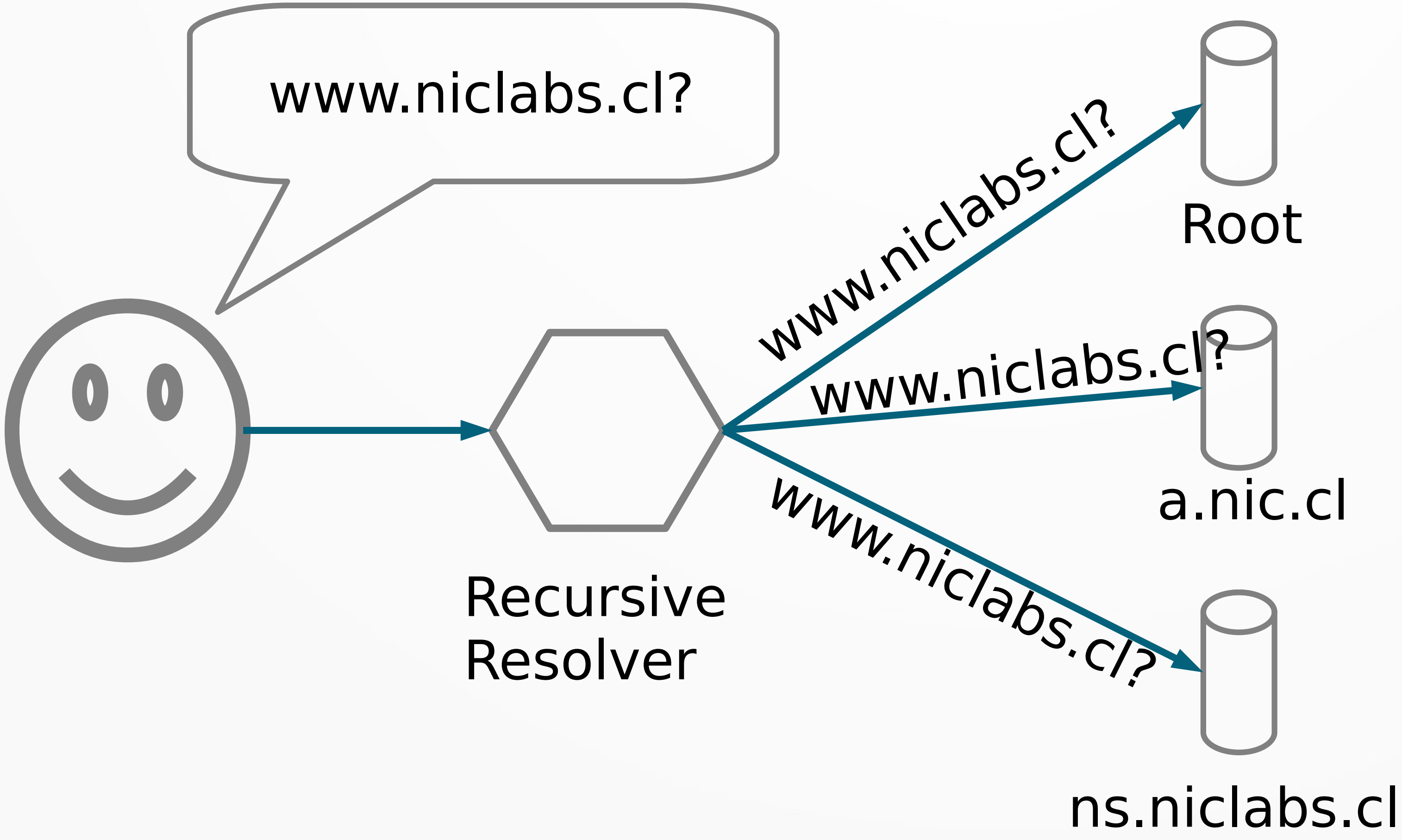
A First Look at QNAME Minimization in the Domain Name System

Wouter B. de Vries, Quirin Scheitle, Moritz Muller, Willem Toorop, Ralph Dolmans, Roland van Rijswijk-Deij

What is the DNS?

Translates Names into Numbers



.cl zone is
delegated to
a.nic.cl

niclabs.cl zone is
delegated to
a.nic.cl

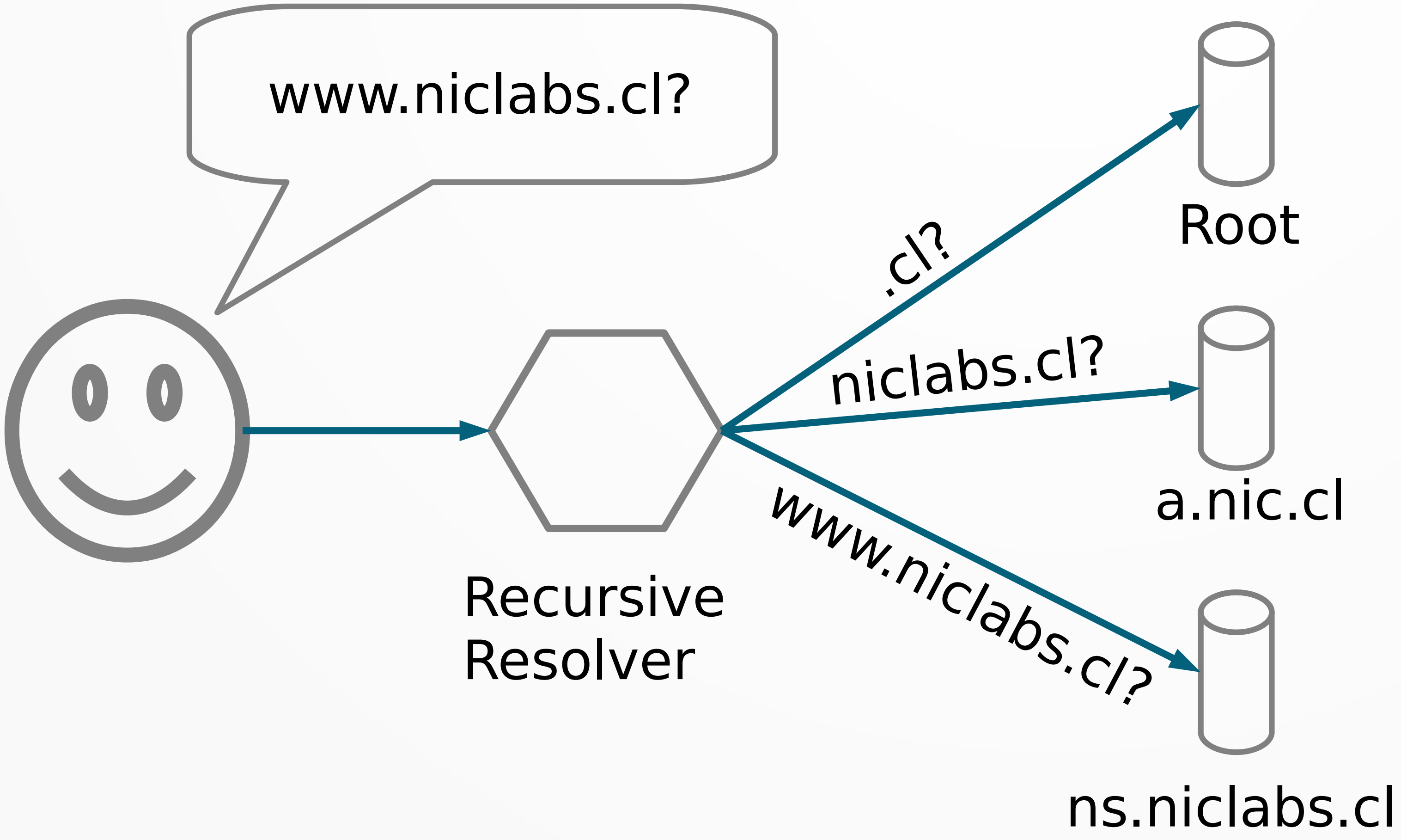
A record:
185.199.108.153
AAAA record:
Sorry, what?
(NOERROR)

