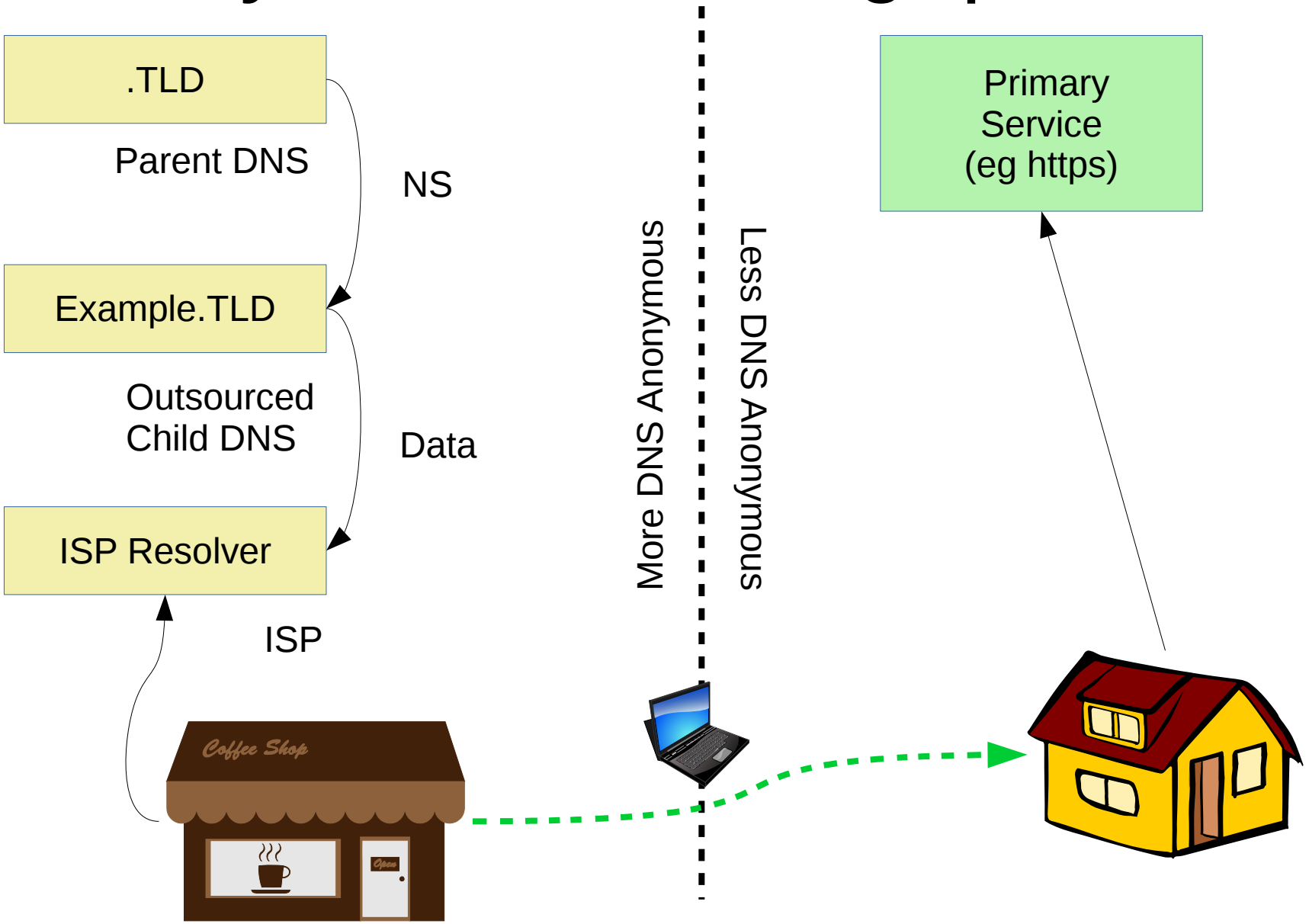
Analyzing and Mitigating Privacy with the DNS Root Service

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

2017 NDSS – I Pondered: Can you avoid asking questions?

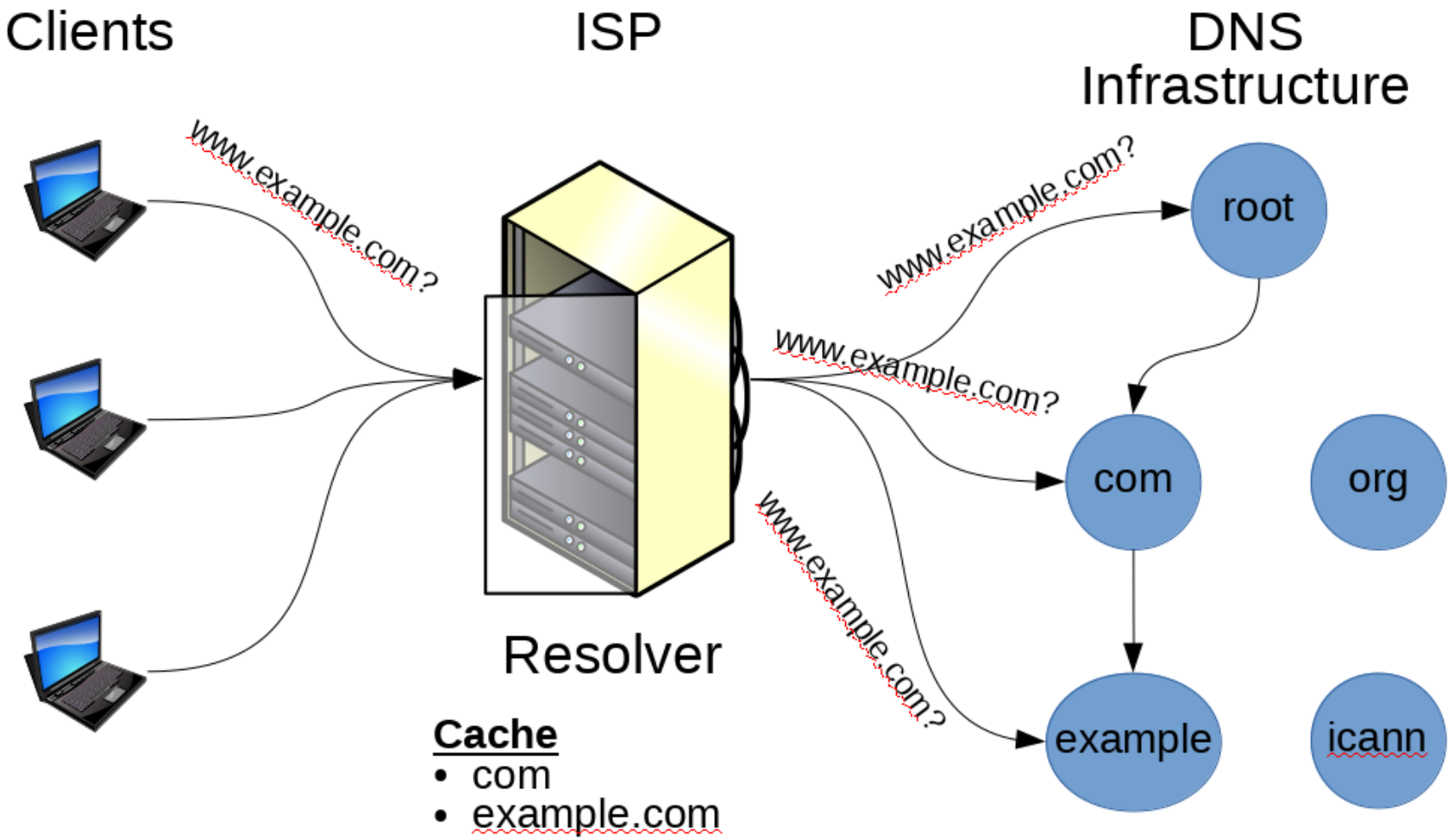


Parental Authoritative Privacy

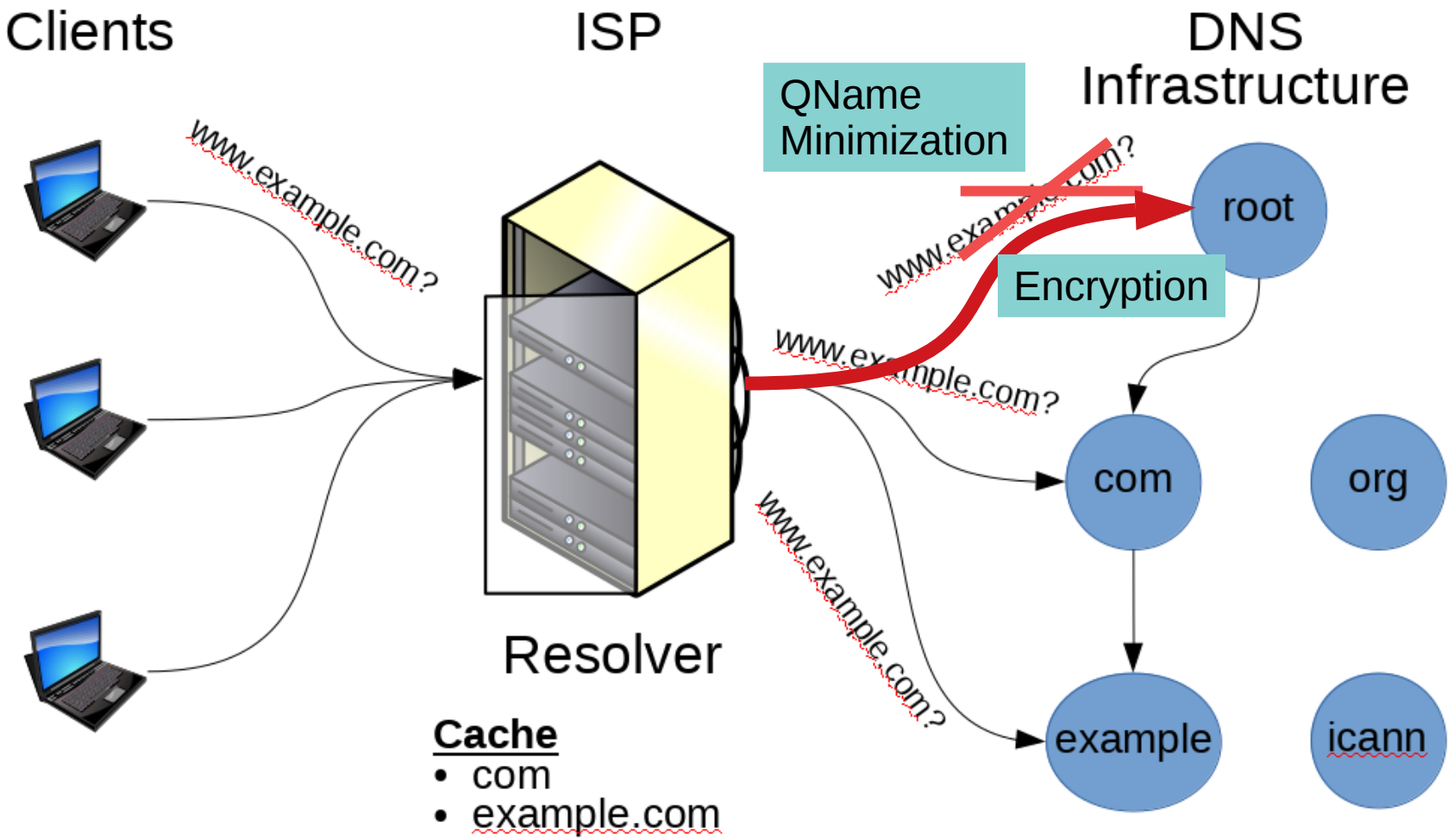
- Does query leakage really reveal anything?
  - What do DNS grandparents see about me?
    - (e.g.) the root?
- Can traffic analysis reveal anything?
- Can temporal analysis reveal anything?

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

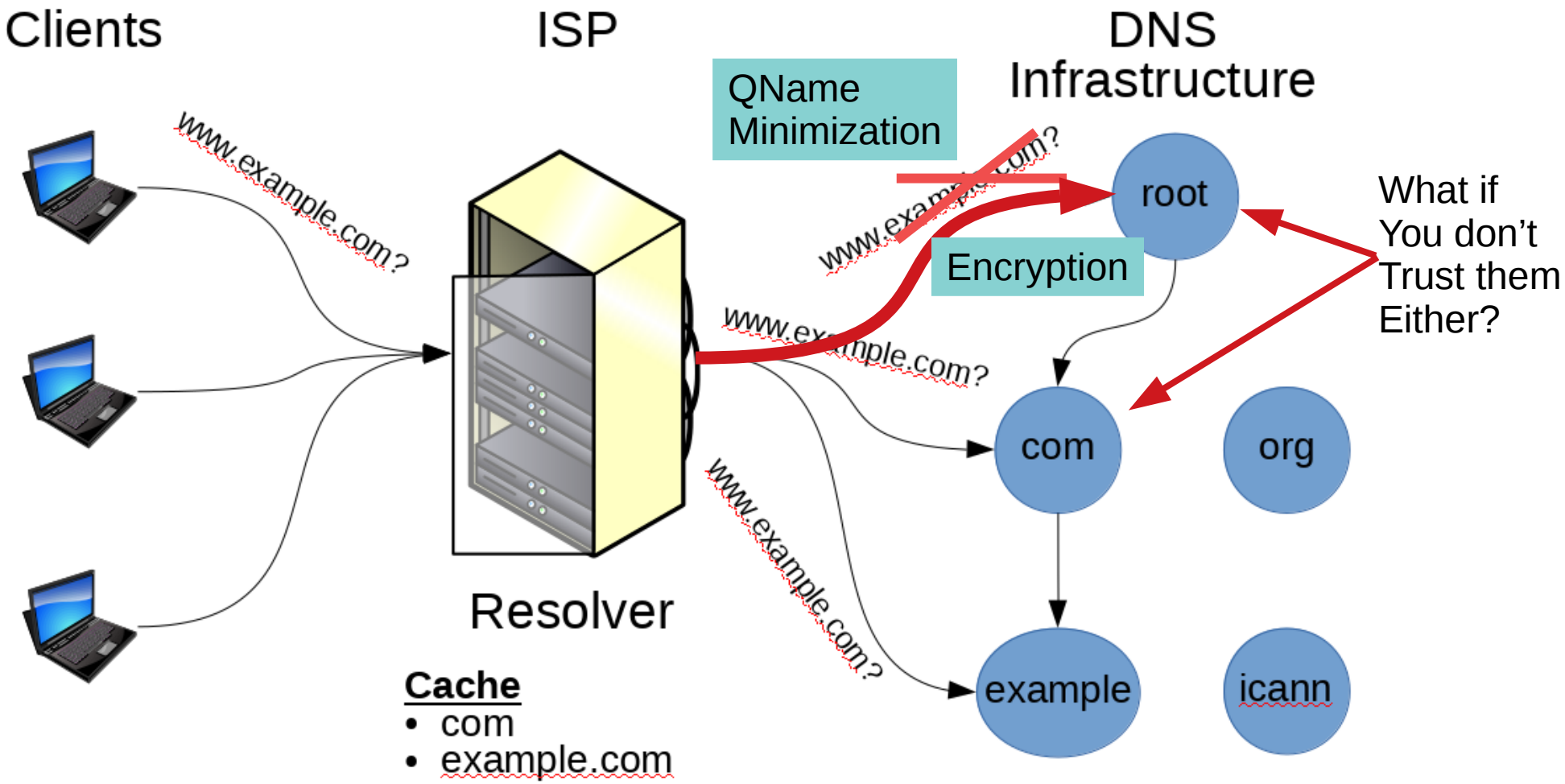
DNS Query Leaking to the Roots



DNS Query Leaking to the Roots



DNS Query Leaking to the Roots



Experiment Plan and Data

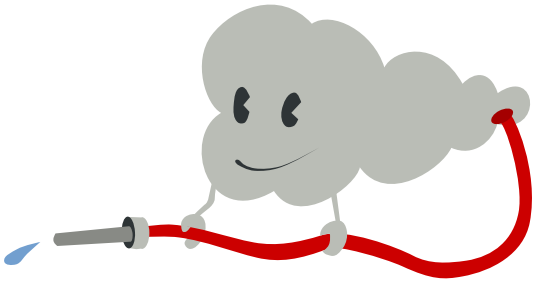
- Two residences
  - Recursive resolvers
  - Static IP
  - Willingness
  - Providing ground truth
- An authoratative server
  - B-Root
  - **One month** of query data: **2017, Jan**.
- Bulk global analysis
  - Quick analysis

