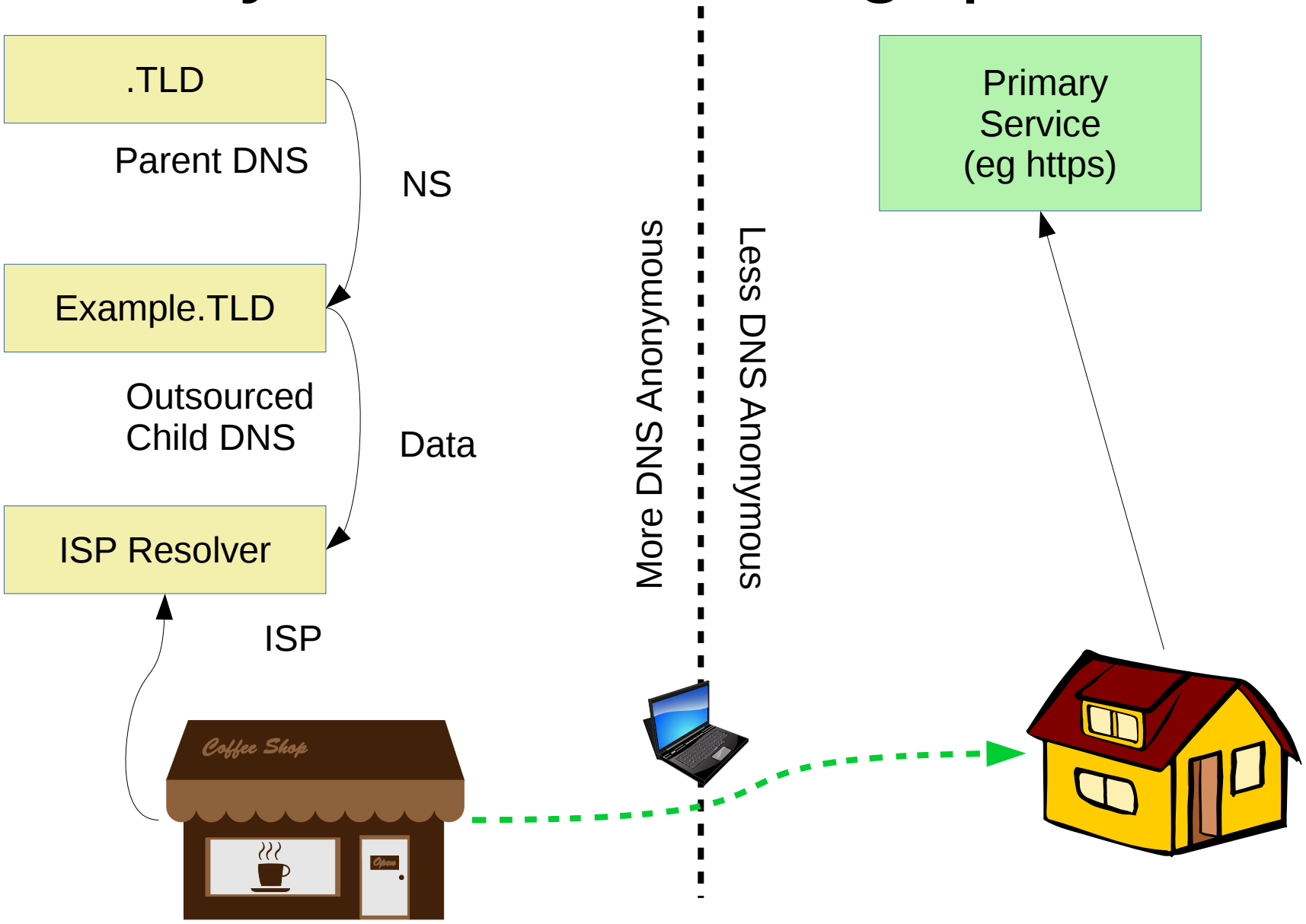
# Analyzing and Mitigating Privacy with the DNS Root Service

Wes Hardaker
USC/ISI
<hardaker@isi.edu>

# Last Year I Pondered: Can you avoid asking questions?

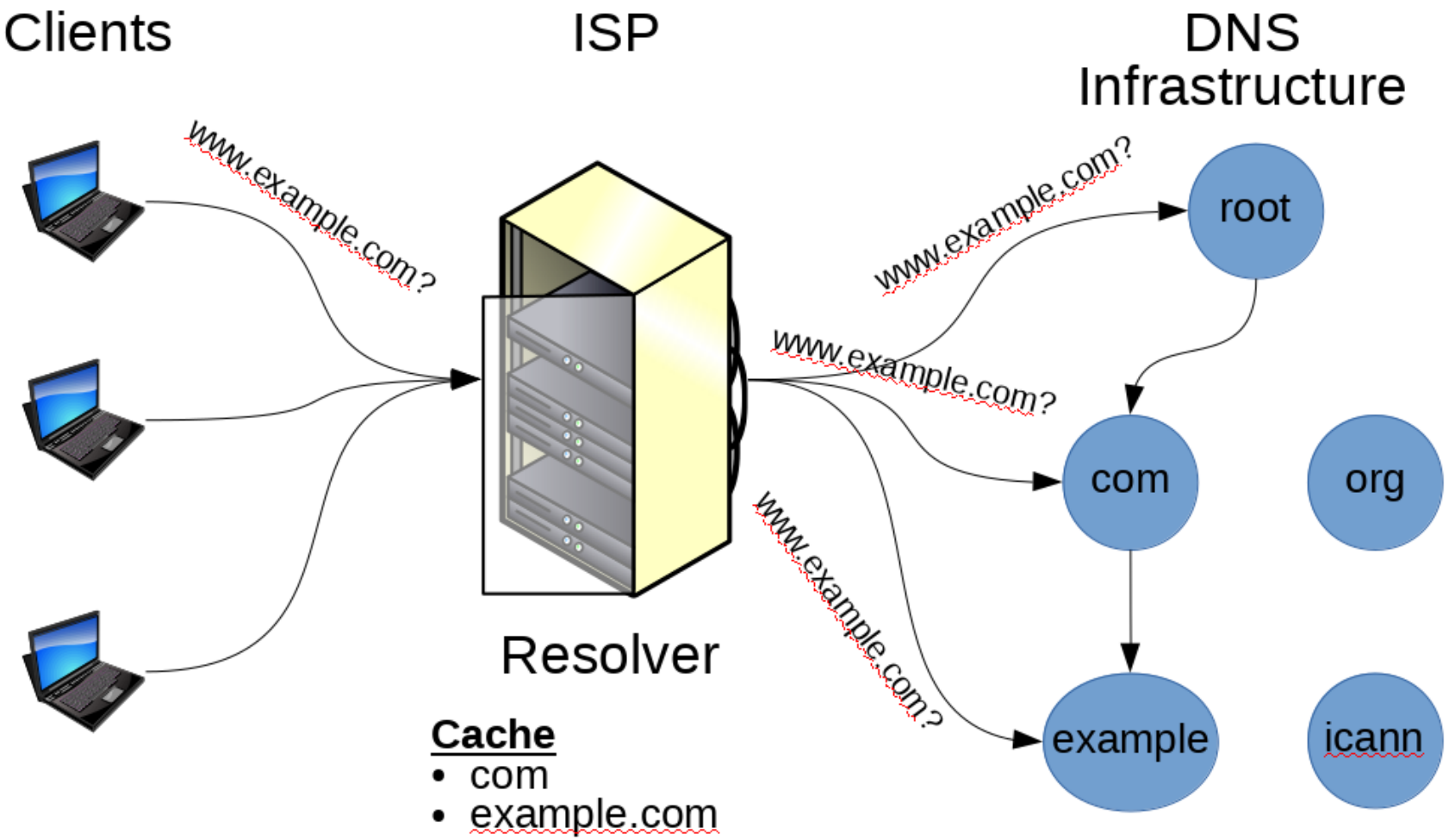


# Which Led Me To More Questions

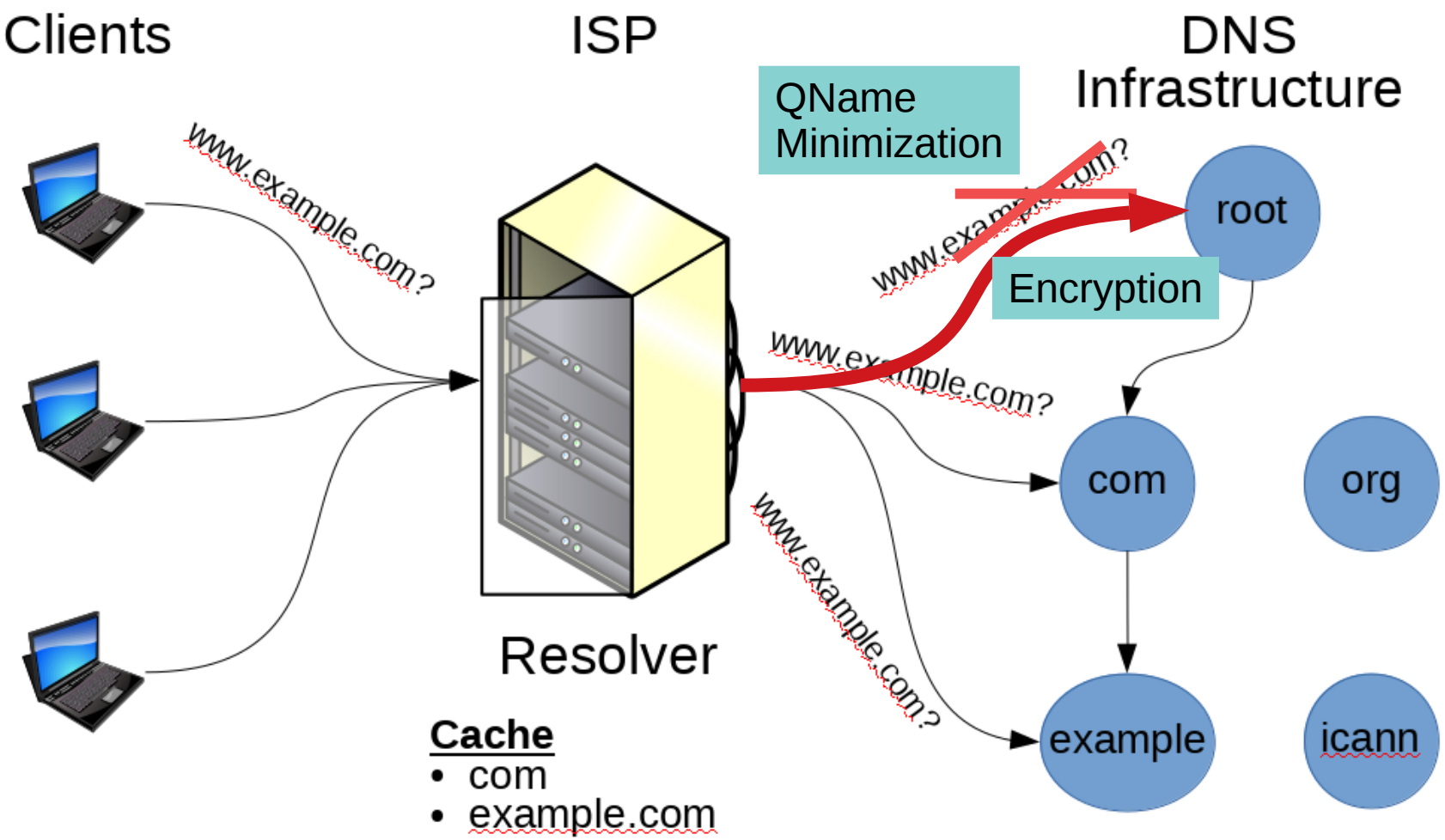
- Does query leakage really reveal anything?
  - What does (e.g.) the root see about me?
- Does traffic analysis reveal anything?
- Does temporal analysis reveal anything?

- How much protection do solutions offer?
  - TLS?
  - Query minimization?
- What offers full protection?

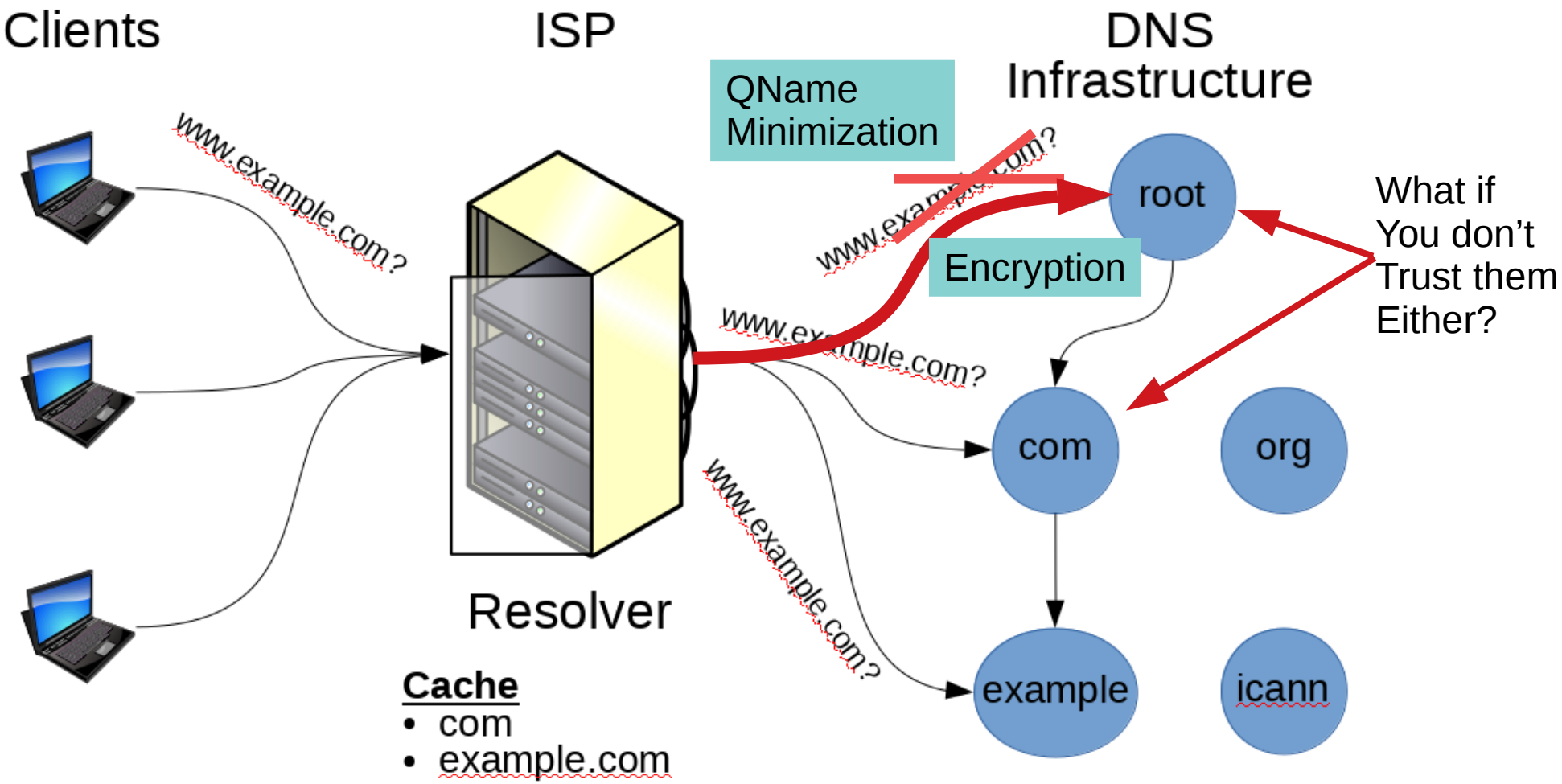
# DNS Query Leaking to the Roots



# DNS Query Leaking to the Roots



# DNS Query Leaking to the Roots



# Experiment Plan and Data

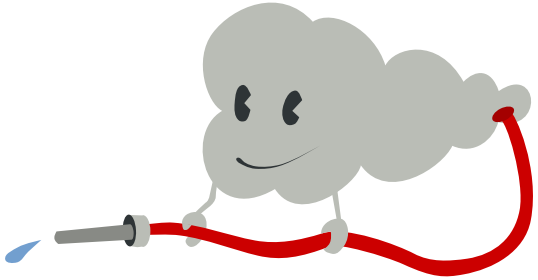
- Two residences
  - Recursive resolvers
  - Static IP
  - Willingness
  - Providing ground truth
- An authoratative server
  - B-Root
  - **One month** of query data: 2017, Jan.
- Bulk global analysis
  - Quick analysis

