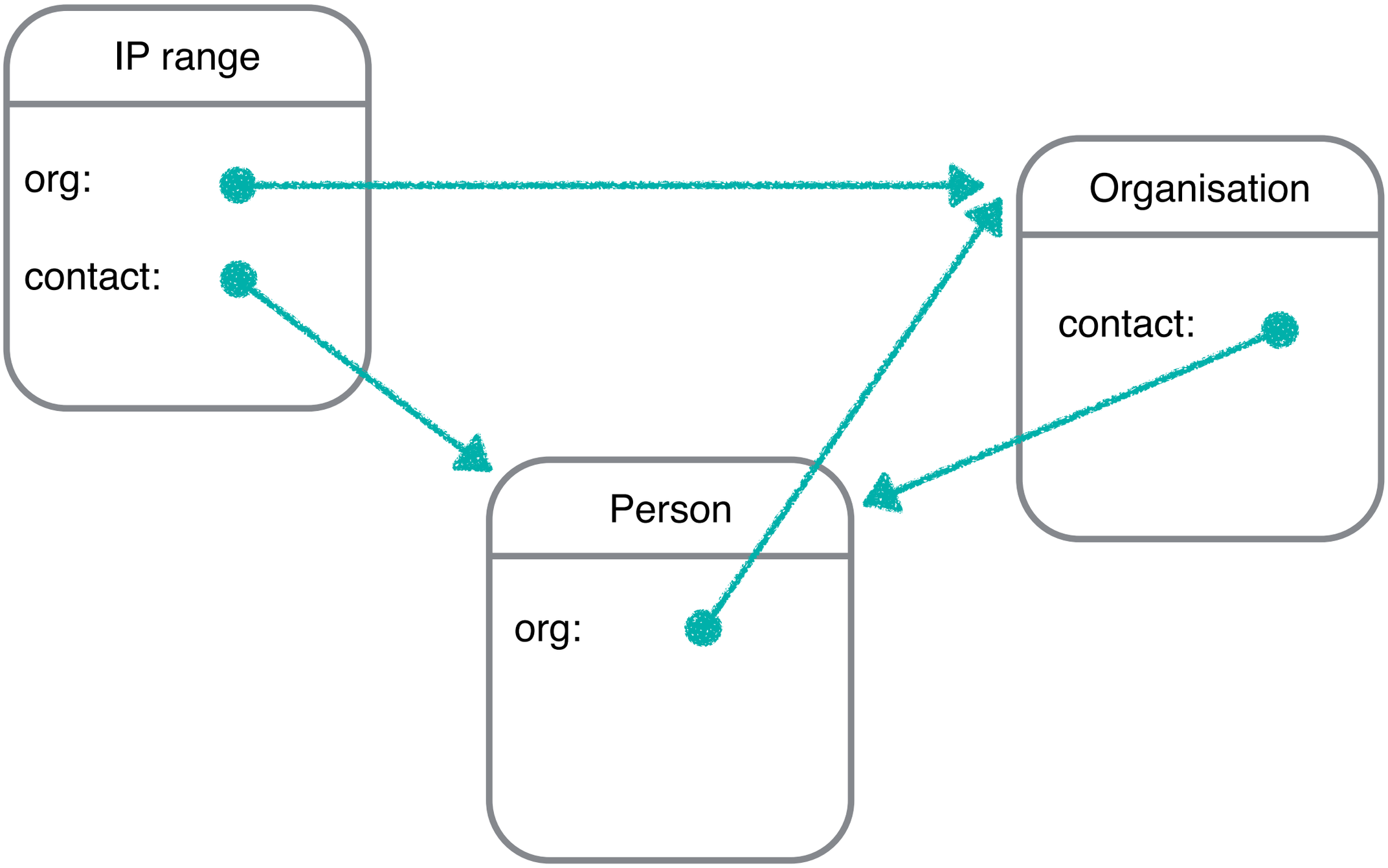
Other Registries

- IANA
  - http://www.iana.org/numbers
- Regional Internet Registries
  - http://whois.arin.net/ui/advanced.jsp
  - http://www.apnic.net/apnic-info/whois_search
  - http://www.afrinic.net/en/services/whois-query
  - http://lacnic.net/cgi-bin/lacnic/whois?lg=EN

RIPE Database Objects

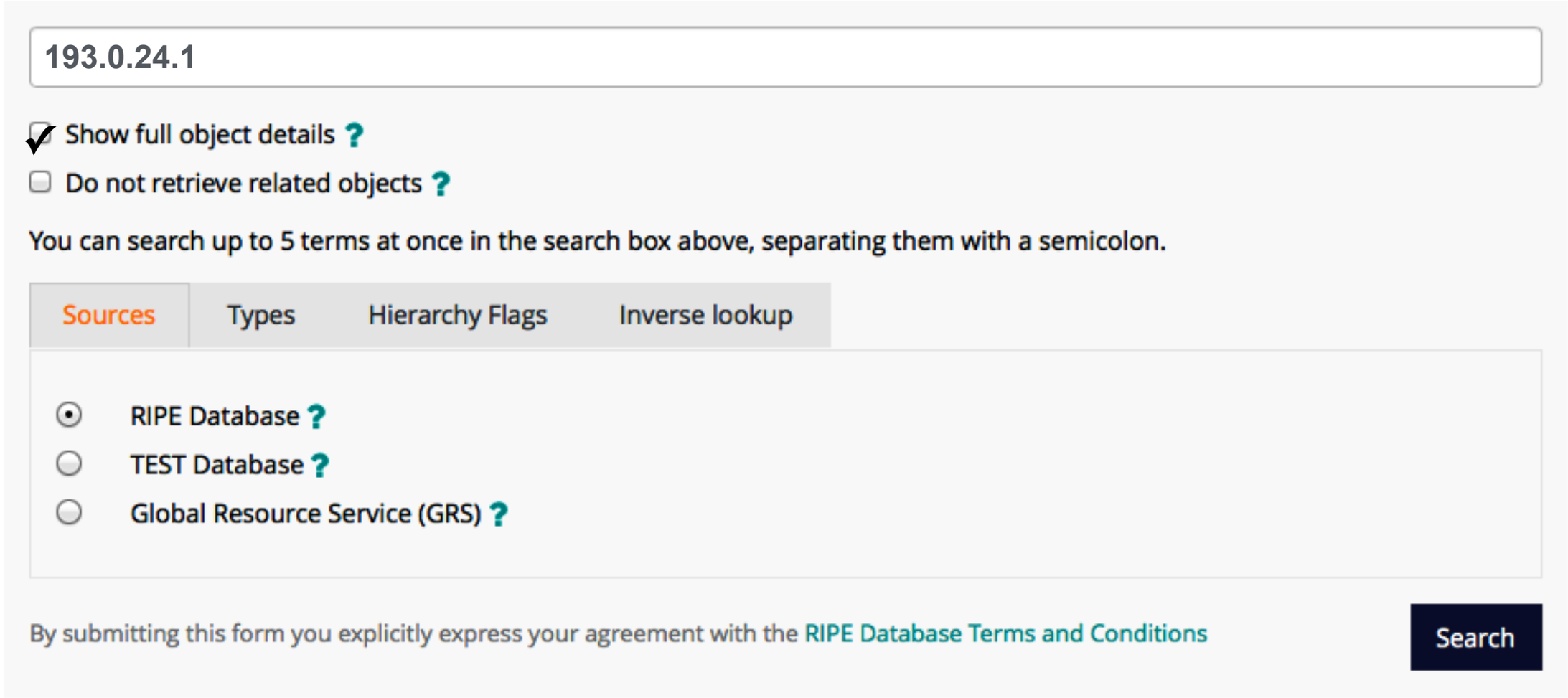
- Resources
  - inetnum, inet6num, aut-num
- Contact
  - organisation, person, role
- Routing
  - route, route6
- Reverse DNS
  - domain
- Object protection
  - mntner

Objects Are Related To Each Other



Querying the RIPE Database

- Web interface
- Command line
- Full Text Search
- Restful API (XML/JSON)

