TTL Violation of DNS Resolvers in the Wild

Protick Bhowmick and Tijay Chung (tijay@vt.edu)
Virginia Tech

This work will be published at PAM'2023

VIRGINIA TECH

Motivation

- TTL can play an important role in both DNS security and performance
  - DNSSEC-signed response's caching period or TLSA records
  - responsiveness of CDN-controlled domains
- Do DNS resolvers respect TTLs?

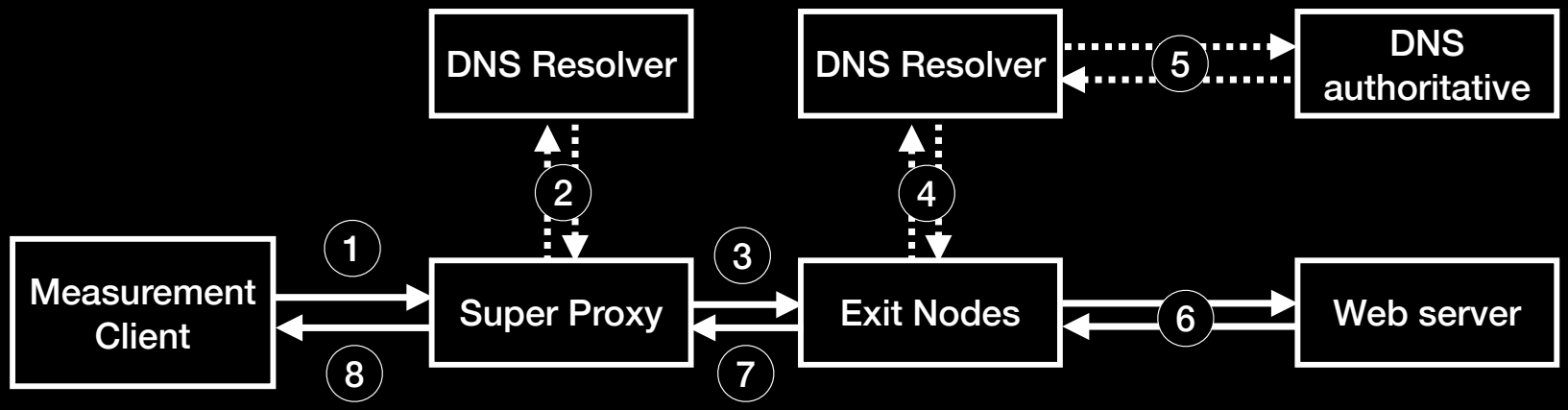
Measuring TTL Violation

- Long thread of studies showed that some resolvers violate TTL
  - Allman [IMC'20], Pang et al [IMC'04], Kyle et al [IMC'13], Moura [RIPE Labs'07]
  - Open resolvers, campus traffic, routers deployed in residential networks, etc.
- Still challenging to understand how such TTL violations exist in the wild and at scale without access to devices or users in affected networks

Residential Proxy

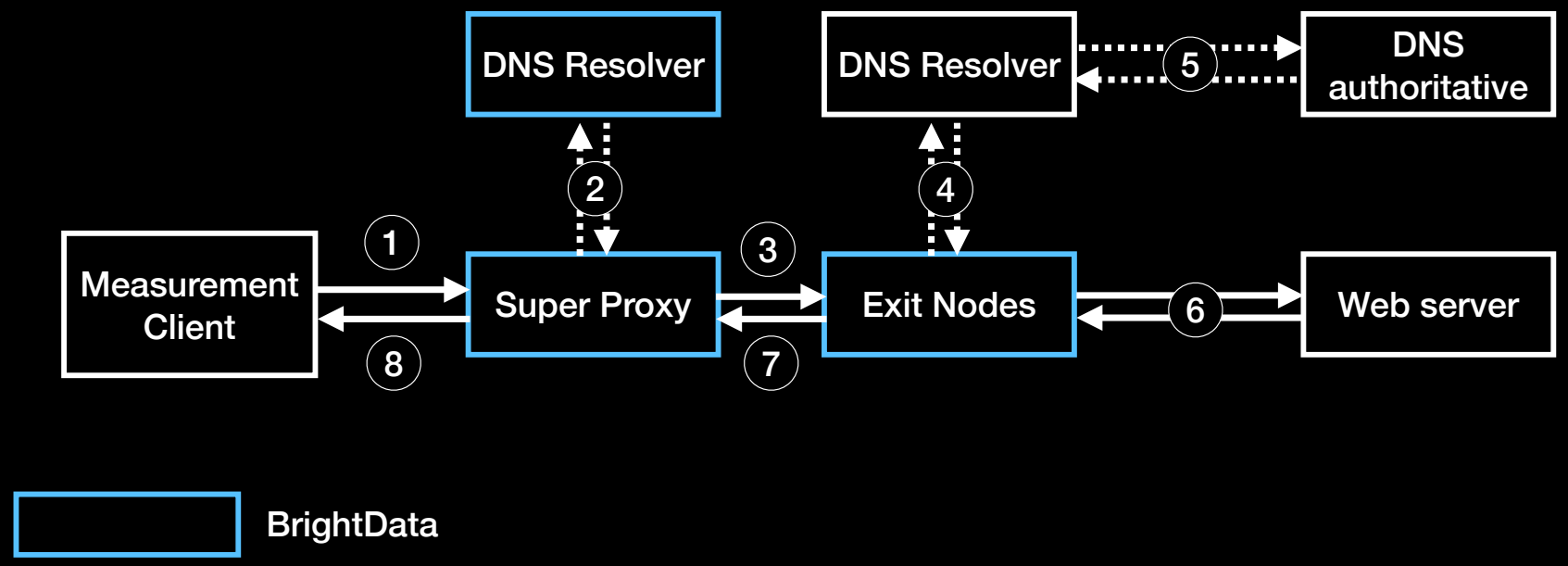
- BrightData
  - HTTP/S services that route traffic via residential nodes (called exit nodes)
- Over 72 million IPs around the globe