# Data Statistics

| | Residence 1 | Residence 2 |
|---|---|---|
| **IPv4 Packets** | 52191 | 2049 |
| **IPv6 Packets** | 27675 | 0 |
| **Total** | 79866 | 2049 |

# Analysis Types

- RRTYPE
- Geographical
- Temporal
- Special Name

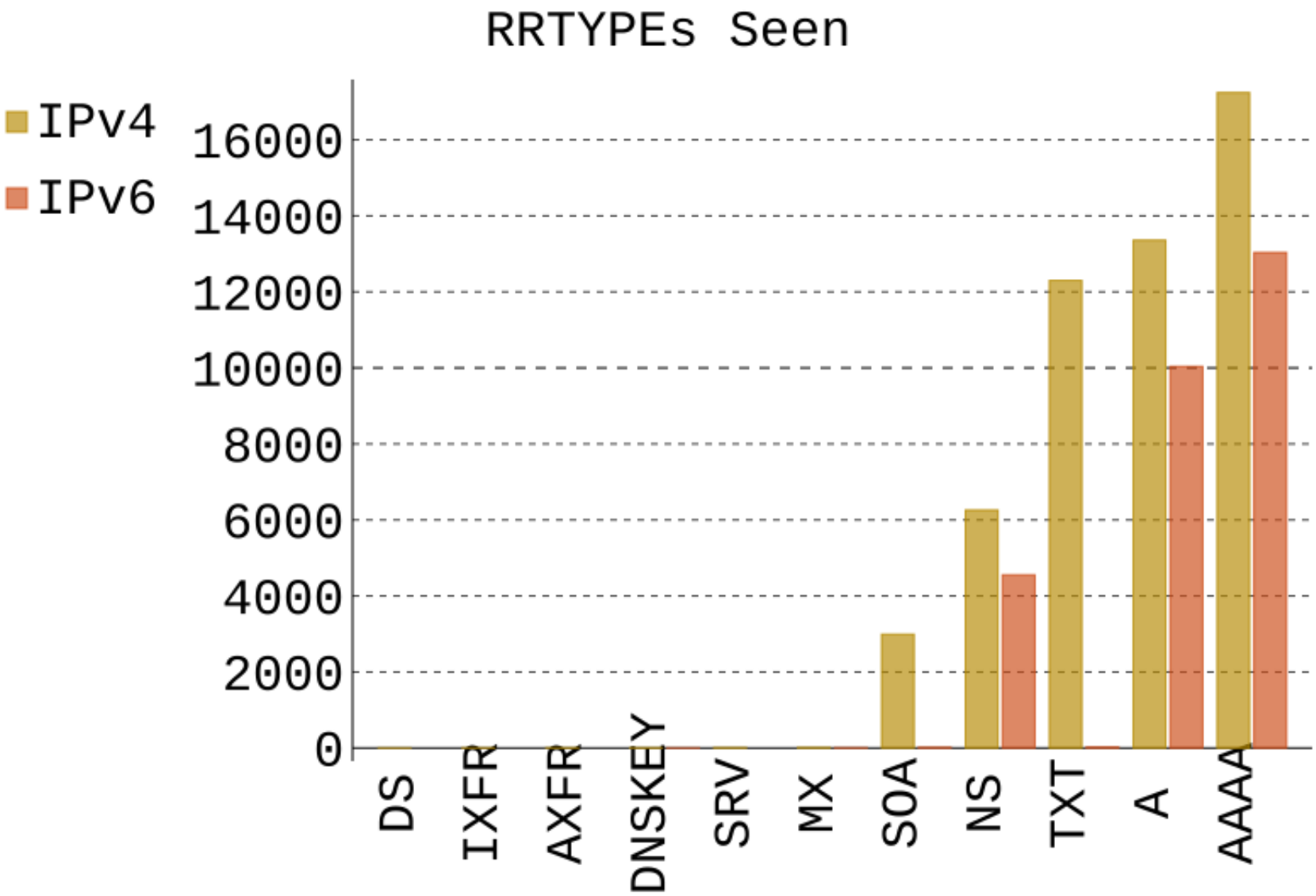


- Warning: Results coming next at firehose rate

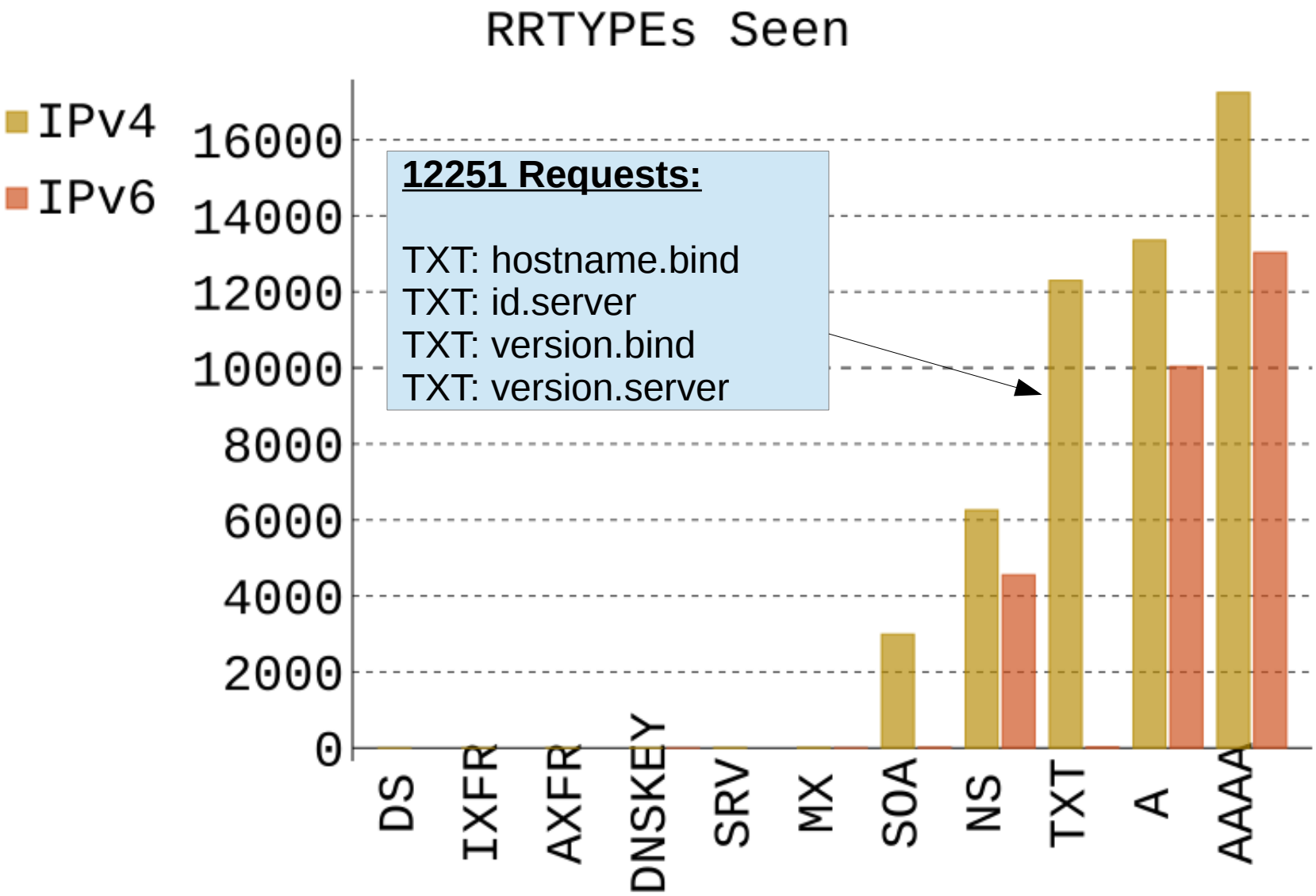
  *(don't try this at home)*

Even more
Analysis in
The paper

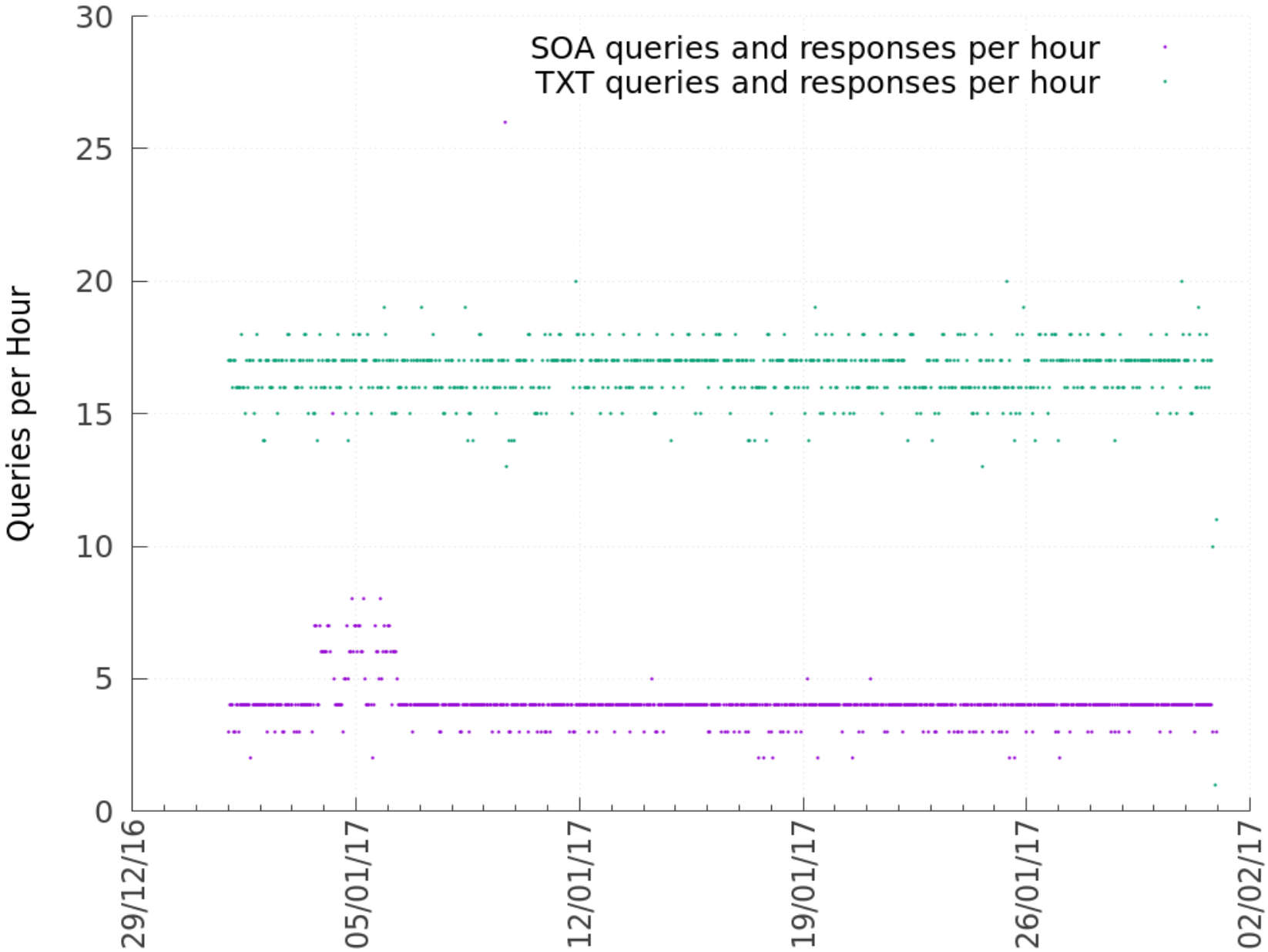