Data Statistics

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

Analysis Types

- RRTYPE
- Geographical
- Temporal
- Special Name

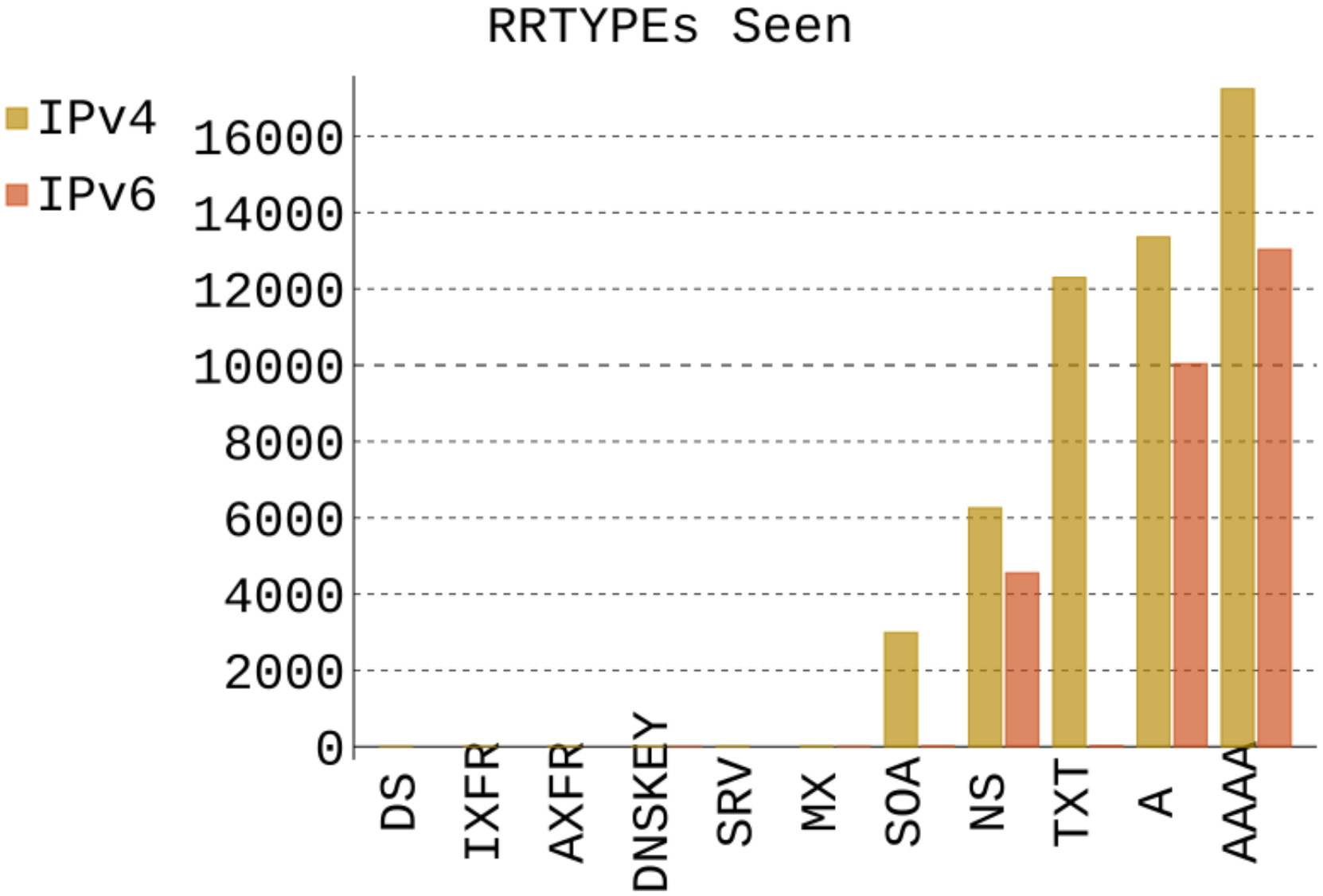


- Warning: Results coming next at firehose rate

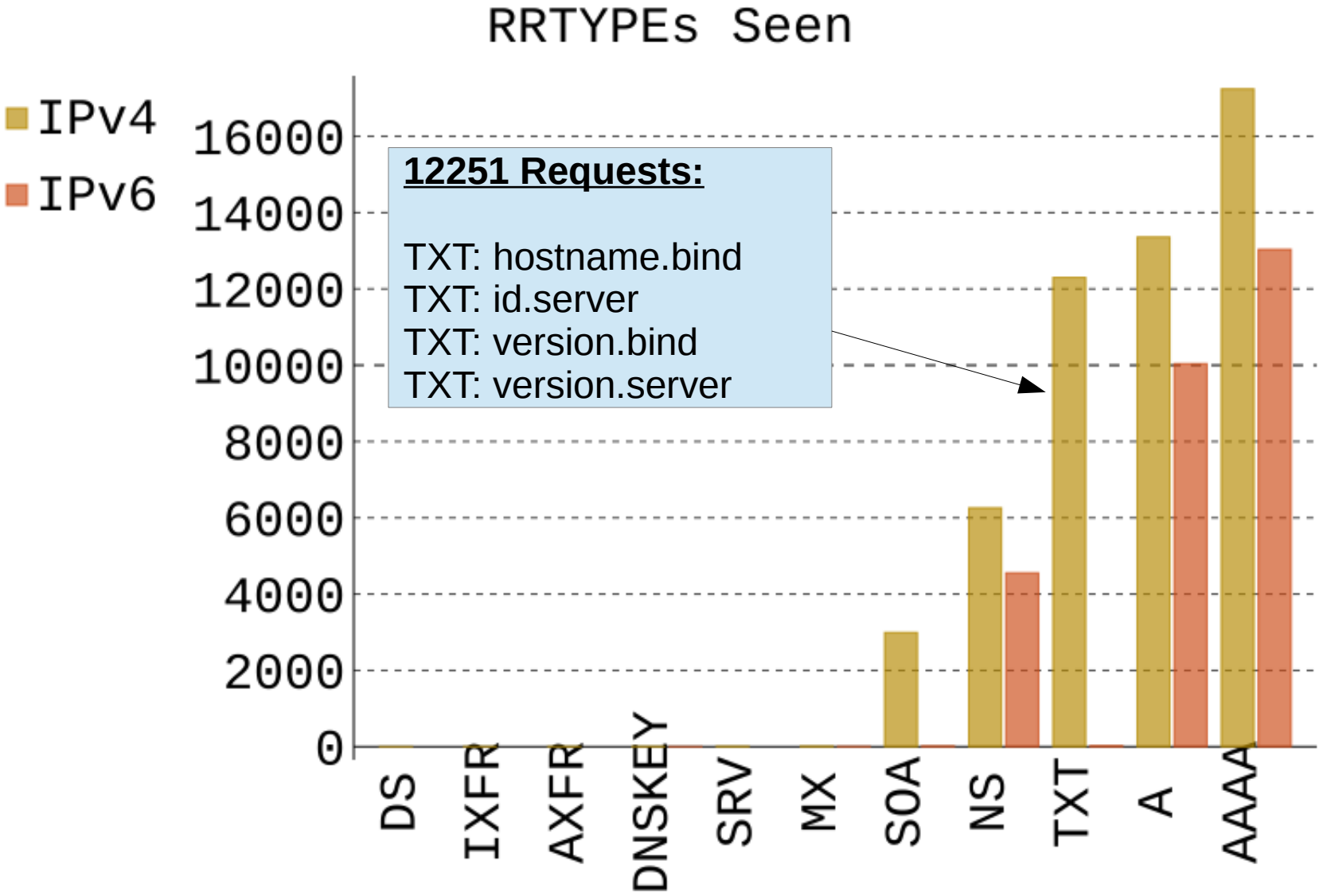
  (don't try this at home)

