DNS Observatory:

The Big Picture of the DNS

Paweł Foremski

Farsight Security / IITiS PAN

pjf@fsi.io

Oliver Gasser

Technical University of Munich

gasser@net.in.tum.de

Giovane C. M. Moura

SIDN Labs / TU Delft

giovane.moura@sidn.nl

FARSIGHT SECURITY

ACM IMC 2019, October 2019, Amsterdam

What’s DNS Observatory?

1. Observe recursive -> authoritative DNS traffic
2. Track the most popular values in queries (eg. IPs)
3. Characterize each “big player” with a set of features

Goals:

- Gain insight into DNS & Internet events
- Diagnose DNS *in the wild*, suggest improvements
- Ongoing work! Published first paper -> let people know

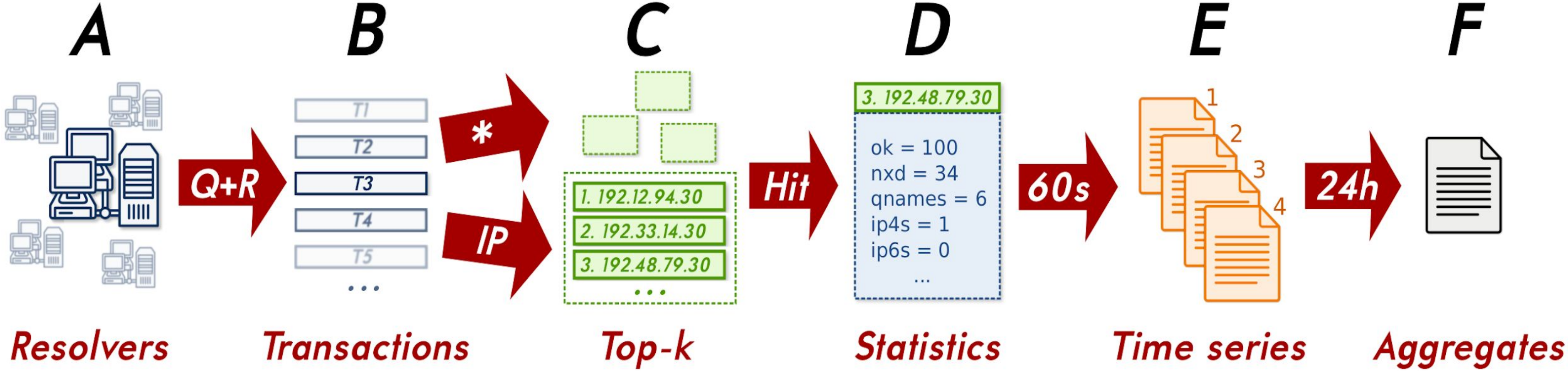
http://pngimg.com/download/66494 (CC BY-NC 4.0)

What's DNS Observatory? #2

- Source: Farsight Security Information Exchange (SIE)
  - Contributors! ISPs, DNS providers, hosting farms, etc.
  - Hundreds of resolvers around the world
  - ~200k / sec real-time observations (passive DNS)
- This paper dataset: January - April 2019
  - total: 1.6 *trillion* DNS transactions
  - eg. 1-minute sample = 2.6 million unique domains (queried FQDNs)
- Why important vs. existing works?
  - Passive (instead of active + lists)
  - Many vantage points (instead of *an* ISP or *a* TLD)
  - Real-time stream processing

http://pngimg.com/download/66494 (CC BY-NC 4.0)

In more detail…



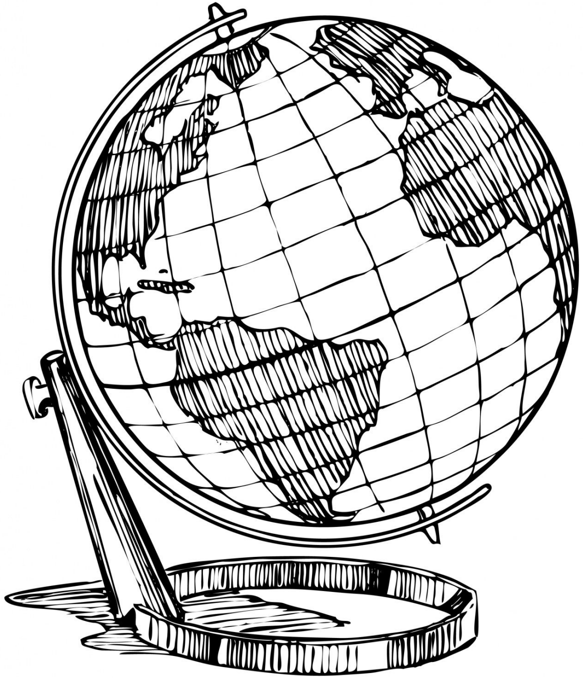
DNS Objects & Traffic Features

- Authoritative DNS servers
  (IP address)
- Effective TLDs and SLDs
  (Public Suffix List)
- Fully-Qualified Domain Names
- QTYPEs
  (A, AAAA, MX, RRSIG, …)
- IPv4 / IPv6 records
  (A, AAAA, ANY)
- …

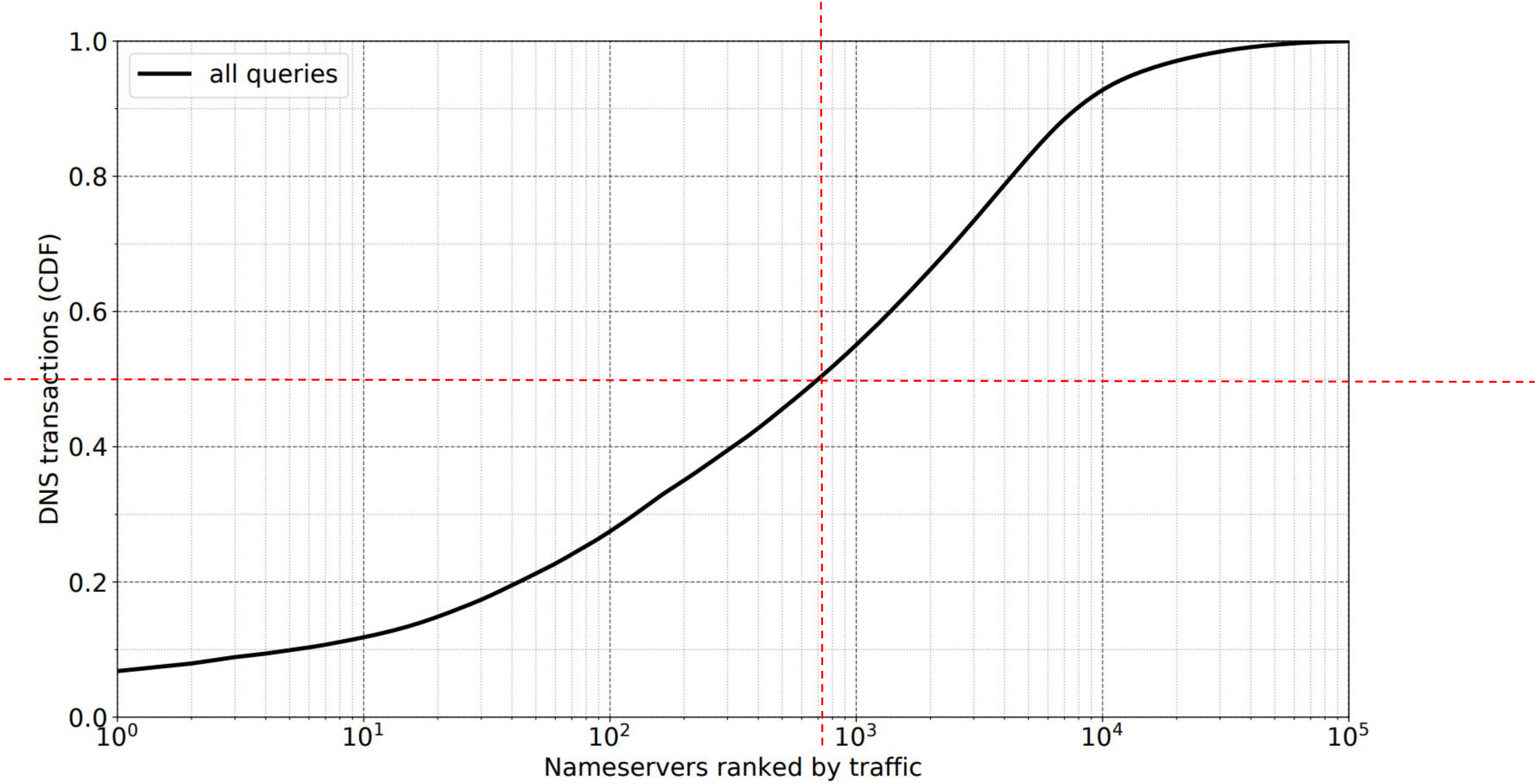
- **Counts of queries and responses, eg.**
  all, answered, SUCCESS, NXDOMAIN, NODATA, has NS records, DNSSEC-signed, etc.
- **Cardinality estimates (HyperLogLog, …), eg.**
  distinct FQDNs, TLDs, SLDs, QTYPEs, IPs seen in ANSWER, authoritative server IPs
- **Histogram estimates (percentiles, top-k, …), eg.**
  server response delay, number of network hops, response size, record TTLs, est. hierarchy level