How it works



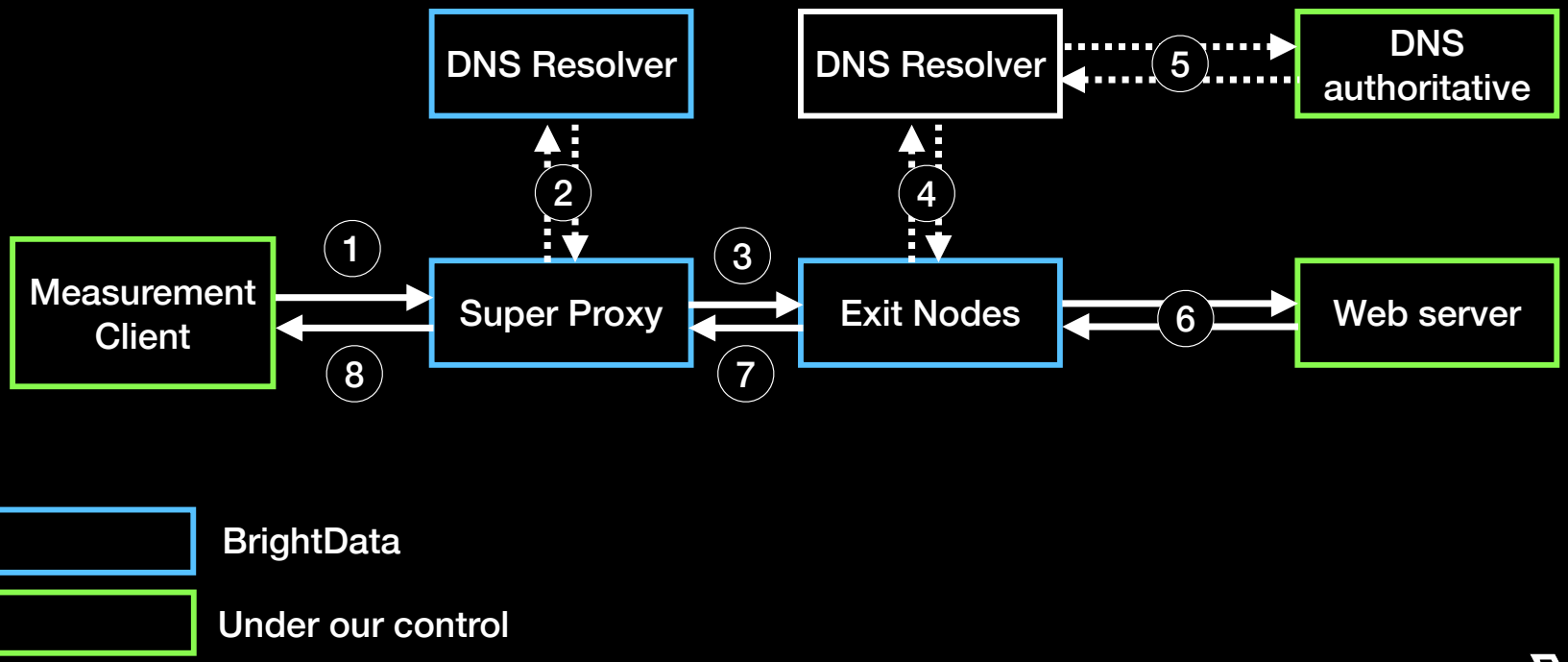
VIRGINIA TECH

How it works



VIRGINIA TECH

How it works



VIRGINIA TECH

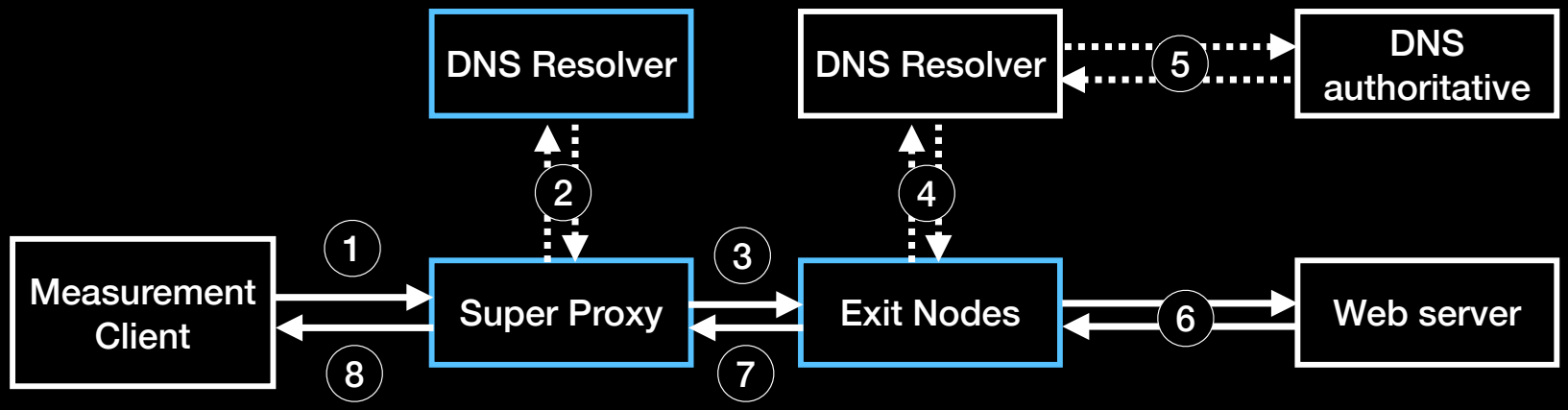
Features

- Supports only HTTP/S
- DNS request location
  - Super proxy or Exit Nodes
  - But Super Proxy always check the validity of URL
- Country selection
- Session
- Logging and debugging
  - Super proxy will return special HTTP headers
    - X-Hola-Unblocker-Debug
    - Unique identifier (zID)