Even more Analysis in The paper

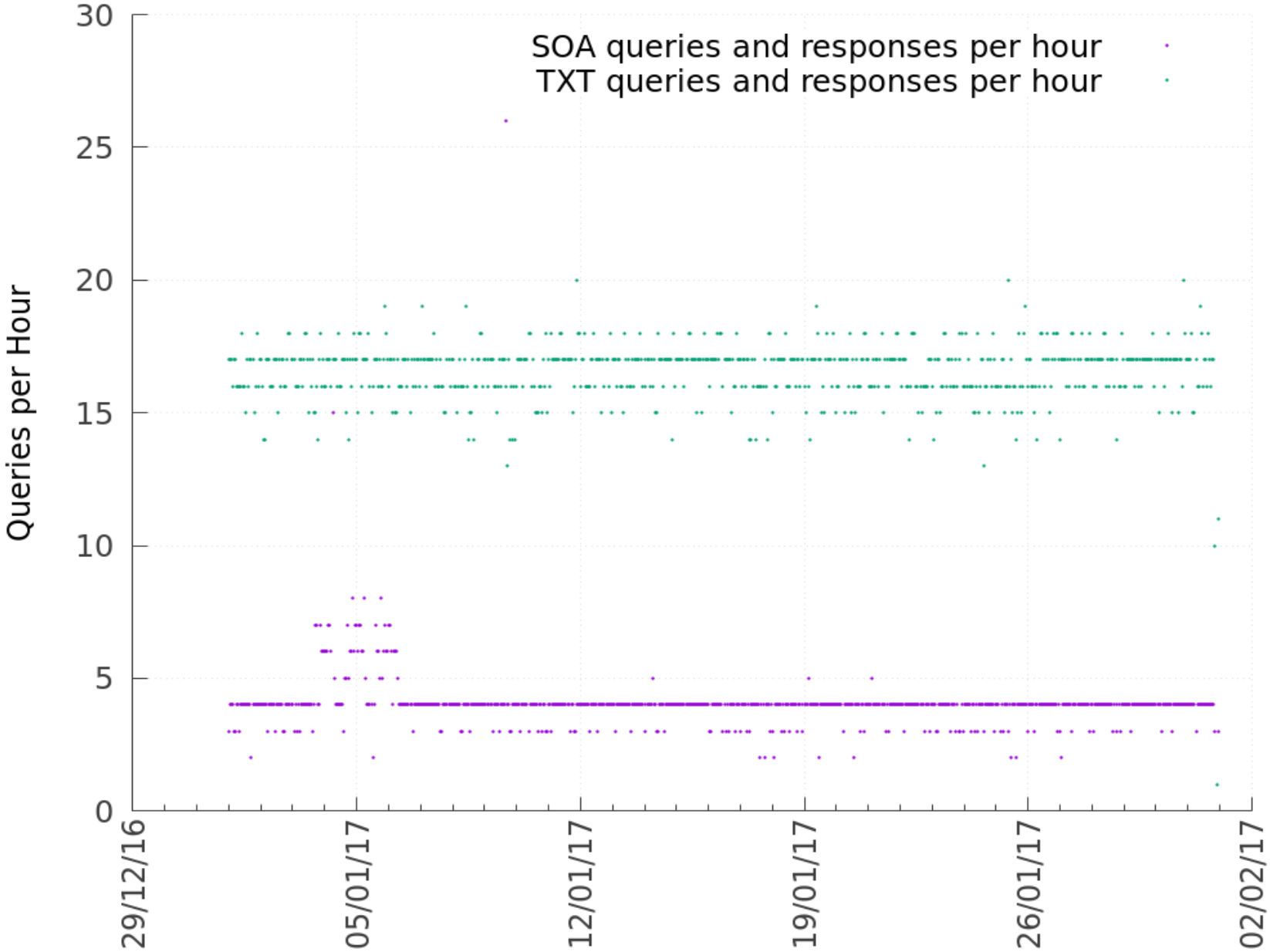
RES1 RRTYPE Analysis



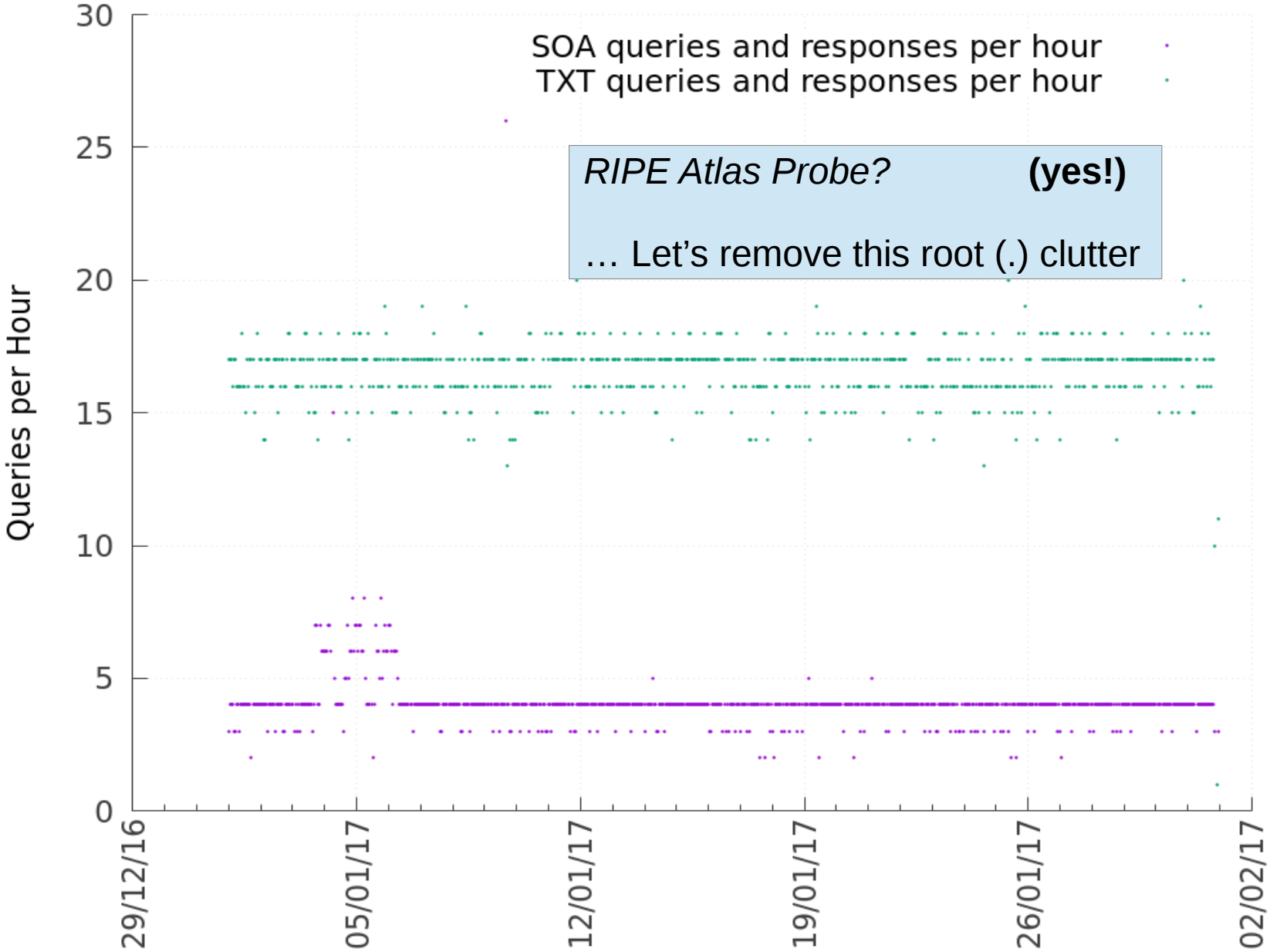
RES1 RRTYPE Analysis



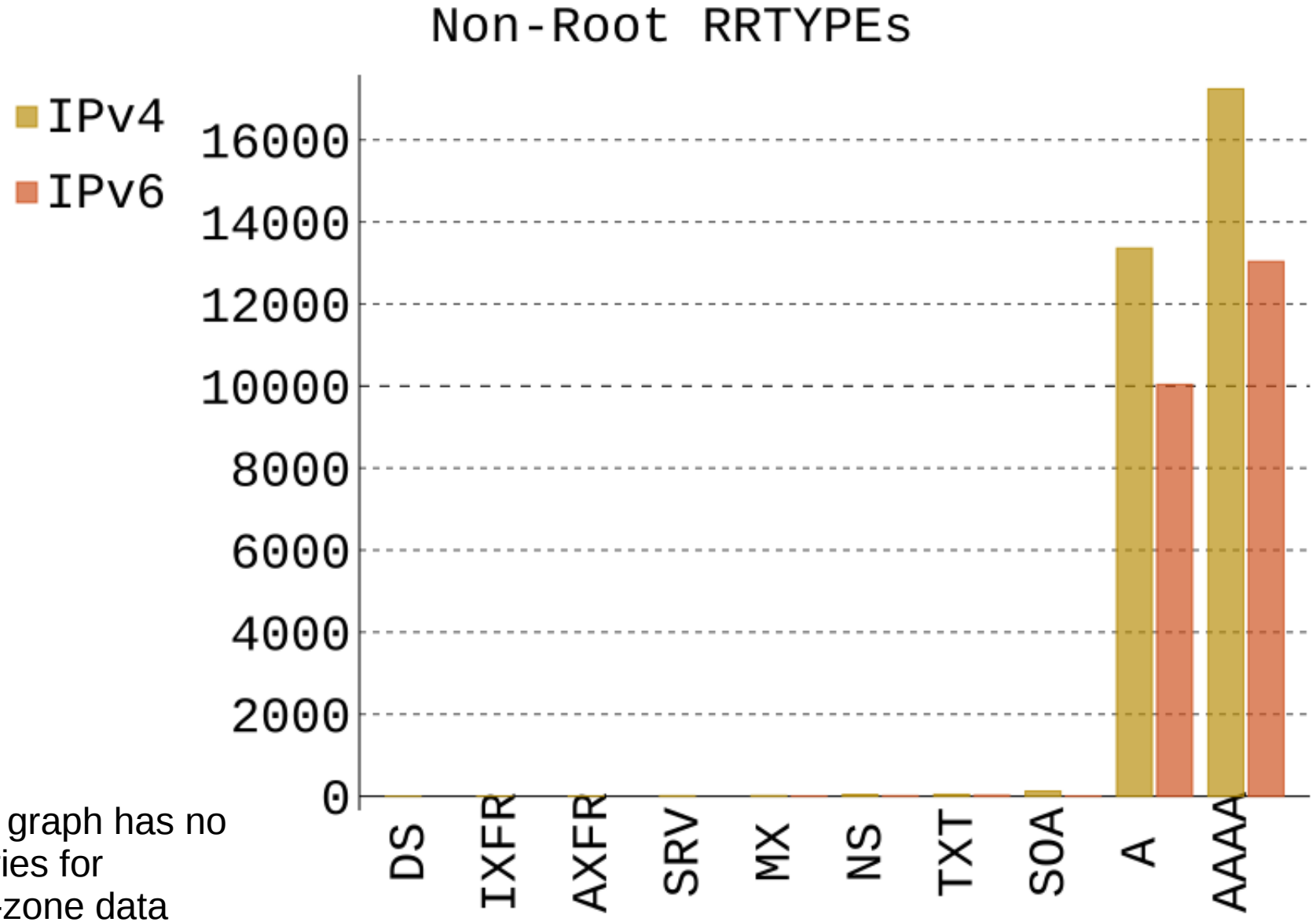
RES1 RRTYPE Analysis



RES1 RRTYPE Analysis

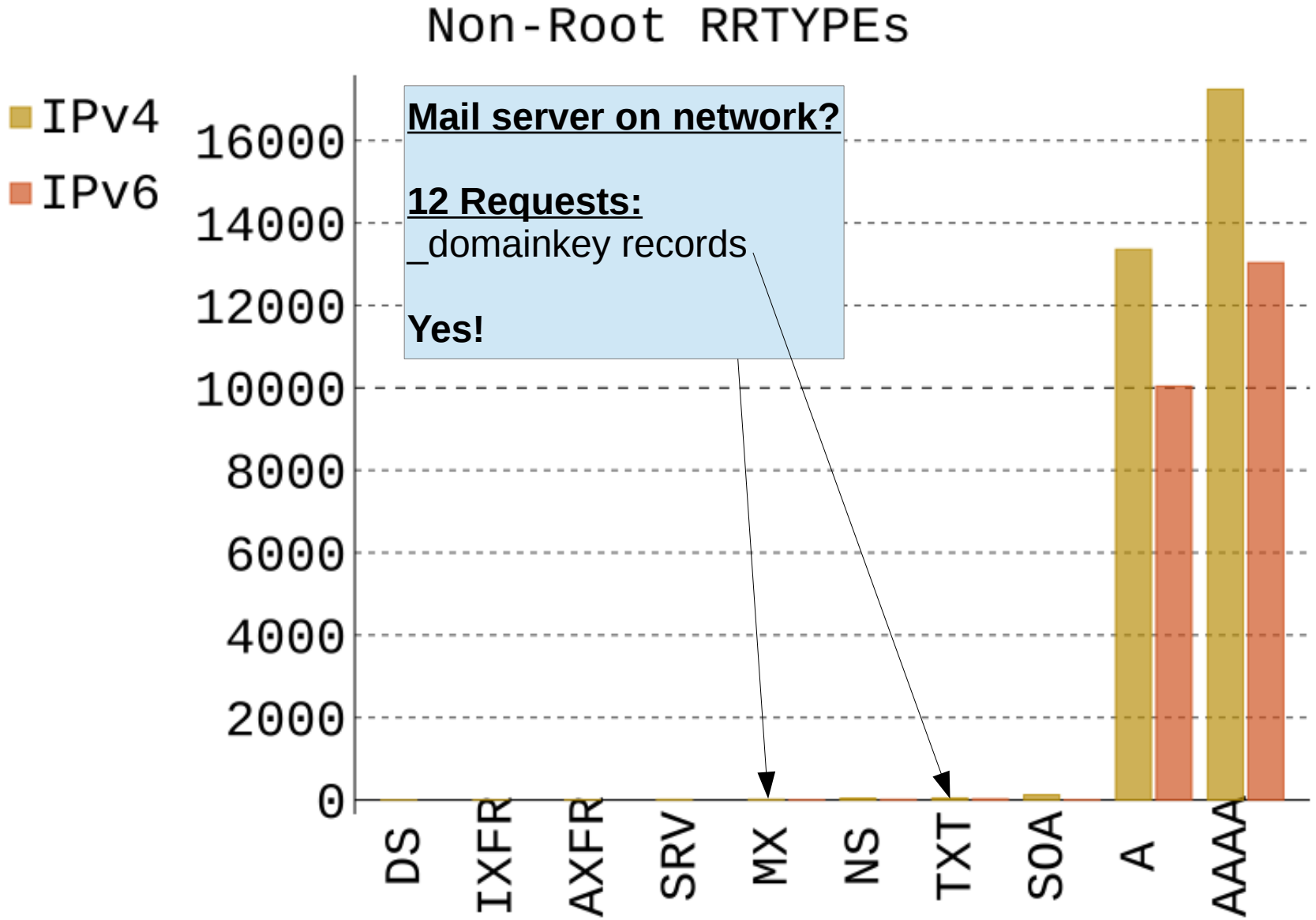


RES1 RRTYPE Analysis – Non Root

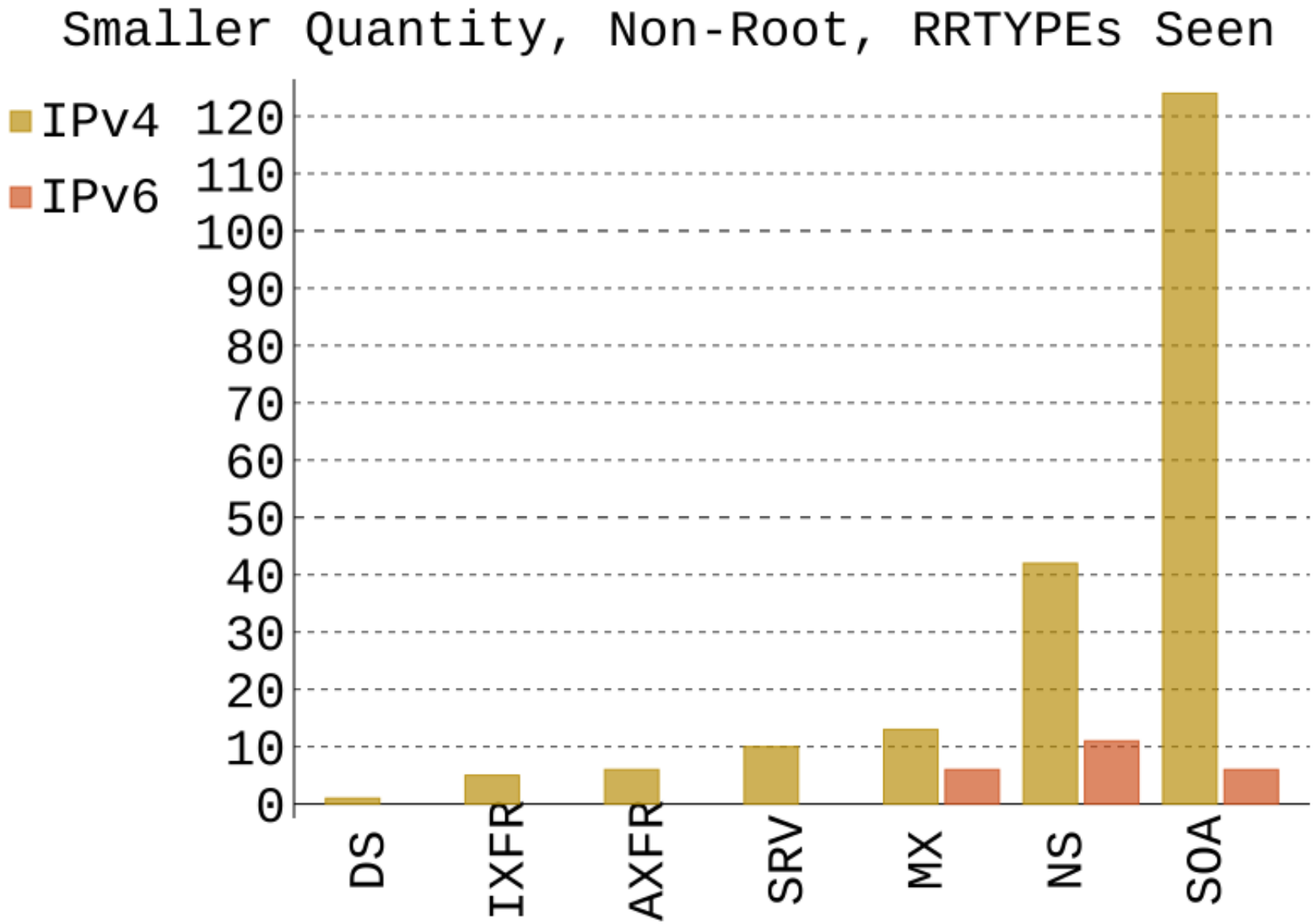


This graph has no queries for root-zone data (i.e. no “.” queries)