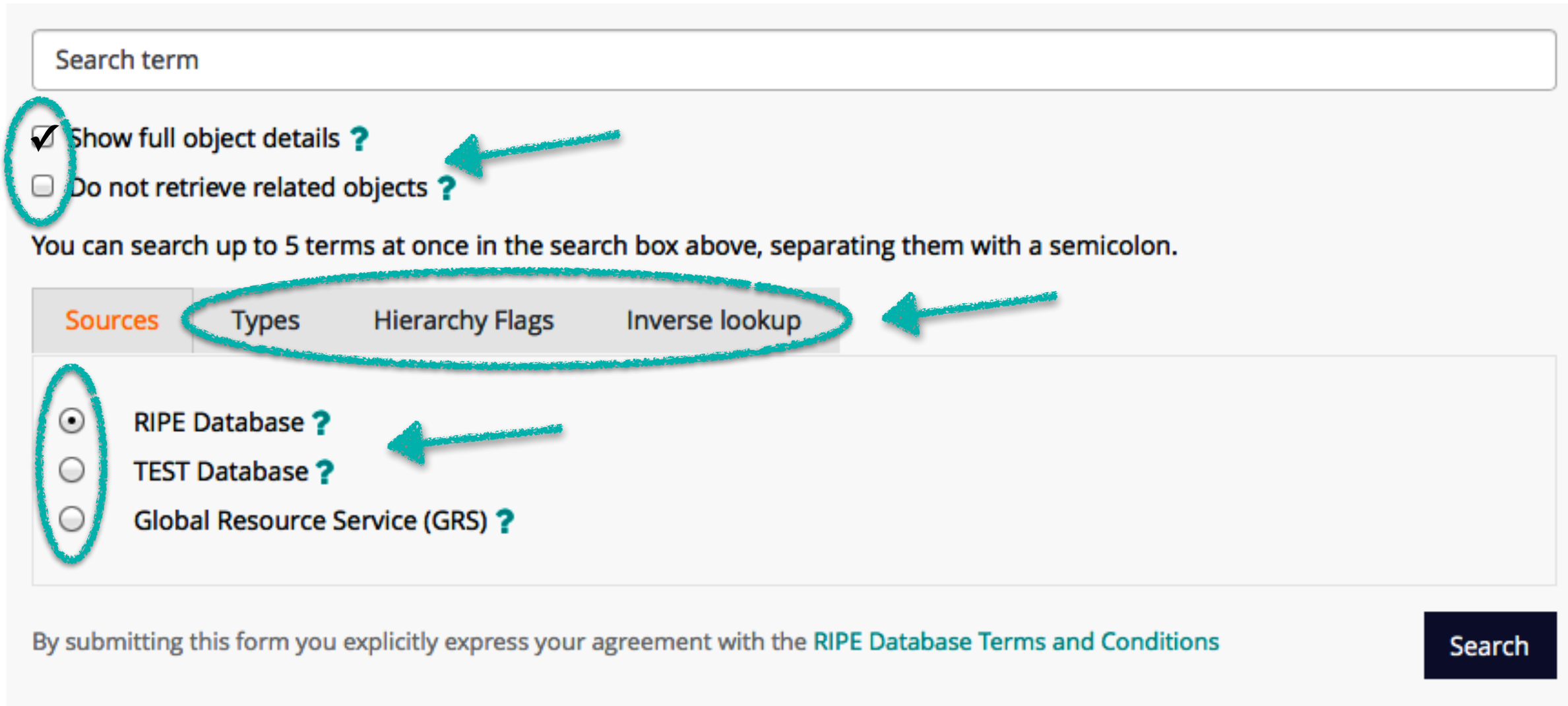


Query Results

```
Responsible organisation: Reseaux IP Europeens Network
Coordination Centre (RIPE NCC)
Abuse contact info: abuse@ripe.net

inetnum:        193.0.24.0 - 193.0.30.255
netname:        RIPENCC-MEETING-PUBLIC
descr:          Reseaux IP Europeens Network Coordination Centre (RIPE NCC)
remarks:        RIPE NCC Training Services & RIPE Meetings
remarks:        This space is used as public space during RIPE meetings
country:        NL
admin-c:        JDR-RIPE
admin-c:        BRD-RIPE
tech-c:         OPS4-RIPE
status:         ASSIGNED PA
mnt-by:         RIPE-NCC-MNT
mnt-routes:     RIPE-NCC-MNT
mnt-domains:    RIPE-NCC-MNT
created:        2013-10-09T14:42:14Z
last-modified:  2013-10-09T14:42:14Z
source:         RIPE
```

Options for Queries



Results With Related Objects

Search term: 193.0.24.1

inetnum: 193.0.24.0 - 193.0.30.255
netname: RIPENCC-MEETING-PUBLIC
descr: RIPE NCC
country: NL
admin-c: JDR-RIPE
admin-c: BRD-RIPE
tech-c: OPS4-RIPE
status: ASSIGNED PA
mnt-by: RIPE-NCC-MNT
created: 2013-10-09T07:58:22Z
last-modified: 2013-10-09T08:34:09Z
source: RIPE

route: 193.0.24.0/21
CKHOLM
MNT
12:17:39Z
0T12:17:39Z

route: 193.0.24.0/21
descr: RIPE-MEETINGS
origin: AS2121
mnt-by: RIPE-NCC-MNT
created: 2008-04-09T11:04:18Z
last-modified: 2012-04-24T10:09:25Z
source: RIPE

role: RIPE NCC Operations
address: Singel 258
addres
addr
phon
f

person: Brian Riddle
address: IT Manager
address: RIPE NCC - Operations

person: Jochem de Ruig
address: RIPE NCC
address: Singel 258
address: 1016AB Amsterdam
address: The Netherlands
phone: +31 20 535 4444
fax-no: +31 20 535 4445
nic-hdl: JDR-RIPE
mnt-by: RIPE-NCC-MNT
created: 2011-02-10T12:04:37Z
last-modified: 2011-02-10T12:04:37Z
source: RIPE

Z

source: RIPE

Results Without Related Objects

Search term: -r 193.0.24.1

inetnum: 193.0.24.0 - 193.0.30.255
netname: RIPENCC-MEETING-PUBLIC
descr: RIPE NCC
country: NL
admin-c: JDR-RIPE
admin-c: BRD-RIPE
tech-c: OPS4-RIPE
status: ASSIGNED PA
mnt-by: RIPE-NCC-MNT
created: 2013-10-09T07:58:22Z
last-modified: 2013-10-09T08:34:09Z
source: RIPE

route: 193.0.24.0/21
descr: RIPE-STOCKHOLM
origin: AS201965
mnt-by: RIPE-NCC-MNT
created: 2015-04-20T12:17:39Z

route: 193.0.24.0/21
descr: RIPE-MEETINGS
origin: AS2121
mnt-by: RIPE-NCC-MNT
created: 2008-04-09T11:04:18Z
last-modified: 2012-04-24T10:09:25Z
source: RIPE

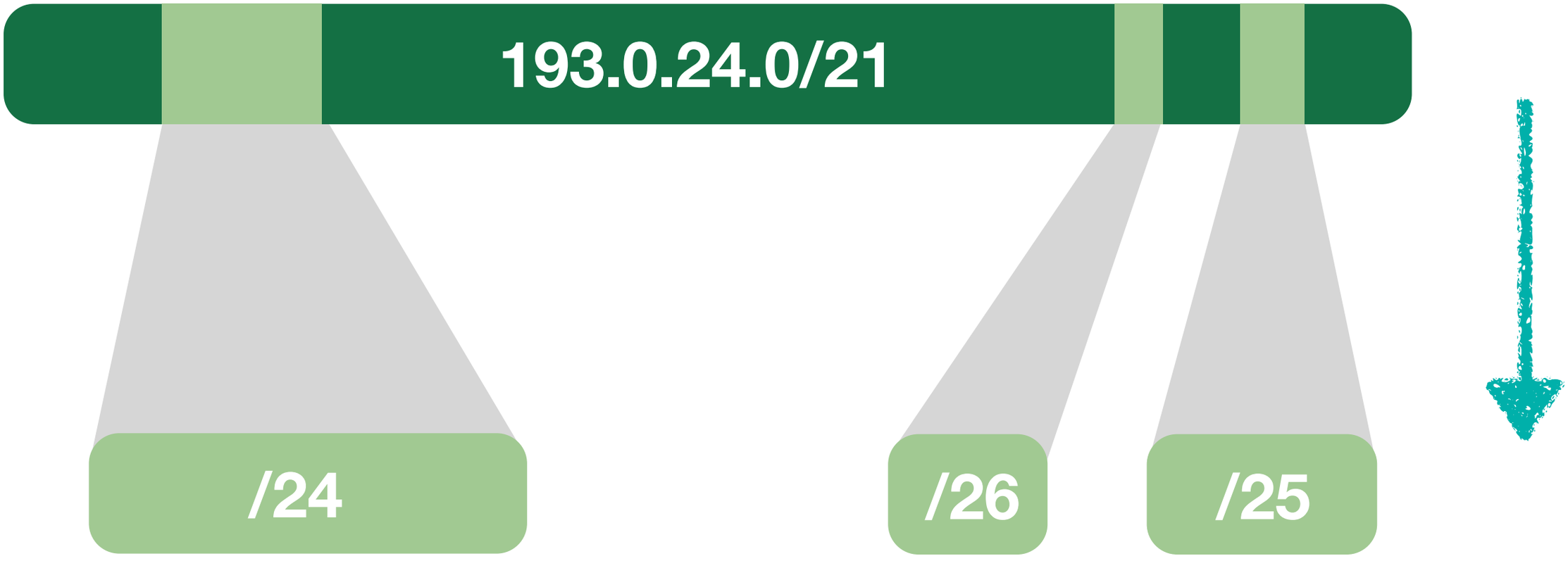
Navigating the Hierarchy

- With IP space, you want to find what is under or above the inetnum object
  - Under = More Specific
  - Above = Less Specific