# RES1 RRTYPE Analysis



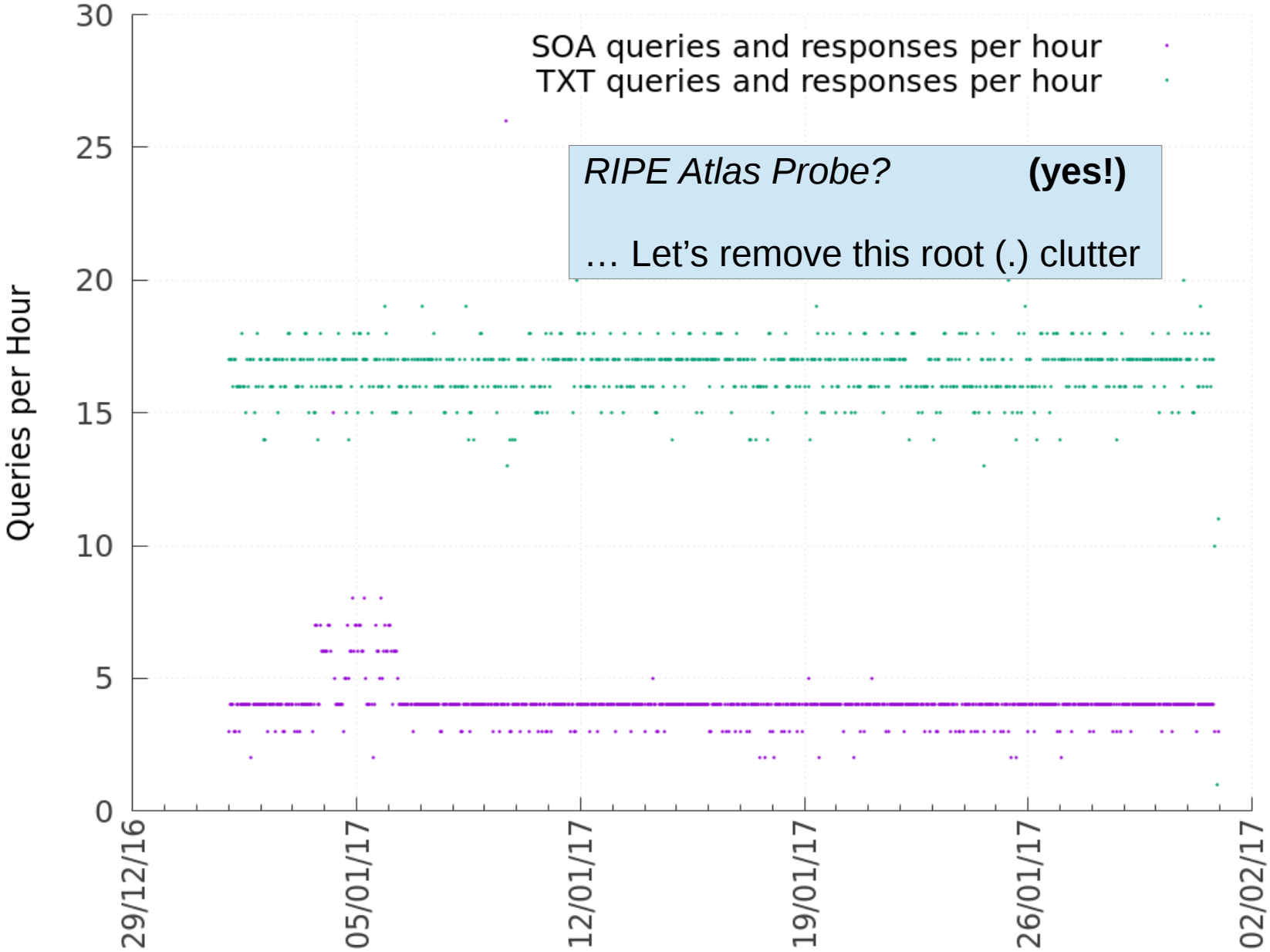
# RES1 RRTYPE Analysis



# RES1 RRTYPE Analysis



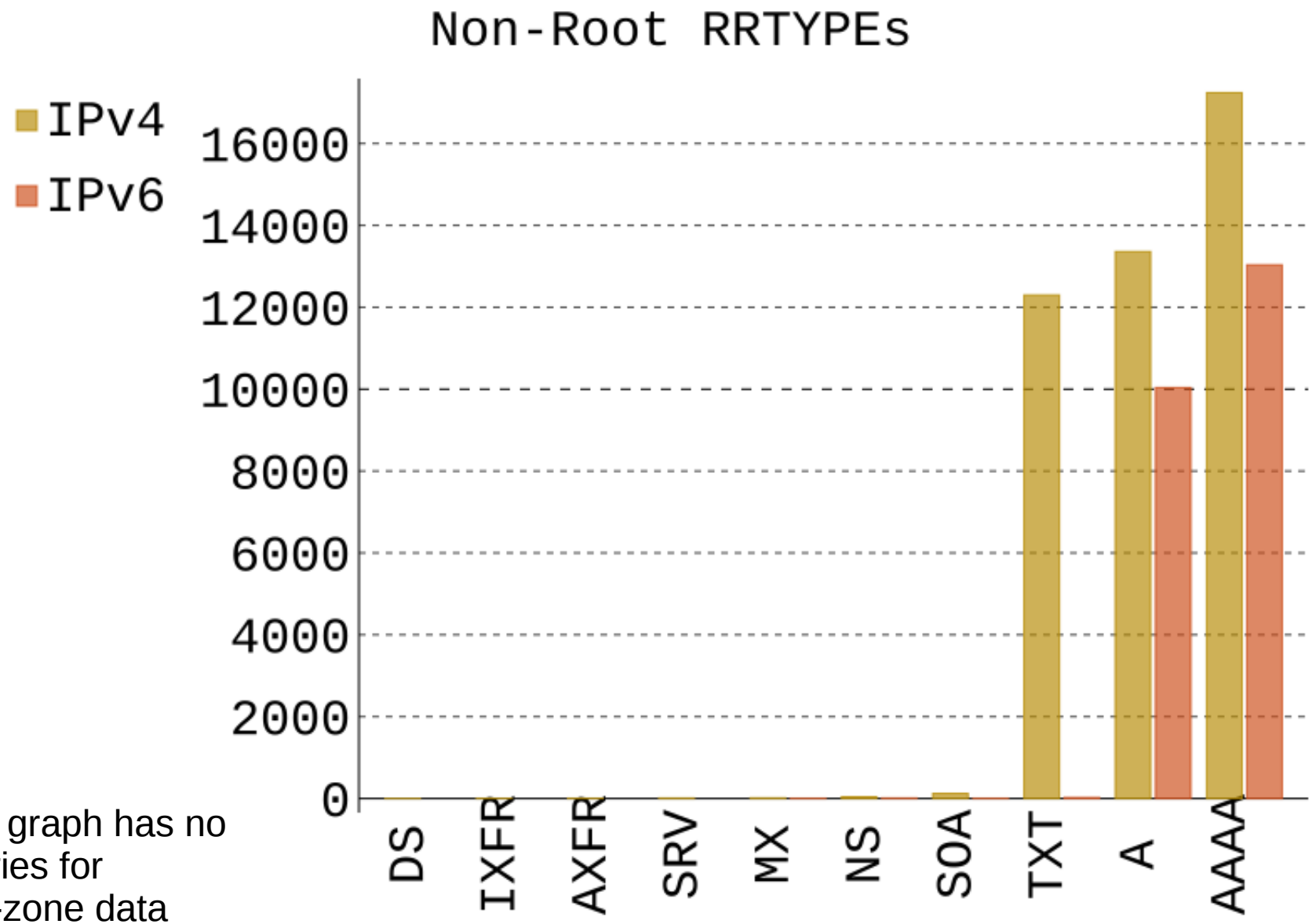
# RES1 RRTYPE Analysis




*RIPE Atlas Probe?* **(yes!)**

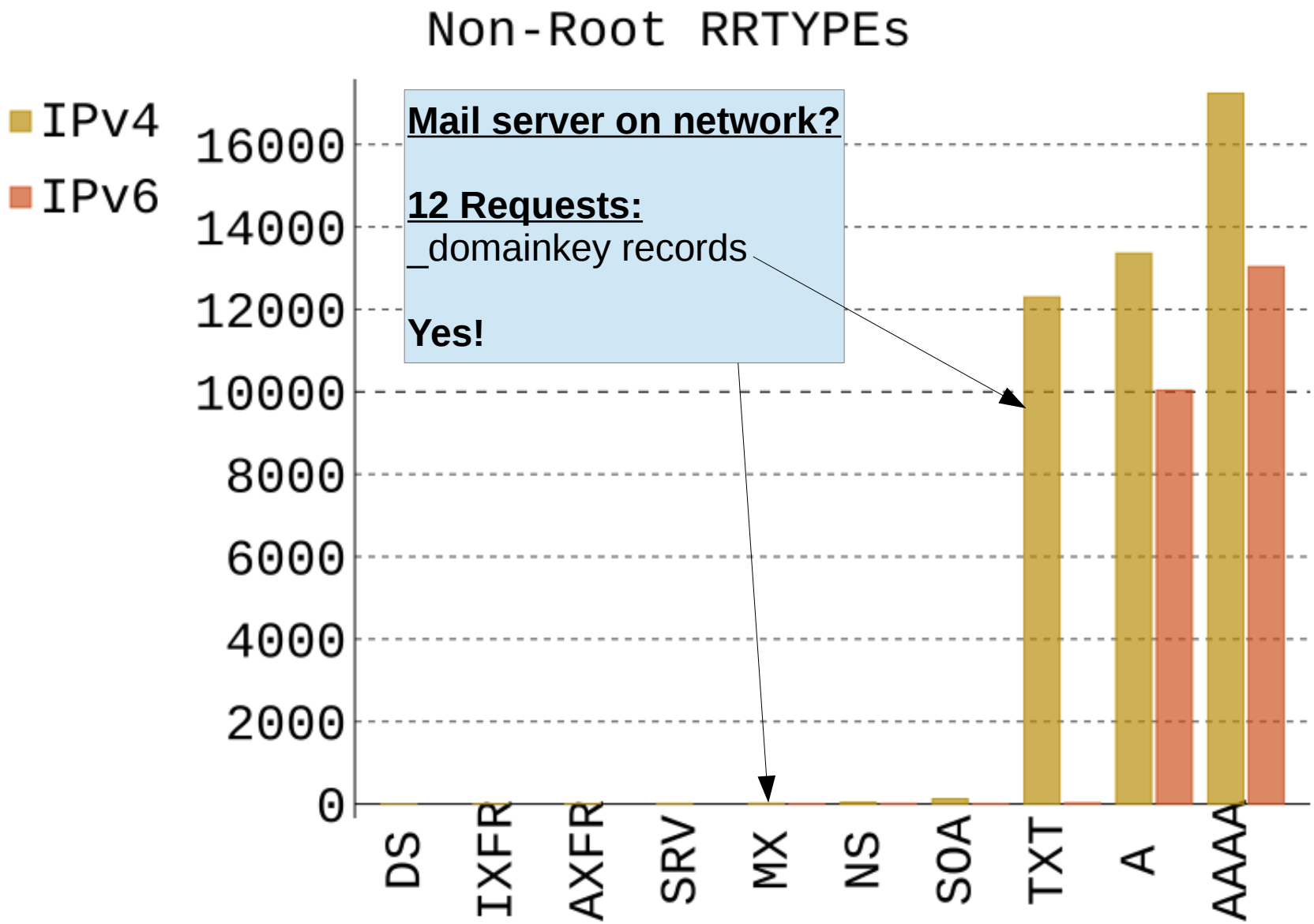
… Let's remove this root (.) clutter

# RES1 RRTYPE Analysis – Non Root

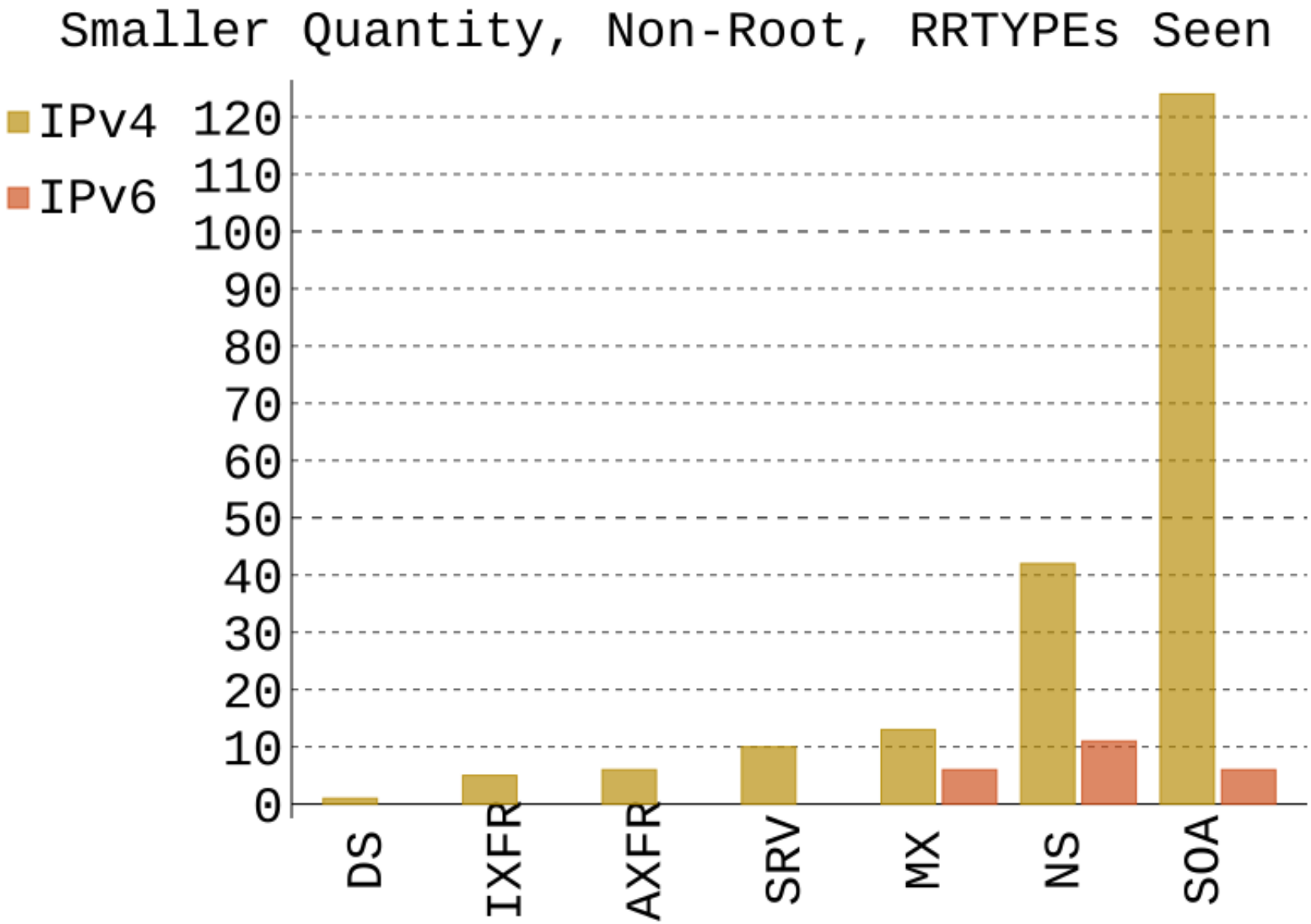



This graph has no queries for root-zone data (i.e. no “.” queries)