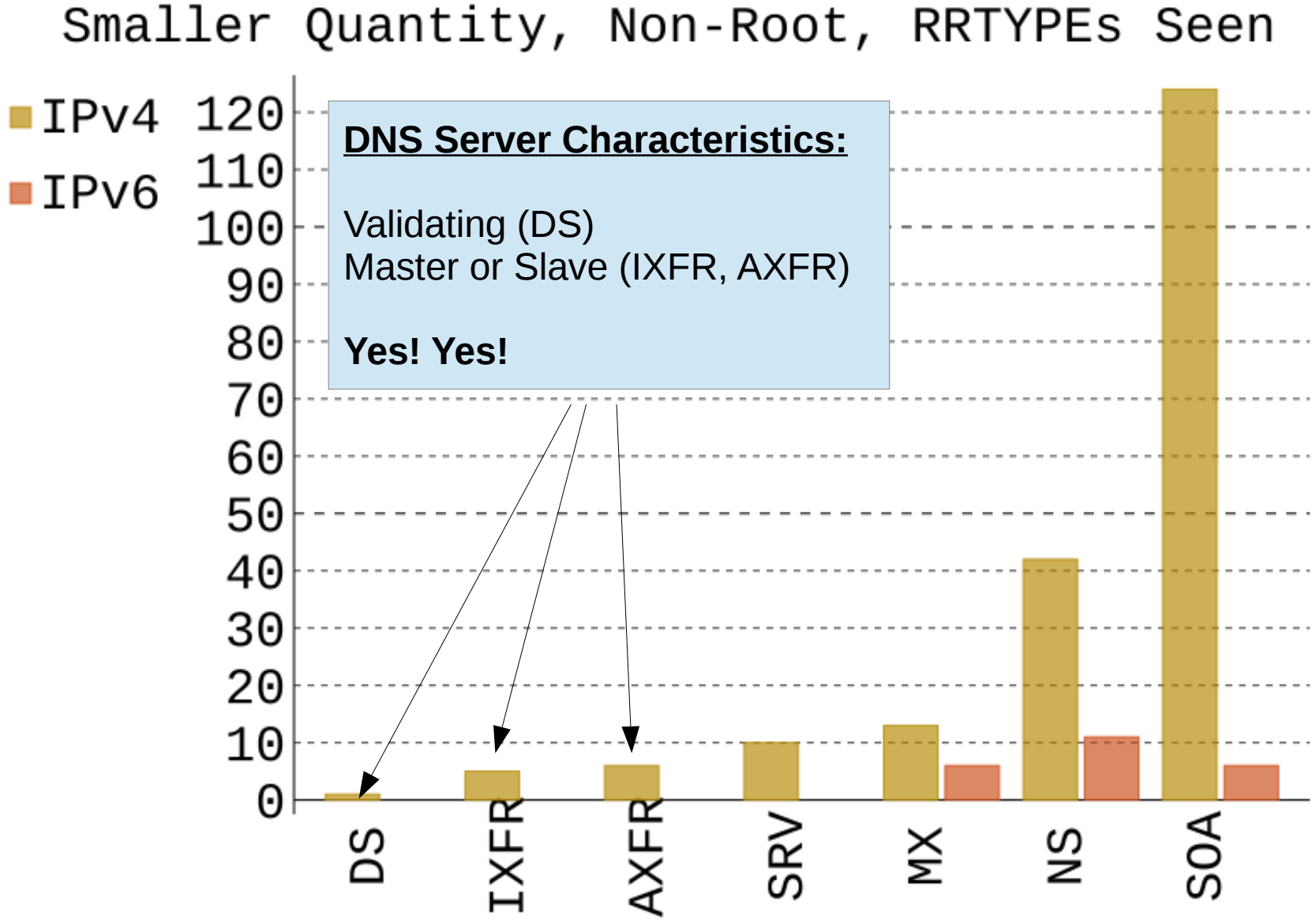
RES1 RRTYPE Analysis – Non Root



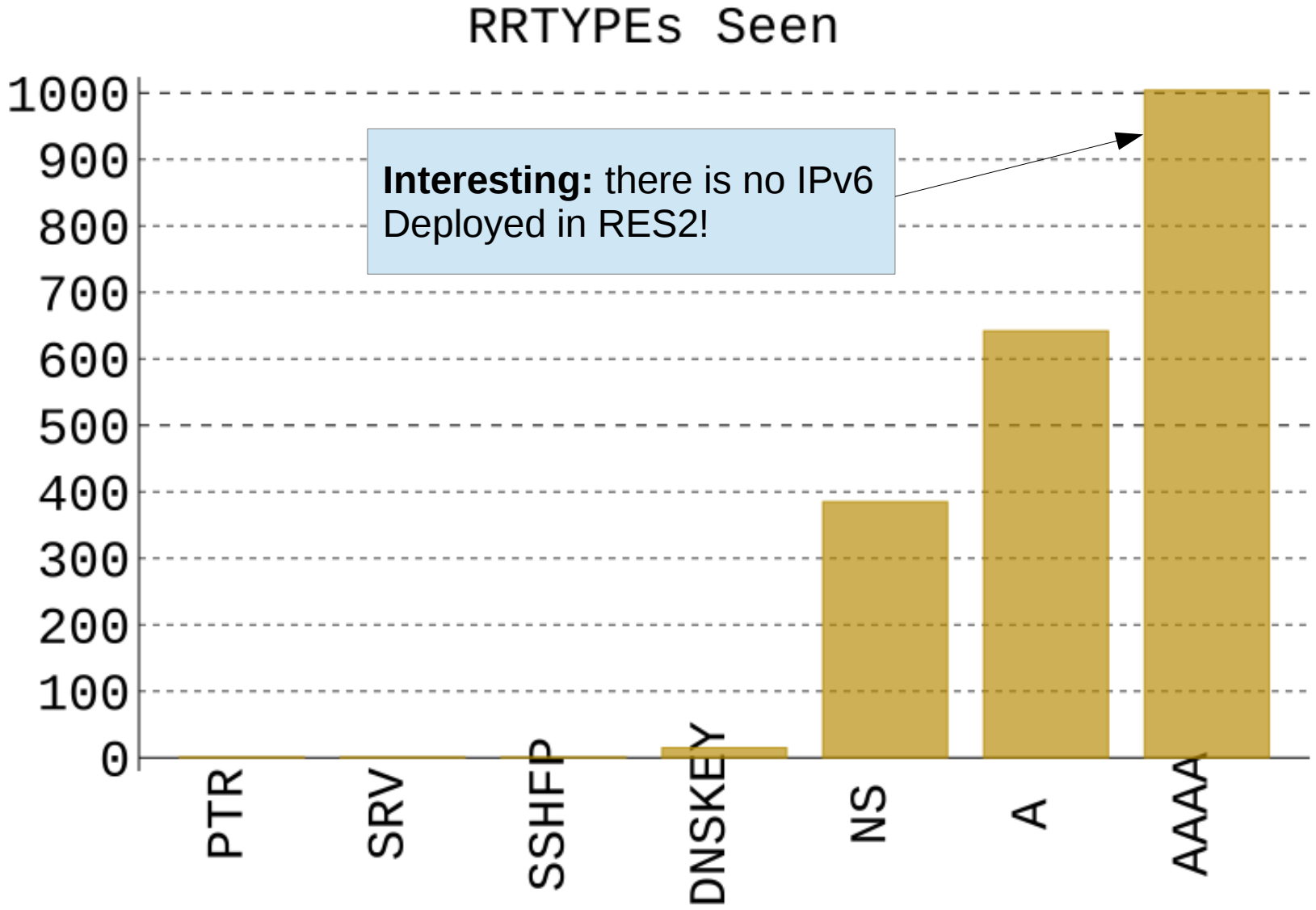
RES1 RRTYPE Analysis – Smaller



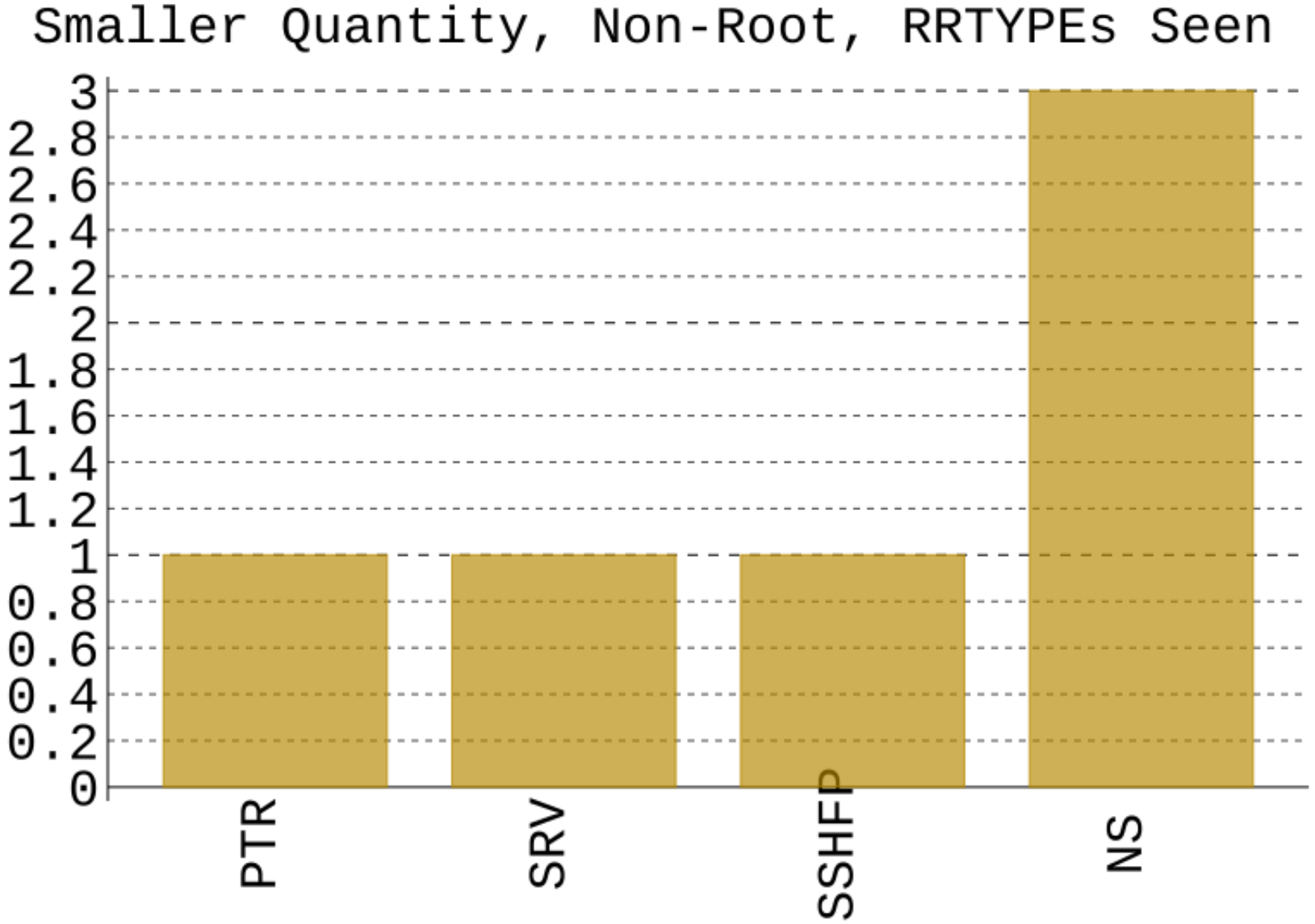
RES1 RRTYPE Analysis – Smaller



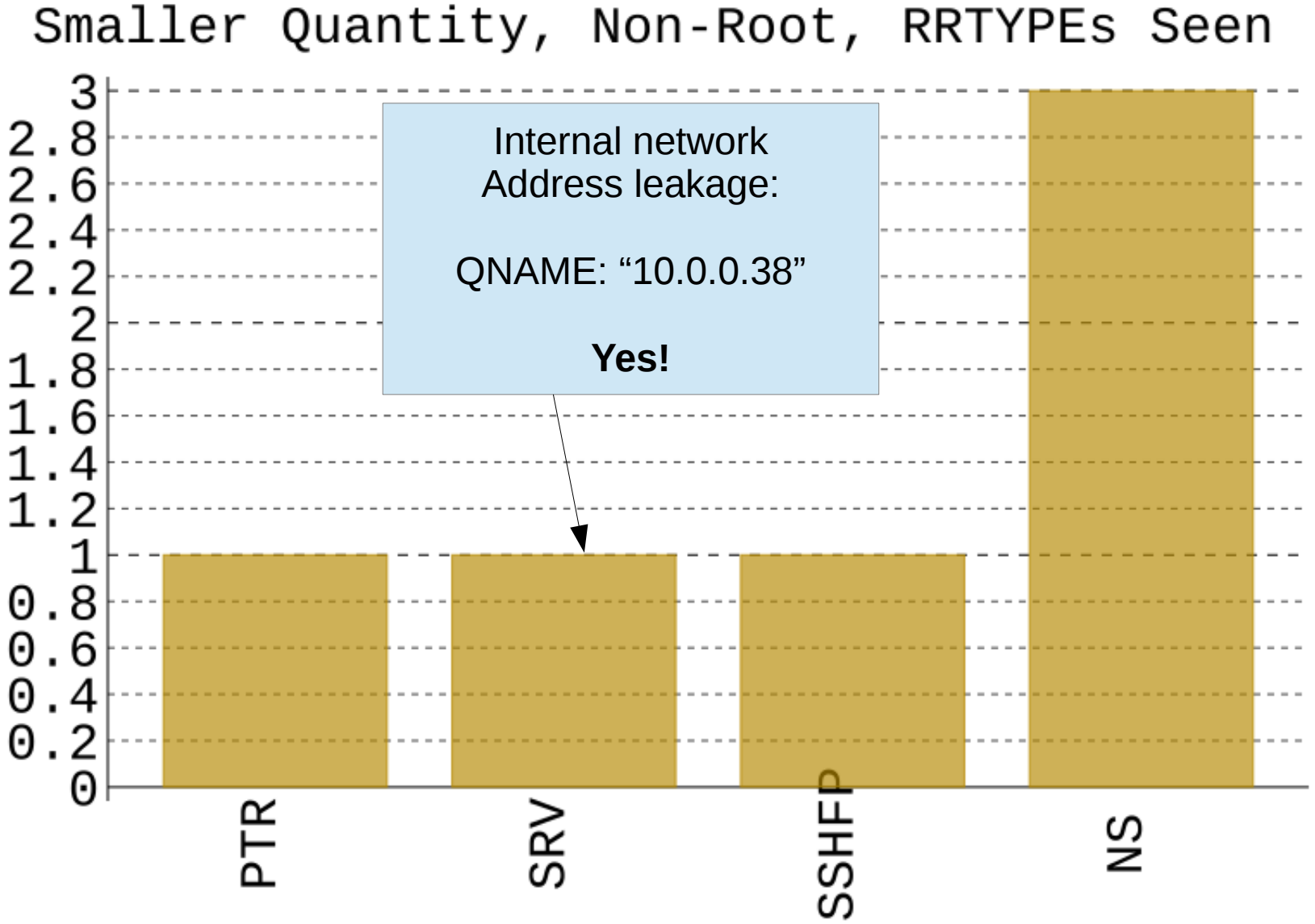
RES2 RRTYPE Analysis



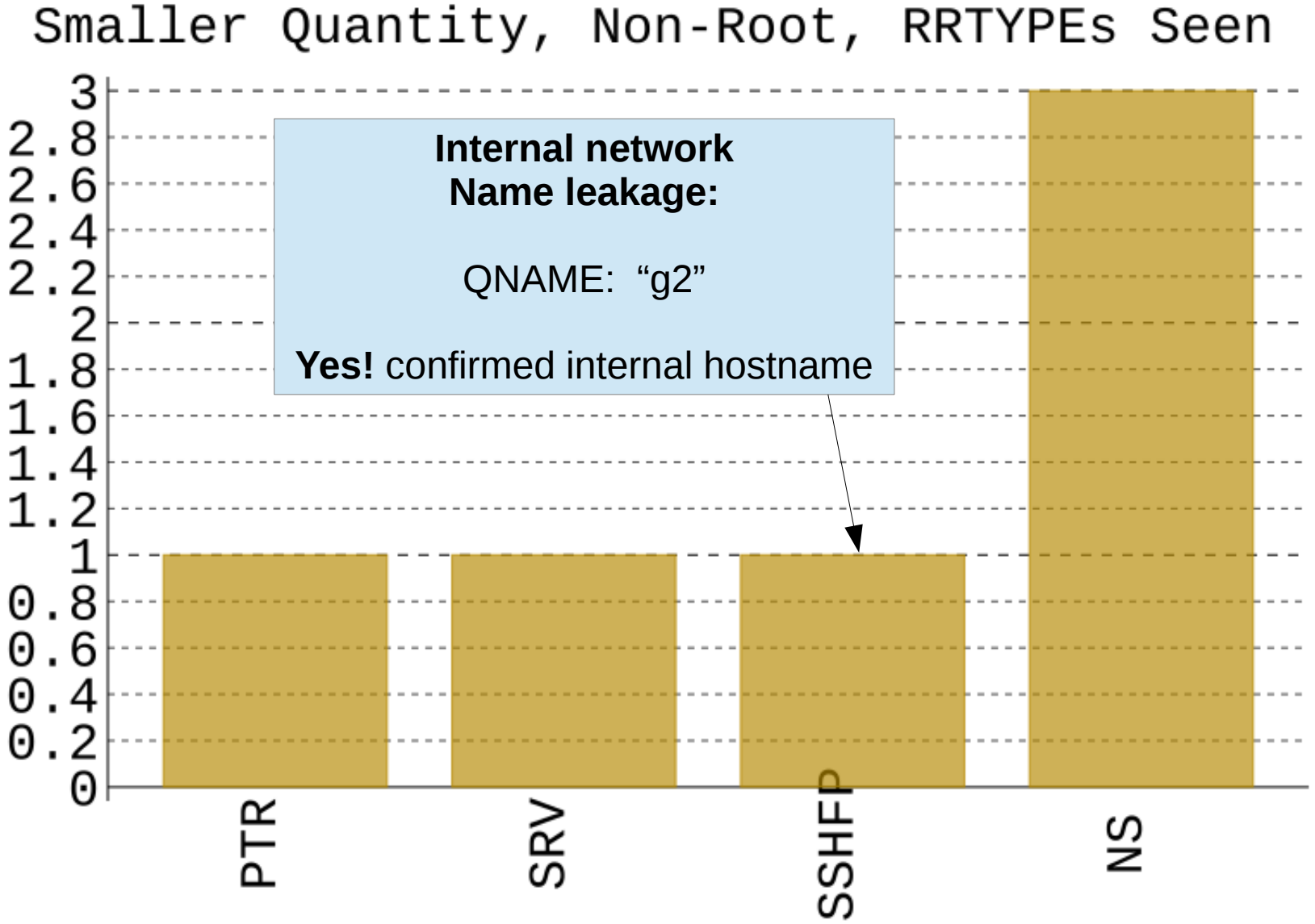
RES2 RRTYPE Analysis