Qname Minimization (QMIN)

RFC7627 – DNS Privacy Considerations (section 2.2)
RFC7816 - DNS Query Name Minimisation to Improve Privacy

Send the minimal amount of data to each authoritative server necessary for the query

DNS with QMIN

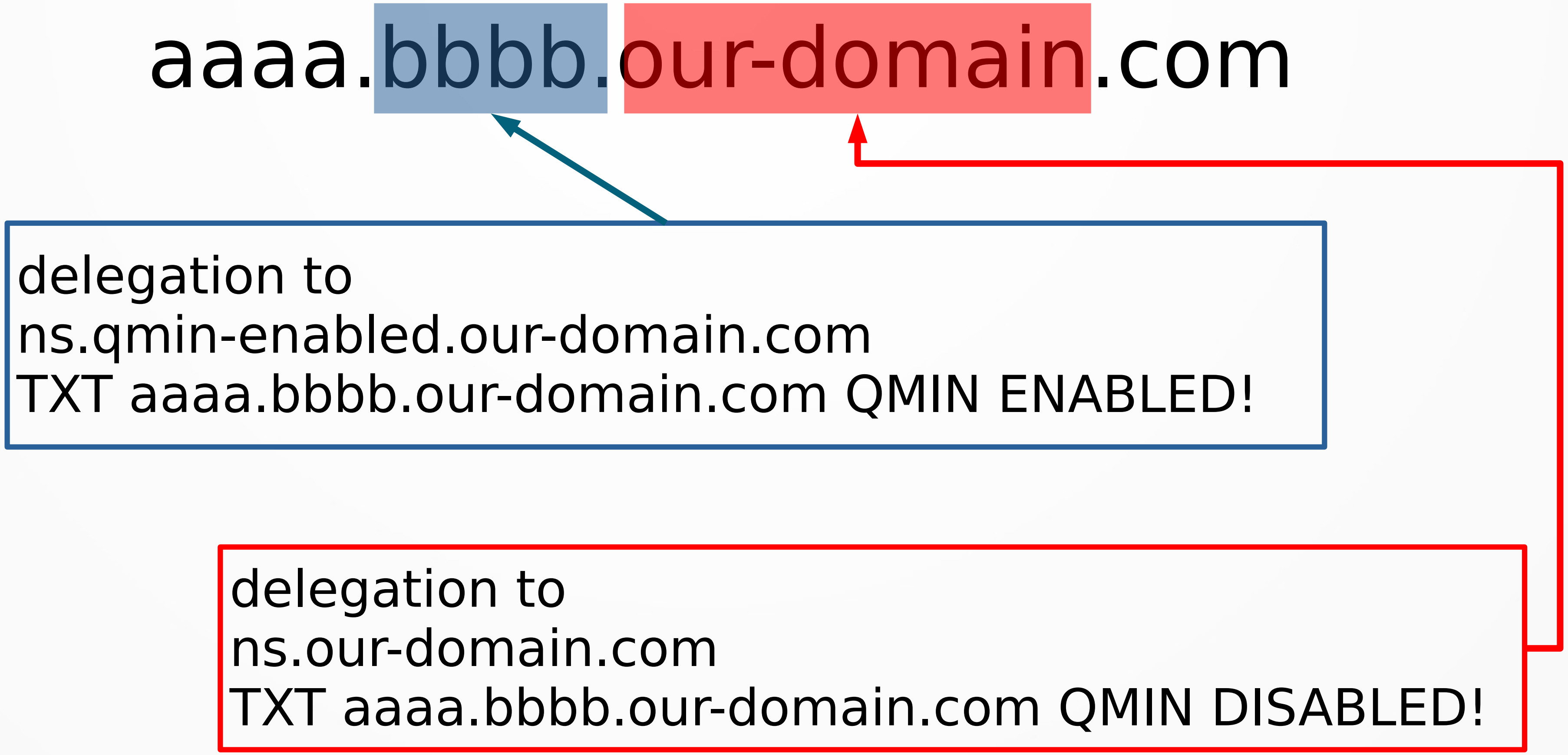


.cl zone is delegated to a.nic.cl

niclabs.cl zone is delegated to a.nic.cl

A record:
185.199.108.153
AAAA record:
Sorry, what?
(NOERROR)