...more coming!

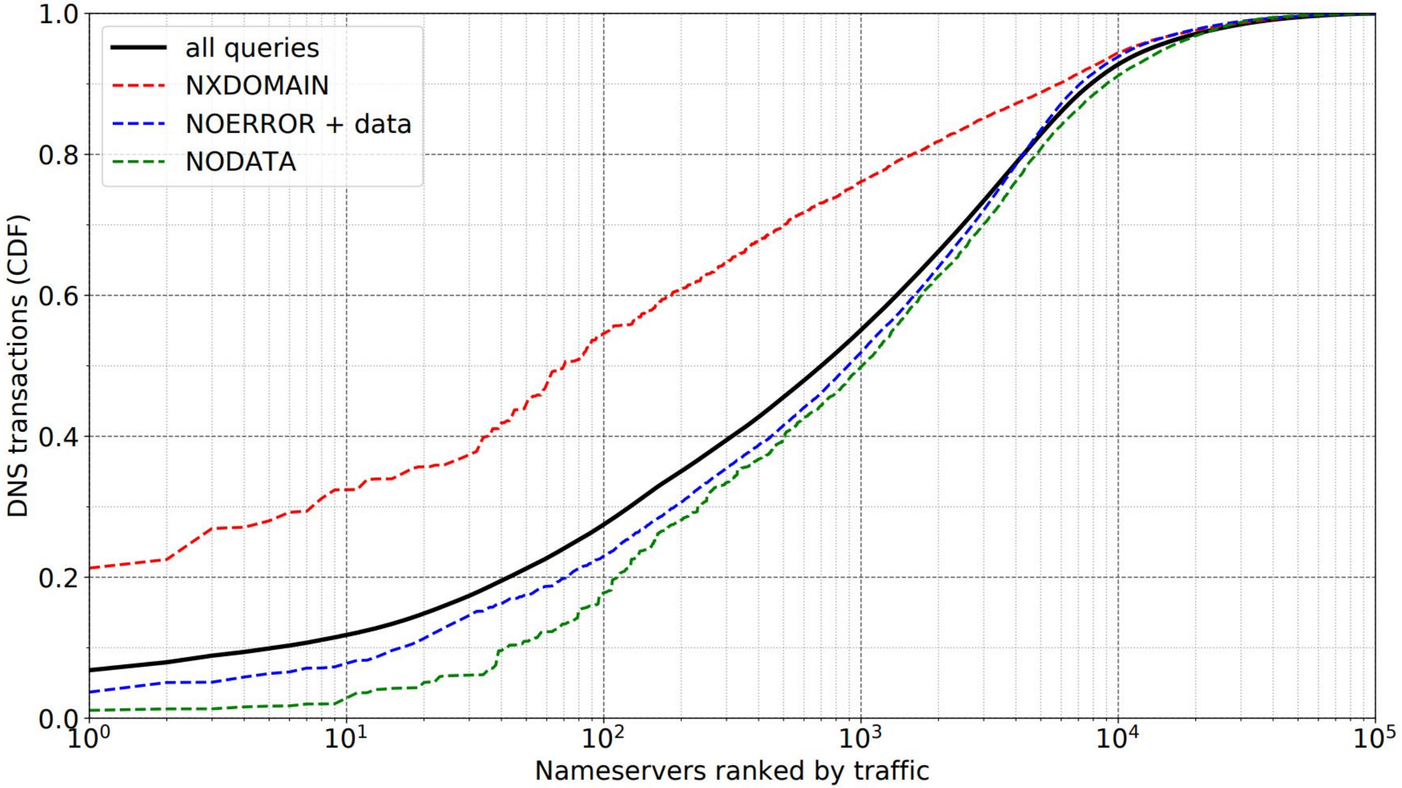
Big Picture



Traffic distribution: top 100K nameservers (95% obs.)