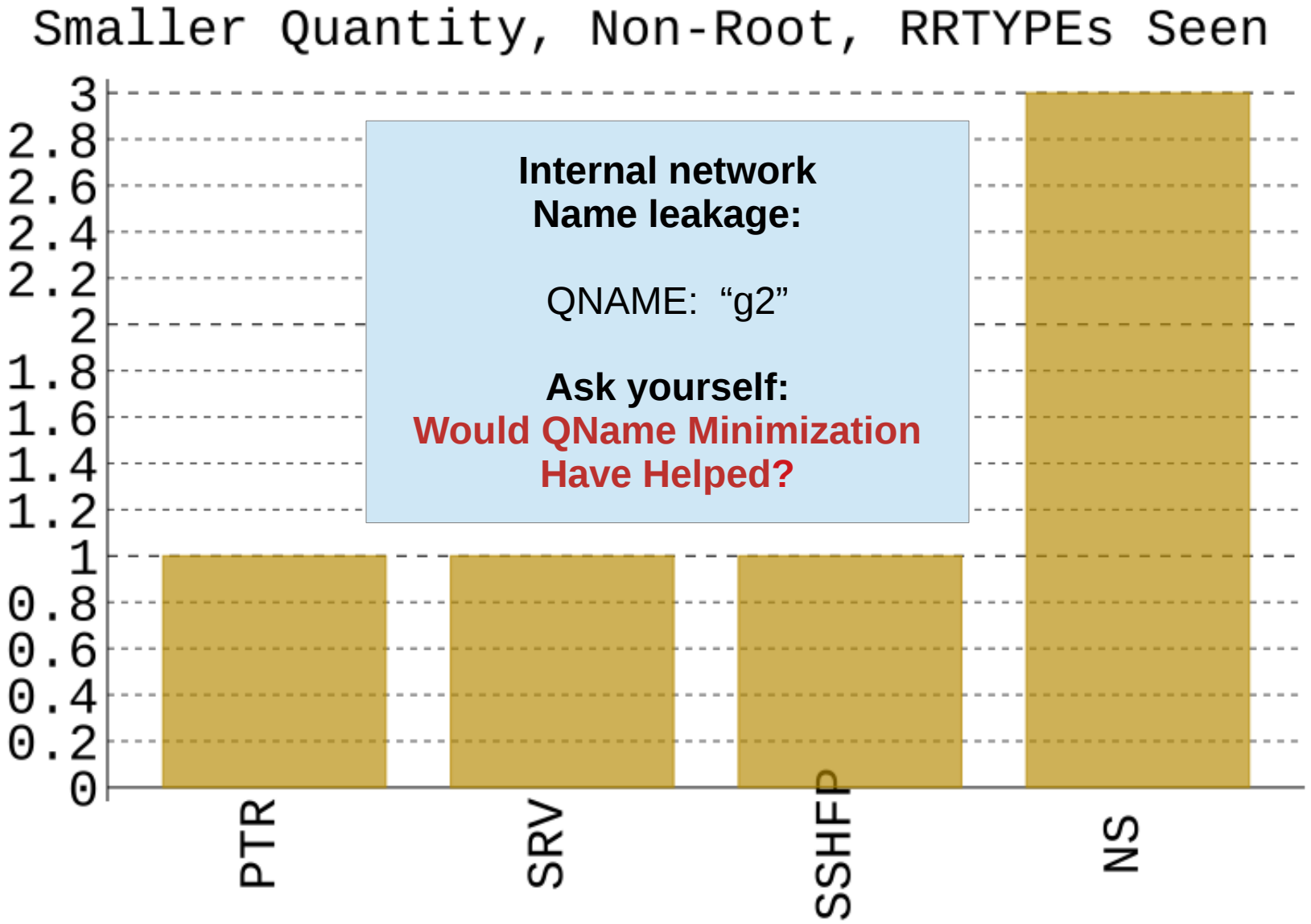
RES2 RRTYPE Analysis



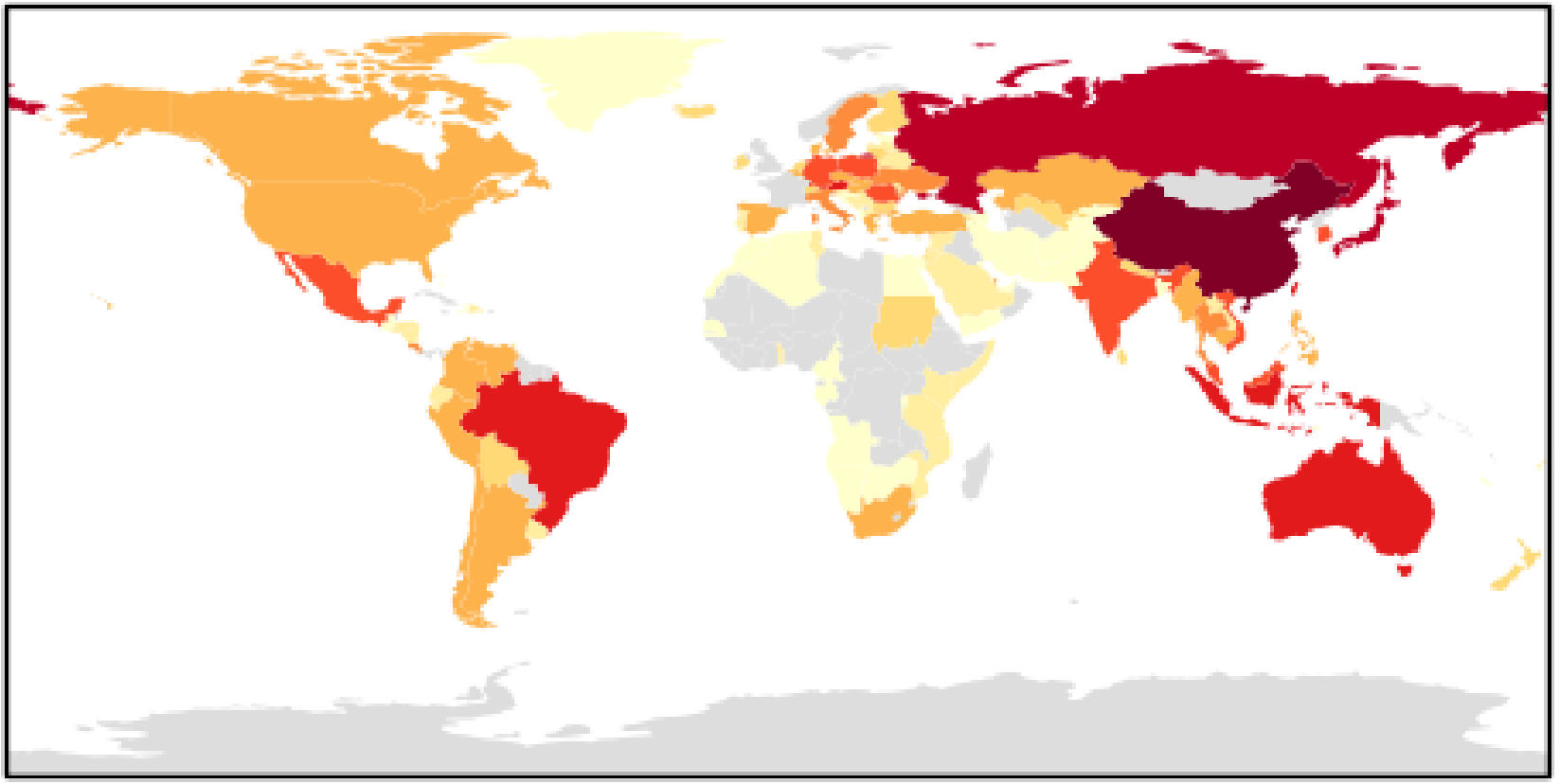
RES2 RRTYPE Analysis



RES2 RRTYPE Analysis

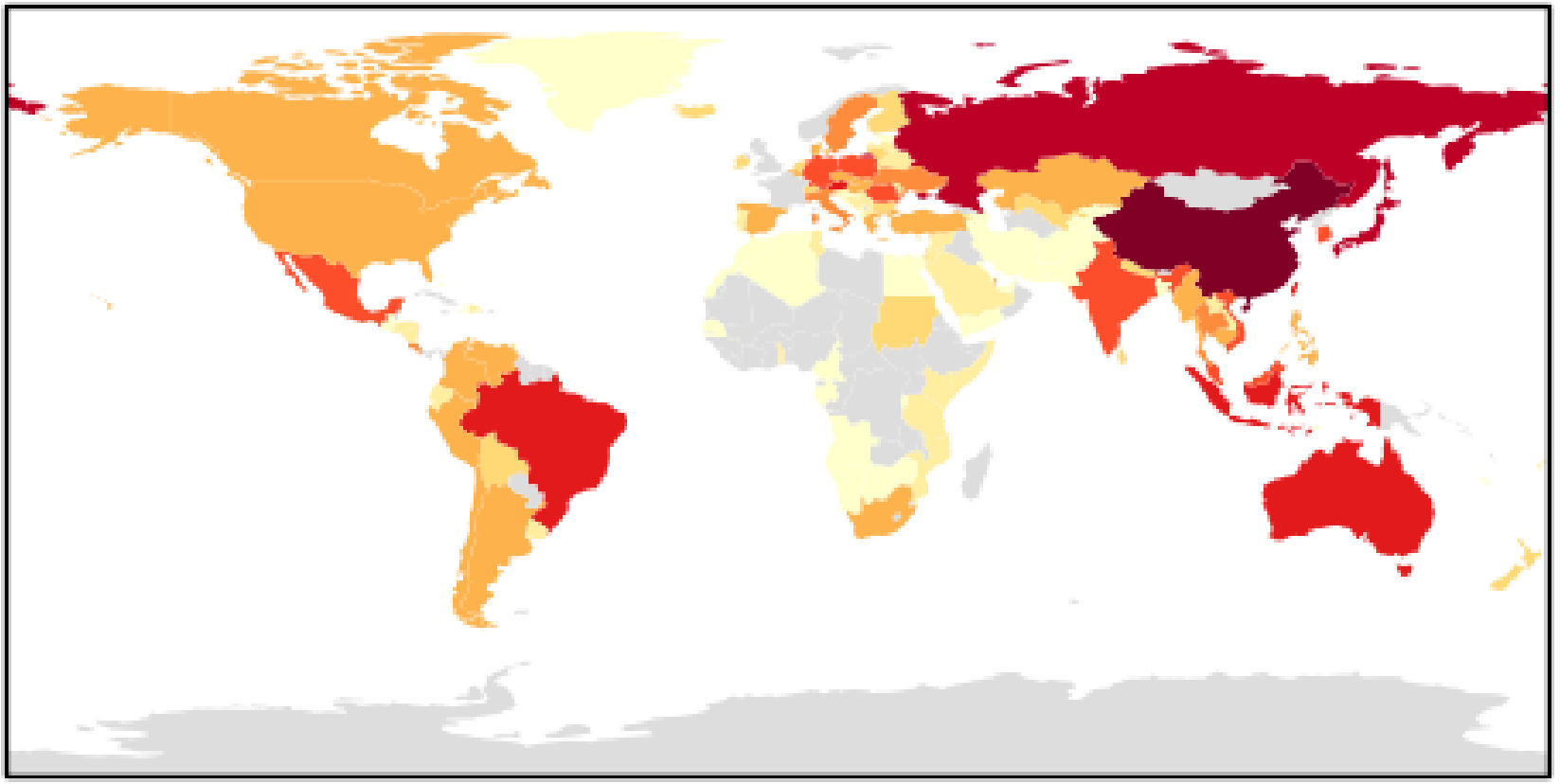


RES1 Geographical Analysis



Heat Map: Most popular CC-TLDs

RES1 Geographical Analysis

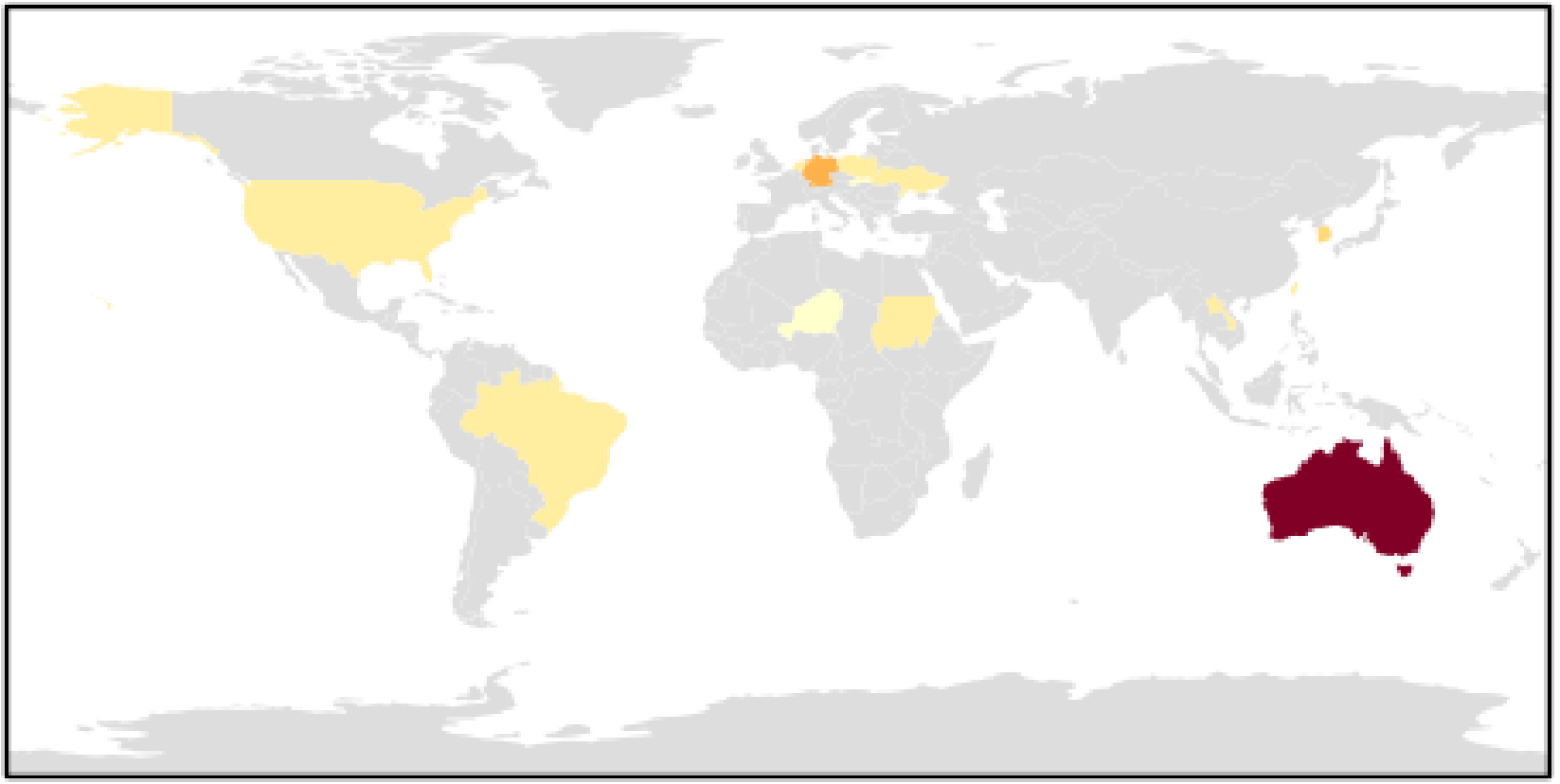


Heat Map: Most popular CC-TLDs