Challenges

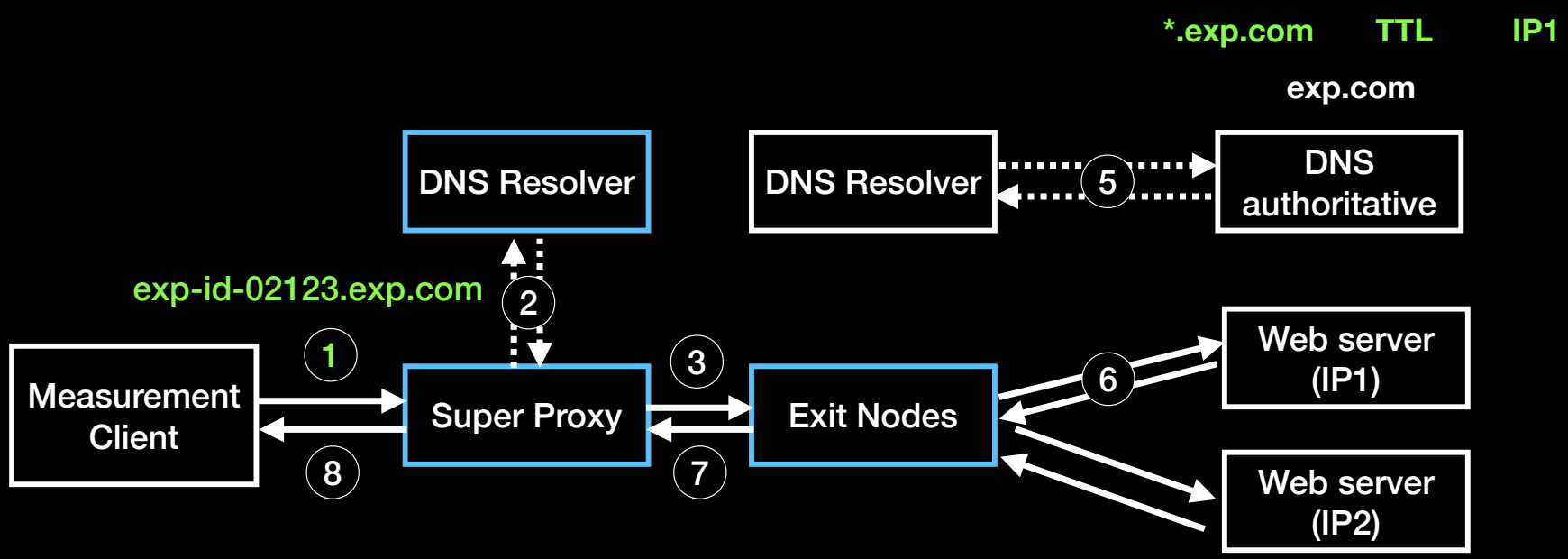
- We are only permitted to send HTTP(s) queries
  - How can we measure DNS resolvers and their TTL violations?