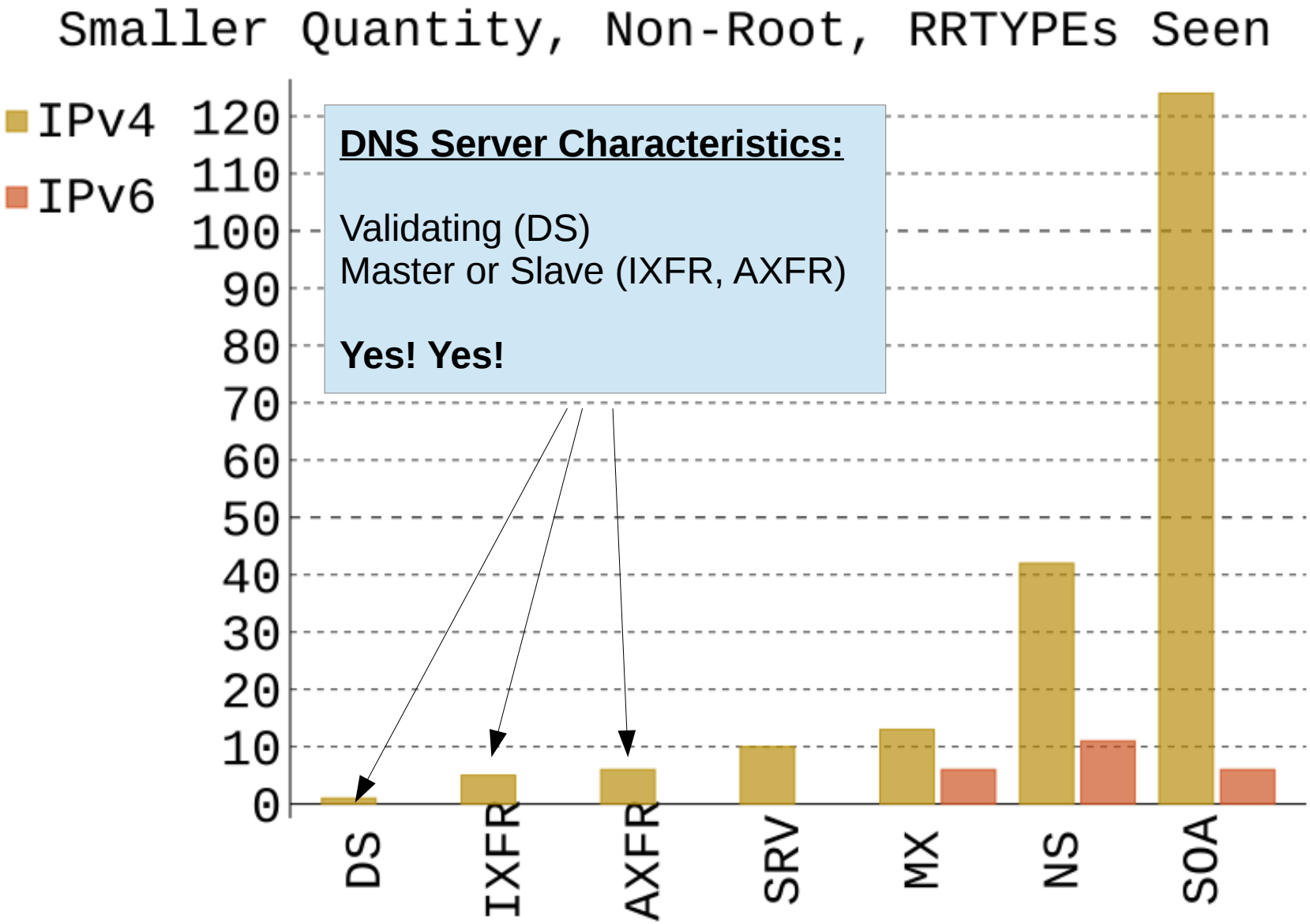
# RES1 RRTYPE Analysis – Non Root



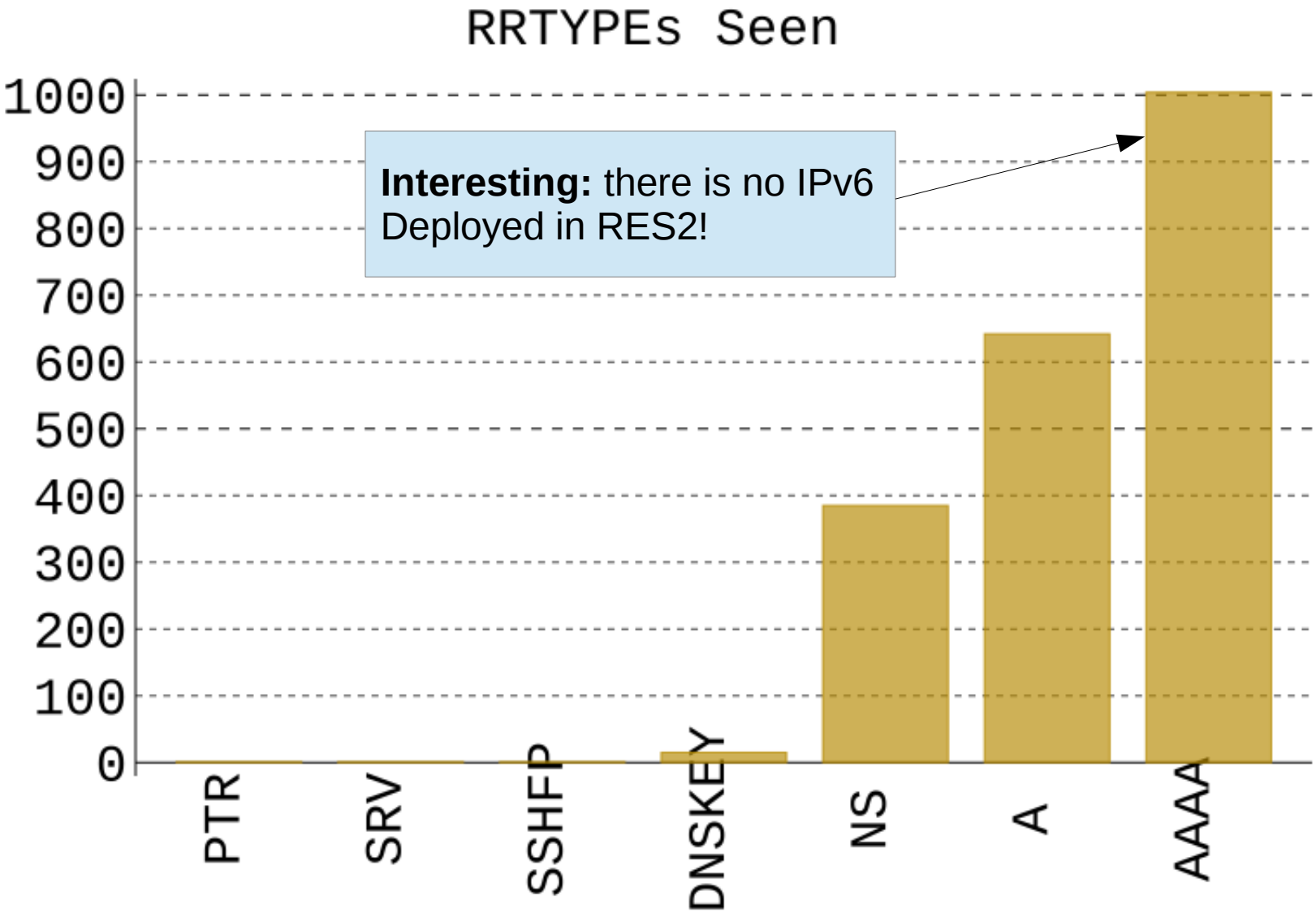
# RES1 RRTYPE Analysis – Smaller



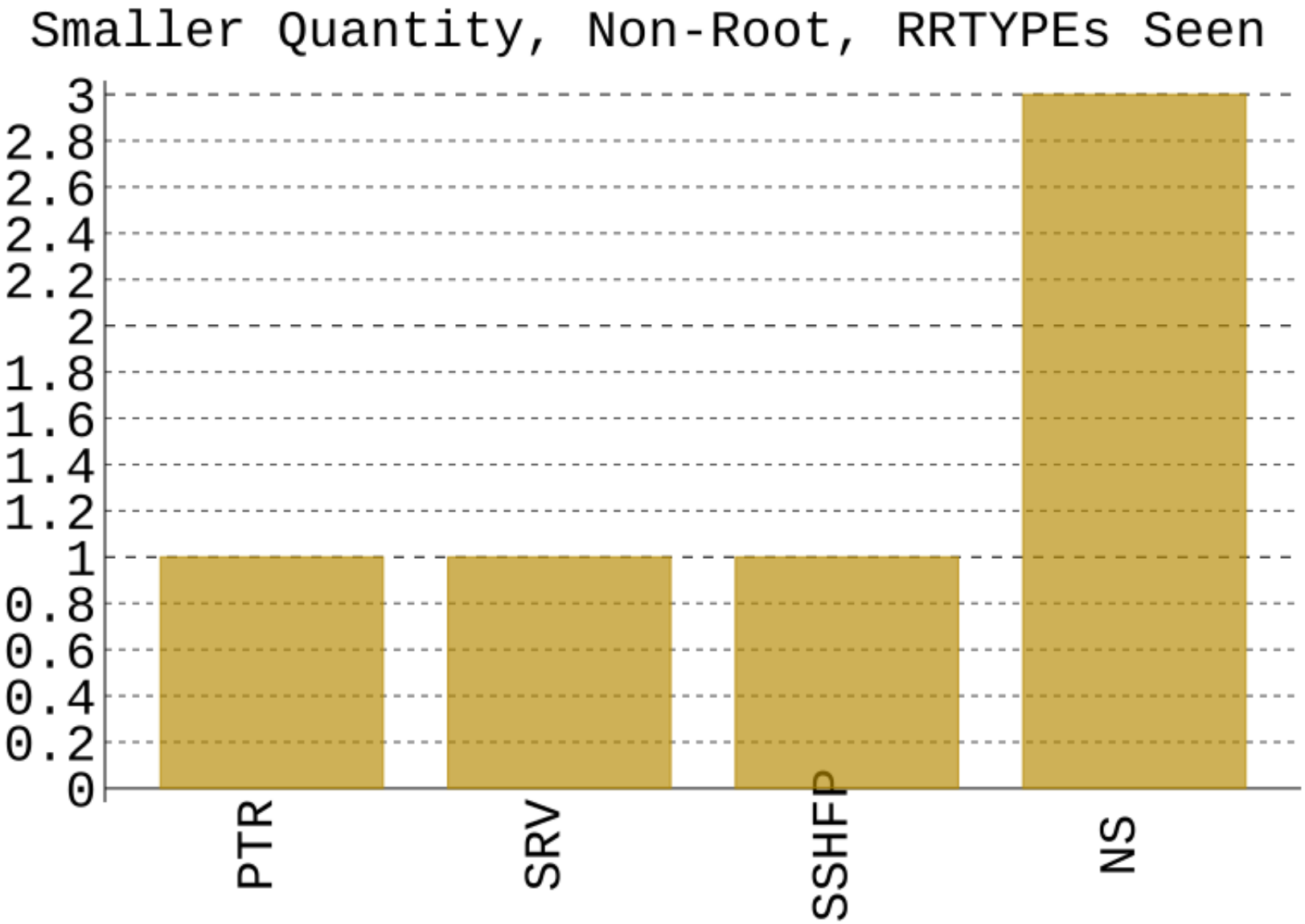
# RES1 RRTYPE Analysis – Smaller



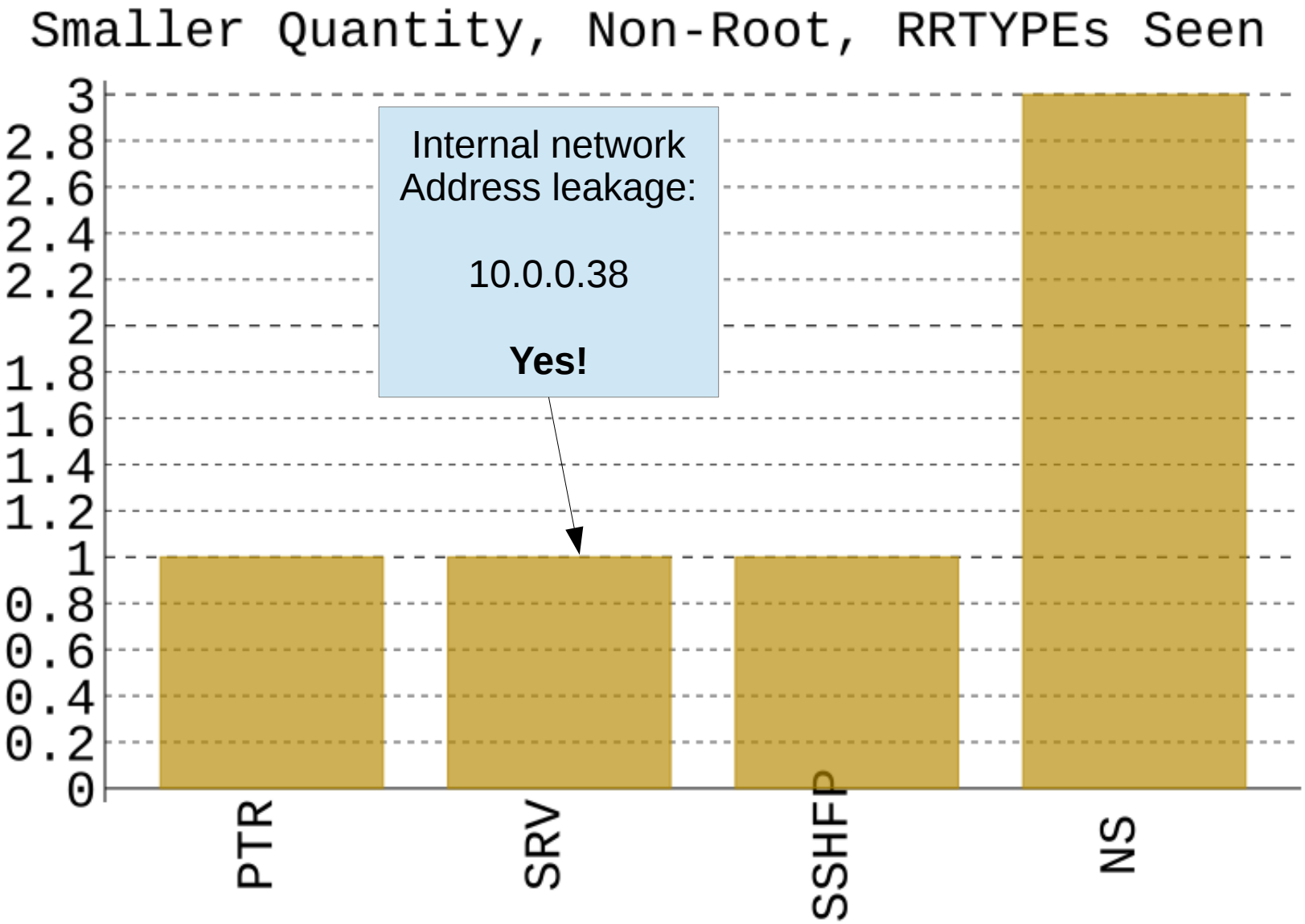
# RES2 RRTYPE Analysis



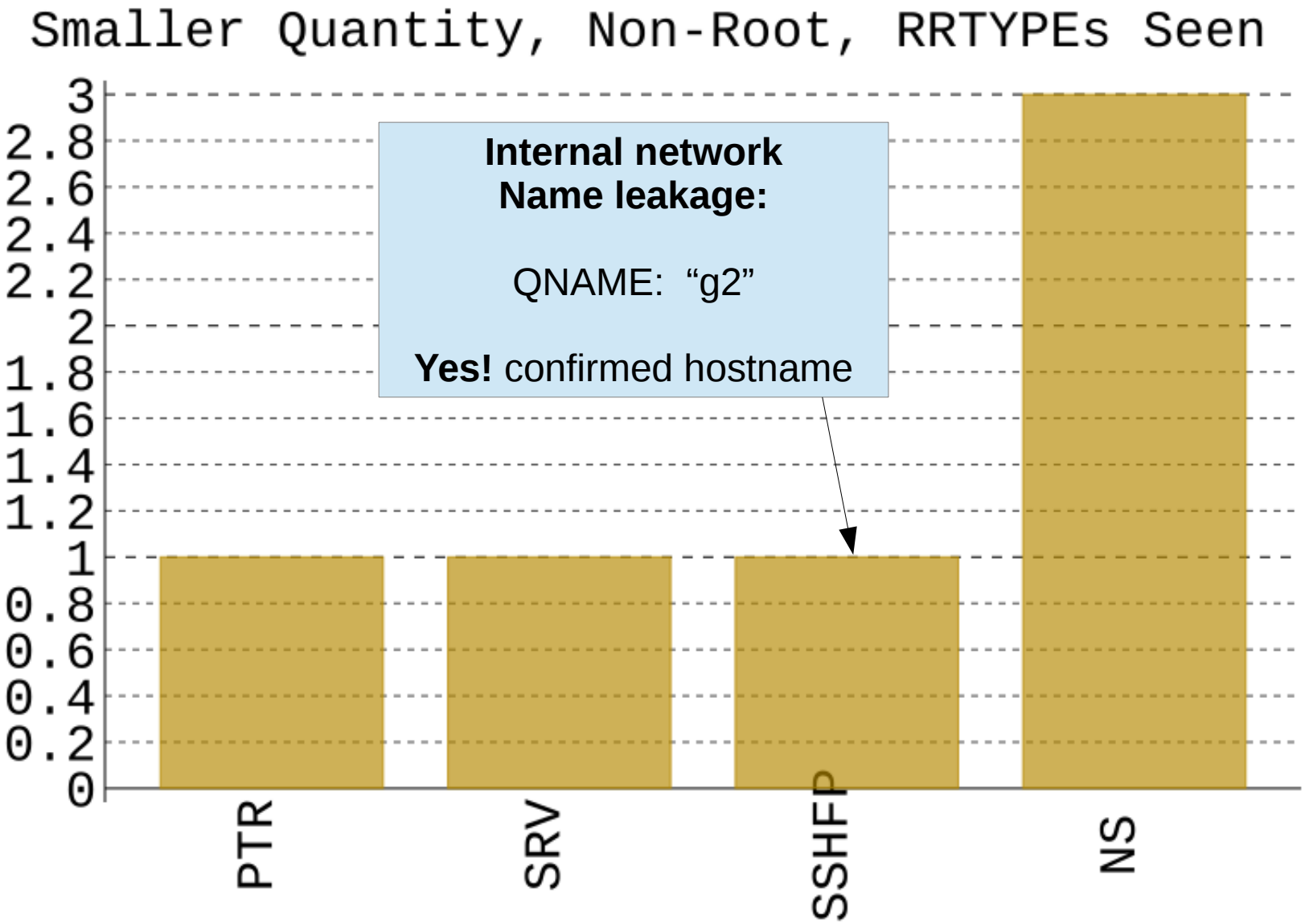