Detecting QMIN



aaaa.bbbb.our-domain.com

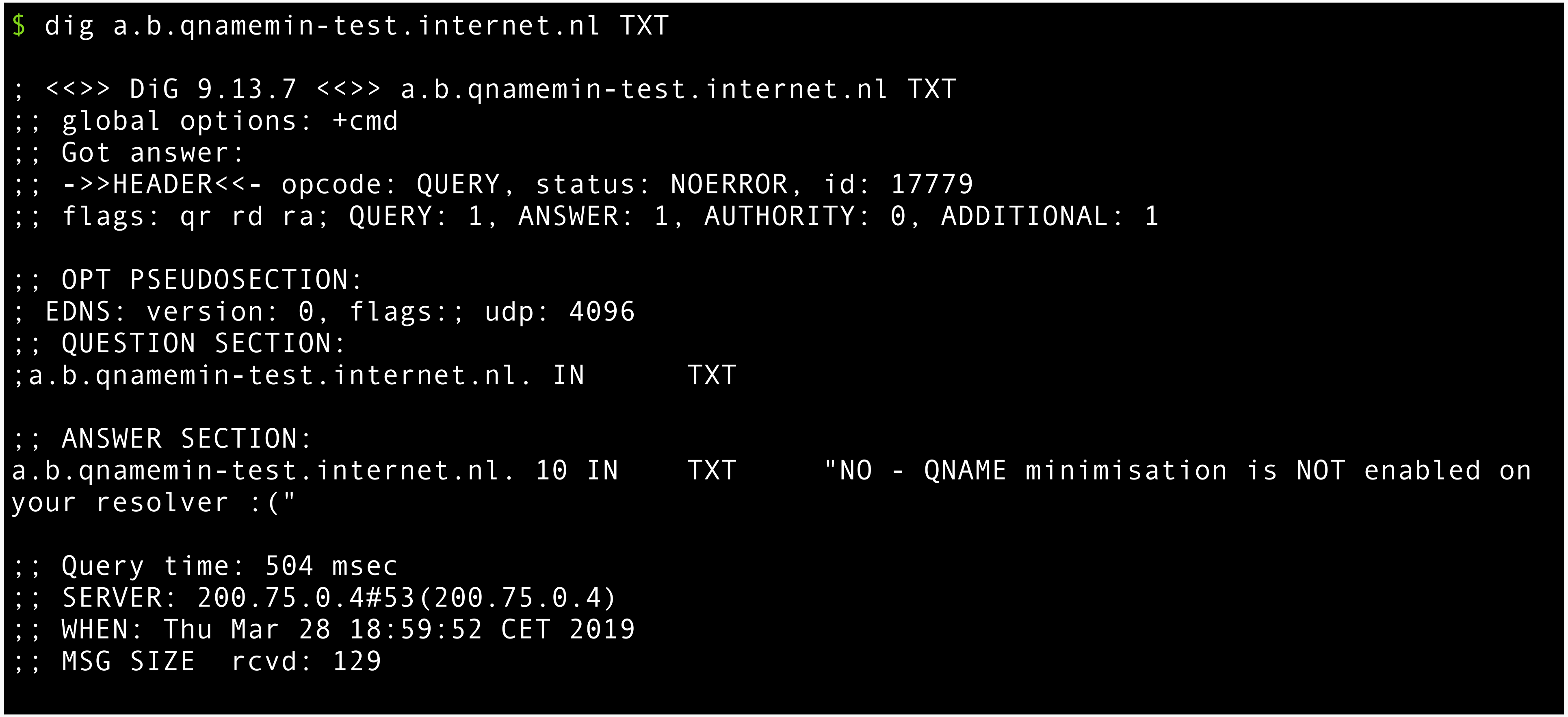
delegation to
ns.qmin-enabled.our-domain.com
TXT aaaa.bbbb.our-domain.com QMIN ENABLED!

delegation to
ns.our-domain.com
TXT aaaa.bbbb.our-domain.com QMIN DISABLED!

QMIN Adoption: RIPE Atlas

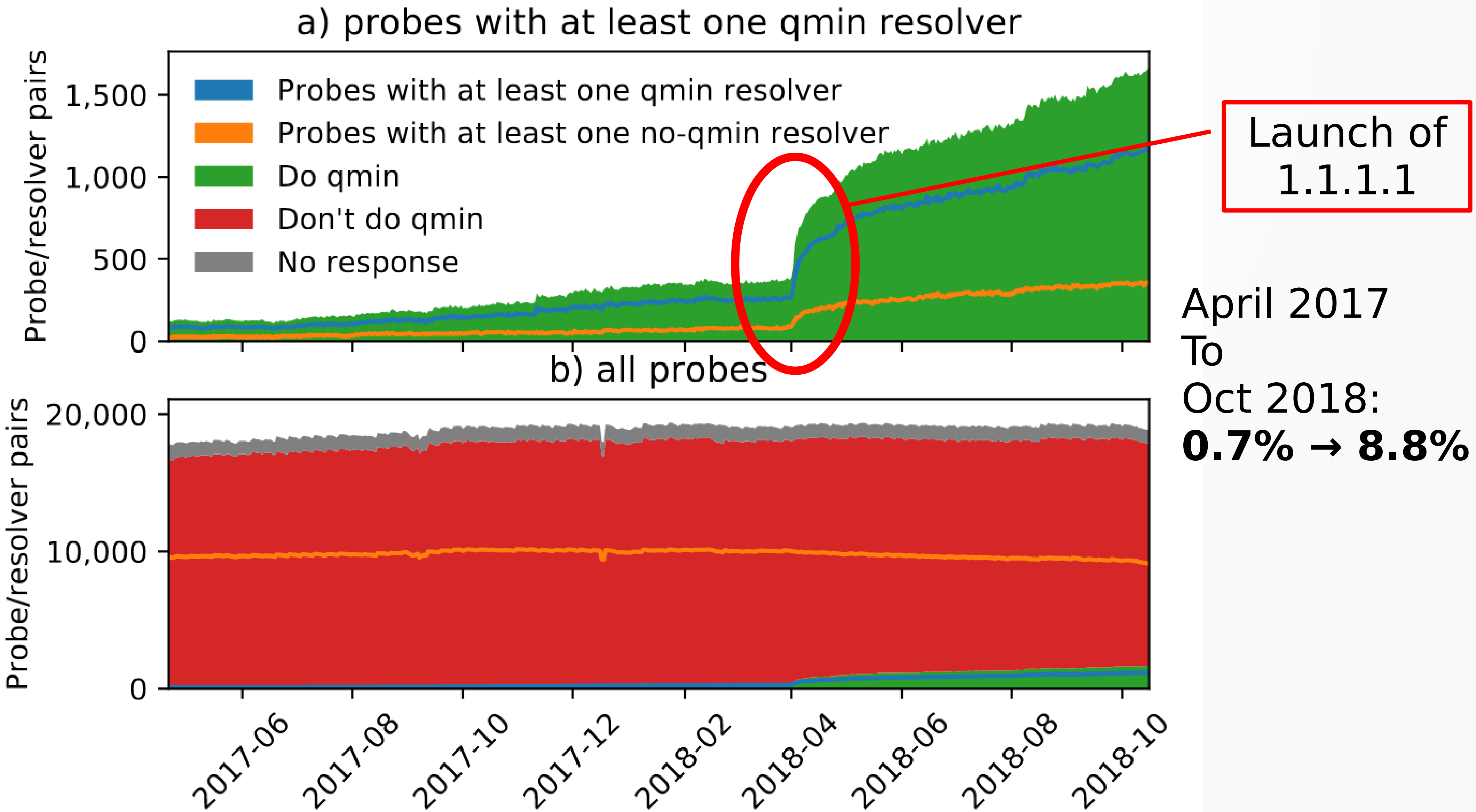
- Measurement running from all probes
- Started April 2017