Lots of communication with China and Russia?

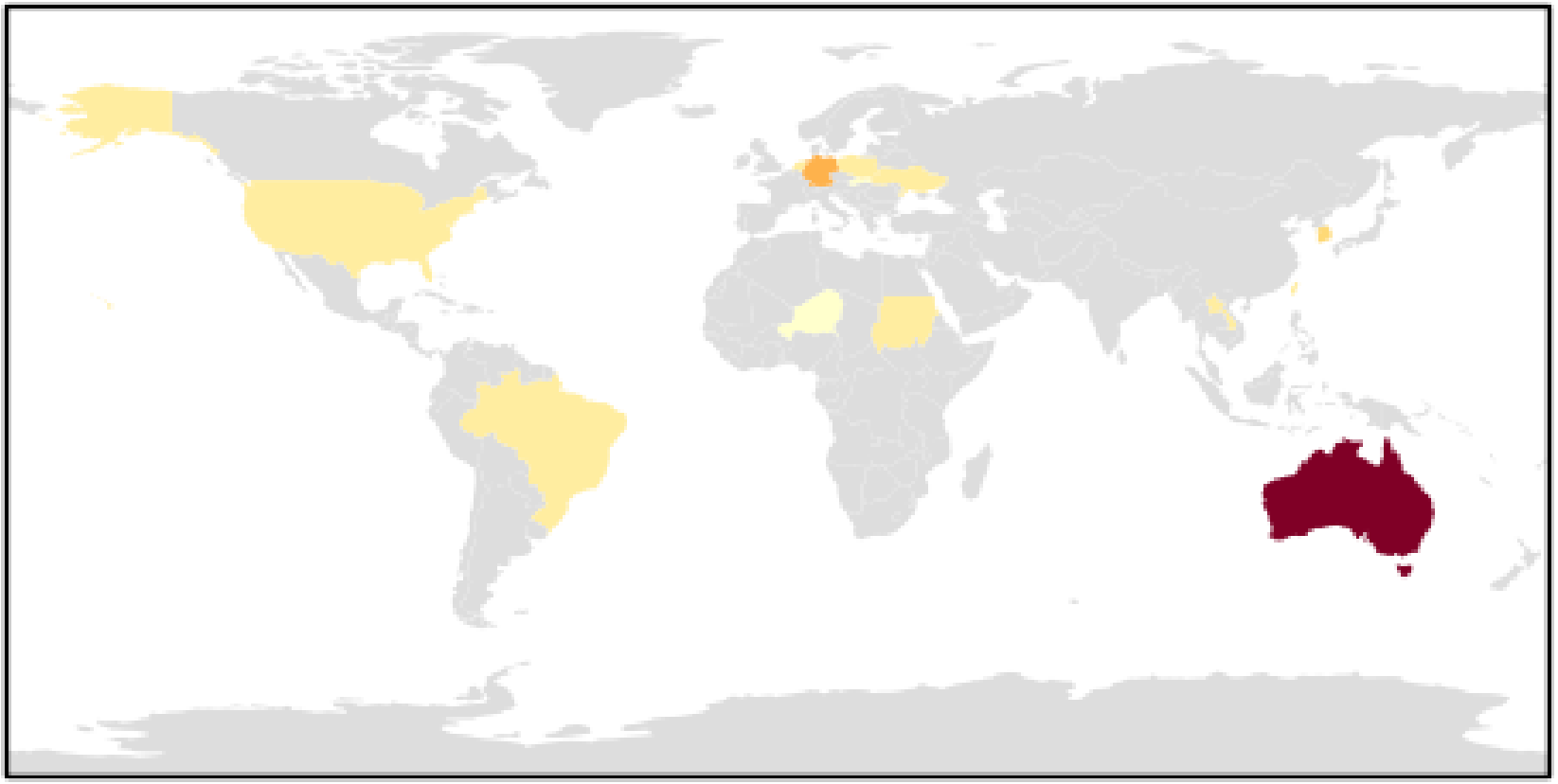
No! Fail! – SPAM

RES2 Geographical Analysis



Heat Map: Most popular CC-TLDs

RES2 Geographical Analysis

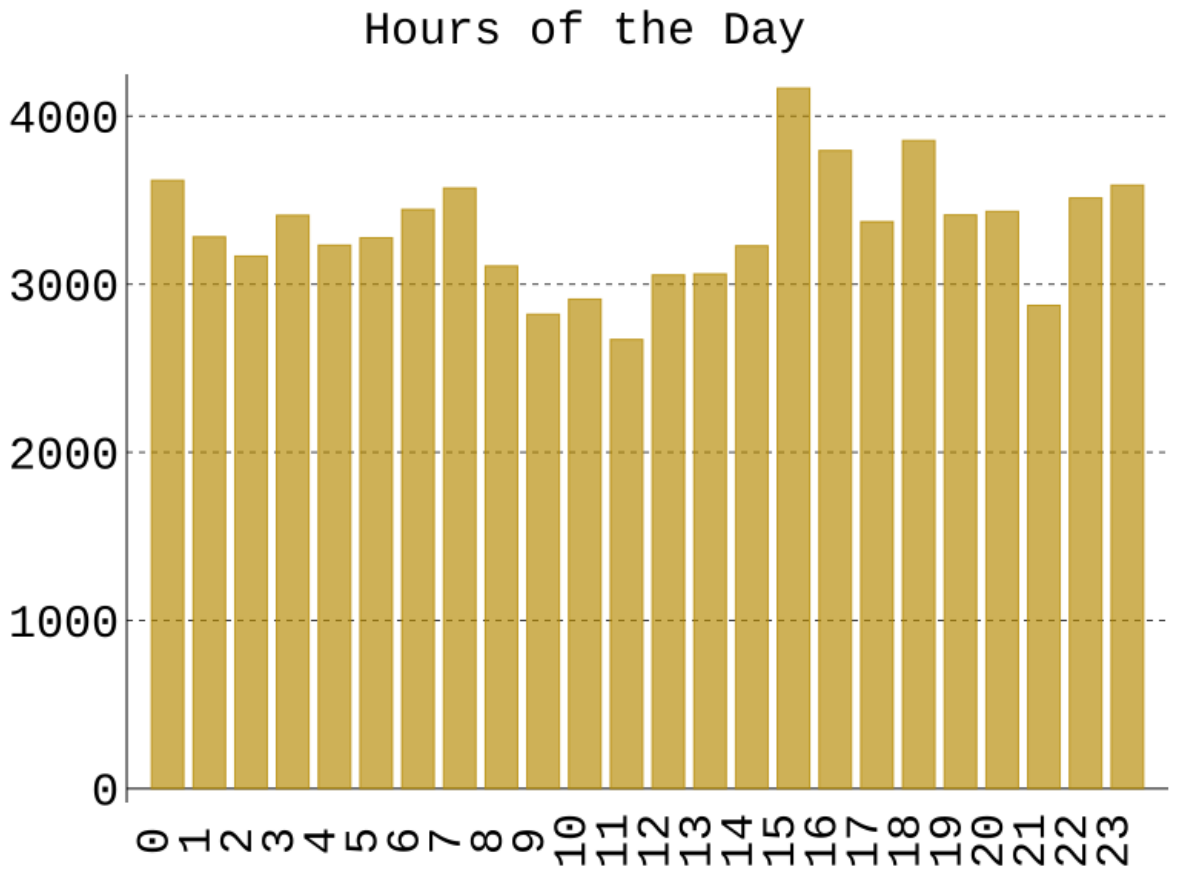


Heat Map: Most popular CC-TLDs

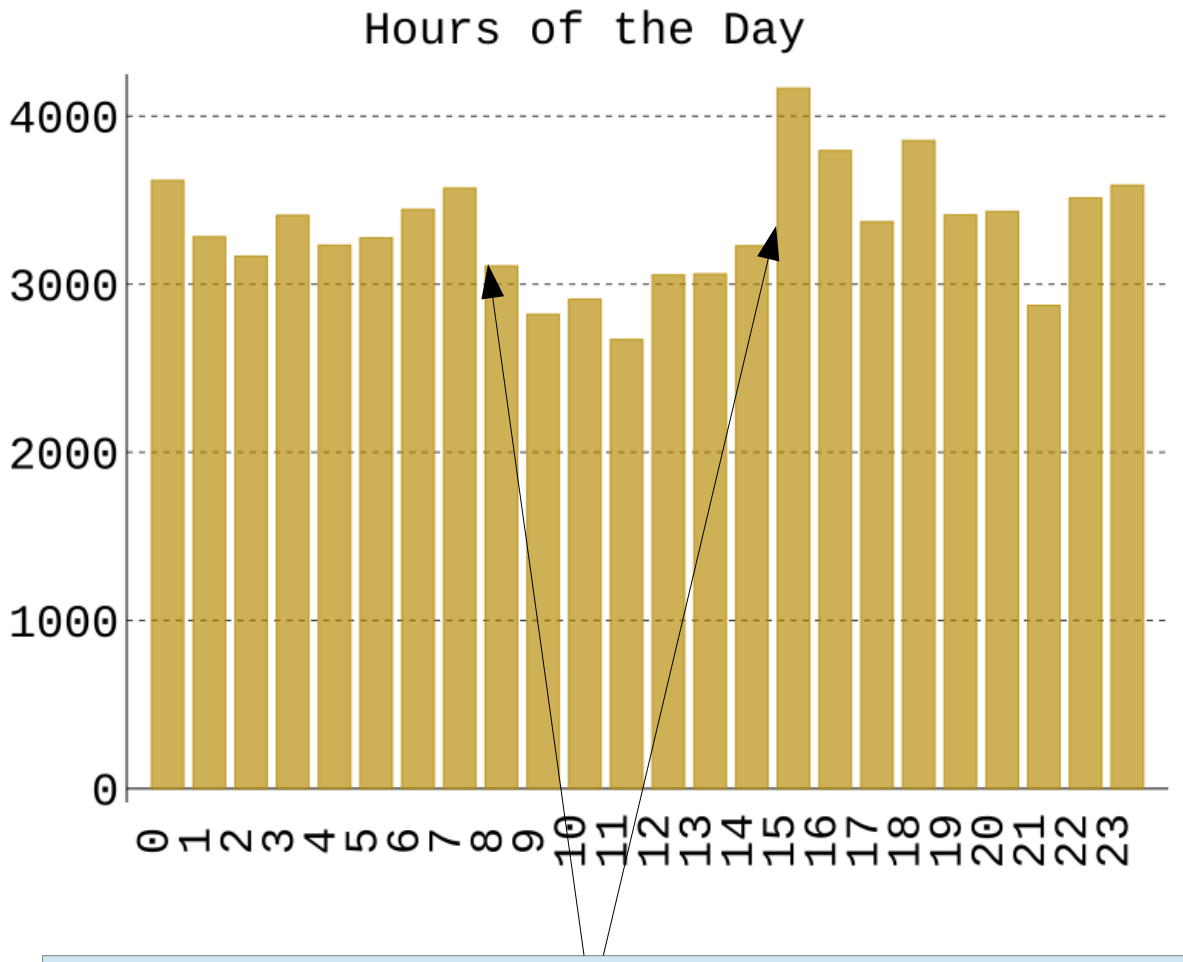
Lots of communication with Australia?