# RES2 RRTYPE Analysis



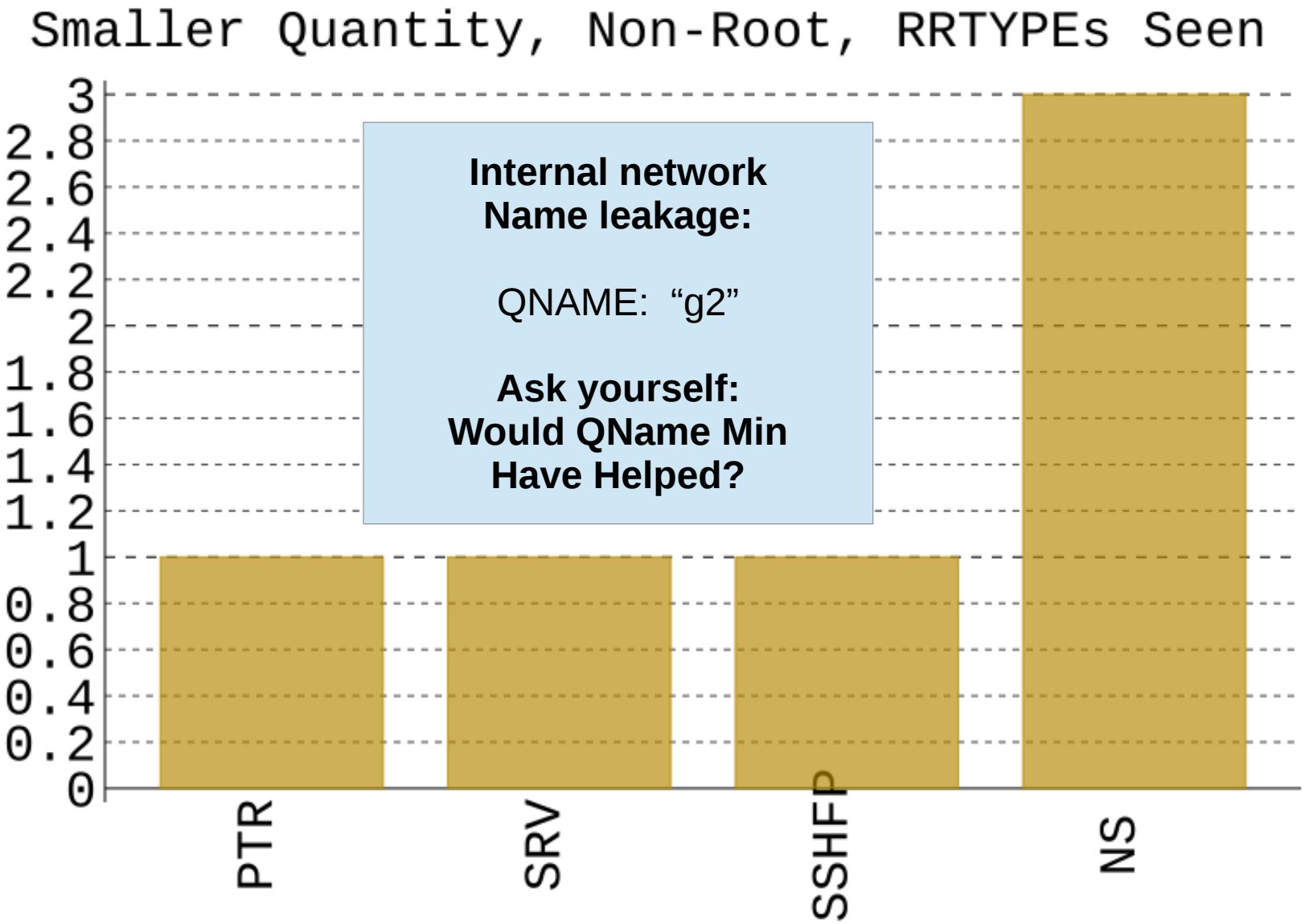
# RES2 RRTYPE Analysis



# RES2 RRTYPE Analysis



# RES2 RRTYPE Analysis

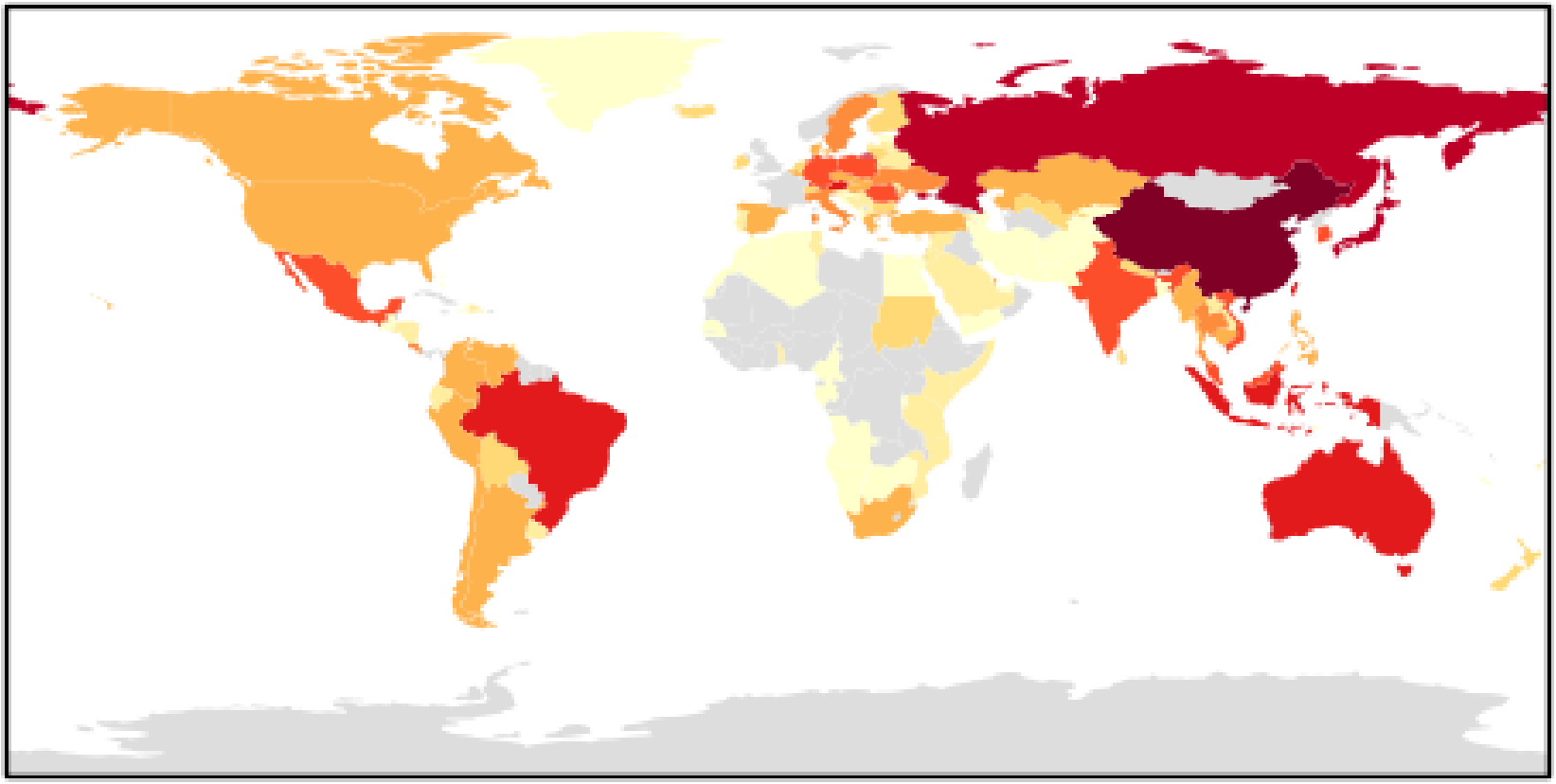



**Internal network Name leakage:**

QNAME: “g2”

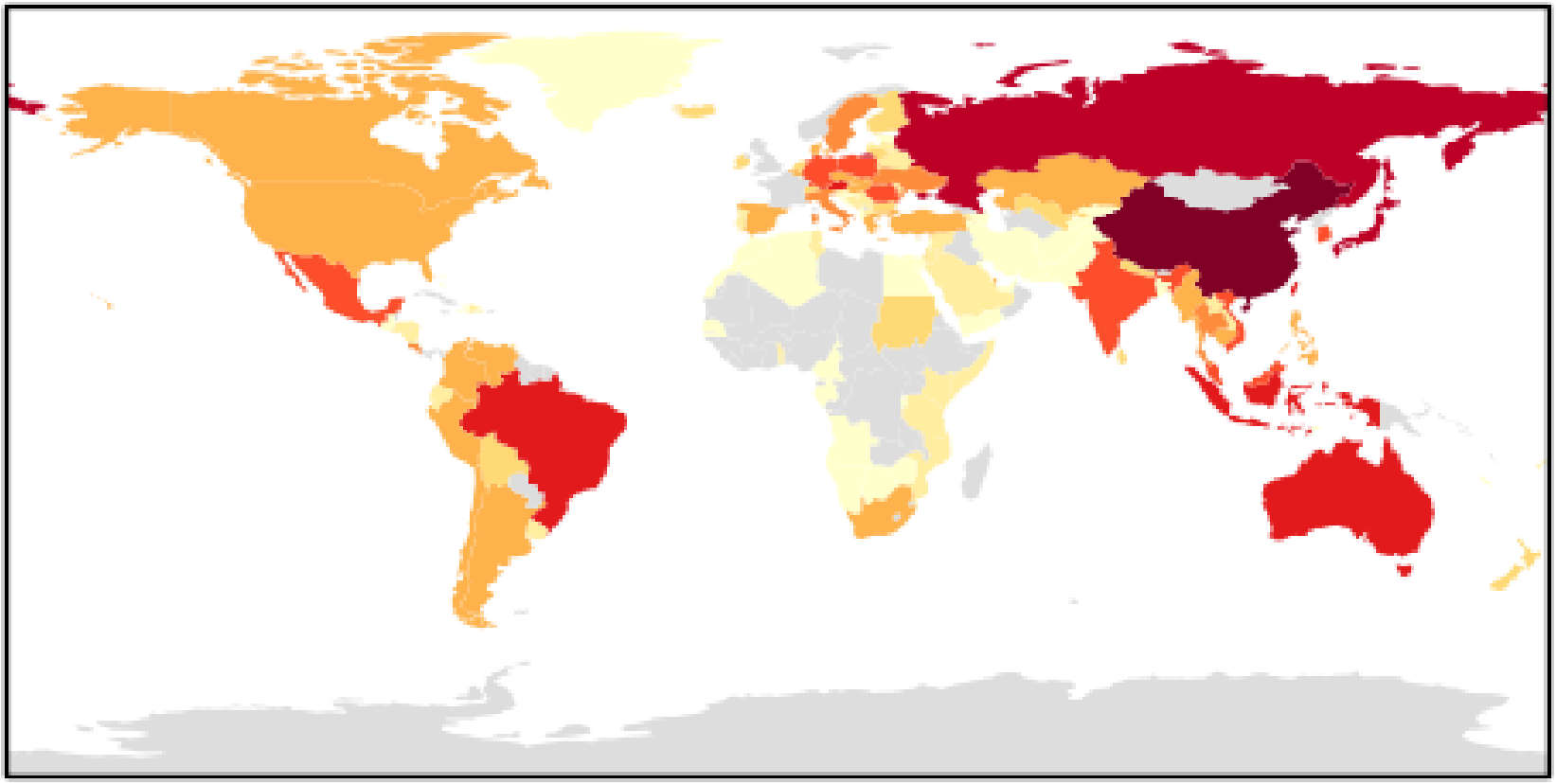
**Ask yourself: Would QName Min Have Helped?**