- Query towards a.b.qnamemin-test.internet.nl



```
$ dig a.b.qnamemin-test.internet.nl TXT

; <<>> DiG 9.13.7 <<>> a.b.qnamemin-test.internet.nl TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17779
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;a.b.qnamemin-test.internet.nl. IN      TXT

;; ANSWER SECTION:
a.b.qnamemin-test.internet.nl. 10 IN    TXT     "NO - QNAME minimisation is NOT enabled on
your resolver :("

;; Query time: 504 msec
;; SERVER: 200.75.0.4#53(200.75.0.4)
;; WHEN: Thu Mar 28 18:59:52 CET 2019
;; MSG SIZE  rcvd: 129
```

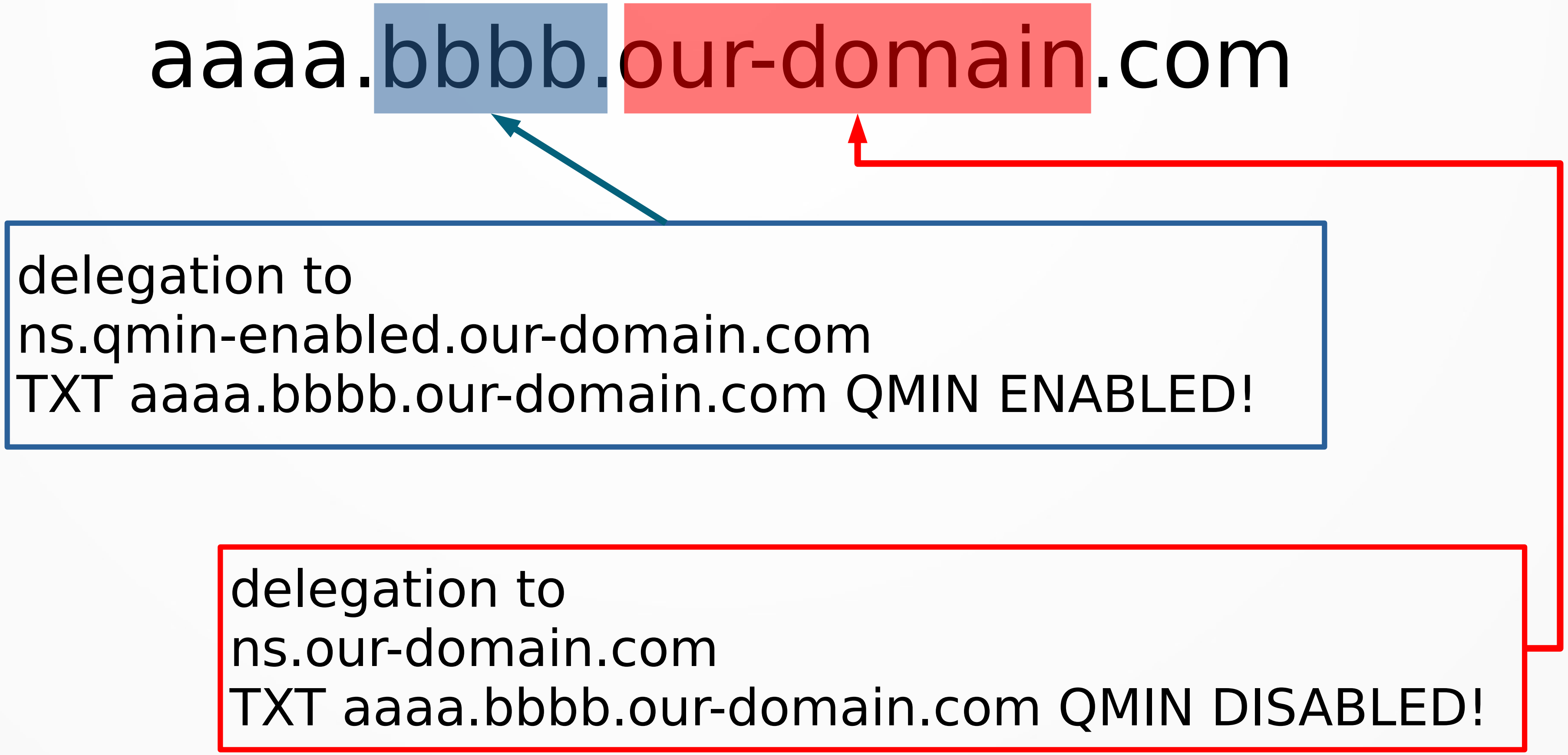
QMIN Adoption: RIPE Atlas



Launch of 1.1.1.1

April 2017
To
Oct 2018:
0.7% → 8.8%

Caching is the enemy
(or: how we messed up)