Initial (and naive) Plan



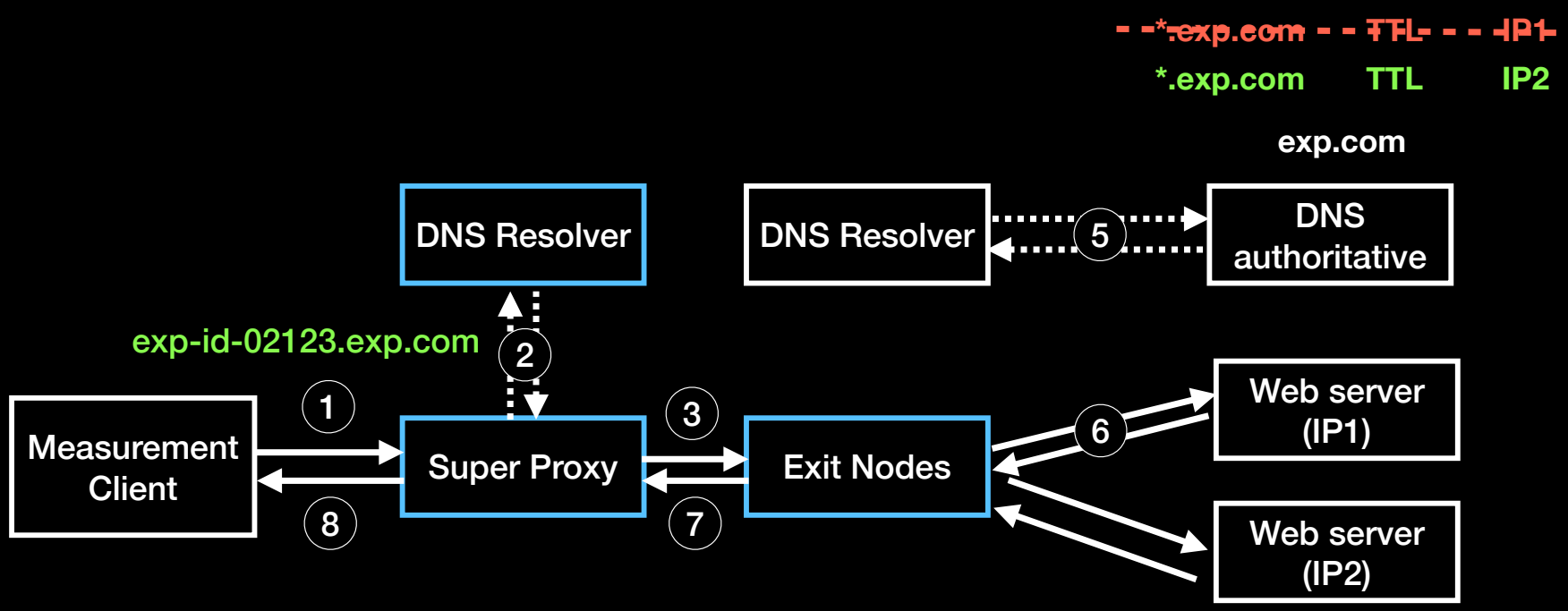
VIRGINIA TECH

Initial (and naive) Plan



VIRGINIA TECH

Initial (and naive) Plan



VIRGINIA TECH

The real DNS resolver structure

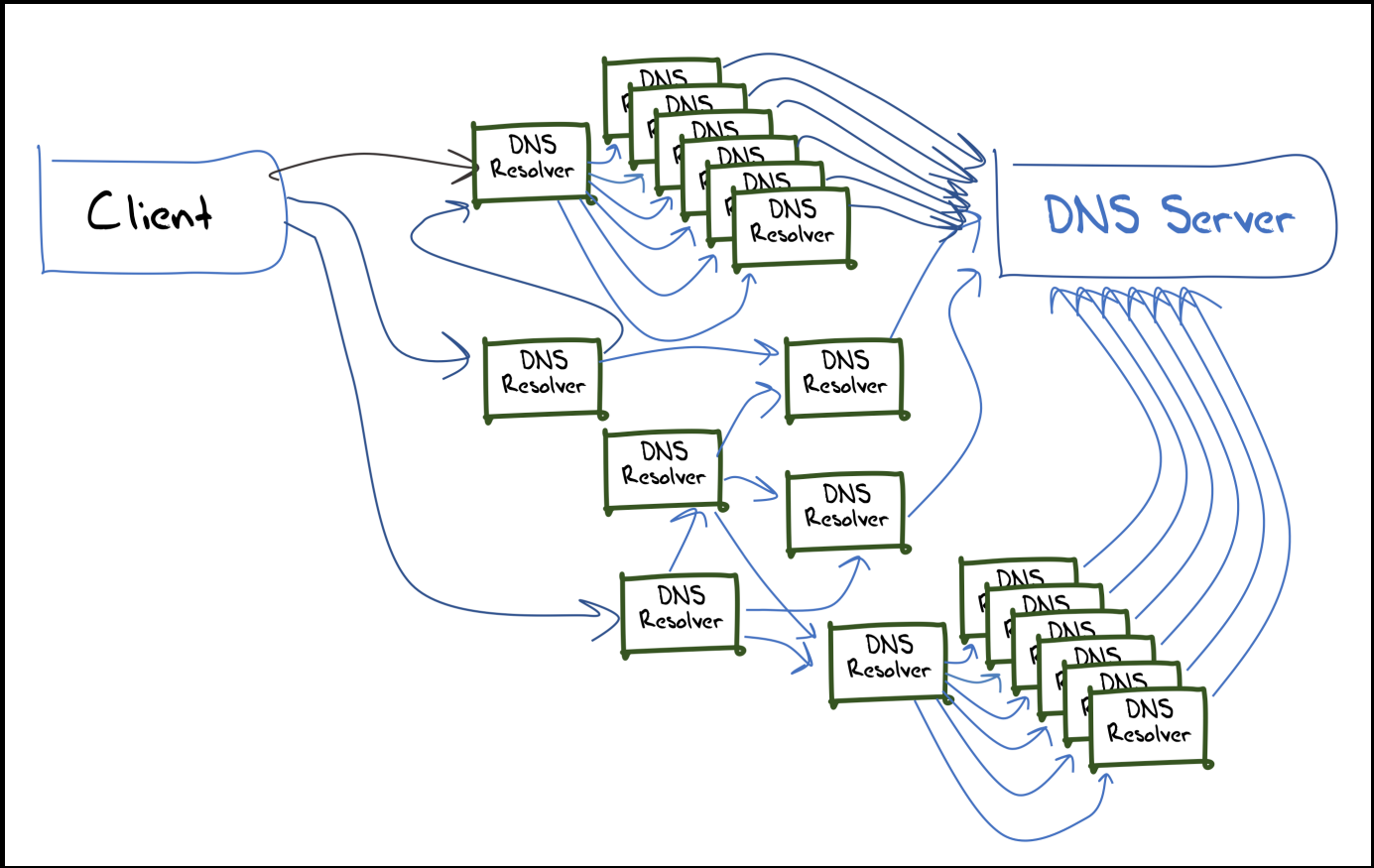


Figure from “DNS Openness” (Geoff Huston)