# RES1 Geographical Analysis



Heat Map: Most popular CC-TLDs

# RES1 Geographical Analysis

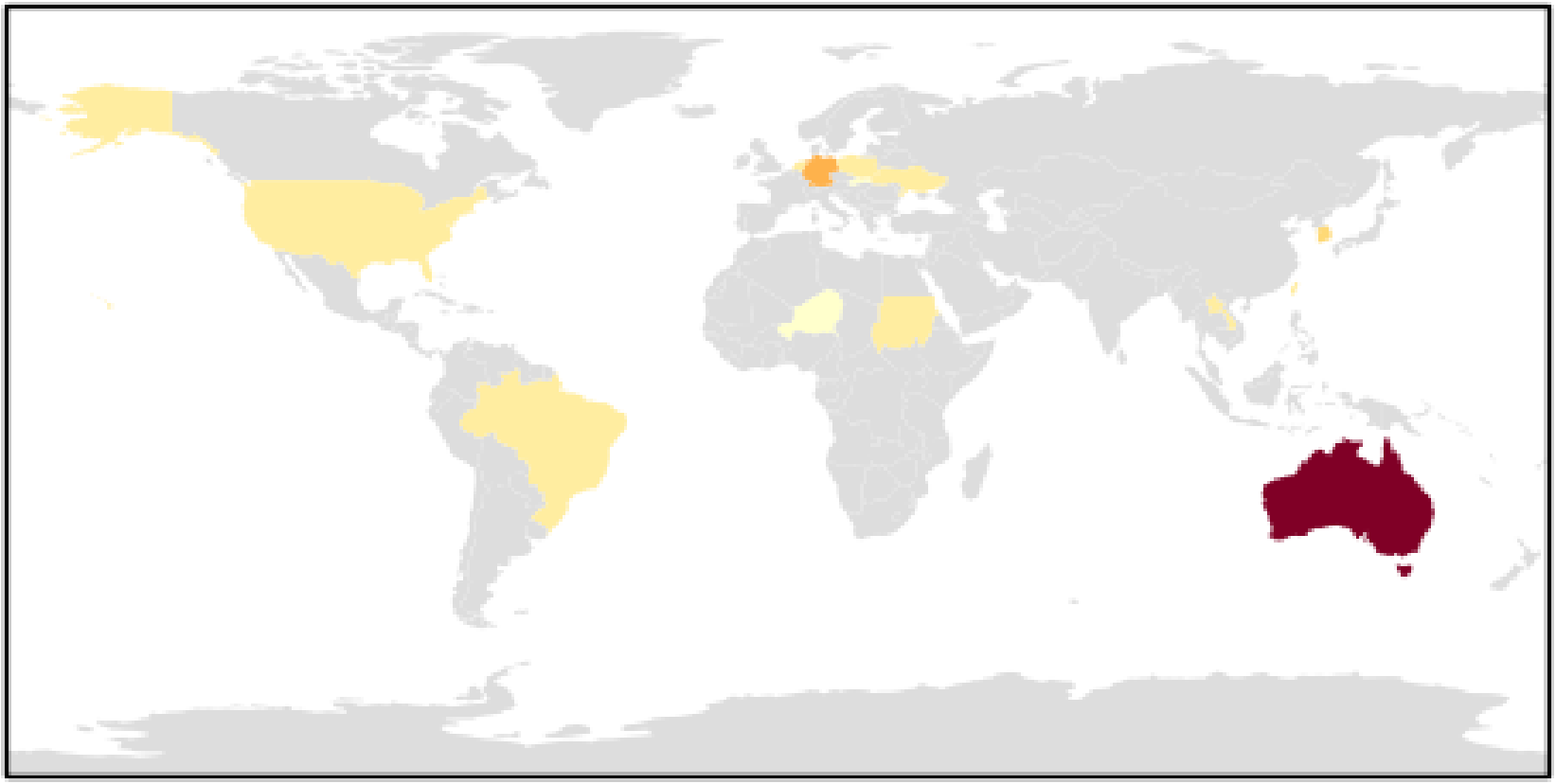


Heat Map: Most popular CC-TLDs

Lots of communication with China and Russia?

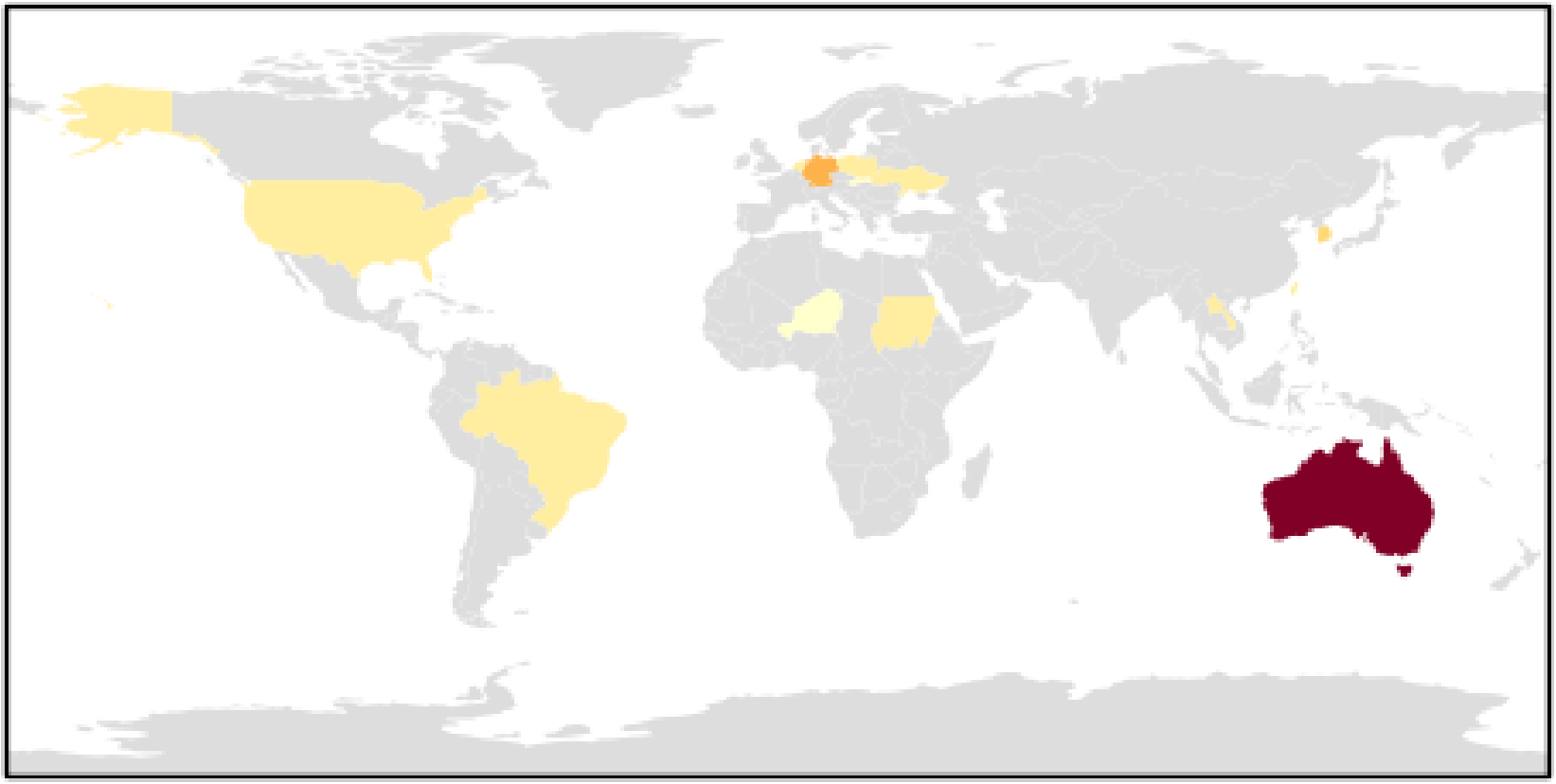
**No! Fail! – SPAM**

# RES2 Geographical Analysis



Heat Map: Most popular CC-TLDs

# RES2 Geographical Analysis

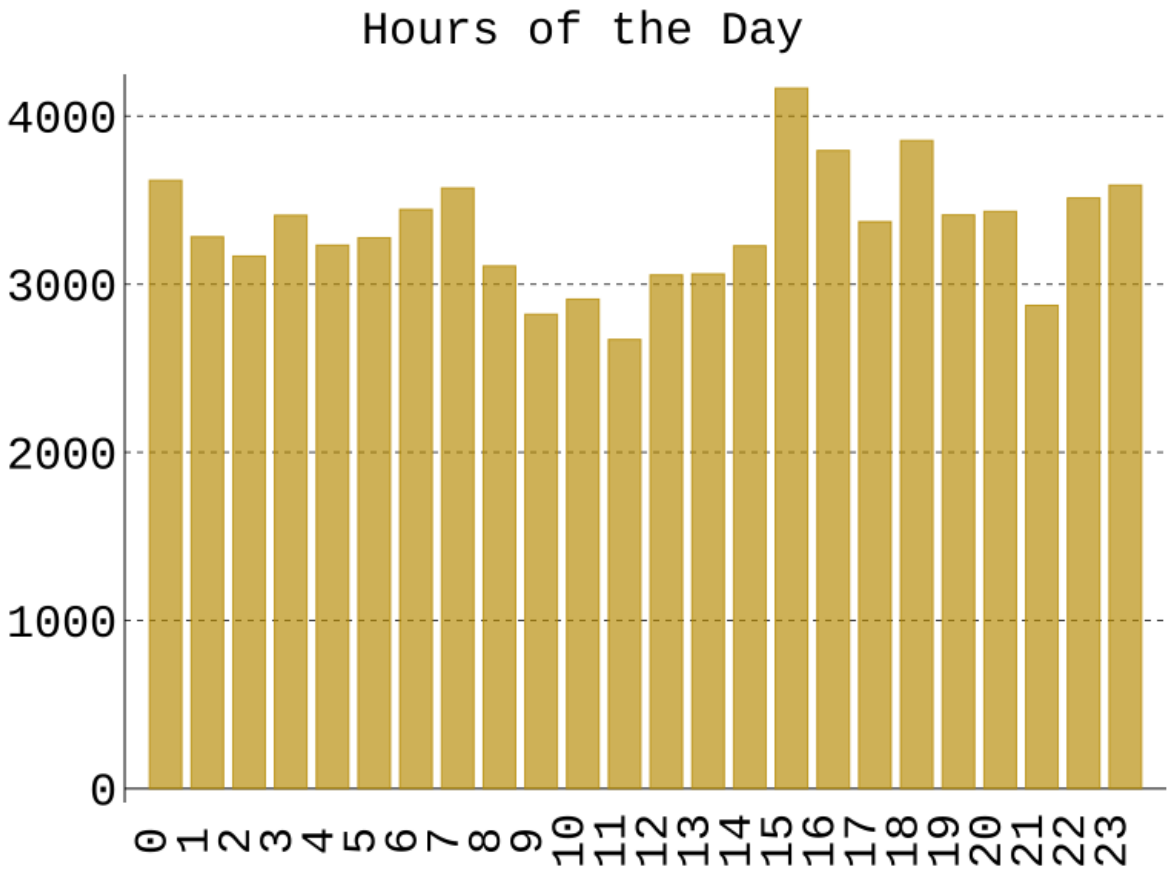


Heat Map: Most popular CC-TLDs

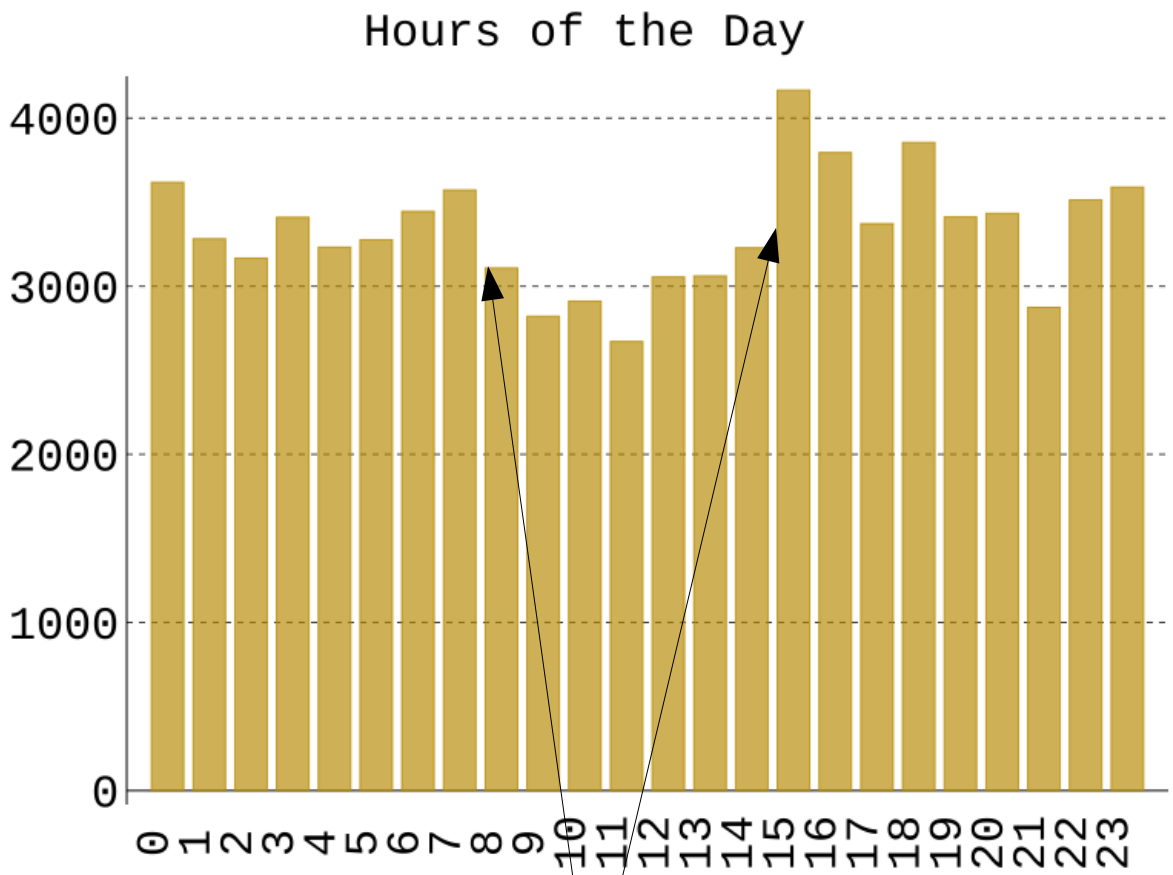
Lots of communication with Australia?