- There are flags: -m, -M, -l, -L
- Also in the “Hierarchy Flags” tab

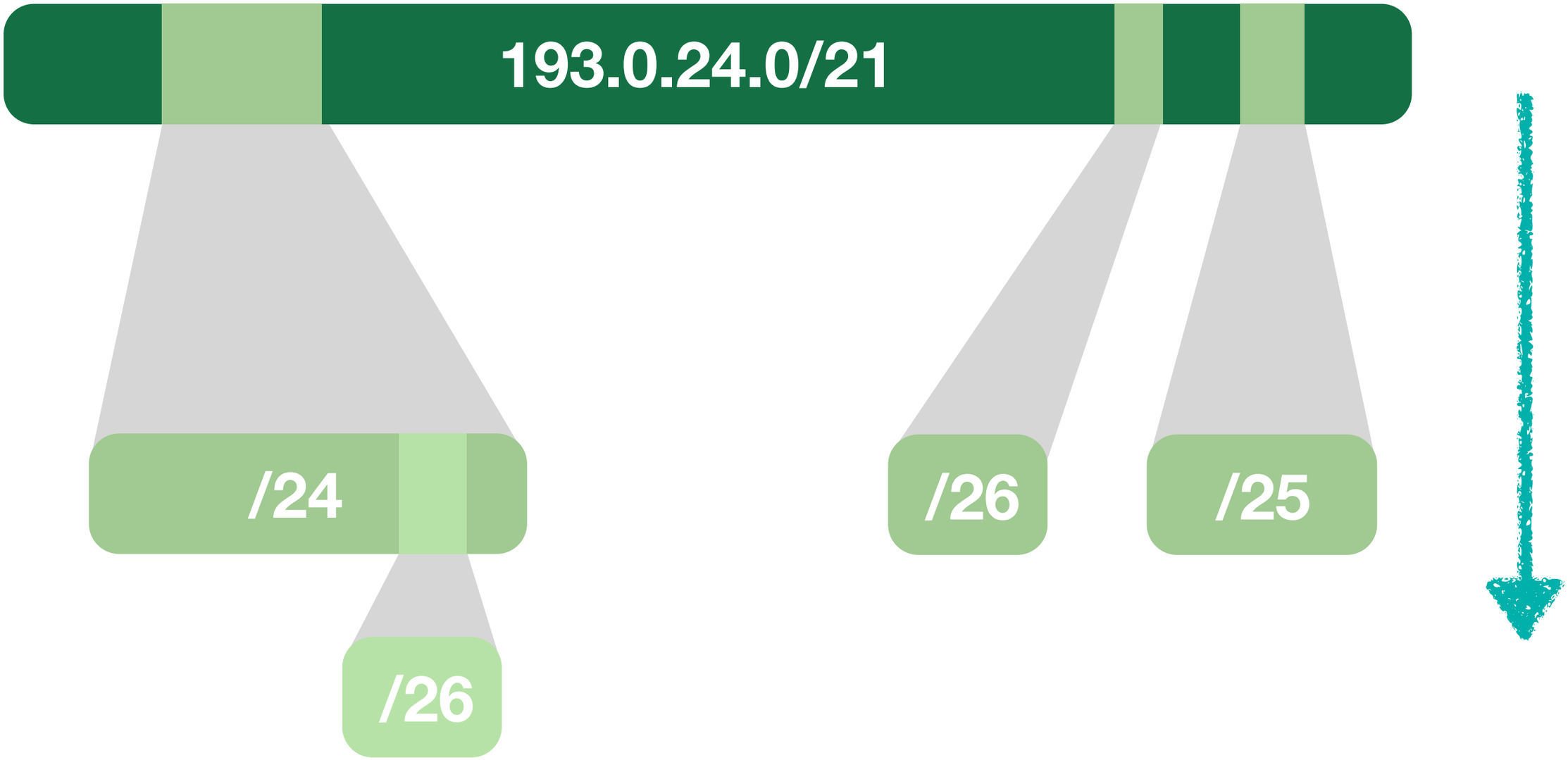
More Specific inetnums: -m

-m 193.0.24.0/21



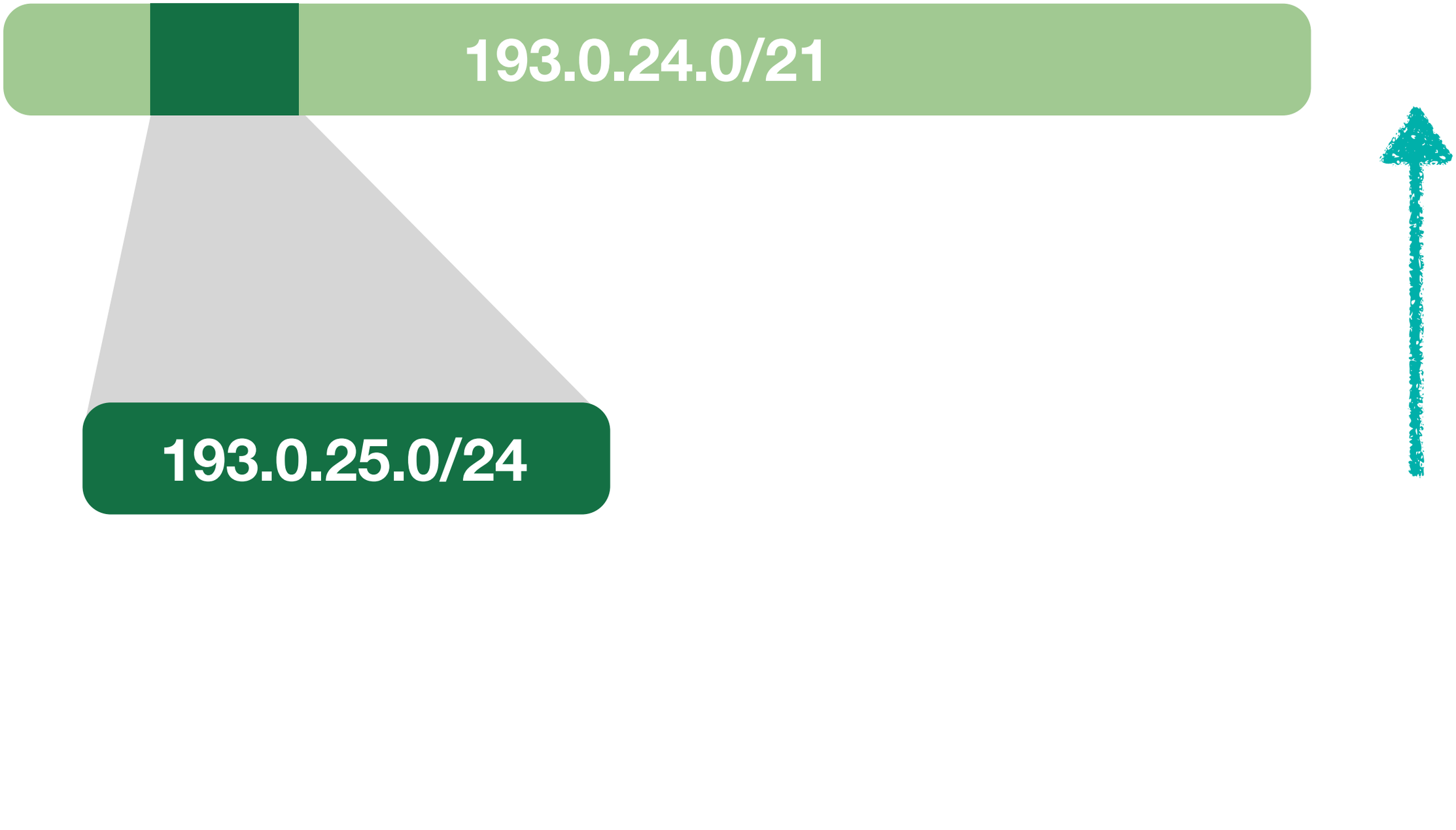
More Specific inetnums: -M

-M 193.0.24.0/21



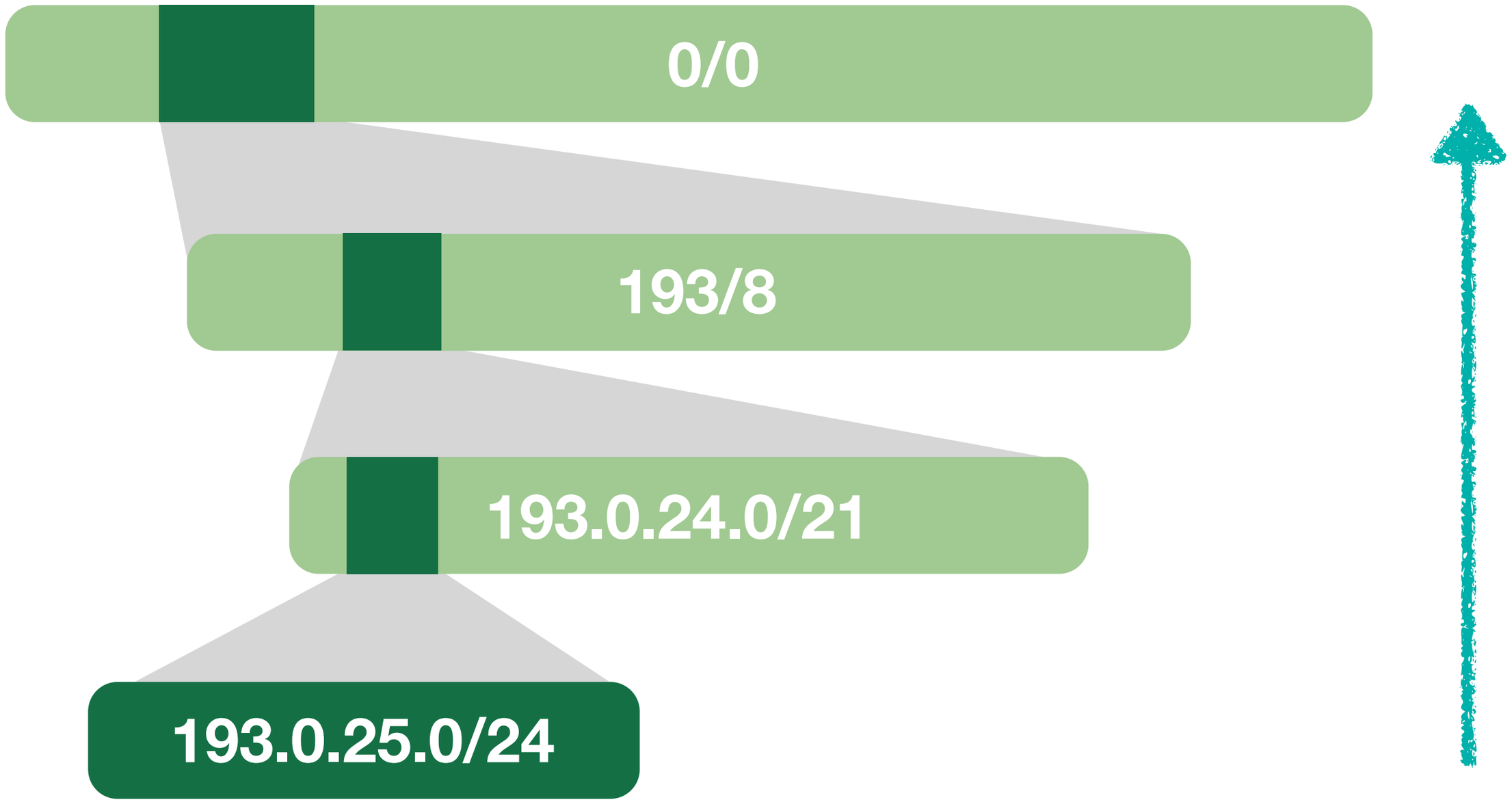
Less Specific inetnums: -l

-l 193.0.25.0/24