The Real DNS resolver structure

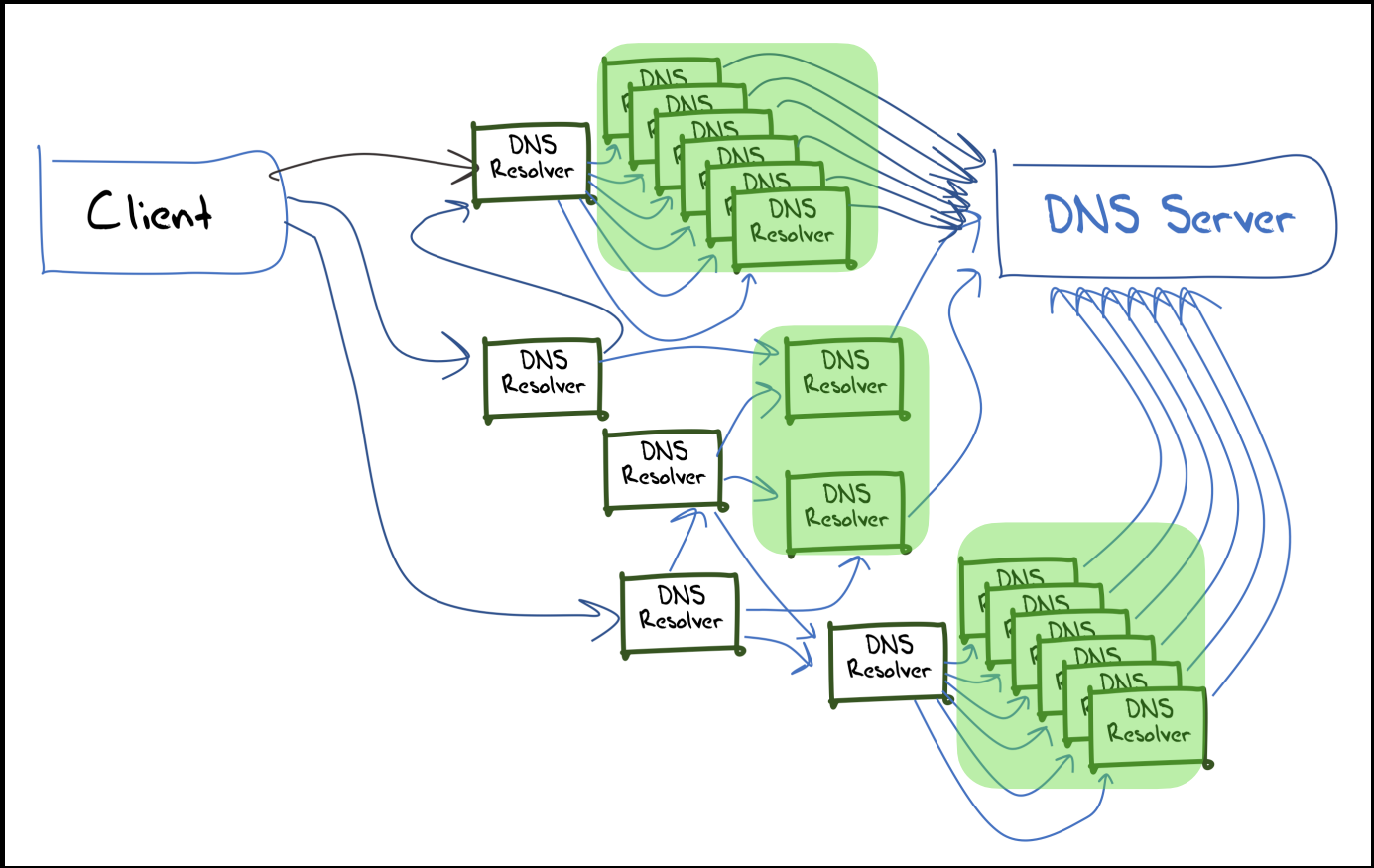
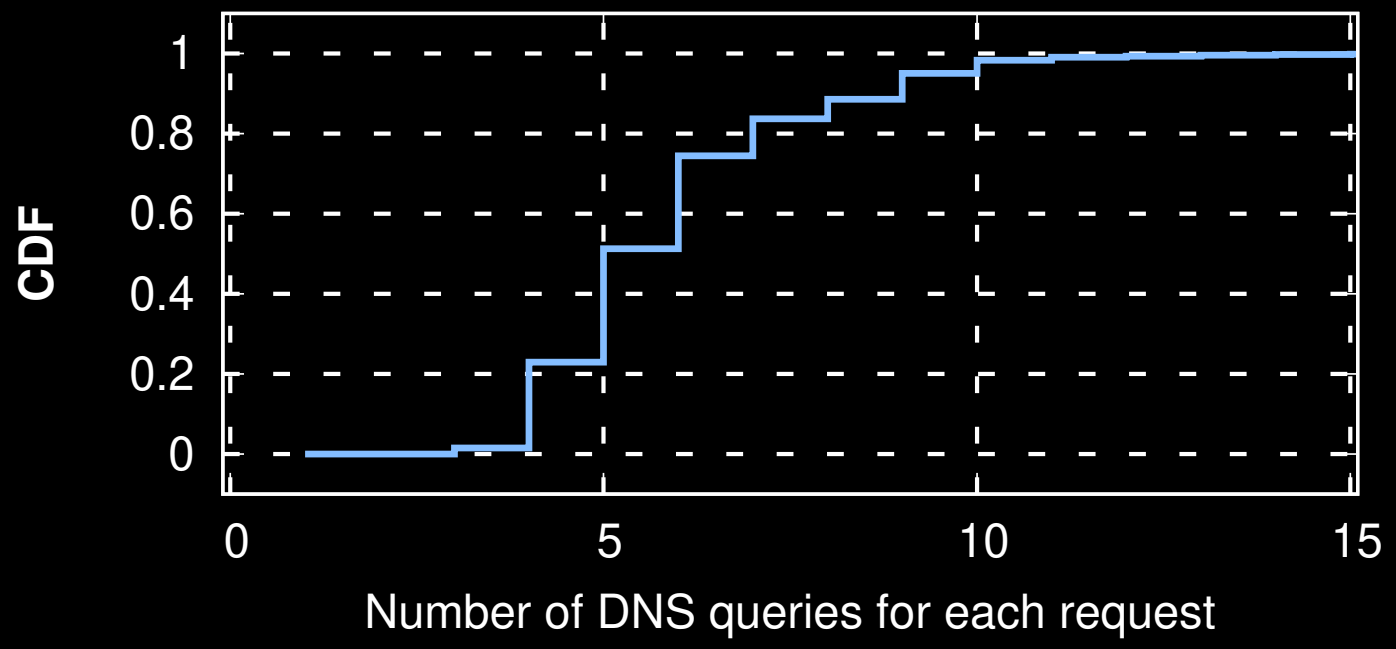