No! Fail!
aridns.net.au – Unknown

RES1: Temporal Analysis – by hour



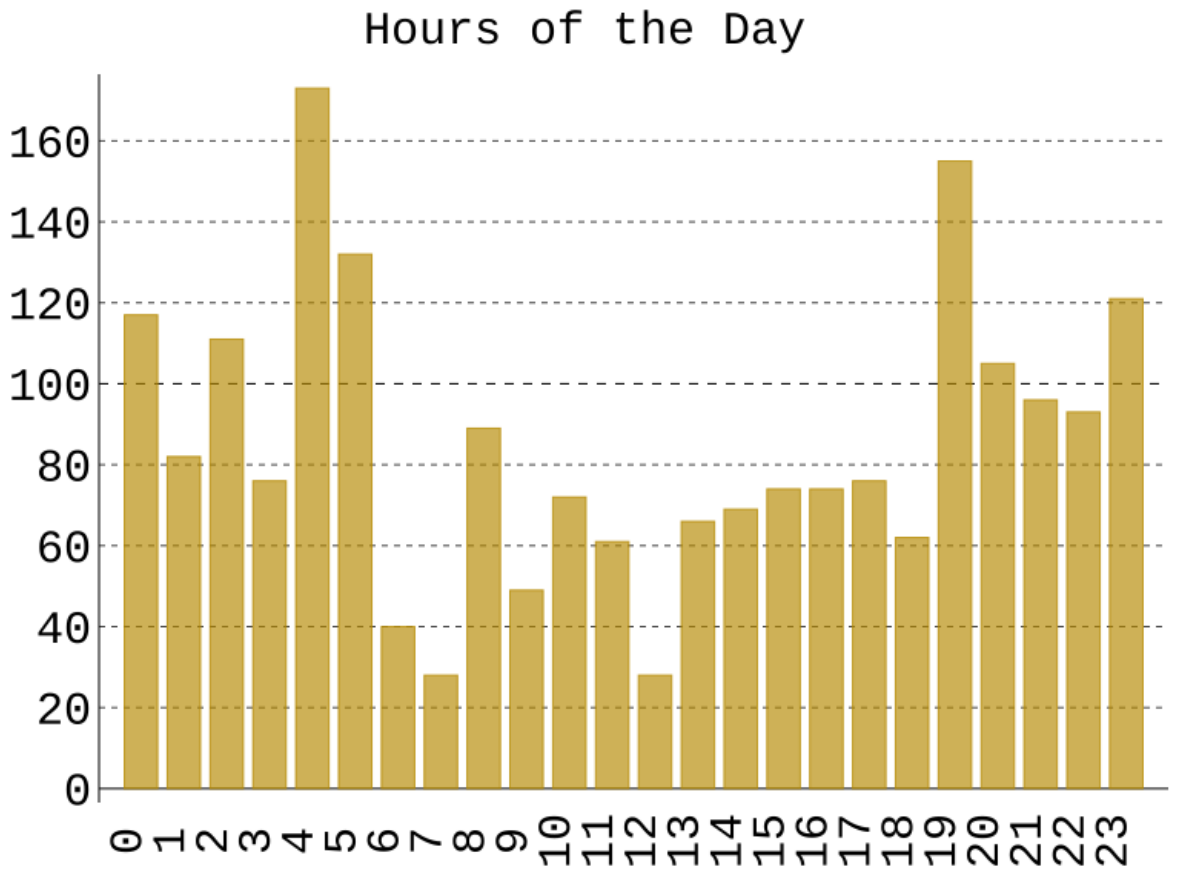
RES1: Temporal Analysis – by hour



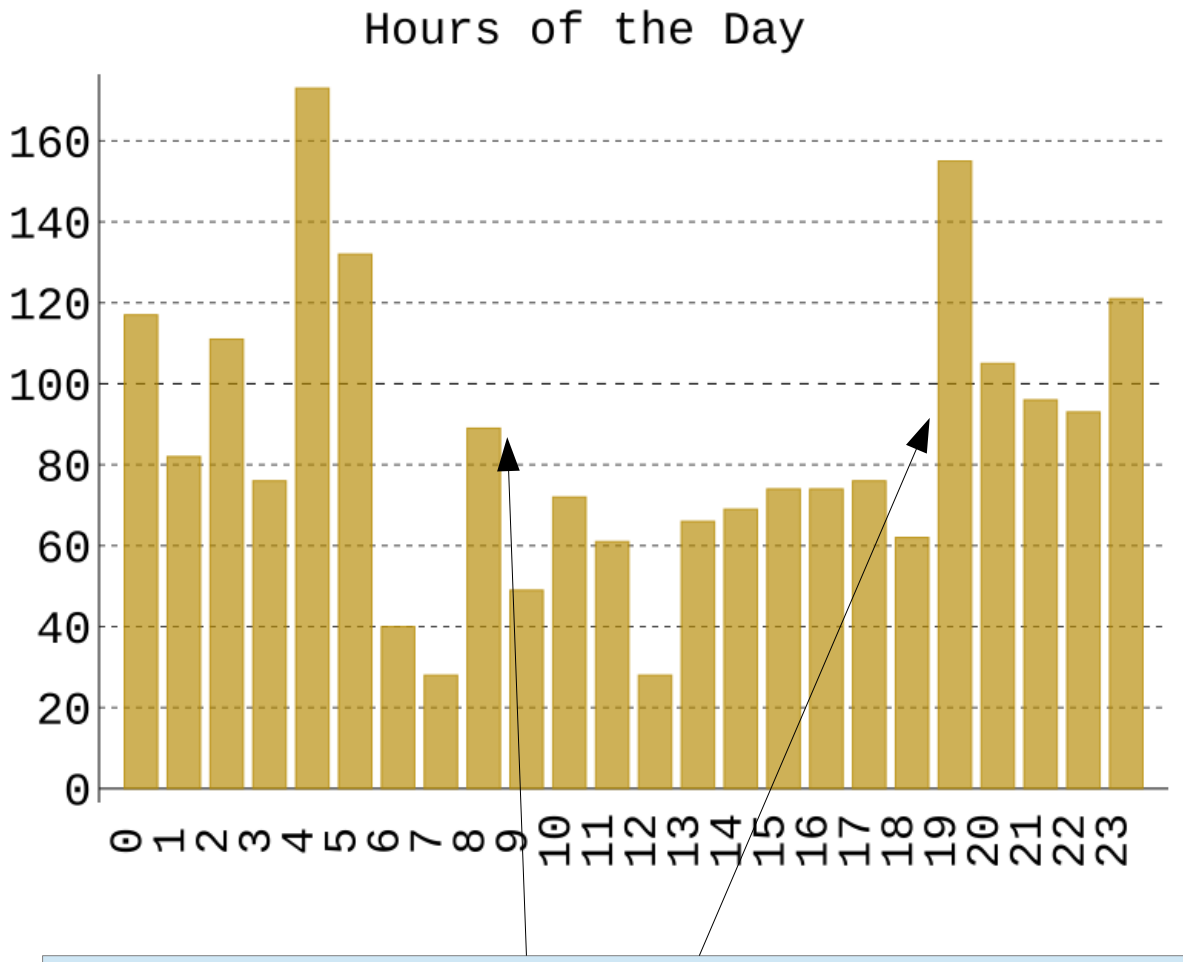
Household sleeping period? TZ offset 6-8 from GMT?

Yes! (7)

RES2: Temporal Analysis – by hour



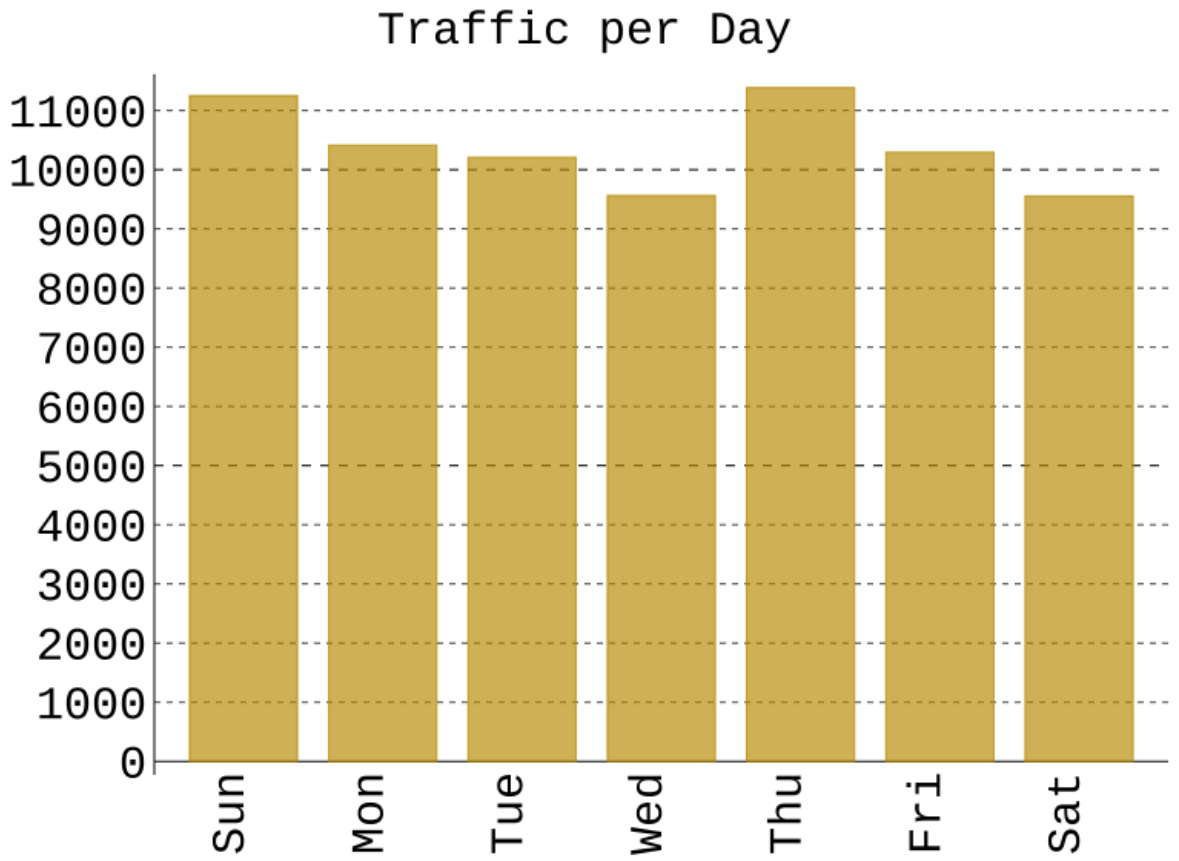
RES2: Temporal Analysis – by hour



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

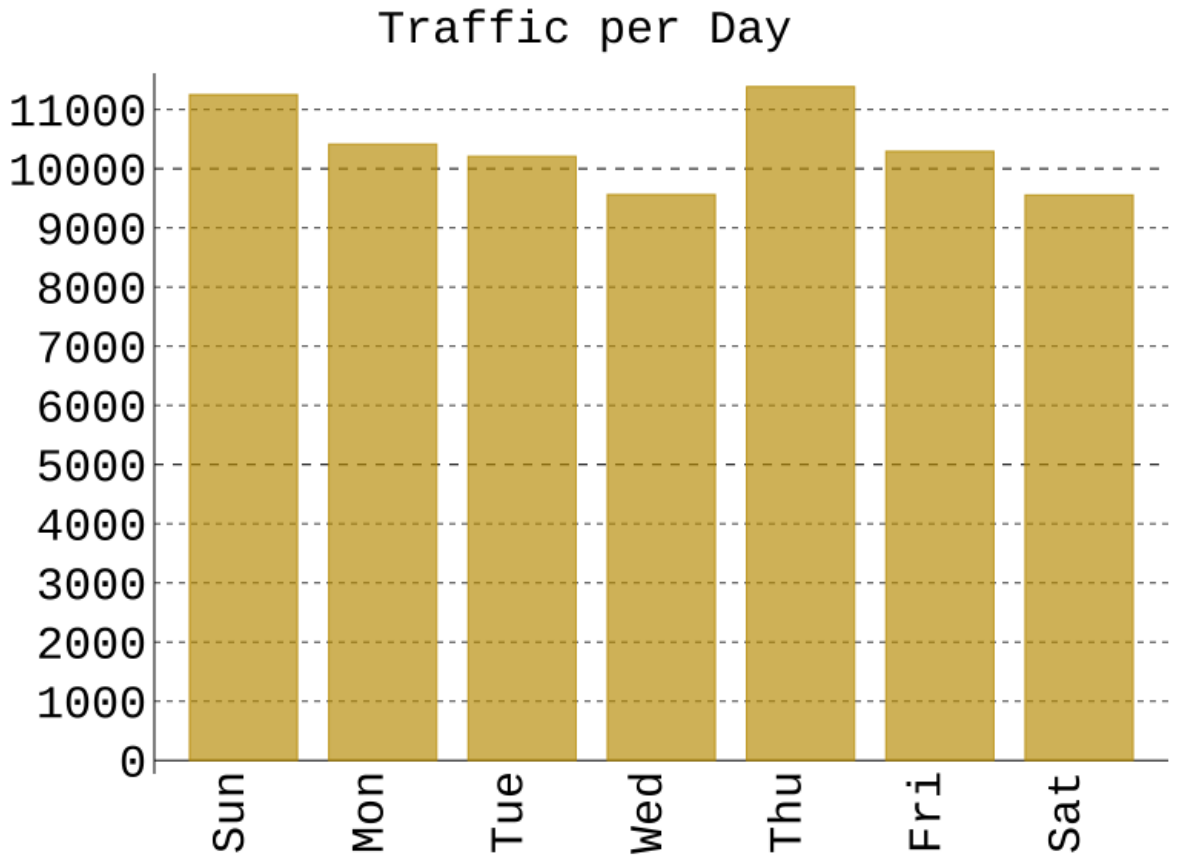
Yes! (4)