**No!  Fail!**
**aridns.net.au – Unknown**

# RES1: Temporal Analysis – by hour



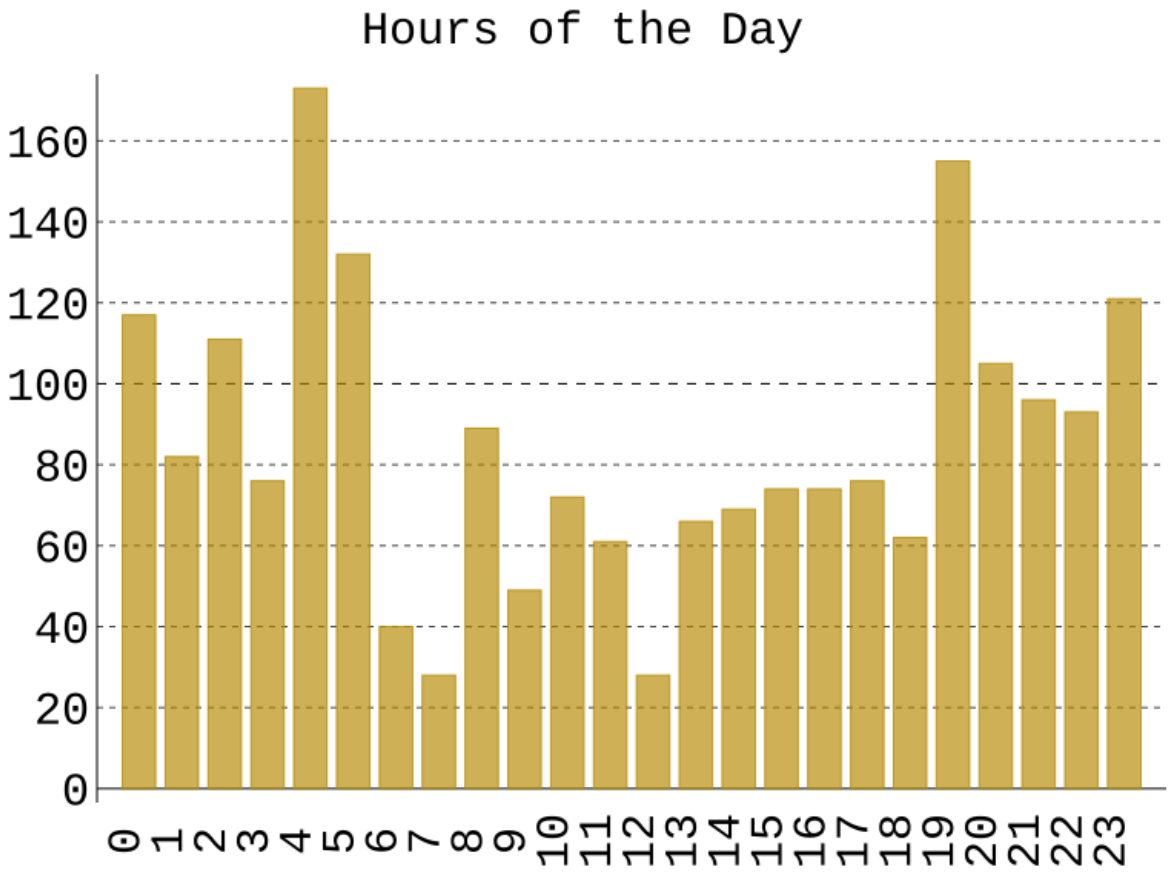
# RES1: Temporal Analysis – by hour



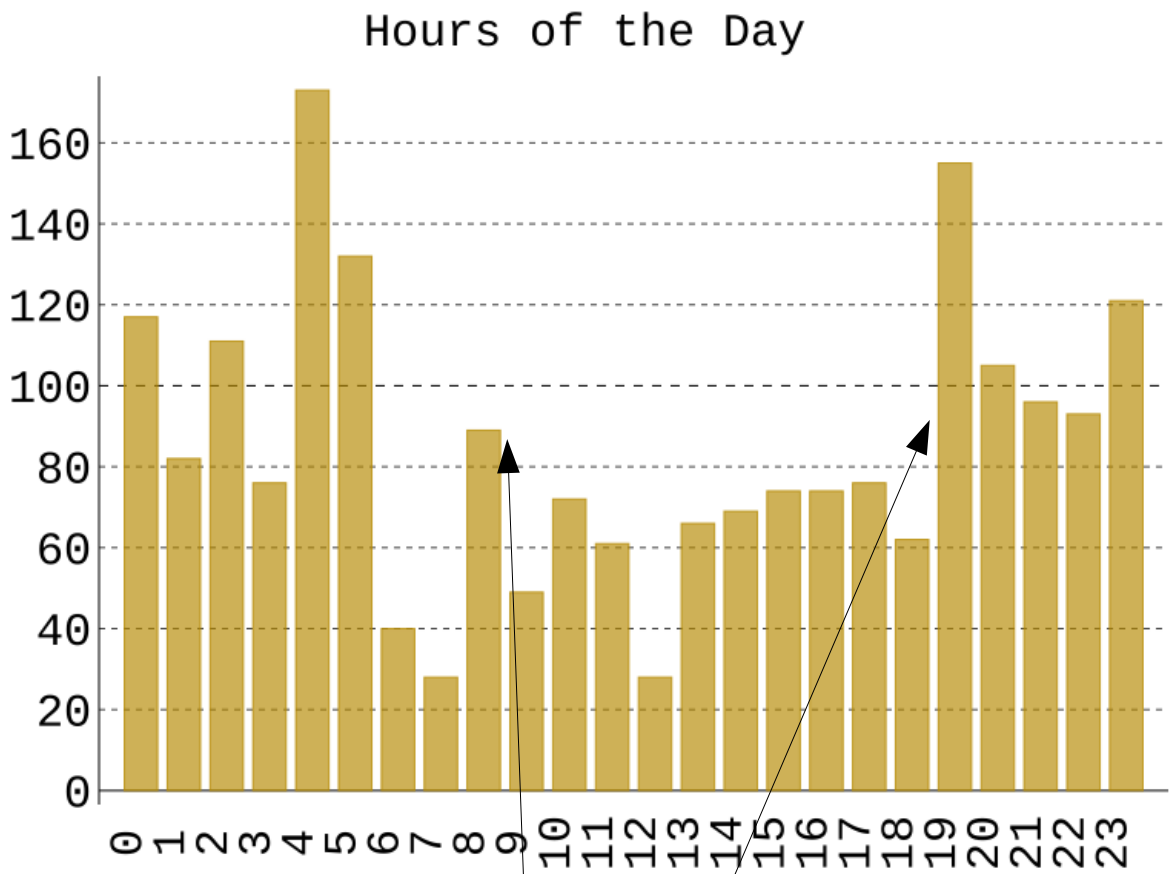

Household sleeping period? TZ offset 6-8 from GMT?

**Yes!** (7)

# RES2: Temporal Analysis – by hour



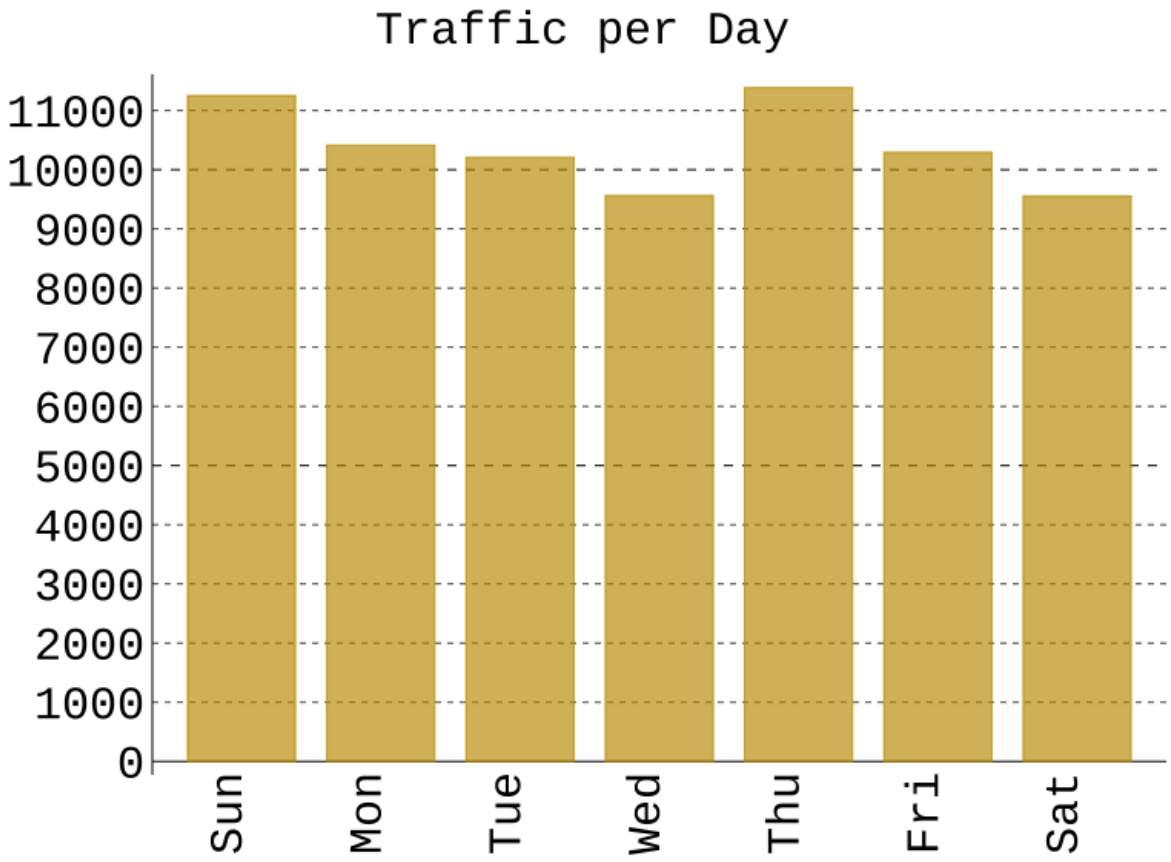
# RES2: Temporal Analysis – by hour




Household sleeping period? TZ offset 4-6 from GMT?

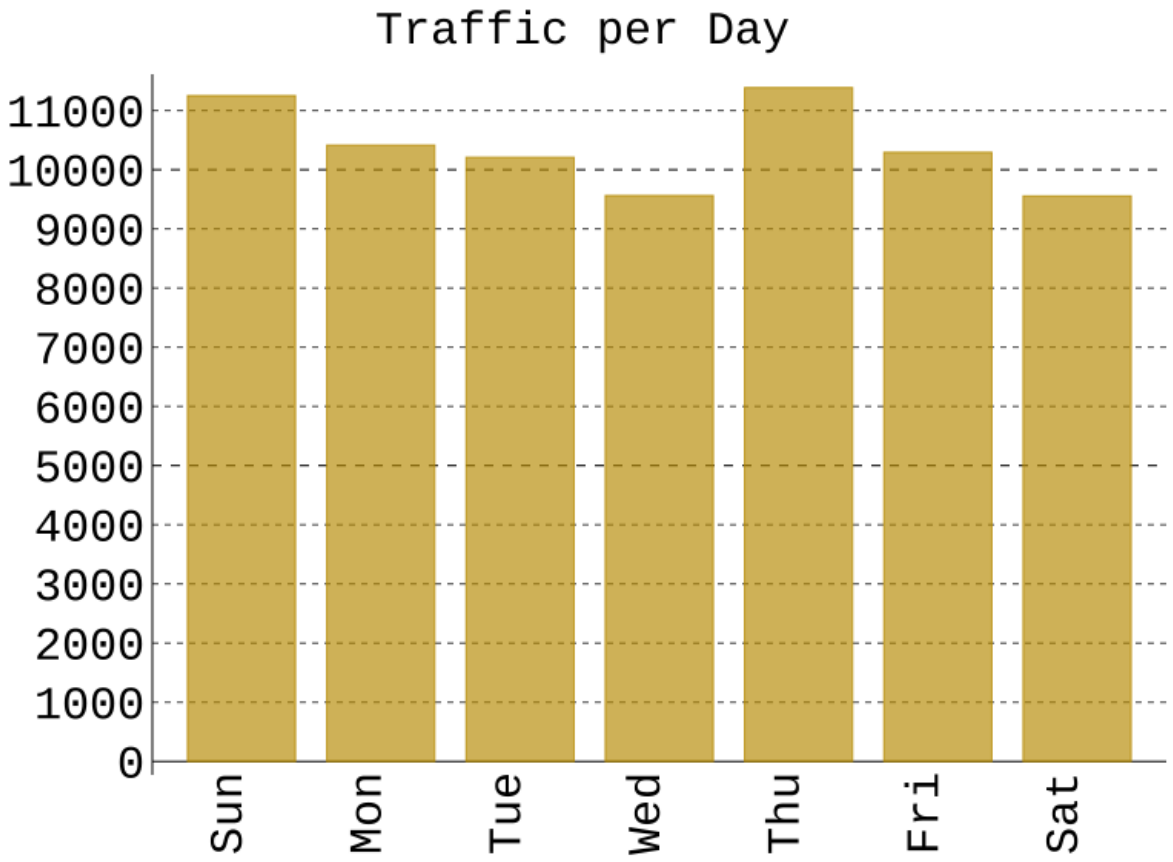
**Yes!** (4)