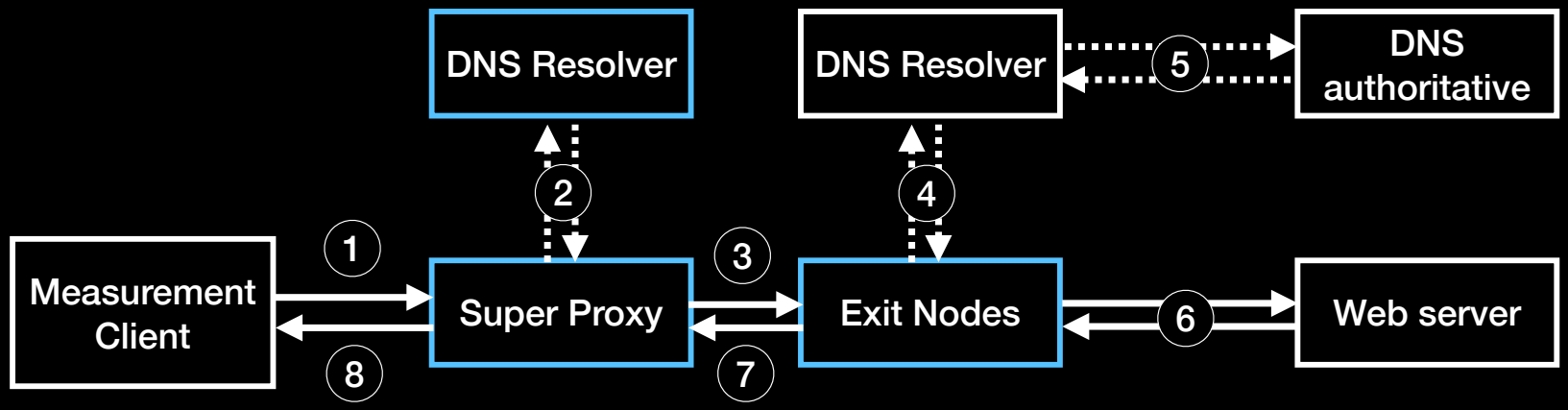
Figure from “DNS Openness” (Geoff Huston)