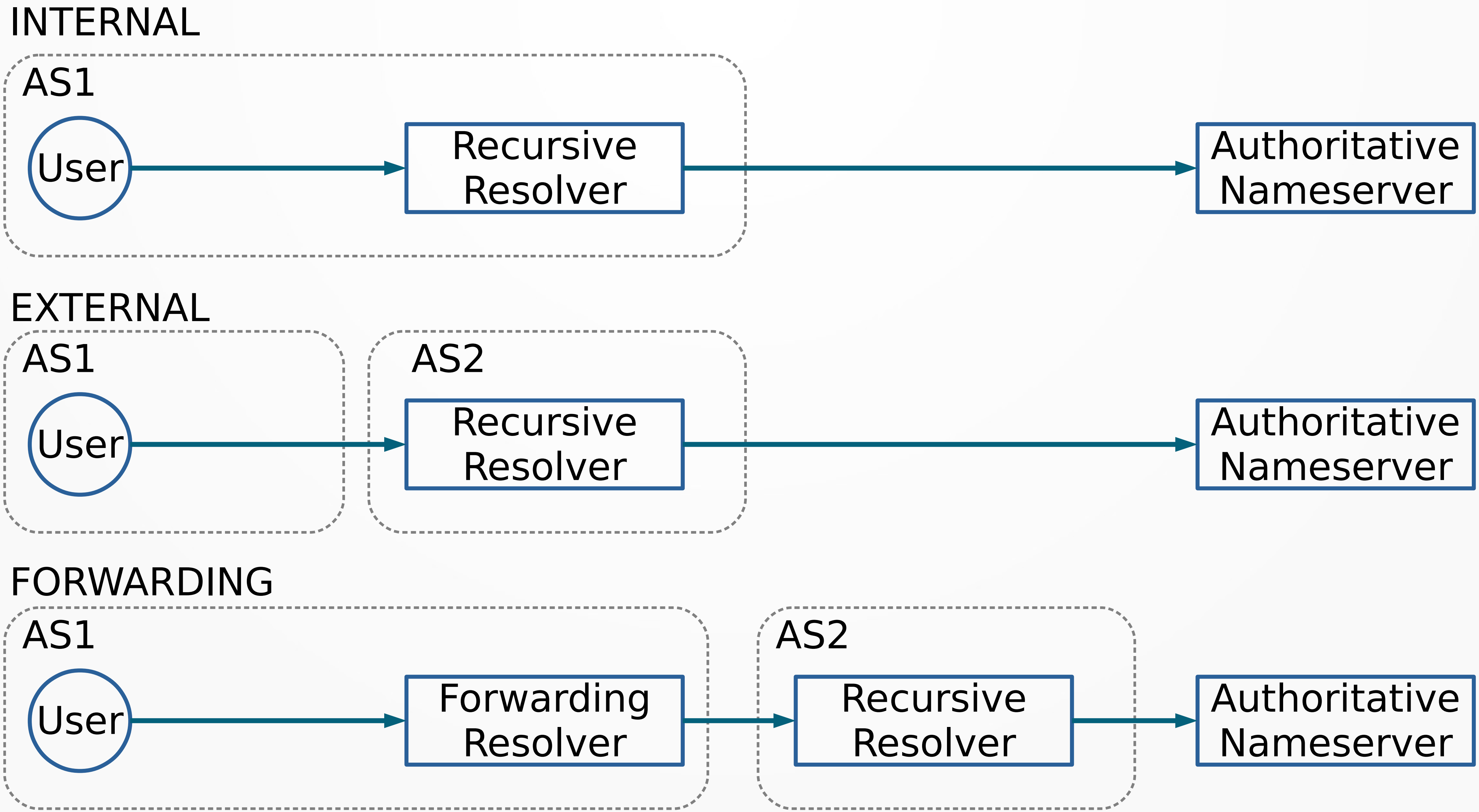


aaaa.bbbb.our-domain.com

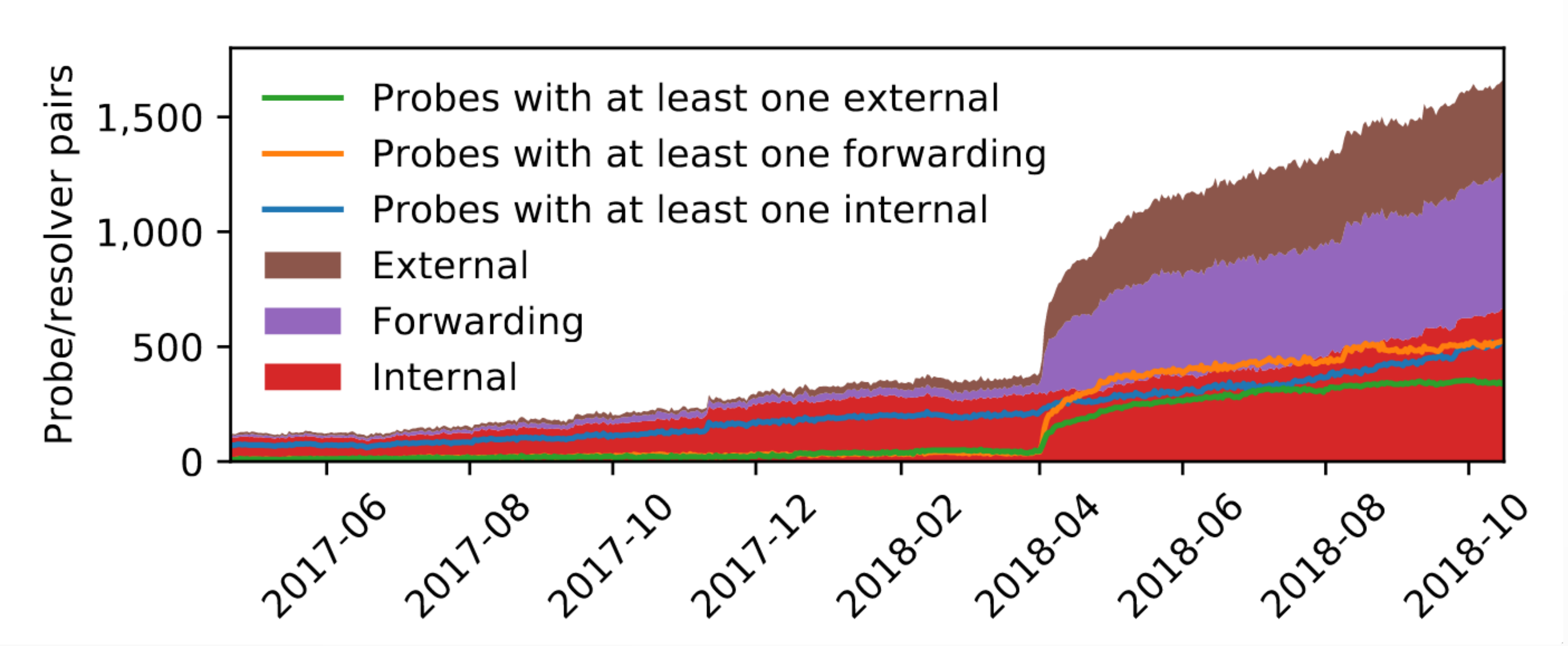
delegation to
ns.qmin-enabled.our-domain.com
TXT aaaa.bbbb.our-domain.com QMIN ENABLED!

delegation to
ns.our-domain.com
TXT aaaa.bbbb.our-domain.com QMIN DISABLED!