RES1: Temporal Analysis – by day



Total traffic for 28 days divided across 7 weekdays

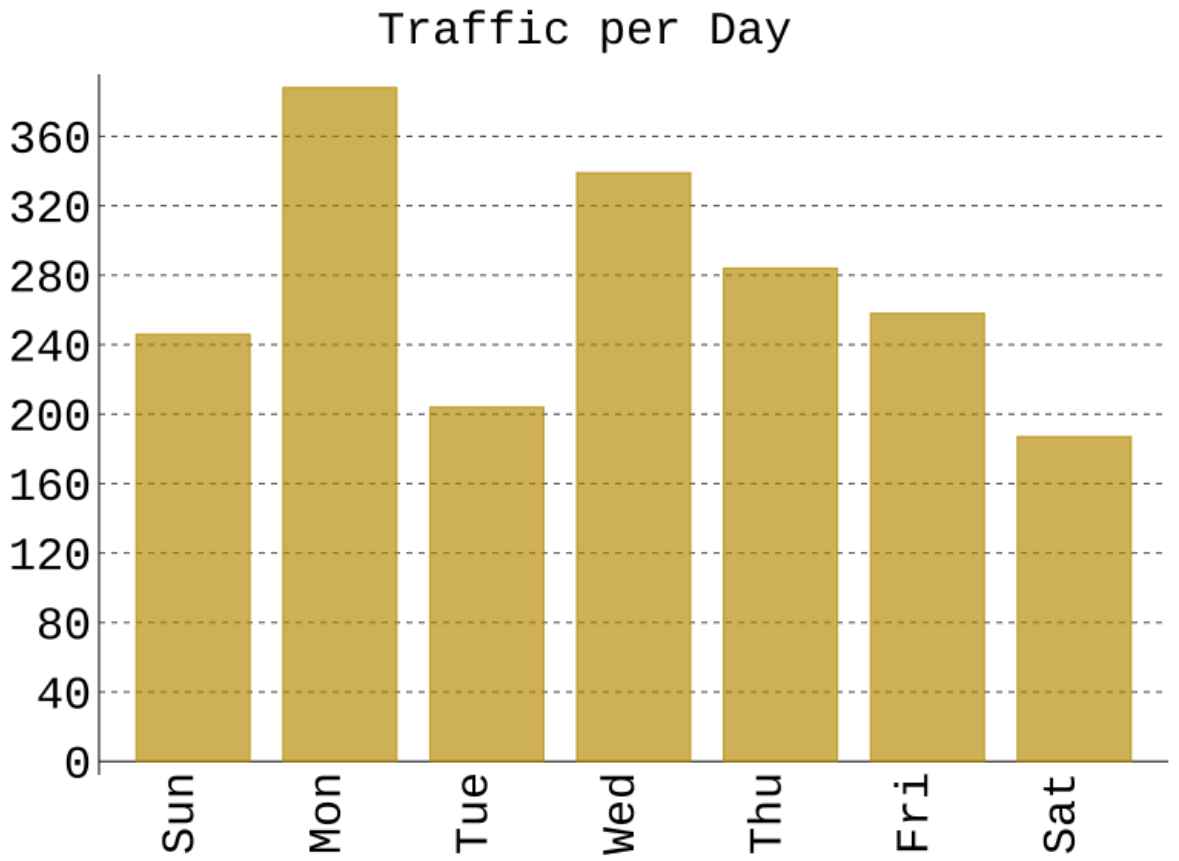
RES1: Temporal Analysis – by day



Fail: Typical 5-workday pattern not discernible

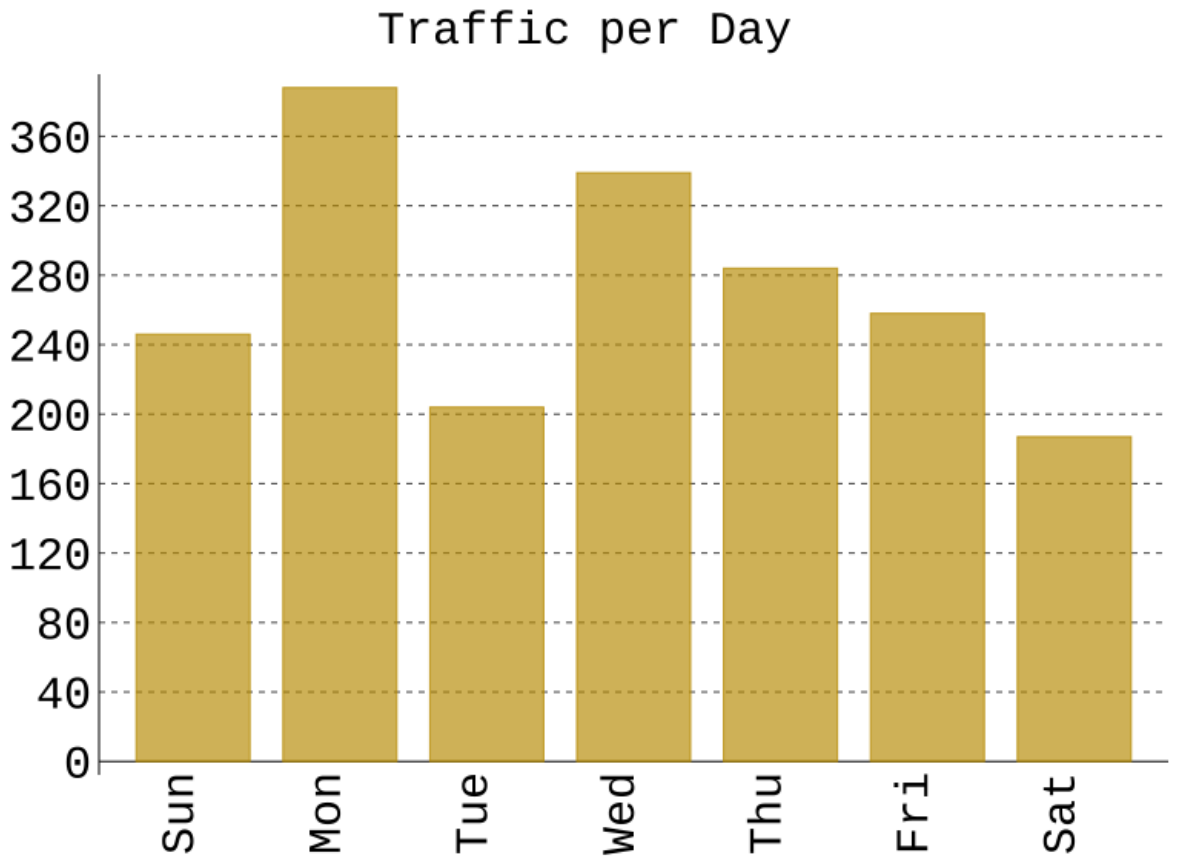
Would likely work for some places though?

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?

SLD Analysis

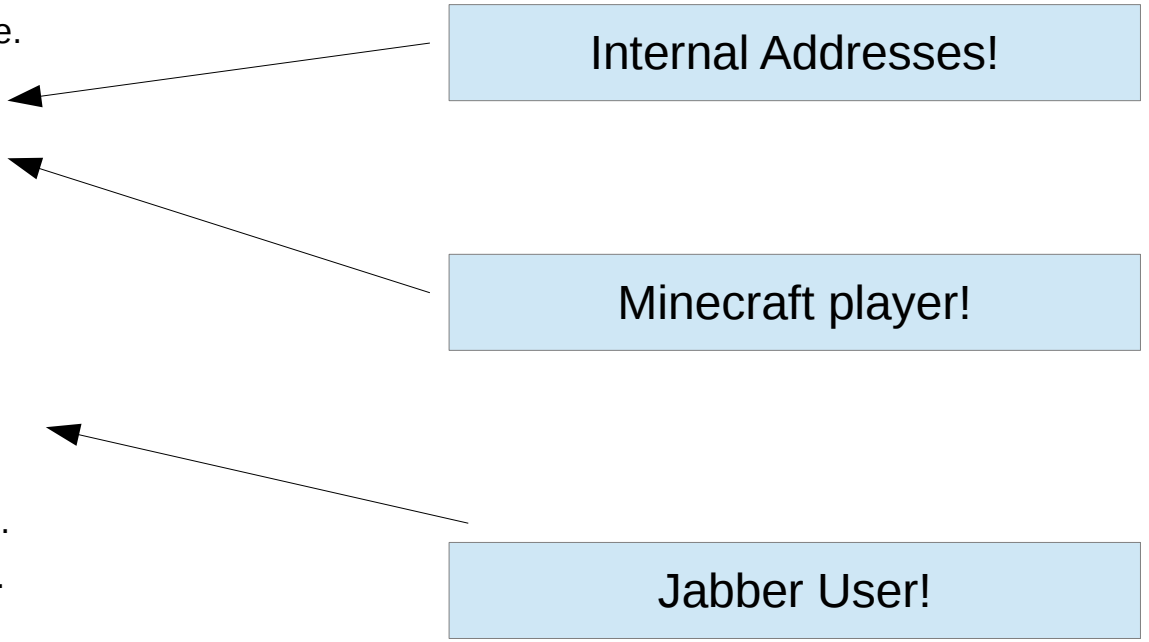
RES1	Count	RES2	Count
Gatech.edu	444	**Fedoraproject.org**	16
Sorbs.net	447	**Samsung.com**	16
Verisigndns.com	451	Surriel.com	17
Register.com	454	Linode.com	21
Nhs.net	473	Iqnection.com	22
Usg.edu	492	**Rpmfusion.net**	22
Edu.tw	502	Msedge.net	25
Net.id	519	Root-servers.net	26
Gtei.net	537	Azuredns-cloud.net	32
Ntt.eu	553	Sosdg.org	35
Tislabs.com	573	Novell.com	42
Apnic.net	575	Google.com	44
Net.au	606	Dreamhost.com	54
co.jp	608	Verisigndns.com	54
Returnpath.net	692	Amazonaws.com	75
Com.cn	693	Msft.net	91
ne.jp	758	Net.au	96
Anexia.at	939	Tislabs.com	103
Net.cn	1266	Shifen.com	204
Msft.net	1475	**Vipcam.org**	260

PSL Breakpoint Analysis

RES1	Count	RES2	Count
A5.com	388	**Samsung.com**	16
Linode.com	406	Surriel.com	17
Cloudflare.com	424	Linode.com	21
Telkom.net.id	436	Iqnection.com	22
Gatech.edu	444	**Rpmfusion.net**	22
Sorbs.net	447	U2.amazonaws.com	22
Verisigndns.com	451	U1.amazonaws.com	24
Register.com	454	Msedge.net	25
Nhs.net	473	Root-servers.net	26
Usg.edu	492	Azuredns-cloud.net	32
Gtei.net	537	Sosdg.org	35
Aridns.net.au	550	Novell.com	42
Ntt.eu	553	Google.com	44
Nintendo.co.jp	559	Dreamhost.com	54
Tislabs.com	573	Verisigndns.com	54
Apnic.net	575	Msft.net	91
Vips.ne.jp	612	Aridns.net.au	96
Returnpath.net	692	Tislabs.com	103
Anexia.at	939	Shifen.com	204
Msft.net	1475	**Vipcam.org**	260

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.



Mitigation Options

1) DNS Query Name minimization

- Send only partial queries

2) TLS-based DNS encryption

- Encrypt against man-in-the-middle

3) LocalRoot

- Slave the root zone
- Eventually will slave others

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

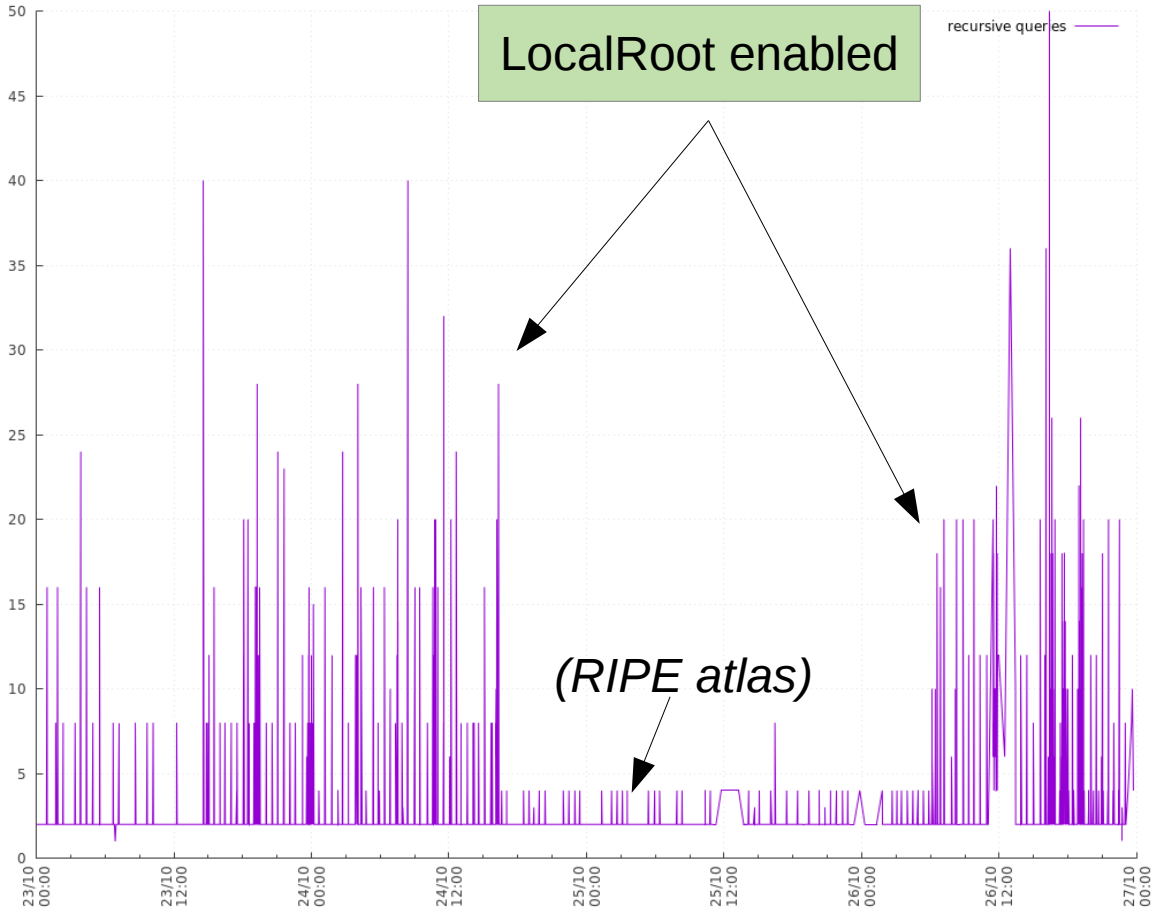
Conclusions:

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/

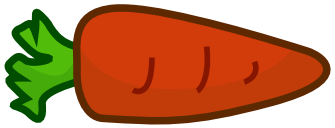
LocalRoot: Don’t Ask Questions In The First Place



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