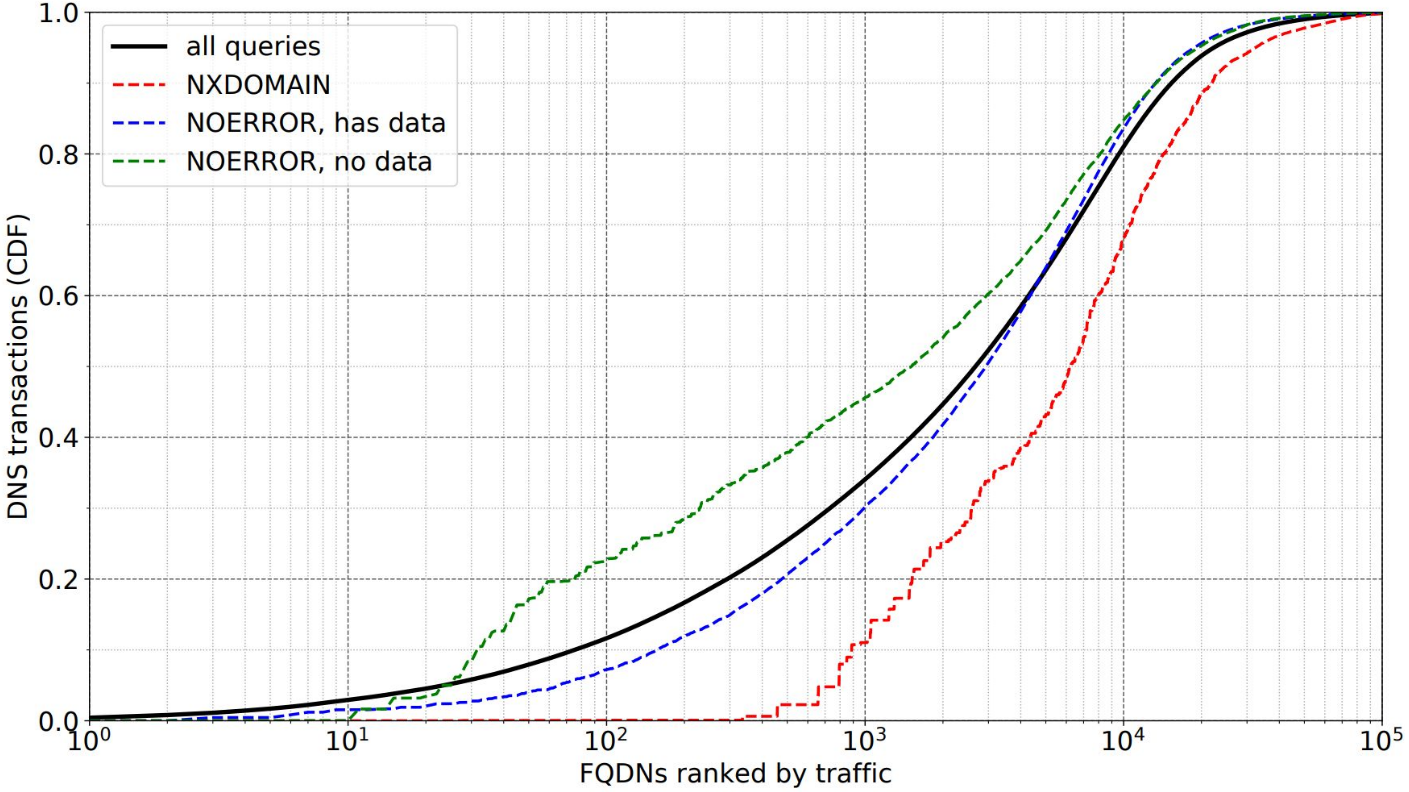


Traffic distribution: top 100K nameservers (95% obs.)



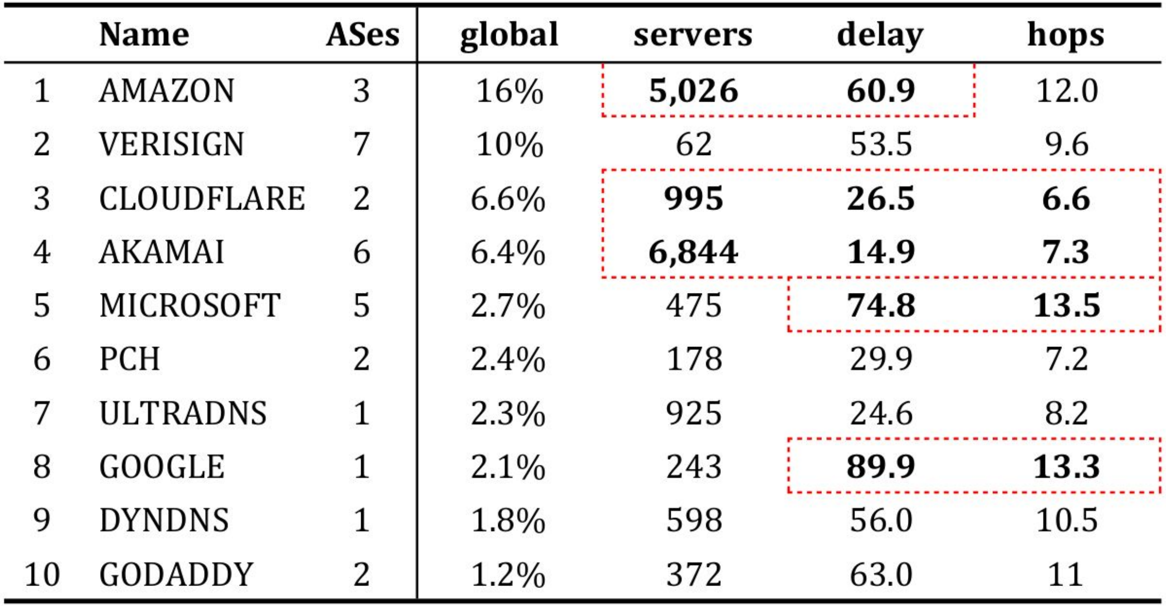
NXD	21%
Data	64%
Nodata	5%

Traffic distribution: top 100K FQDNs (23% obs.)



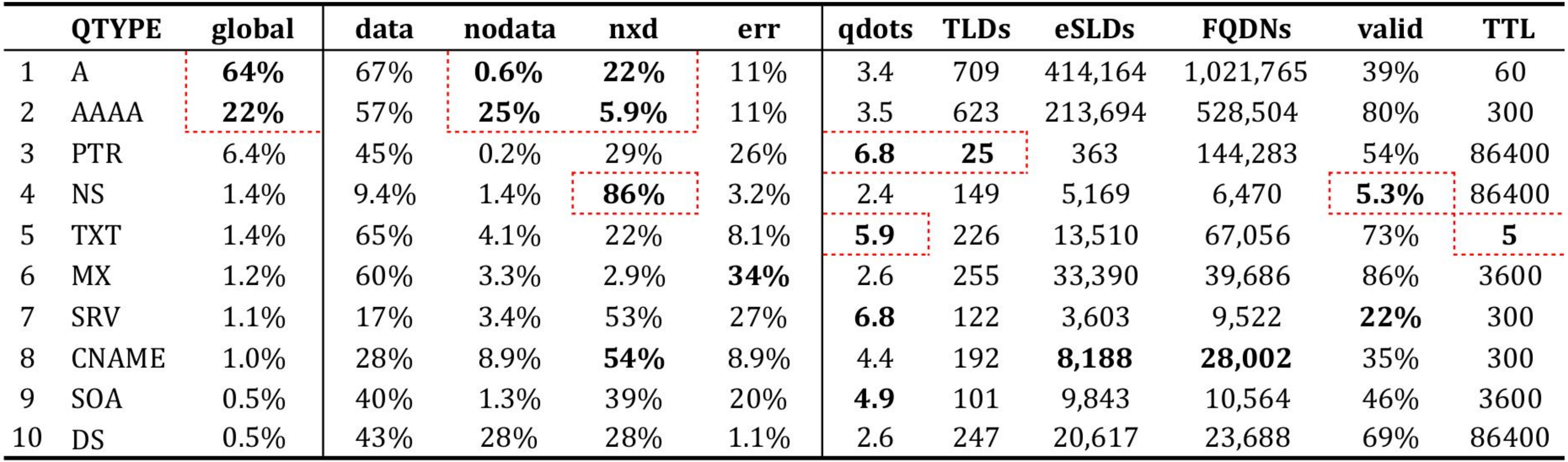
NXD	1.5%
Data	70%
Nodata	10%

Traffic distribution: top AS names (>50% obs.)