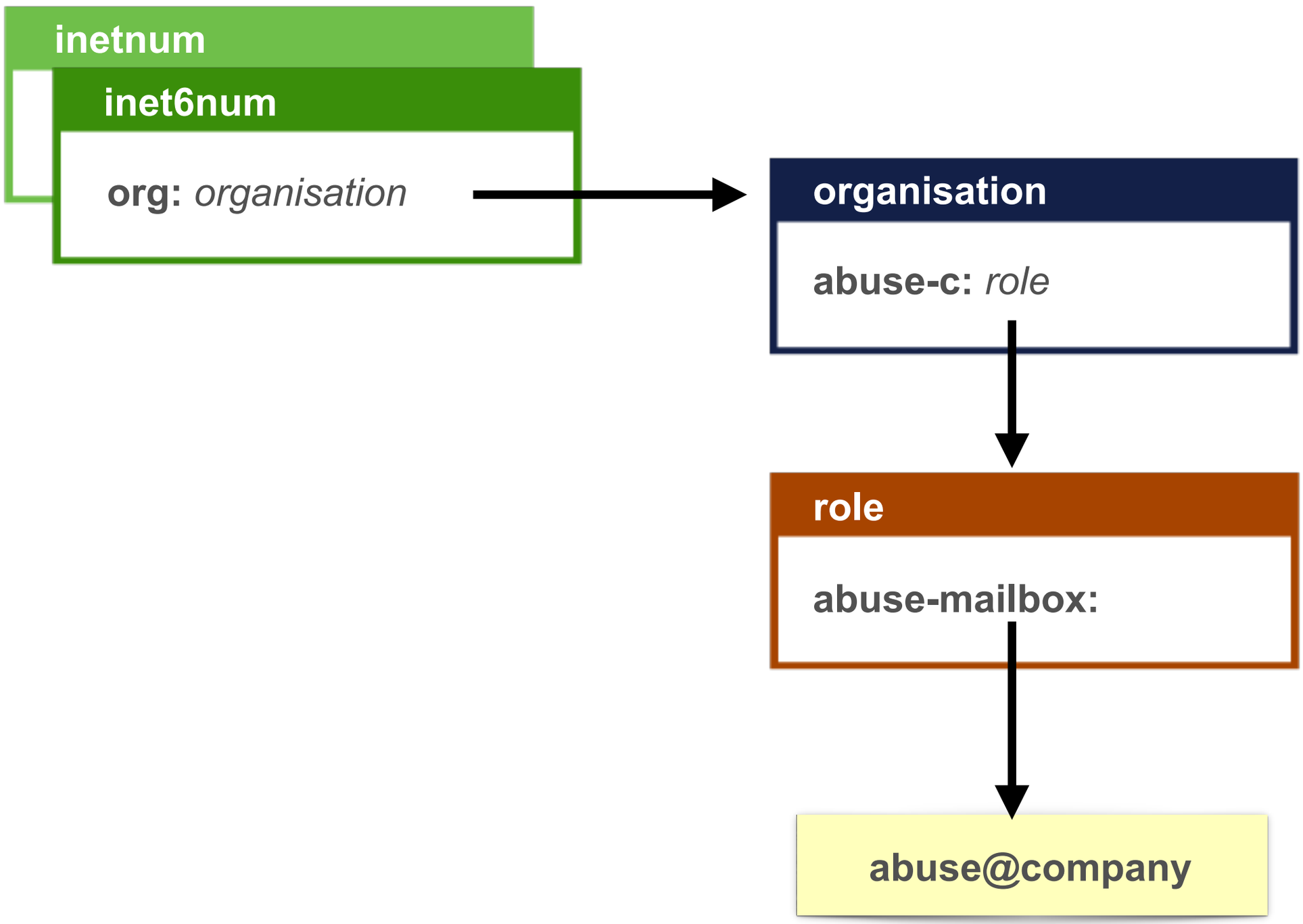


Less Specific inetnums: -L

-L 193.0.25.0/24



Where is the abuse-c?



Inverse Lookup

JD-RIPE

☑ Show full object details ?

☑ Do not retrieve related objects ?

You can search up to 5 terms at once in the search box above, separating them with a semicolon.

Sources | Types | Hierarchy Flags | Inverse lookup

?