# RES1: Temporal Analysis – by day




Total traffic for 28 days divided across 7 weekdays

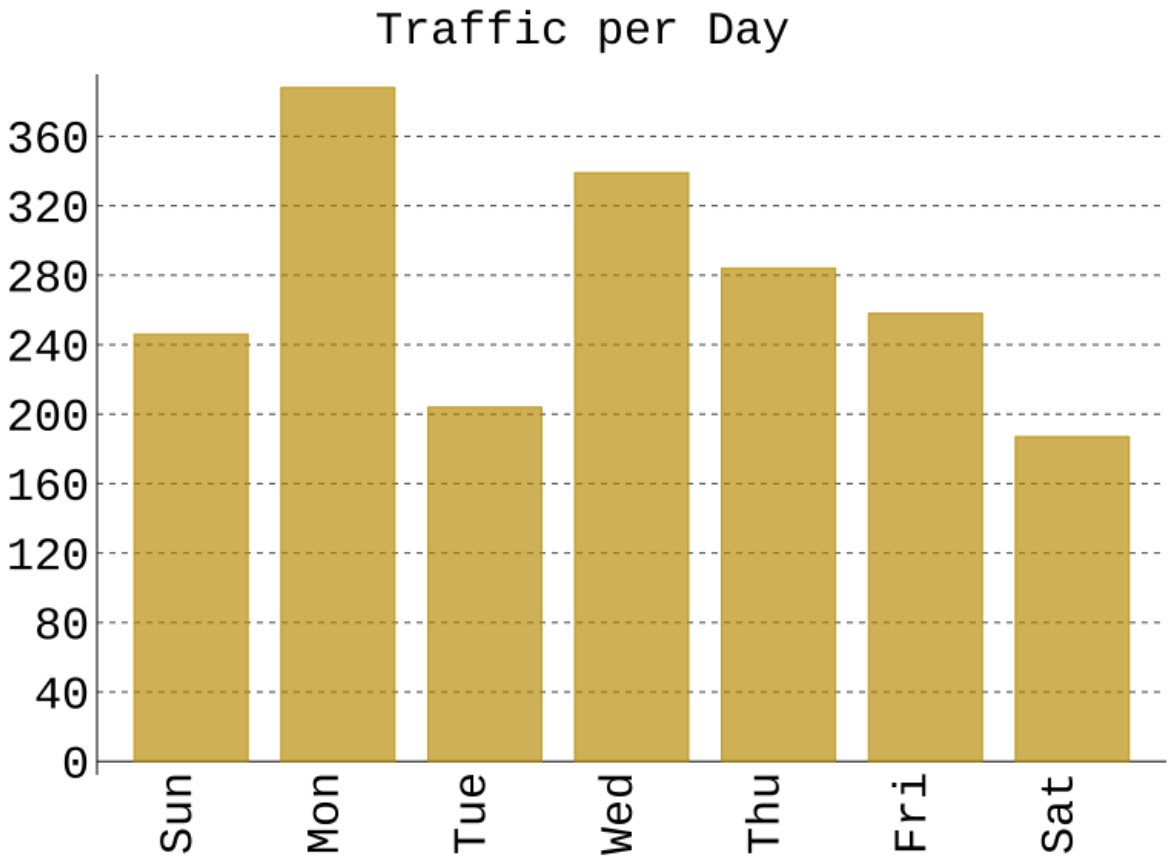
# RES1: Temporal Analysis – by day




**Fail:** Typical 5-workday pattern not discernible

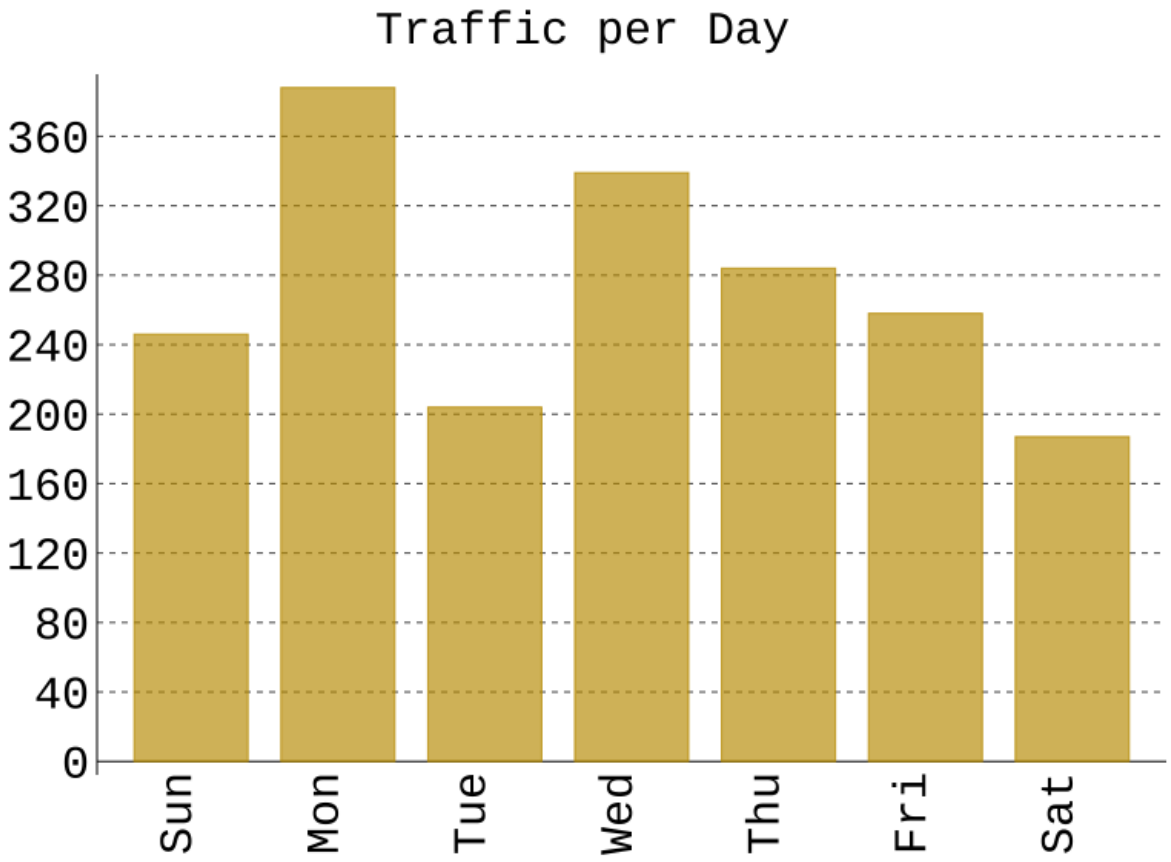
Would likely work for some places though?

# RES2: Temporal Analysis – by day




Total traffic for 28 days divided across 7 weekdays

# RES2: Temporal Analysis – by day




**Fail:** Typical 5-workday pattern not discernible

Would likely work for some places though?

# RES1 Names containing “_”

- _adsp._domainkey.ihjqljmo.cc.
- _adsp._domainkey.linkedin.chi.namibia.na.
- _adsp._domainkey.newsbank.club.
- _adsp._domainkey.till.name.
- _adsp._domainkey.user1-computer.i-did-not-set-mail-host-address--so-tickle-me.
- _adsp._domainkey.uzps.co.sy.
- _adsp._domainkey.xtreamues.trade.
- **_minecraft._tcp.10.0.0.18.**
- **_minecraft._tcp.10.0.0.2.**
- **_minecraft._tcp.73.41.83.66.**
- dkim._domainkey.speedbring.win.
- libglesv1_cm.so.
- mesmtp._domainkey.mad.paris.
- **_xmpp-server._tcp.pandion.im.**
- postfix._domainkey.luffy.cx.
- testglxgetprocaddress_genentry.sh.
- testpatchentrypoints_gldispatch.sh.

Internal Addresses!

Minecraft player!

Jabber User!

# Mitigation Options

## 1) DNS Query Name minimization

- Send only partial queries

## 2) TLS-based DNS encryption

- Encrypt against man-in-the-middle

New!!

## 3) LocalRoot – RFC7706

- Slave the root zone
- Eventually slave others

# https://localroot.isi.edu/

LocalRoot: Serve Yourself *{Beta}*

hardaker@isi.edu
About LocalRoot
Getting Started
Your TSIG Keys
Your Servers
Logout

## Server List

| Administrative Name | Address | TSIG | Enabled | Active | Delete | Config |
|---|---|---|---|---|---|---|
| **10.0.0.2** | 10.0.0.2 | my cool TSIG key: p9ibZHNqKIqxHbtav5OU6g== | ✓ | ✗ | 🗑 | [get config] |

Add a New Server

*(Click on the enabled buttons to toggle)*

*Servers will not be listed **active** until an hour after an initial AXFR has been seen.*

# https://localroot.isi.edu/

LocalRoot: Serve Yourself *{Beta}*

hardaker@isi.edu
About LocalRoot
Getting Started
Your TSIG Keys
Your Servers
Logout

## Configuration Generator

Select from the following parameters to change the configuration code generated below:

Full recursive resolver configuration

Your generated bind configuration for **10.0.0.2** at **10.0.0.2 is:**

edit

```
//
// TSIG keys
//
key "my_cool_TSIG_key" {
    algorithm hmac-sha256;
    secret    "p9ibZHNqKIqxHbtav5OU6g==";
};

//
// upstream servers to transfer from
//

server 128.9.36.81 { keys { "my_cool_TSIG_key"; };}; // localroot.isi.edu



//
// The slave definition for the root zone
//   includes all servers we can transfer data from
```

# Mitigation Option Comparison

| Analysis Method | Qname Min. | TLS | LocalRoot / 7706 |
|---|---|---|---|
| IP Version | N | N | P |
| RRType | Y | P | Y |
| Geographical | N | P | Y |
| Temporal | N | N | Y |
| TLD | N | P | Y |
| SLD | Y | P | Y |
| PSL | Y | P | Y |
| Special Names | Y | P | Y |

1 2 3

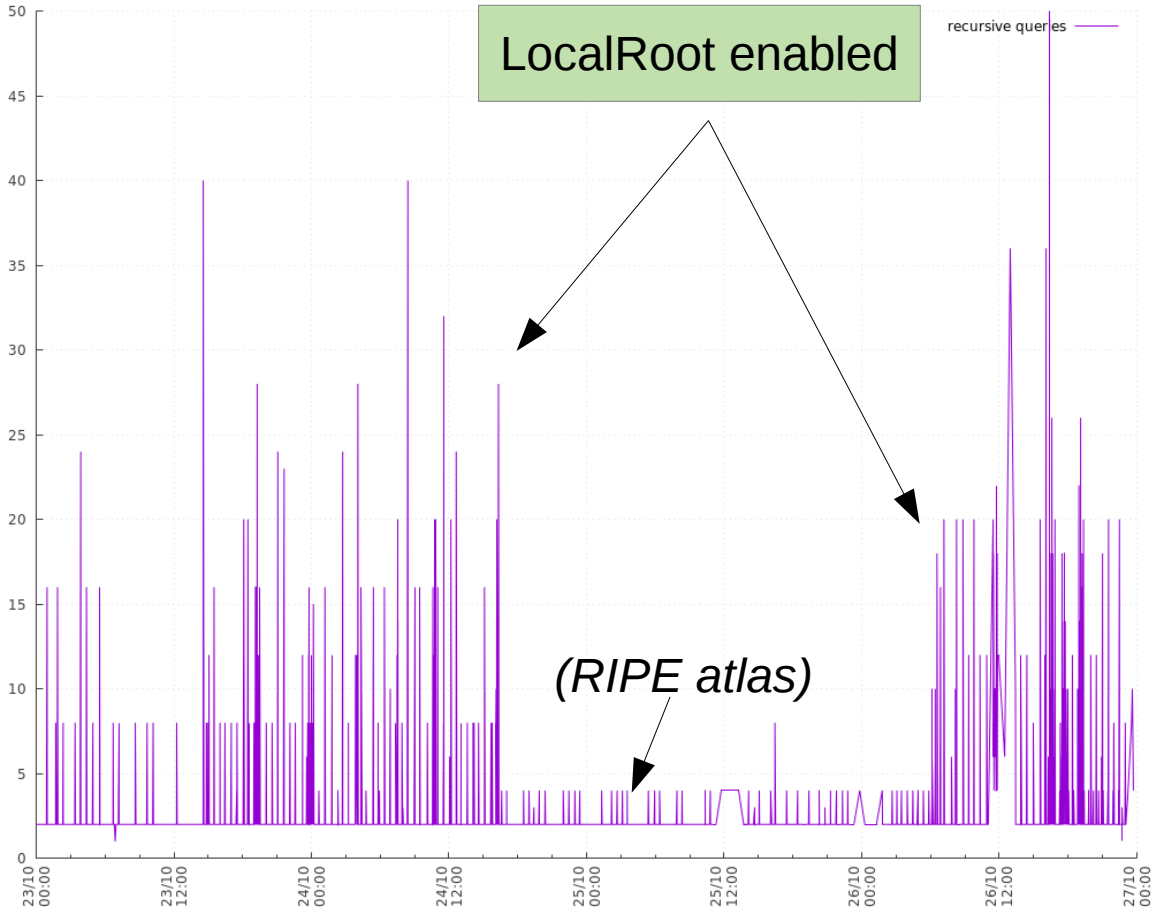
Conclusions:

Note: We only touched the tip of the analysis iceberg

1) Qname Minimization doesn't help geographical and temporal analysis
2) Encryption only works against MiM – not against parental DNS servers
3) The only way to truly be private: **don't ask any questions!!**

https://localroot.isi.edu/

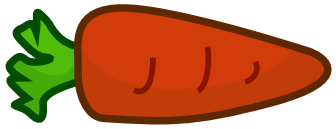
# LocalRoot: Don’t Ask Questions




https://localroot.isi.edu/

# Conclusions

- QName Minimization and TLS only go so far
  - Traffic analysis discloses other sensitive data
  - You still need to trust the parent hierarchy
- More data studies are needed
  - *(great thanks to Robert Story for his residence data)*
- Distributed naming and push models win



- https://localroot.isi.edu/
  - Solves much of this, but only for the root *(currently)*
  - Cost: bandwidth and memory