QMIN Adoption: Resolver Types



QMIN Adoption: Resolver Types

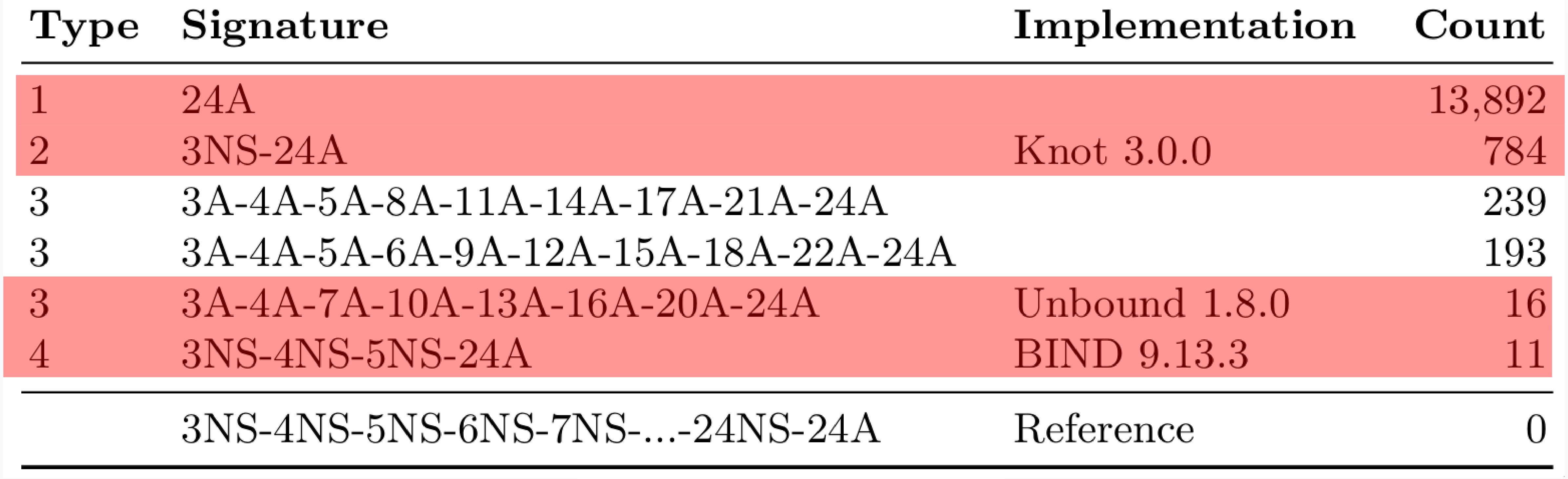


- **9 Nov, 2017:** Versatel Deutschland
- **2 Aug, 2017:** Init7 (Switzerland)
- **1 Feb, 2018:** OVH Systems
- **1 May, 2018:** M-Net Telekommunikations (Germany)

Types of QMIN: Signatures

- Not all implementations of QMIN are the same (in fact, none of them are)
- RIPE Atlas to the rescue, using all probes (9,410), one off measurement
- a.b.c.d.e.f.g.h.j..{probe-id}.{random}.domain.com (24 labels).

QMIN signatures



Type	Signature	Implementation	Count
1	24A		13,892
2	3NS-24A	Knot 3.0.0	784
3	3A-4A-5A-8A-11A-14A-17A-21A-24A		239
3	3A-4A-5A-6A-9A-12A-15A-18A-22A-24A		193
3	3A-4A-7A-10A-13A-16A-20A-24A	Unbound 1.8.0	16
4	3NS-4NS-5NS-24A	BIND 9.13.3	11
	3NS-4NS-5NS-6NS-7NS-...-24NS-24A	Reference	0

Open Resolvers

- Rapid7 Dataset with UDP Port 53 responsive IPs (IPv4): 8 Million IPs
- 64% respond
- 32% respond with NOERROR
- 72% (1.2M) respond with the correct answer
- 110k unique source IPs observed at authoritative server
- 1.6% support QMIN (19.7k)
  - Mostly Cloudflare source IPs