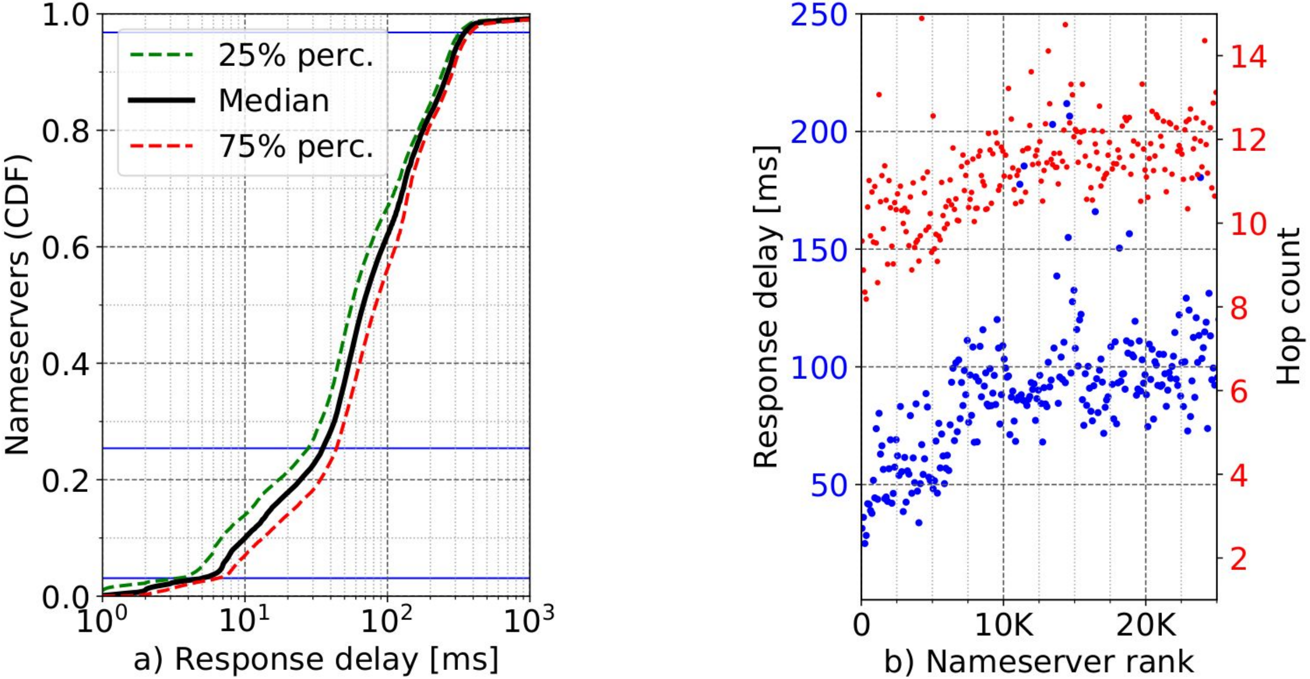
	Name	ASes	global	servers	delay	hops
1	AMAZON	3	16%	**5,026**	**60.9**	12.0
2	VERISIGN	7	10%	62	53.5	9.6
3	CLOUDFLARE	2	6.6%	**995**	**26.5**	**6.6**
4	AKAMAI	6	6.4%	**6,844**	**14.9**	**7.3**
5	MICROSOFT	5	2.7%	475	**74.8**	**13.5**
6	PCH	2	2.4%	178	29.9	7.2
7	ULTRADNS	1	2.3%	925	24.6	8.2
8	GOOGLE	1	2.1%	243	**89.9**	**13.3**
9	DYNDNS	1	1.8%	598	56.0	10.5
10	GODADDY	2	1.2%	372	63.0	11

Traffic distribution: QTYPEs (99.5% obs.)

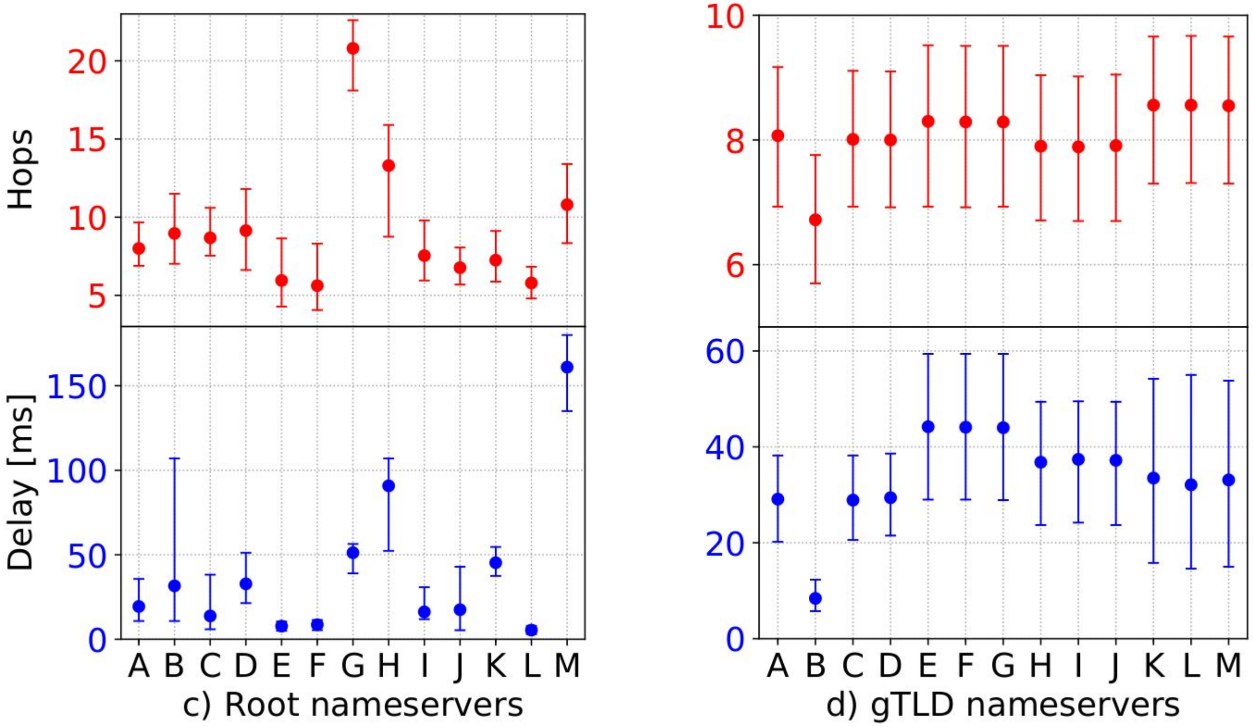


	QTYPE	global	data	nodata	nxd	err	qdots	TLDs	eSLDs	FQDNs	valid	TTL
1	A	**64%**	67%	**0.6%**	**22%**	11%	3.4	709	414,164	1,021,765	39%	60
2	AAAA	**22%**	57%	**25%**	**5.9%**	11%	3.5	623	213,694	528,504	80%	300
3	PTR	6.4%	45%	0.2%	29%	26%	**6.8**	**25**	363	144,283	54%	86400
4	NS	1.4%	9.4%	1.4%	**86%**	3.2%	2.4	149	5,169	6,470	**5.3%**	86400
5	TXT	1.4%	65%	4.1%	22%	8.1%	**5.9**	226	13,510	67,056	73%	**5**
6	MX	1.2%	60%	3.3%	2.9%	**34%**	2.6	255	33,390	39,686	86%	3600
7	SRV	1.1%	17%	3.4%	53%	27%	**6.8**	122	3,603	9,522	**22%**	300
8	CNAME	1.0%	28%	8.9%	**54%**	8.9%	4.4	192	**8,188**	**28,002**	35%	300
9	SOA	0.5%	40%	1.3%	39%	20%	**4.9**	101	9,843	10,564	46%	3600
10	DS	0.5%	43%	28%	28%	1.1%	2.6	247	20,617	23,688	69%	86400

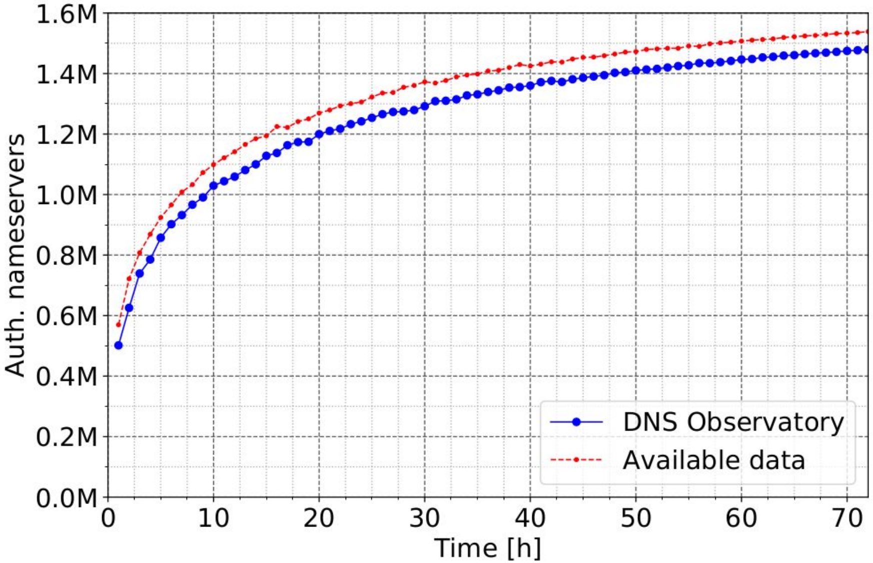
Performance: response delay & network hops