☐ abuse-mailbox	☐ member-of	☐ nserver
☐ admin-c	☐ mnt-by	☐ org
☐ auth	☐ mnt-domains	☐ origin
☐ author	☐ mnt-irt	☑ person
☐ fingerpr	☐ mnt-lower	☐ ping-hdl
☐ form	☐ mnt-nfy	☐ referral-by
☐ irt-nfy	☐ mnt-ref	☐ ref-nfy
☐ local-as	☐ mnt-routes	☐ tech-c
☐ mbrs-by-ref	☐ notify	☐ upd-to
		☐ zone-c

By submitting this form you explicitly express your agreement with the RIPE Database Terms and Conditions

Search

Referenced person object

inet6num:	2001:db8::/32
descr:	my IPv6 range
mnt-by:	RIPE-NCC-HM-MNT
org:	ORG-BB2-RIPE
admin-c:	JE777-RIPE
tech-c:	JD1-RIPE

aut-num:	AS64551
descr:	my AS number
mnt-by:	RIPE-NCC-HM-MNT
org:	ORG-BB2-RIPE
tech-c:	JD1-RIPE
tech-c:	LA789-RIPE

mntner:	LIR-MNT
admin-c:	JD1-RIPE
tech-c:	LA789-RIPE
mnt-by:	LIR-MNT

role:	Bluelight Staff
nic-hdl:	BLS77-RIPE
admin-c:	JD1-RIPE
address:	Sesame Street 1
e-mail:	staff@example.org

-i person JD1-RIPE

person:	John Smith
nic-hdl:	JD1-RIPE
address:	Sesame Street 1
phone:	+1 555 0101
e-mail:	john@example.org
mnt-by:	LIR-MNT

Referenced person object

inet6num:	2001:db8::/32
descr:	my IPv6 range
mnt-by:	RIPE-NCC-HM-MNT
org:	ORG-BB2-RIPE
admin-c:	JE777-RIPE
tech-c:	JD1-RIPE

aut-num:	AS64551
descr:	my AS number
mnt-by:	RIPE-NCC-HM-MNT
org:	ORG-BB2-RIPE
admin-c:	**JD1-RIPE**
tech-c:	LA789-RIPE

mntner:	LIR-MNT
admin-c:	**JD1-RIPE**
tech-c:	LA789-RIPE
mnt-by:	LIR-MNT

role:	Bluelight Staff
nic-hdl:	BLS77-RIPE
admin-c:	**JD1-RIPE**
address:	Sesame Street 1
e-mail:	staff@example.org

-i admin-c JD1-RIPE

person:	John Smith
nic-hdl:	JD1-RIPE
address:	Sesame Street 1
phone:	+1 555 0101
e-mail:	john@example.org
mnt-by:	LIR-MNT

Referenced Organisation

inet6num:	2001:db8::/32
descr:	My IPv6 range
org:	**ORG-BB2-RIPE**
admin-c:	JE777-RIPE
tech-c:	JD1-RIPE

inetnum:	85.23.16.0/21
descr:	My v4 allocation
org:	**ORG-BB2-RIPE**
admin-c:	JE777-RIPE
tech-c:	JD1-RIPE

inetnum:	85.111.185.0/21
descr:	Other v4 allocation
org:	**ORG-BB2-RIPE**
admin-c:	JE777-RIPE
tech-c:	JD1-RIPE

aut-num:	AS64551
descr:	my AS number
org:	**ORG-BB2-RIPE**
admin-c:	JE777-RIPE
tech-c:	JD1-RIPE

-i org ORG-BB2-RIPE

organisation:	ORG-BB2-RIPE
admin-c:	JD1-RIPE
tech-c:	LA789-RIPE
abuse-c:	**AR789-RIPE**
mnt-by:	LIR-MNT

Full Text Search

RIPE Database text search

This service allows searches over the full text of the RIPE Database object data.

The search is done on object text without regard for any relationships. Multiple search terms should be separated with a space.

bluelight

Advanced Search

By submitting this form you explicitly express your agreement with the RIPE Database Terms and Conditions

Search

Search results

This is the RIPE Database full text search service.
The RIPE Database is subject to Terms and Conditions.

[1] 2 3

domain: 205.149.82.in-addr.arpa
descr=Reverse delegation for **Bluelight** 2nd/24

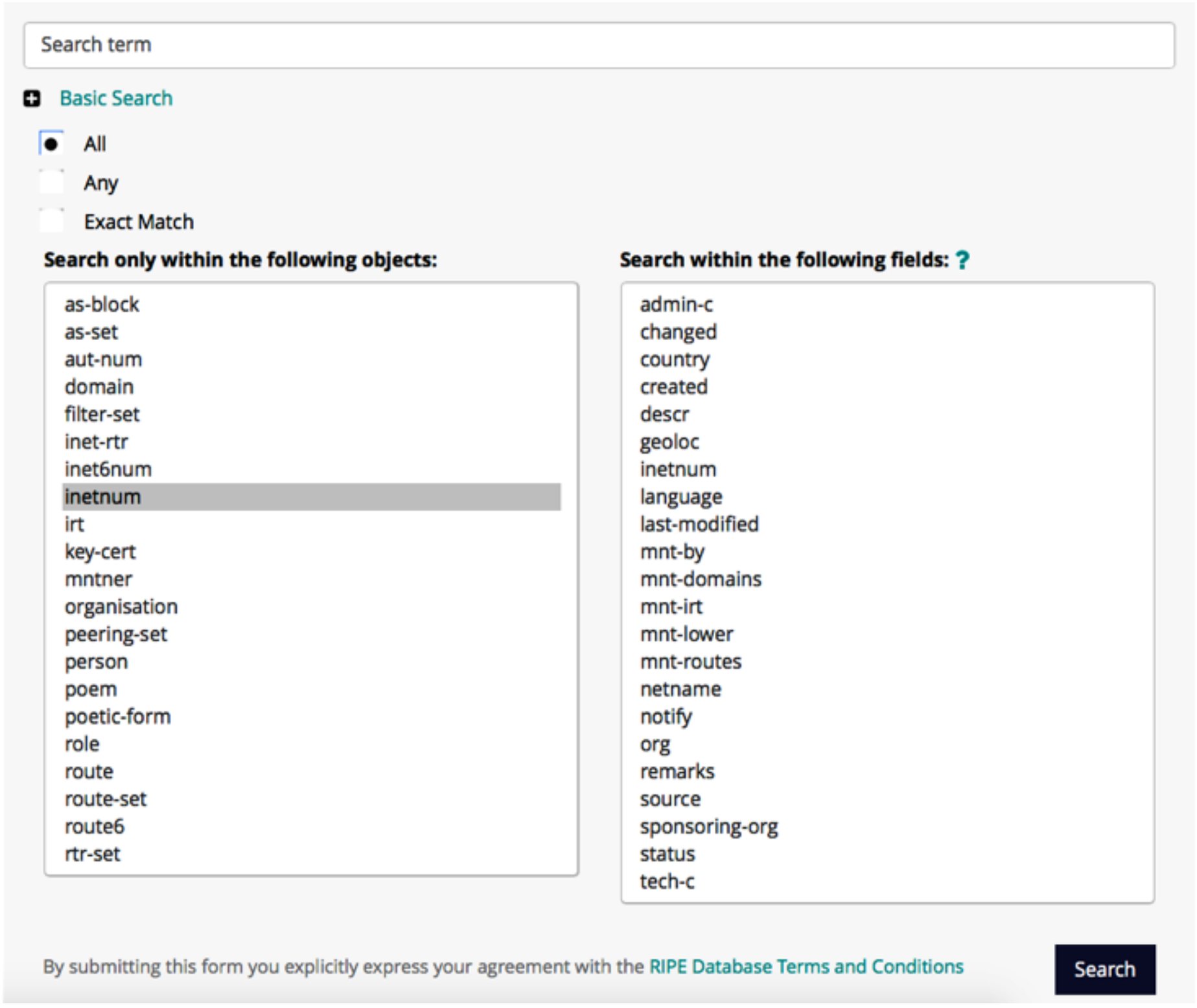
domain: 210.149.82.in-addr.arpa
descr=Reverse delegation for **Bluelight** 2nd/24

domain: 201.156.178.IN-ADDR.ARPA
mnt-by=RO-**BLUELIGHT**, descr=**BLUELIGHT**

domain: 200.156.178.IN-ADDR.ARPA
mnt-by=RO-**BLUELIGHT**, descr=**BLUELIGHT**

inet6num: 2a01:4f8:201:31ea::/64
netname=**BLUE-LIGHT**

Full Text Search - Advanced



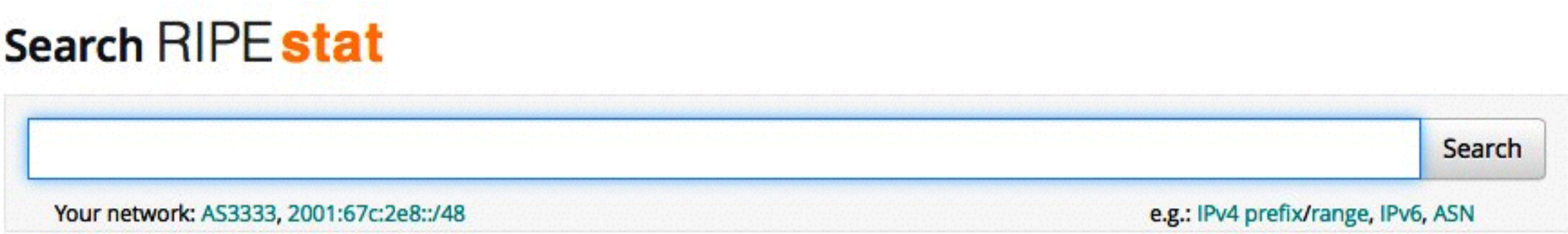
RIPEstat

Explanation

What is RIPEstat?