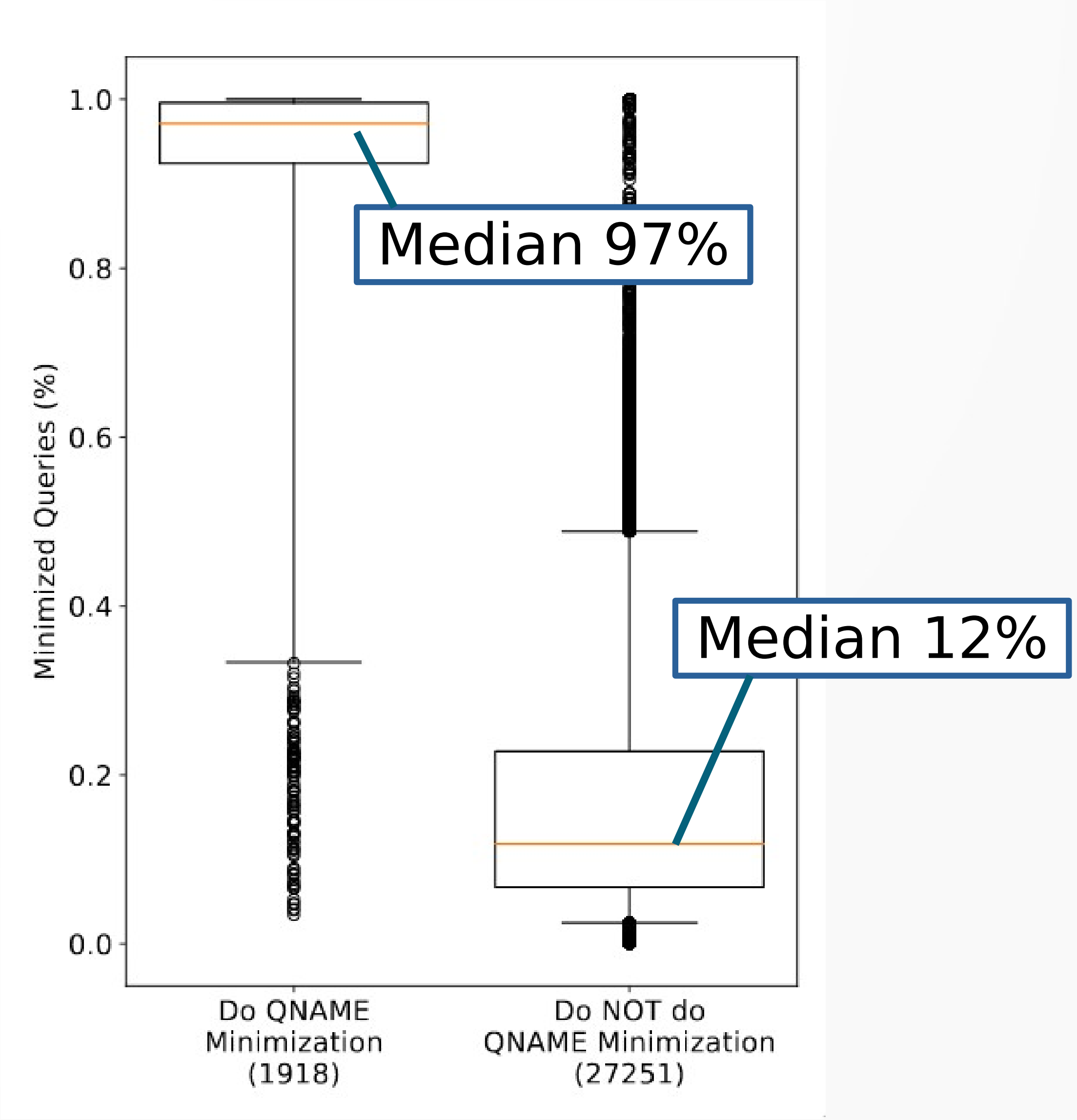
Takeaway: many open resolvers are simply forwarding to large public DNS providers. To drive QMIN adoption it would be efficient to target those (e.g. Google).

Passive measurements .nl and K-root

- **Active** measurements are great, but **passive** measurements can be good too! (But they include some hand waving)
- 400 billion queries at the .nl authoritative, from 2017-06-01 to 2018-09-30
- 12 billion queries at the K-root on 2017-04-11, 2018-04-10 (DITL)
- Heuristic
  - single label query at K-root signifies a minimized query
  - two label query at .nl signifies a minimized query.

Validating the heuristic

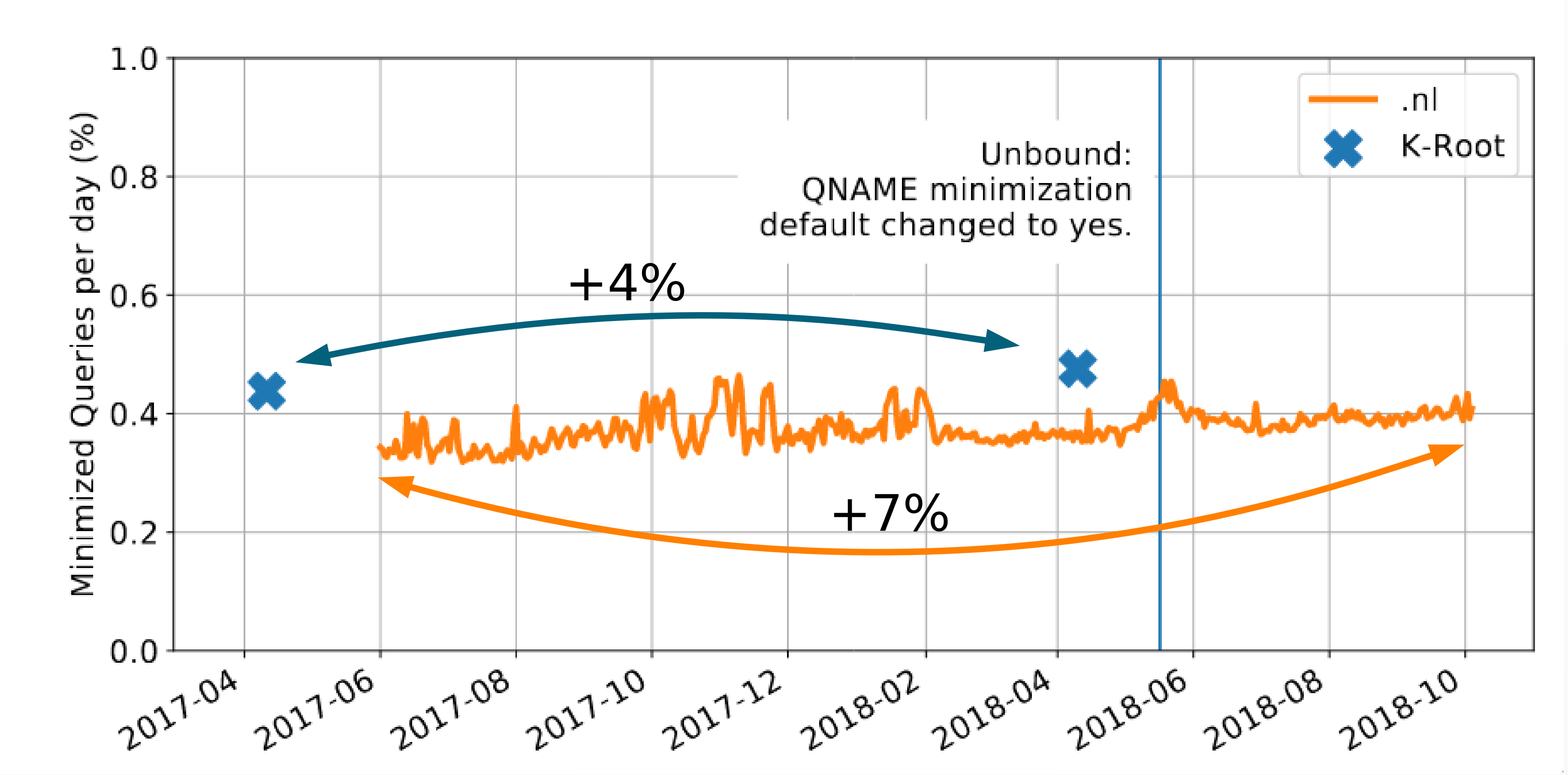
- Take the sources of queries from the open resolver scan, looking at the received label lengths
- Shows a reasonable signal