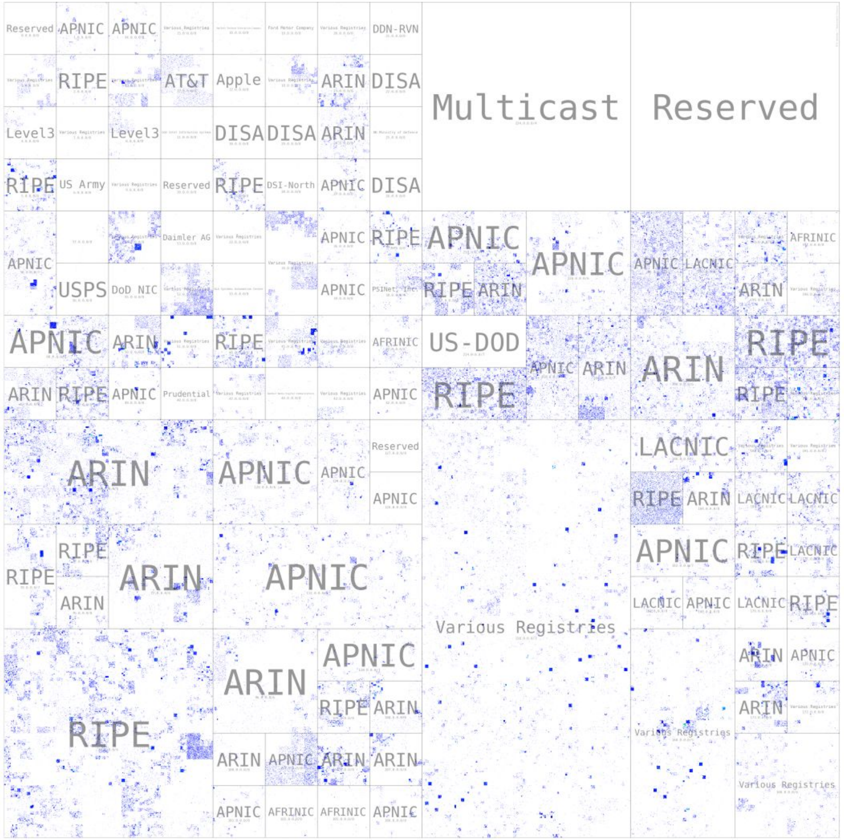


Performance: roots & gTLDs

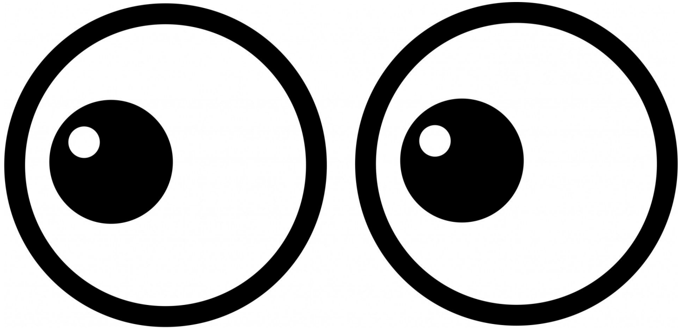


How many auth. nameservers on the Internet?





Happy Eyeballs



Happy Eyeballs v2 (HE)

1. Send concurrent A and AAAA queries
2. Collect responses
3. Start IP address race, give preference to IPv6

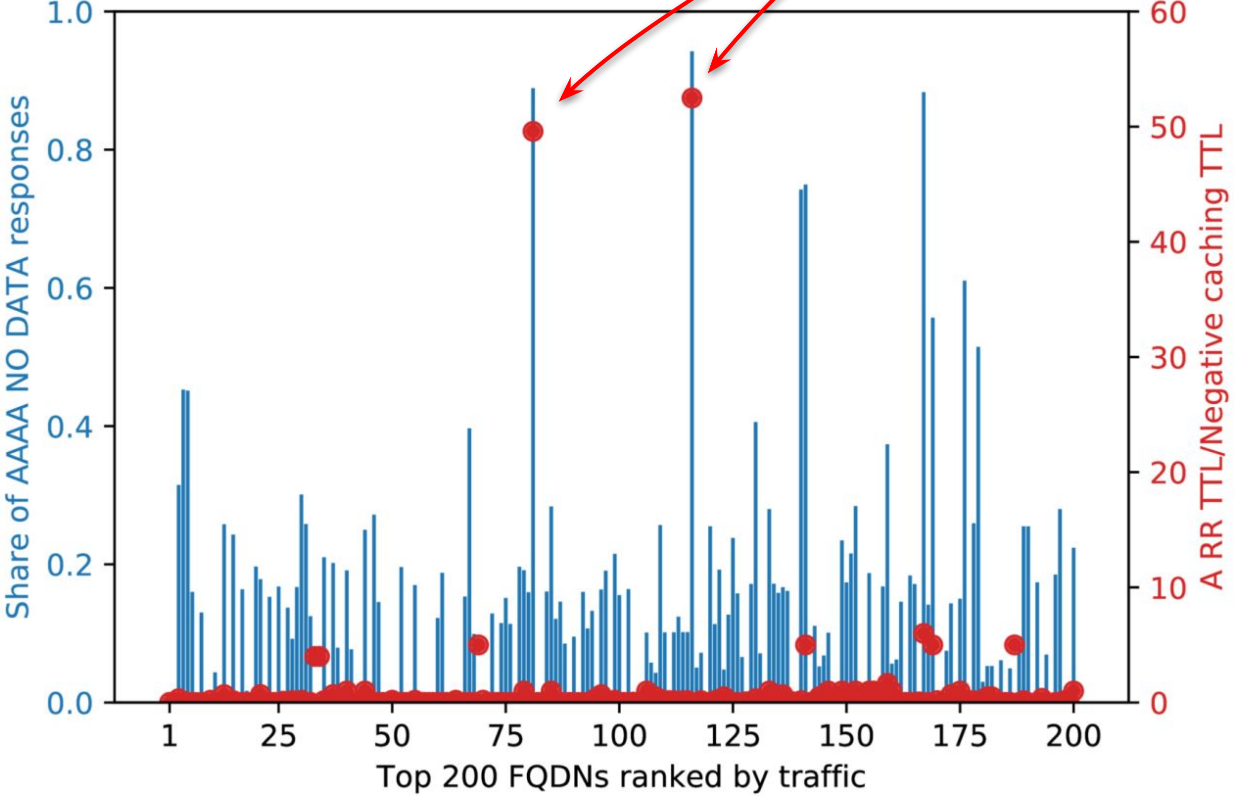
Happy Eyeballs v2 (HE): RFC 8305

1. Send concurrent A and AAAA queries
2. Collect responses
3. Start IP address race, give preference to IPv6

> Both queries SHOULD be made as soon after one another as possible, with the AAAA query made first and immediately followed by the A query.
>
> If a positive A response is received first (...), the client SHOULD wait a short time for the AAAA response to ensure that preference is given to IPv6 (...). This delay will be referred to as the "Resolution Delay".
>
> The recommended value for the Resolution Delay is 50 milliseconds.