of resolvers that Our DNS authoritative server sees



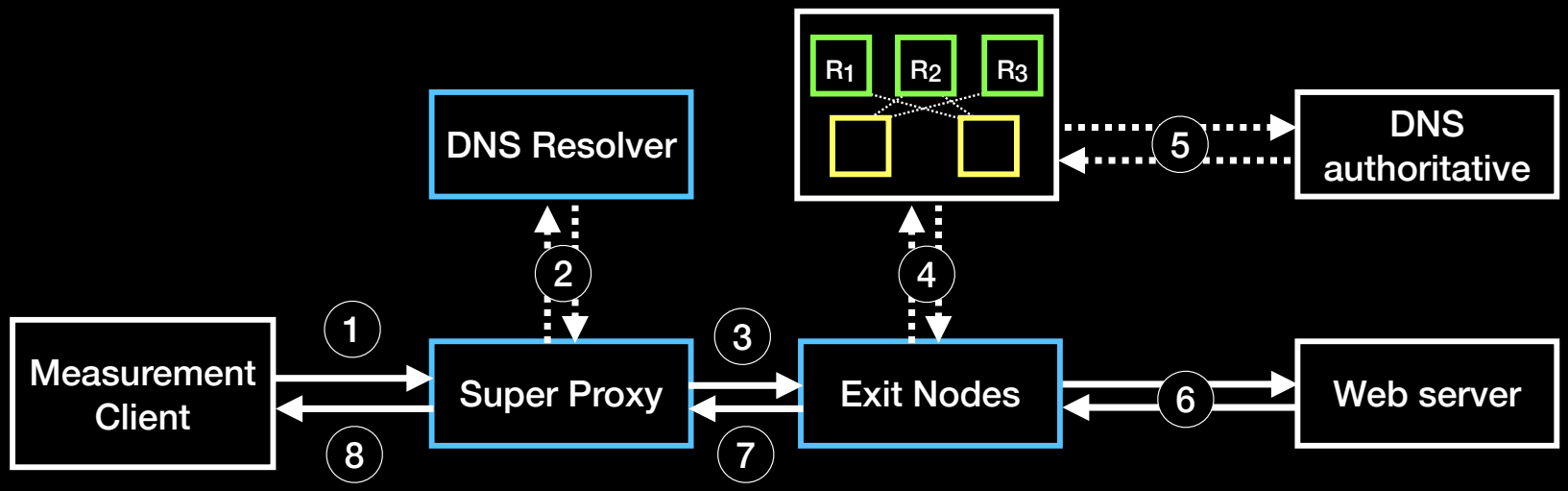
VIRGINIA TECH

Initial (Naive) Plan



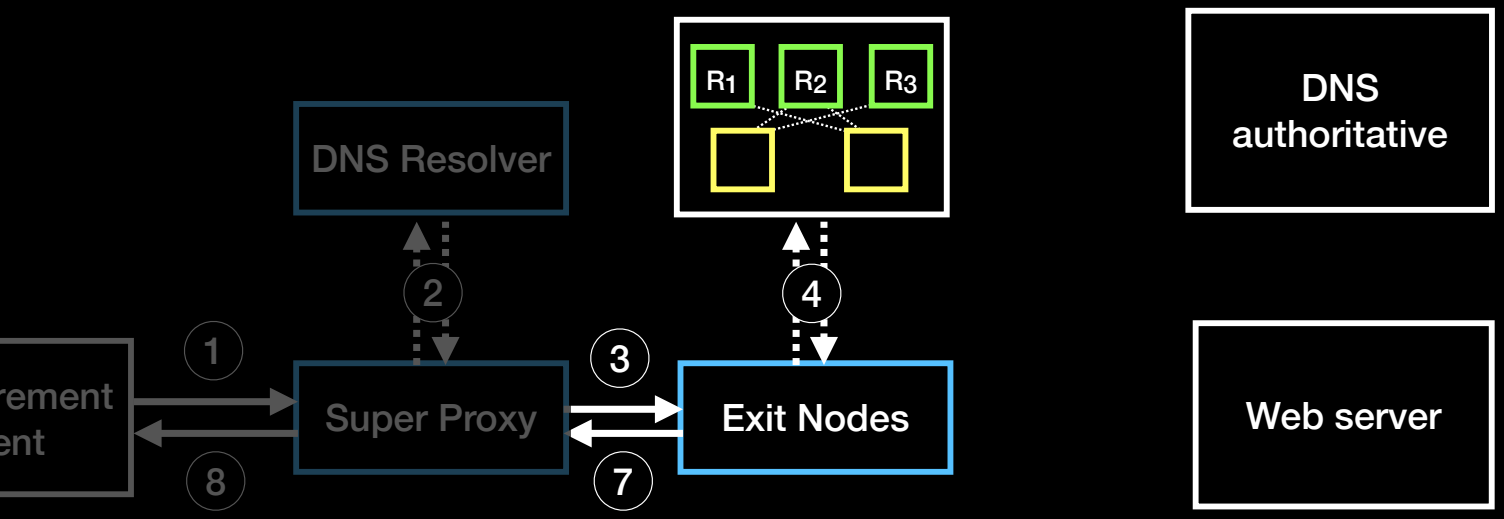
VIRGINIA TECH

Revised Measurement Infastructure



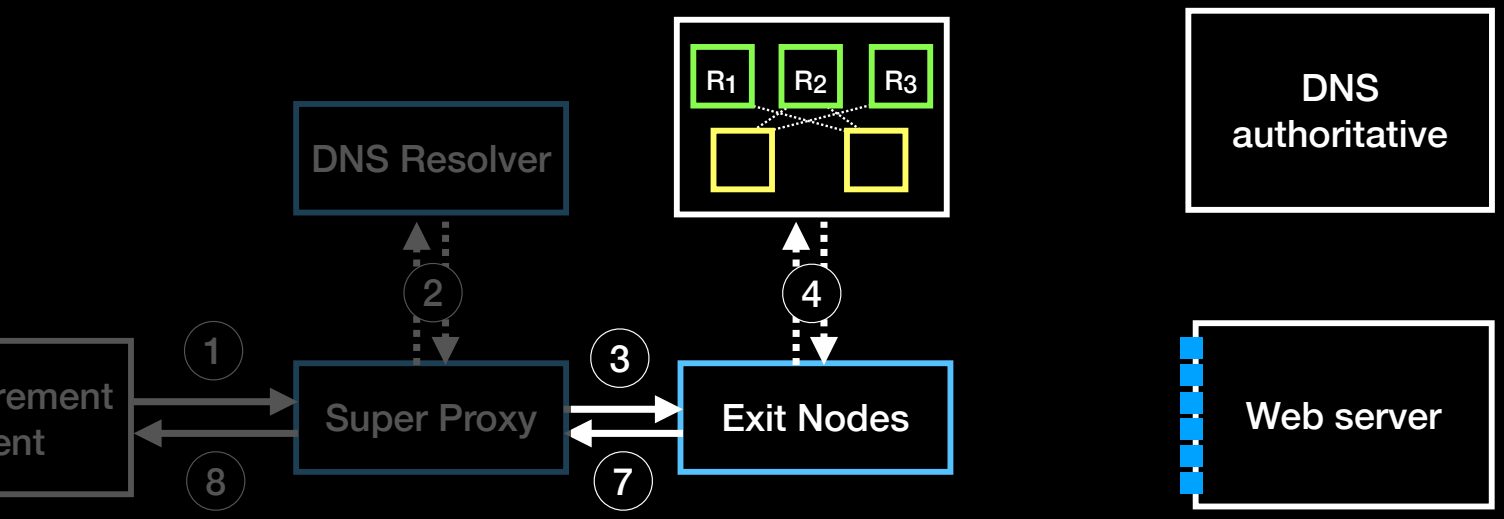
VIRGINIA TECH

Revised Measurement Infastructure