Median 97%

Median 12%

QMIN at .nl and K-root

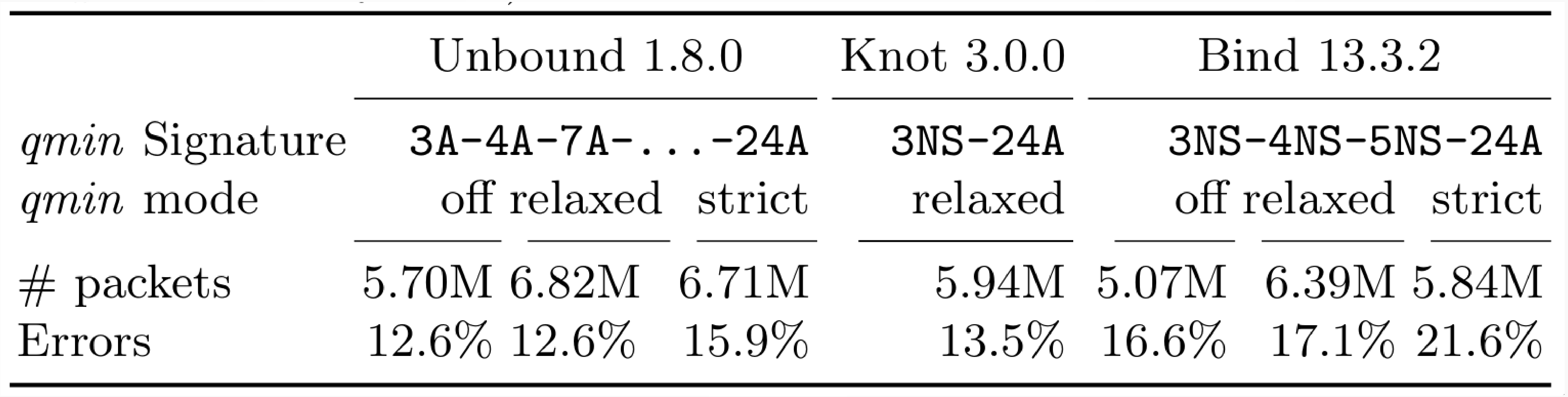


Unbound:
QNAME minimization
default changed to yes.

Performance
Unbound vs Bind vs Knot

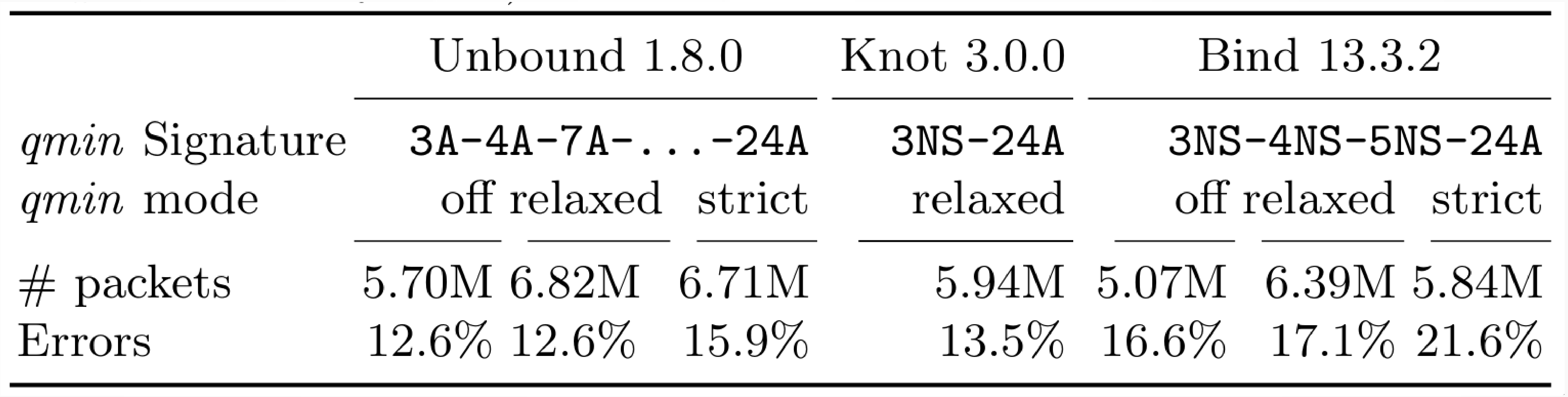
In a controlled experiment:

- Resolve 1.56M domain names from 2 weeks aggregated Umbrella list
- Sort the list in multiple orders to even out caches
- Set the cache size for each resolver to 4GB, start each run with an empty cache



	Unbound 1.8.0			Knot 3.0.0	Bind 13.3.2		
qmin Signature	3A-4A-7A-...-24A			3NS-24A	3NS-4NS-5NS-24A		
qmin mode	off	relaxed	strict	relaxed	off	relaxed	strict
# packets	5.70M	6.82M	6.71M	5.94M	5.07M	6.39M	5.84M
Errors	12.6%	12.6%	15.9%	13.5%	16.6%	17.1%	21.6%

Performance
Unbound vs Bind vs Knot



	Unbound 1.8.0			Knot 3.0.0	Bind 13.3.2		
qmin Signature	3A-4A-7A-...-24A			3NS-24A	3NS-4NS-5NS-24A		
qmin mode	off	relaxed	strict	relaxed	off	relaxed	strict
# packets	5.70M	6.82M	6.71M	5.94M	5.07M	6.39M	5.84M
Errors	12.6%	12.6%	15.9%	13.5%	16.6%	17.1%	21.6%

- Strict mode, unsurprisingly, increases the error rate. An increase of 3.3% in error rate equals 50k domains.
- Unbound’s choice for using A records for lookups instead of NS appears to decrease the error rate
- Increase of 15-26% in number of packets

Note: other differences than the qmin implementation influence our results (e.g. caching strategies).

Conclusions

- Qmin is more complex than it looks
- Qmin can be a security issue (DDoS risk)
- Qmin can impact performance and result quality

Despite these issues, we find that the increase in query privacy is definitely worth it, and expect further adoption in the coming years.

Dataset

Dataset and scripts are publicly available
https://traces.simpleweb.org

Final slide

Thanks!