- One interface for multiple data sources

http://stat.ripe.net/



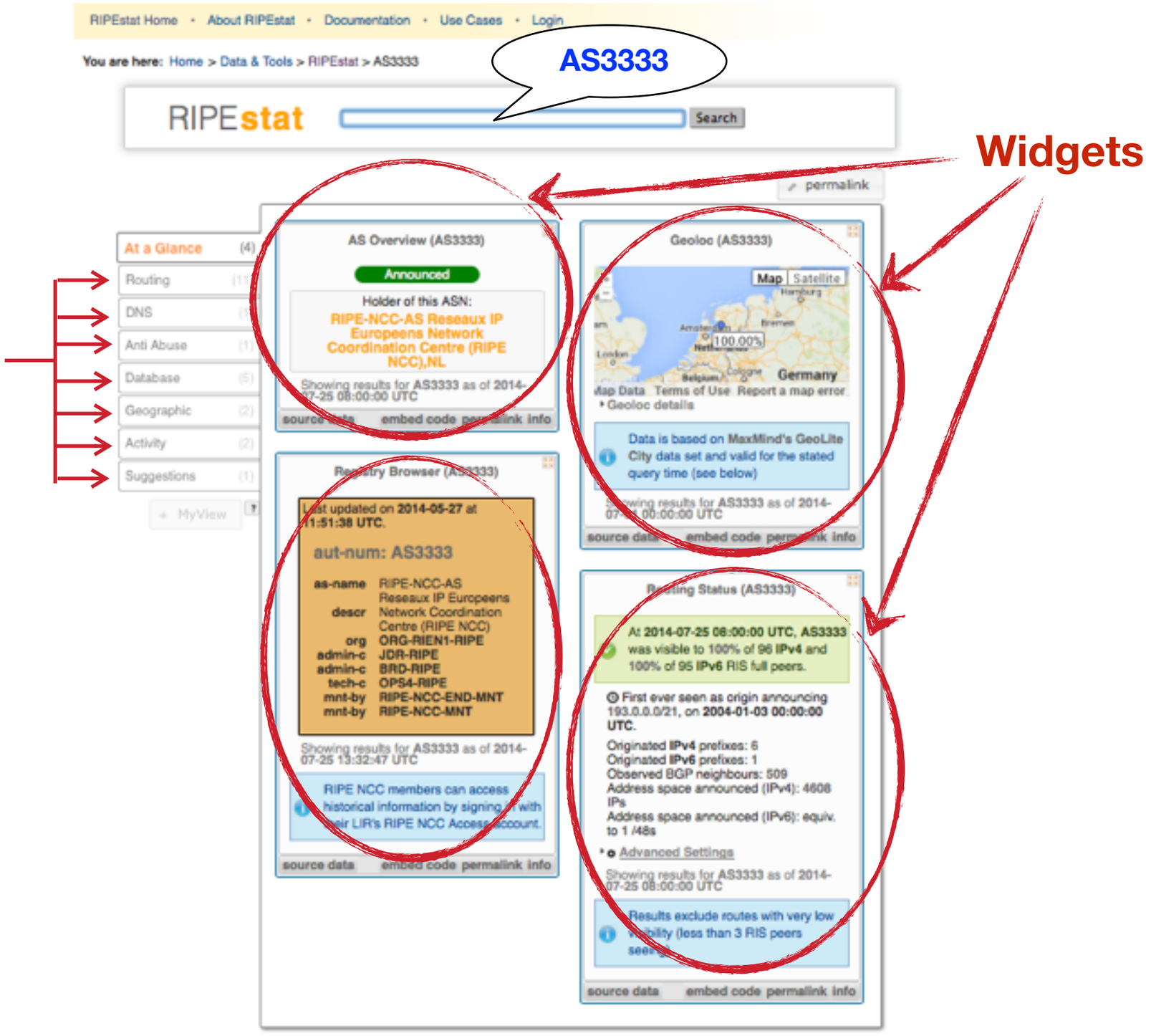
What can you query?

- IPv6 address
- IPv4 address
- ASN
- Hostname
- Country code

RIPEstat:

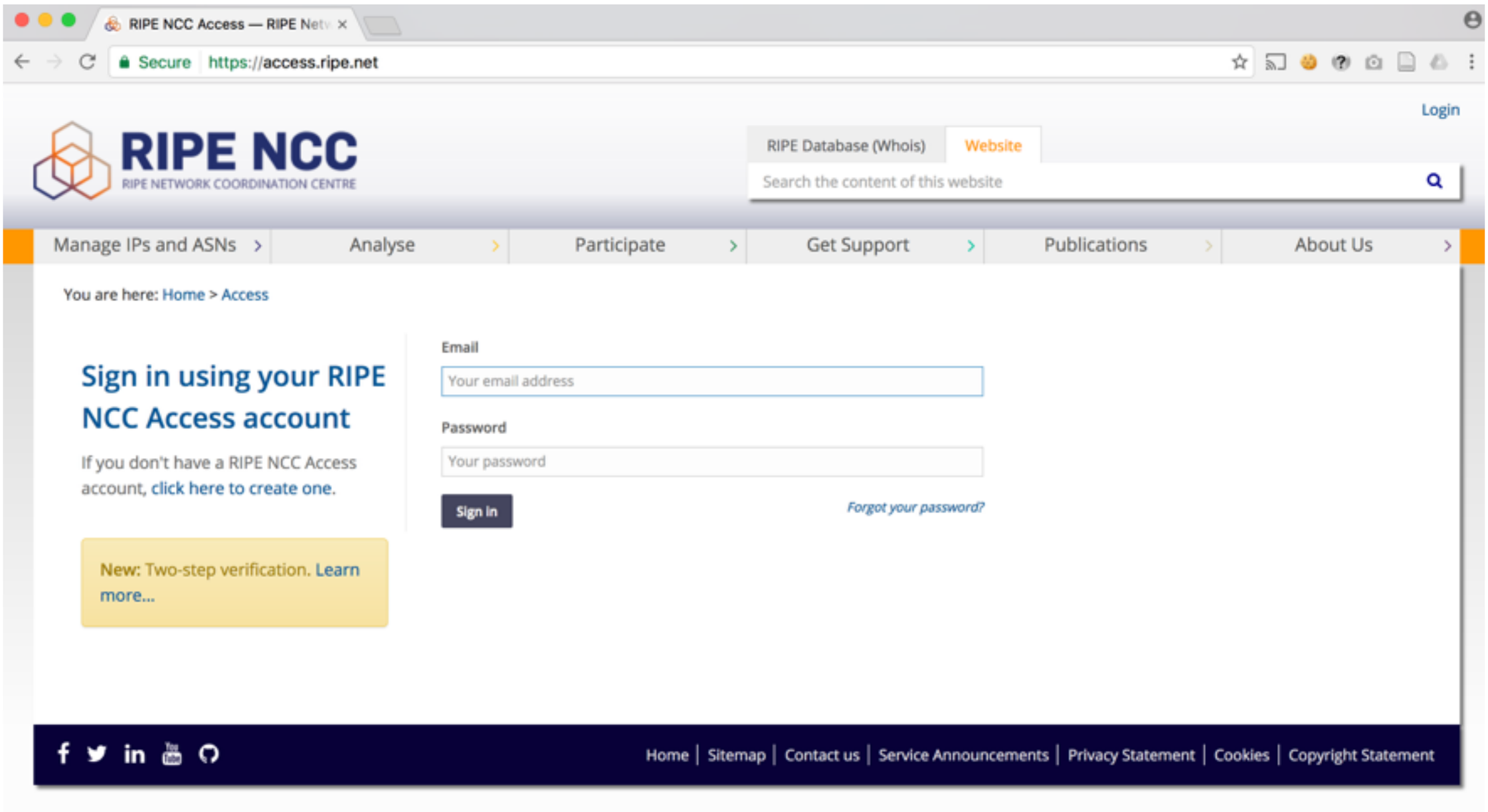
- **One interface for all IP resources related data**
  - Registry data, routing, reverse DNS, active measurements, 3rd party data (blacklist, geolocation)