HE vs. DNS: seen in the wild

TTL = 10-15 min
Negative TTL = 15 *seconds*



Why read?

Didn’t say & Take-aways

- How TTLs impact query volumes?
- How to predict upcoming DNS changes?
- Did we see many QNAME minimization (qmin) deployments?
- How DNS could be improved for HE?

- We invite you (academic researchers) to access the data
- Long-term goal: make parts publicly available

- DNS Observatory provides birds-eye view on the DNS

- ~50% of seen DNS transactions:
  - Top 1K nameservers
  - Top 10 AS owners

- Consider HE effects of low negative caching TTLs

DNS Observatory:

The Big Picture of the DNS

Paweł Foremski

Farsight Security / IITiS PAN

pjf@fsi.io @pforemski

Oliver Gasser

Technical University of Munich
gasser@net.in.tum.de

Giovane C. M. Moura

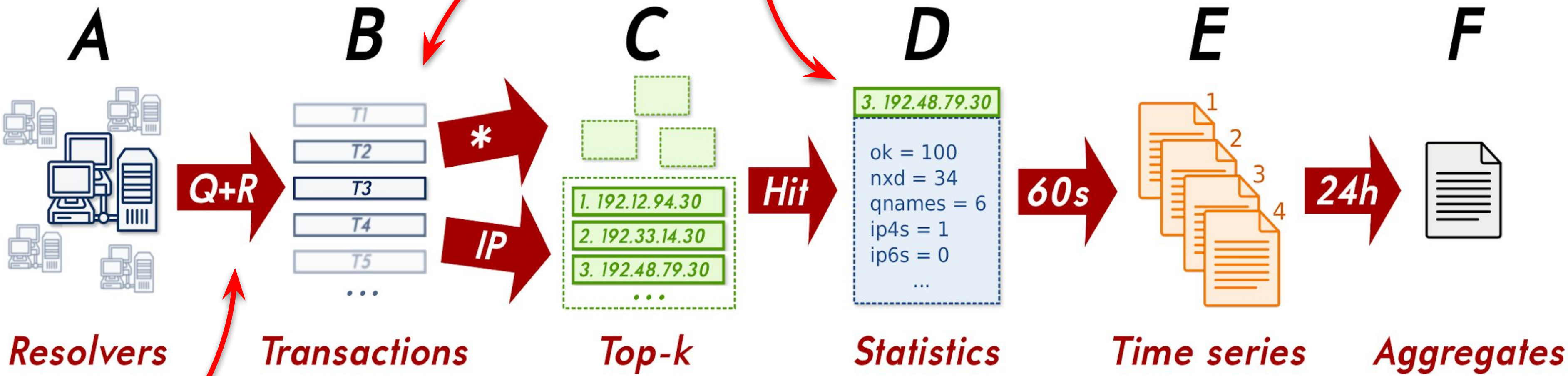
SIDN Labs / TU Delft
giovane.moura@sidn.nl

ACM Internet Measurement Conference 2019
October 2019, Amsterdam

Backup slides

User privacy?

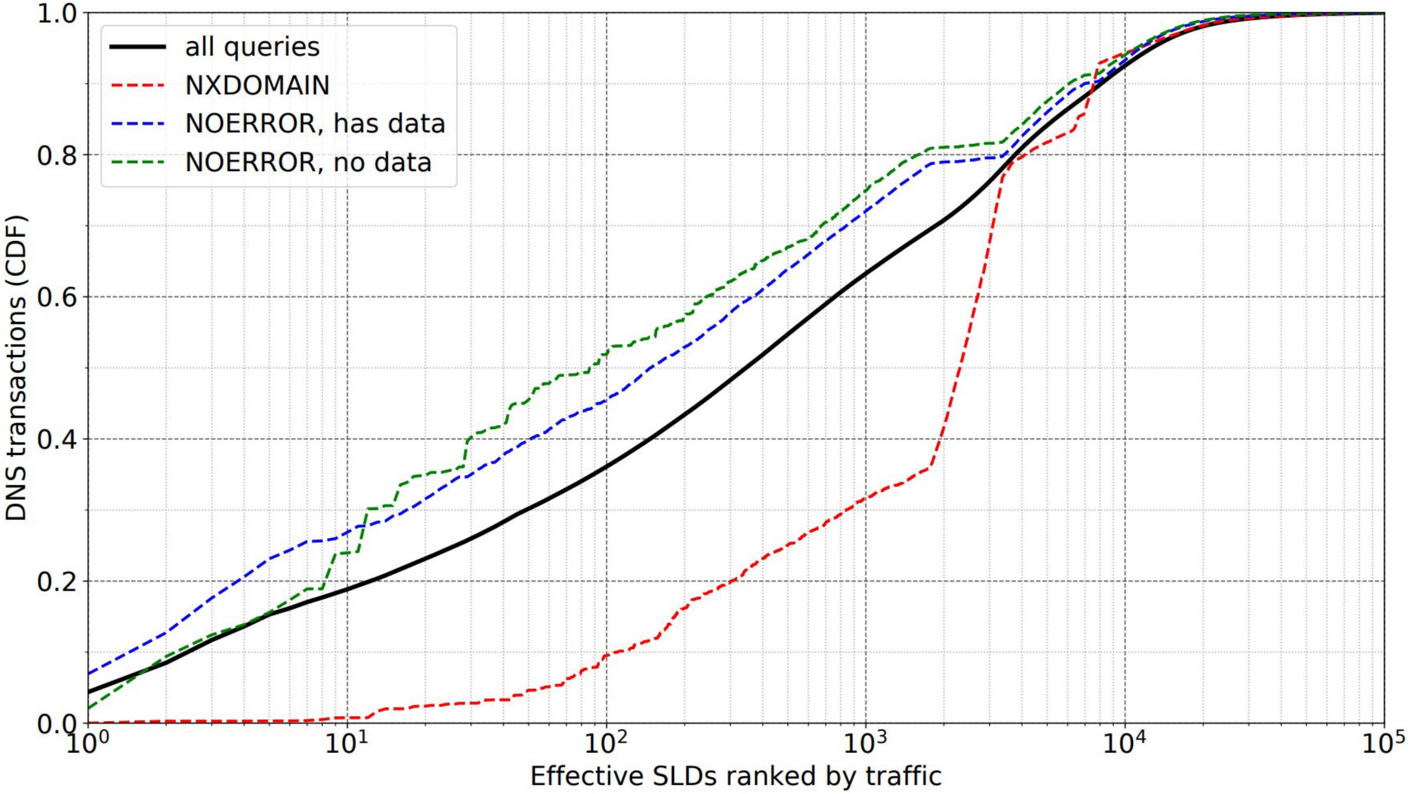
Drop transaction details (eg. EDNS0)



Traffic "above" resolvers

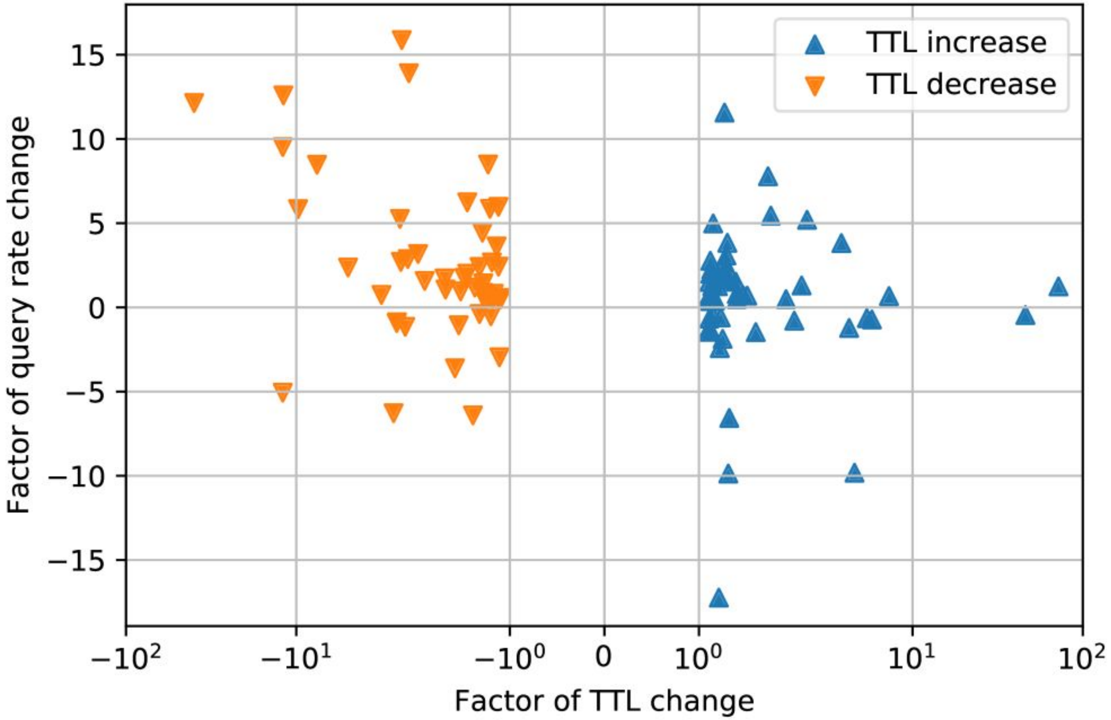
Aggregate, drop unpopular stuff

Traffic distribution: top 100K SLDs (69% obs.)

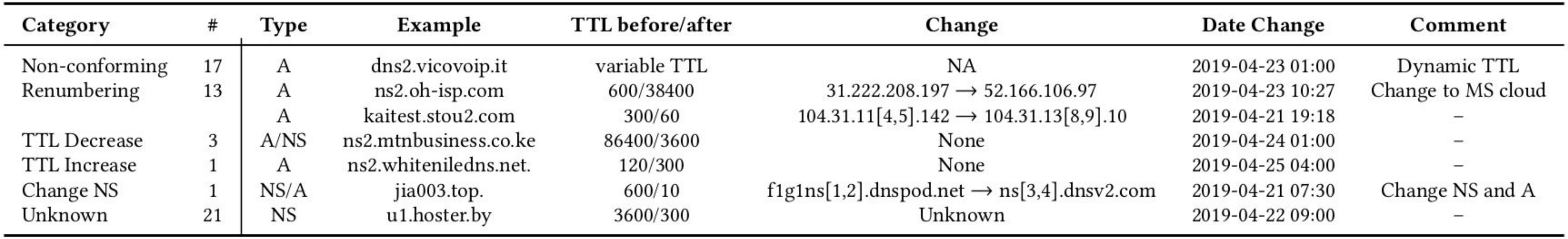


NXD	19%
Data	68%
Nodata	7%

Impact on query rate



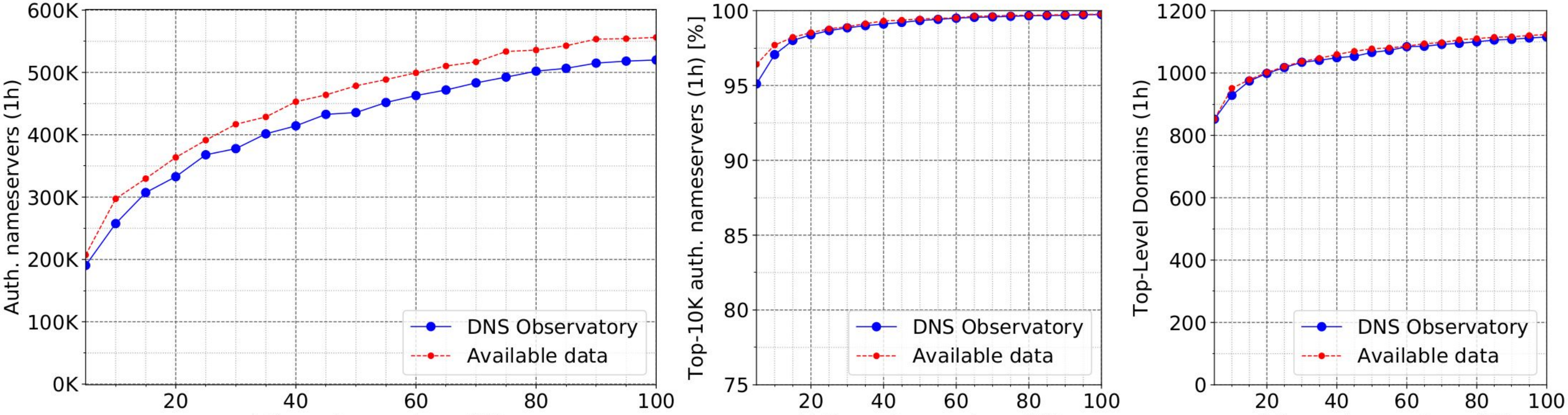
Upcoming change?



Category	#	Type	Example	TTL before/after	Change	Date Change	Comment
Non-conforming	17	A	dns2.vicovoip.it	variable TTL	NA	2019-04-23 01:00	Dynamic TTL
Renumbering	13	A	ns2.oh-isp.com	600/38400	31.222.208.197 → 52.166.106.97	2019-04-23 10:27	Change to MS cloud
		A	kaitest.stou2.com	300/60	104.31.11[4,5].142 → 104.31.13[8,9].10	2019-04-21 19:18	–
TTL Decrease	3	A/NS	ns2.mtnbusiness.co.ke	86400/3600	None	2019-04-24 01:00	–
TTL Increase	1	A	ns2.whiteniledns.net.	120/300	None	2019-04-25 04:00	–
Change NS	1	NS/A	jia003.top.	600/10	f1g1ns[1,2].dnspod.net → ns[3,4].dnsv2.com	2019-04-21 07:30	Change NS and A
Unknown	21	NS	u1.hoster.by	3600/300	Unknown	2019-04-22 09:00	–