Default Results



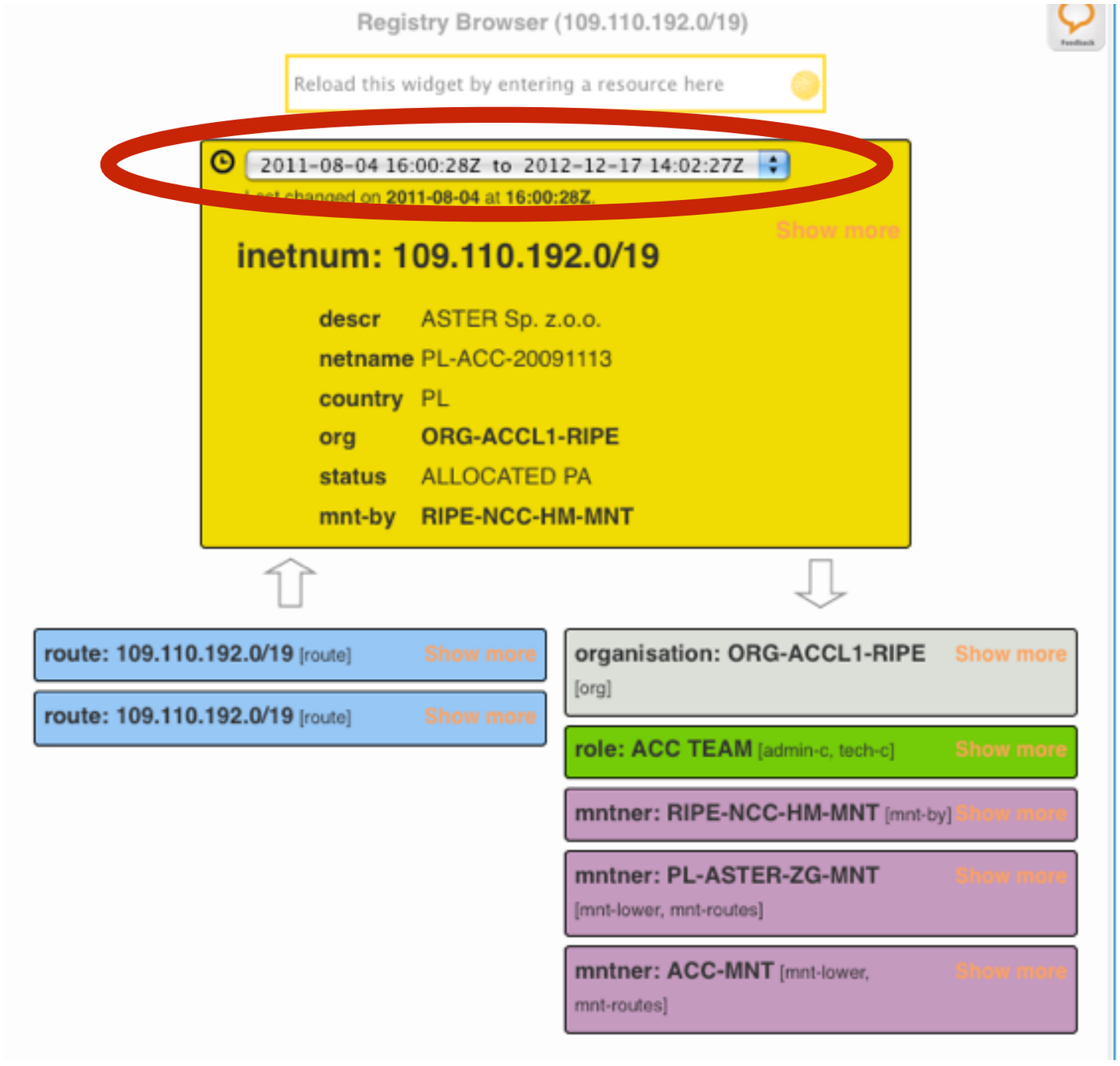
Create a RIPE NCC Access Account

https://access.ripe.net



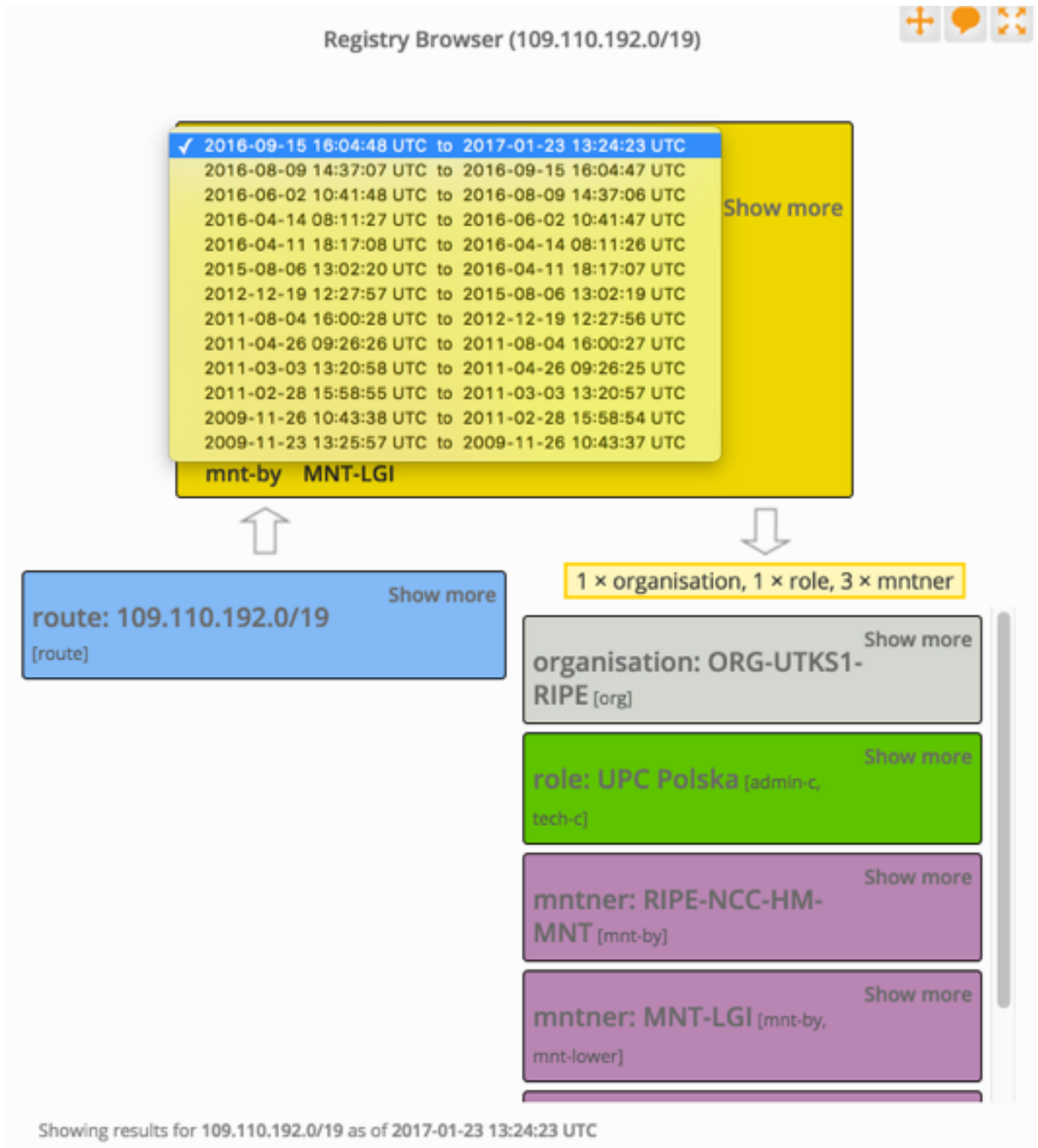
Registry Browser Widget

- click on another object to refocus query

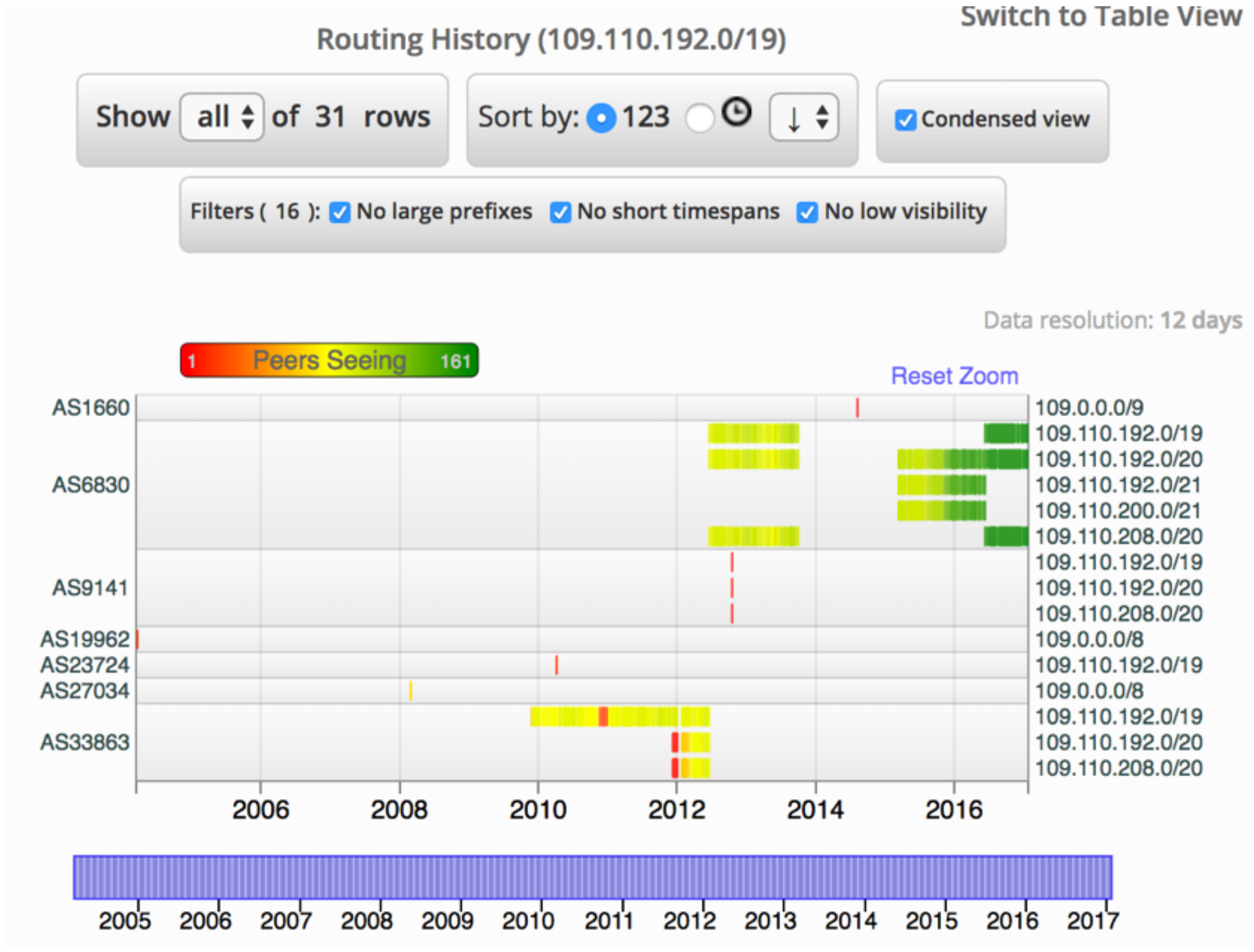


Registry Browser Widget

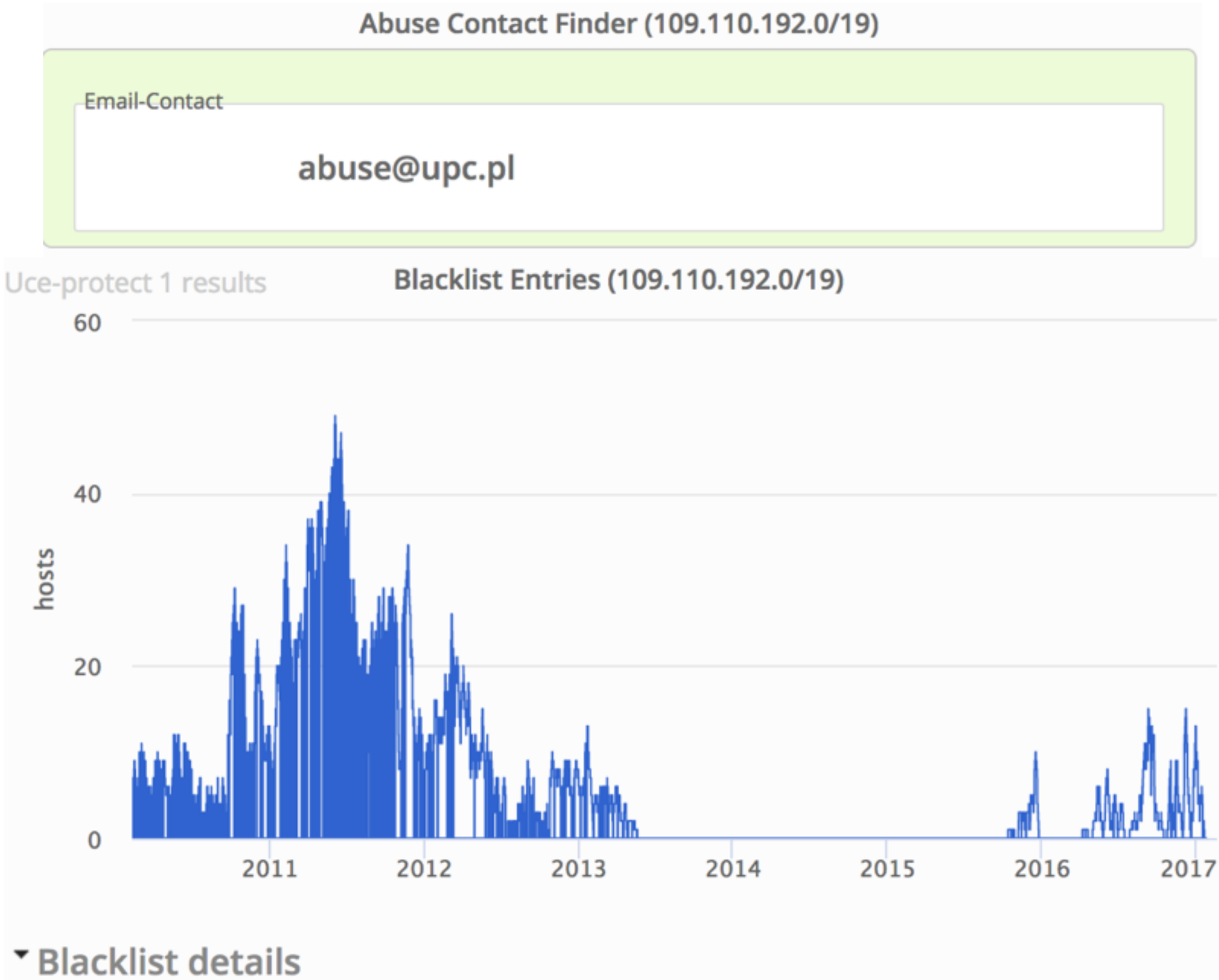
- historic information one click away



Routing History Widget



Anti Abuse & Blacklist Entries



RIPE NCC WHOIS client

Source code can be found here:

ftp://ftp.ripe.net/ripe/tools/dbase/software/ripe-whois-client-3.2.2.tar.gz

- Only to be used with RIPE WHOIS DB
- ‘whois help’ show all options
- --list-versions
- --diff-versions <version-number:version-number>
- --show-version <version-number>

RIPE NCC WHOIS client

--list-versions

```
ivo$ /usr/local/bin/whois --list-versions 193.0.0.0/21

1       2003-03-17 13:15   ADD/UPD
2       2003-04-12 08:32   ADD/UPD
3       2003-05-22 13:20   ADD/UPD
4       2004-10-22 14:43   ADD/UPD
5       2004-10-31 03:08   ADD/UPD
```

RIPE NCC WHOIS client

--show-version

```
ivo$ /usr/local/bin/whois --show-version 2 193.0.0.0/21
```

```
inetnum:        193.0.0.0 - 193.0.7.255
netname:        RIPE-NCC
descr:          RIPE Network Coordination Centre
descr:          Amsterdam, Netherlands
remarks:        Used for RIPE NCC infrastructure.
country:        NL
admin-c:        AMR68-RIPE
tech-c:         OPS4-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-MNT
mnt-lower:      RIPE-NCC-MNT
source:         RIPE # Filtered
```

RIPE NCC WHOIS client

--diff-versions

```
ivo$ /usr/local/bin/whois --diff-versions 2:3 193.0.0.0/21
```

```
% Difference between version 2 and 3 of object "193.0.0.0 - 193.0.7.255"

@@ -7,2 +7,3 @@
 admin-c:        AMR68-RIPE
+admin-c:        RDK-RIPE
 tech-c:         OPS4-RIPE
```

Questions