Table 4: TTL changes detected and classification

Data representativeness

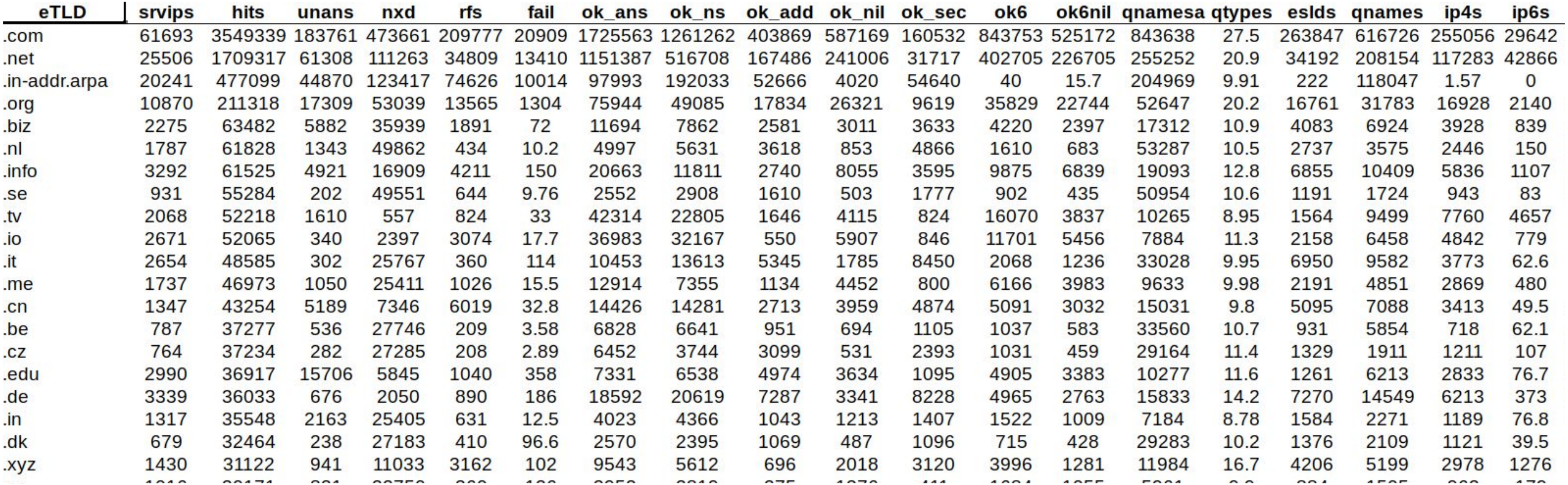


a) Recursive resolvers [%]

b) Recursive resolvers [%]

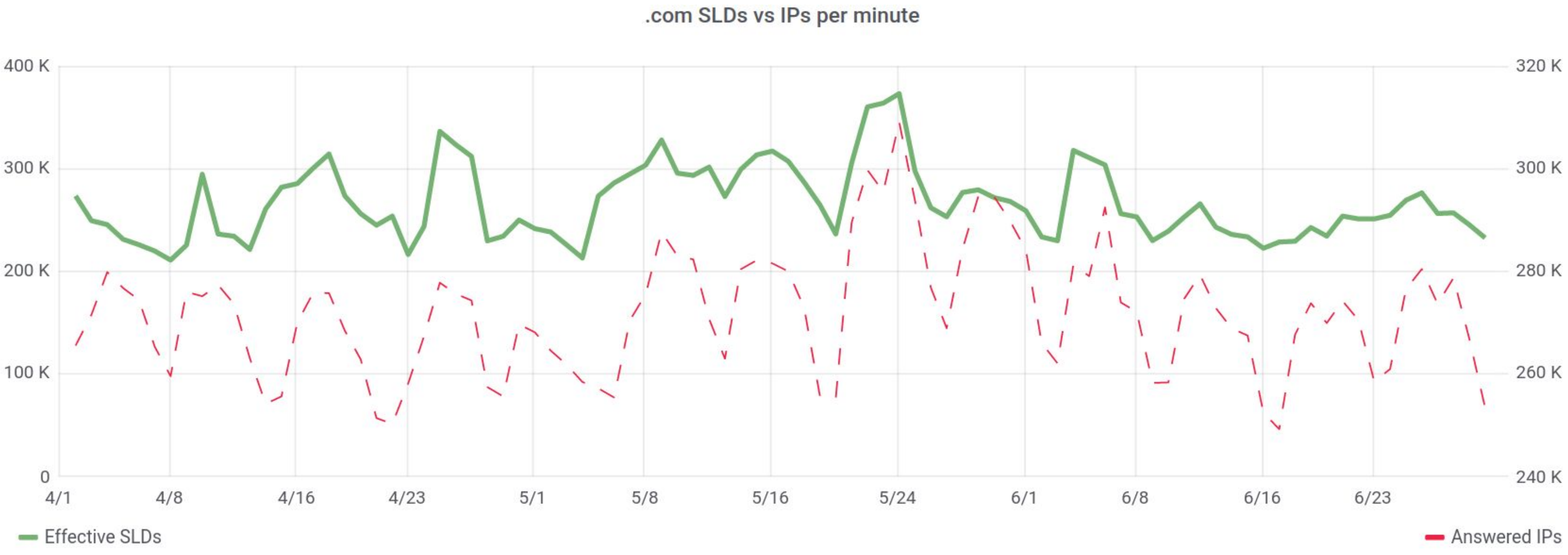
c) Recursive resolvers [%]

Example: 1-minute snapshot



eTLD	srvips	hits	unans	nxd	rfs	fail	ok_ans	ok_ns	ok_add	ok_nil	ok_sec	ok6	ok6nil	qnamesa	qtypes	eslds	qnames	ip4s	ip6s
.com	61693	3549339	183761	473661	209777	20909	1725563	1261262	403869	587169	160532	843753	525172	843638	27.5	263847	616726	255056	29642
.net	25506	1709317	61308	111263	34809	13410	1151387	516708	167486	241006	31717	402705	226705	255252	20.9	34192	208154	117283	42866
.in-addr.arpa	20241	477099	44870	123417	74626	10014	97993	192033	52666	4020	54640	40	15.7	204969	9.91	222	118047	1.57	0
.org	10870	211318	17309	53039	13565	1304	75944	49085	17834	26321	9619	35829	22744	52647	20.2	16761	31783	16928	2140
.biz	2275	63482	5882	35939	1891	72	11694	7862	2581	3011	3633	4220	2397	17312	10.9	4083	6924	3928	839
.nl	1787	61828	1343	49862	434	10.2	4997	5631	3618	853	4866	1610	683	53287	10.5	2737	3575	2446	150
.info	3292	61525	4921	16909	4211	150	20663	11811	2740	8055	3595	9875	6839	19093	12.8	6855	10409	5836	1107
.se	931	55284	202	49551	644	9.76	2552	2908	1610	503	1777	902	435	50954	10.6	1191	1724	943	83
.tv	2068	52218	1610	557	824	33	42314	22805	1646	4115	824	16070	3837	10265	8.95	1564	9499	7760	4657
.io	2671	52065	340	2397	3074	17.7	36983	32167	550	5907	846	11701	5456	7884	11.3	2158	6458	4842	779
.it	2654	48585	302	25767	360	114	10453	13613	5345	1785	8450	2068	1236	33028	9.95	6950	9582	3773	62.6
.me	1737	46973	1050	25411	1026	15.5	12914	7355	1134	4452	800	6166	3983	9633	9.98	2191	4851	2869	480
.cn	1347	43254	5189	7346	6019	32.8	14426	14281	2713	3959	4874	5091	3032	15031	9.8	5095	7088	3413	49.5
.be	787	37277	536	27746	209	3.58	6828	6641	951	694	1105	1037	583	33560	10.7	931	5854	718	62.1
.cz	764	37234	282	27285	208	2.89	6452	3744	3099	531	2393	1031	459	29164	11.4	1329	1911	1211	107
.edu	2990	36917	15706	5845	1040	358	7331	6538	4974	3634	1095	4905	3383	10277	11.6	1261	6213	2833	76.7
.de	3339	36033	676	2050	890	186	18592	20619	7287	3341	8228	4965	2763	15833	14.2	7270	14549	6213	373
.in	1317	35548	2163	25405	631	12.5	4023	4366	1043	1213	1407	1522	1009	7184	8.78	1584	2271	1189	76.8
.dk	679	32464	238	27183	410	96.6	2570	2395	1069	487	1096	715	428	29283	10.2	1376	2109	1121	39.5
.xyz	1430	31122	941	11033	3162	102	9543	5612	696	2018	3120	3996	1281	11984	16.7	4206	5199	2978	1276

Example: time series for .com (30 days)


.com SLDs vs IPs per minute
400 K
300 K
200 K
100 K
320 K
300 K
280 K
260 K
240 K
4/1
4/8
4/16
4/23
5/1
5/8
5/16
5/24
6/1
6/8
6/16
6/23
Effective SLDs
Answered IPs