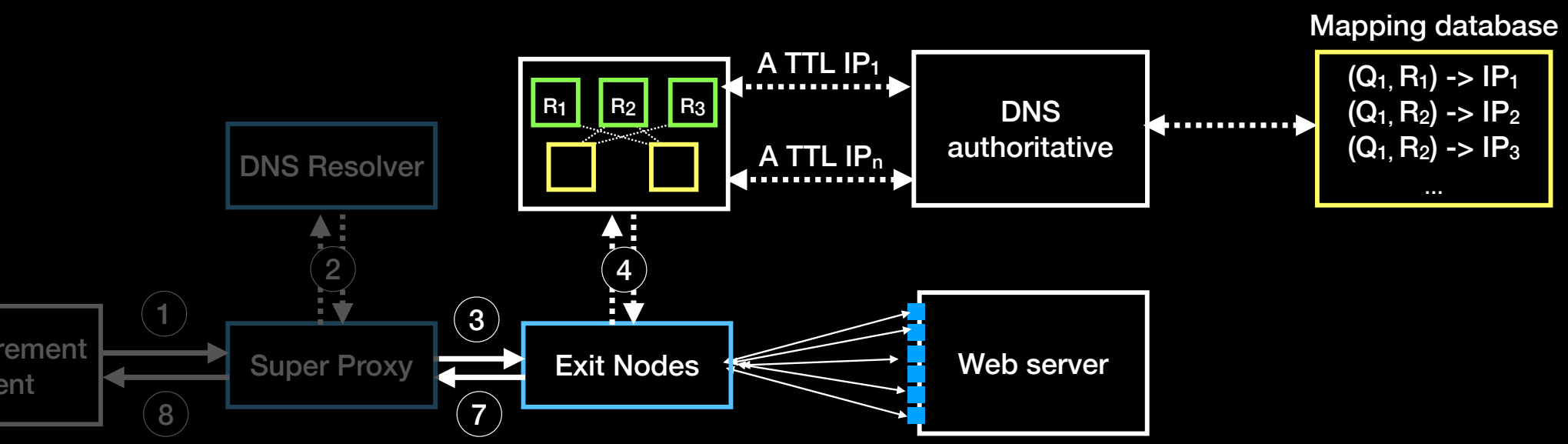
VIRGINIA TECH

Revised Measurement Infastructure



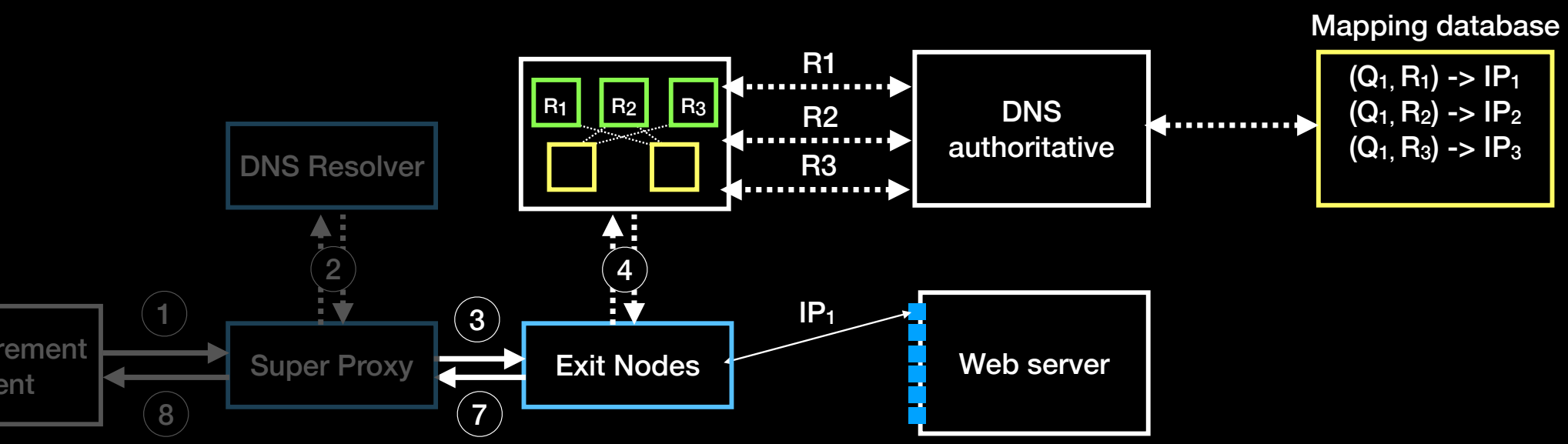
VIRGINIA TECH

Revised Measurement Infastructure



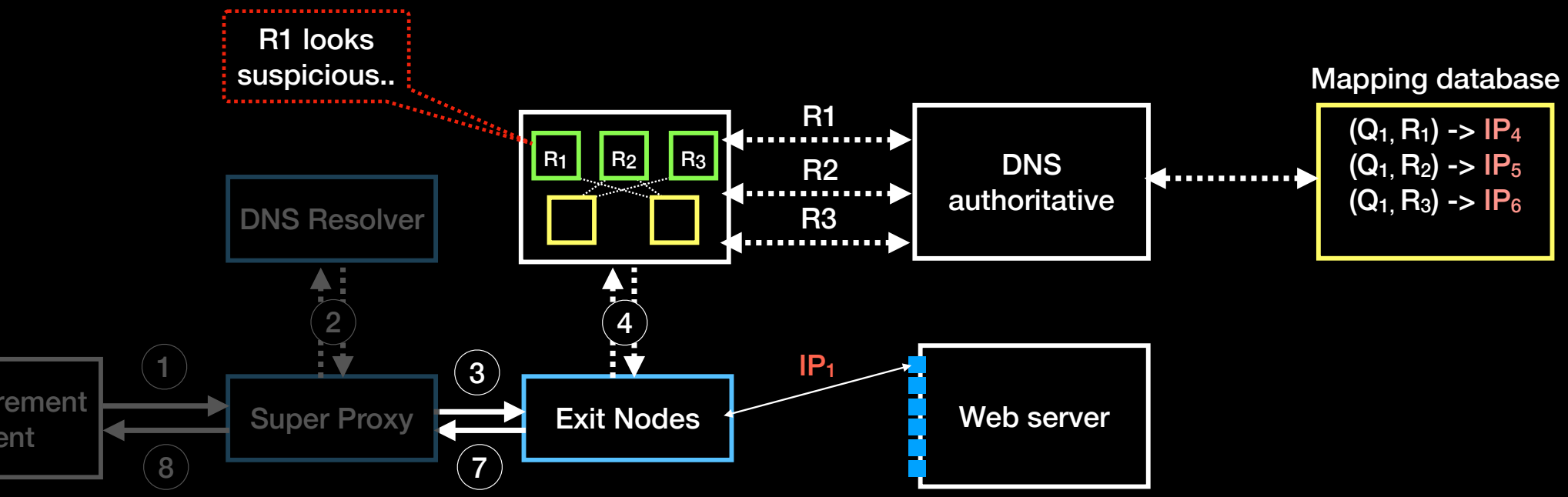
VIRGINIA TECH

Example
First DNS Request



VIRGINIA TECH

Example
Second DNS Request (After TTL expires)



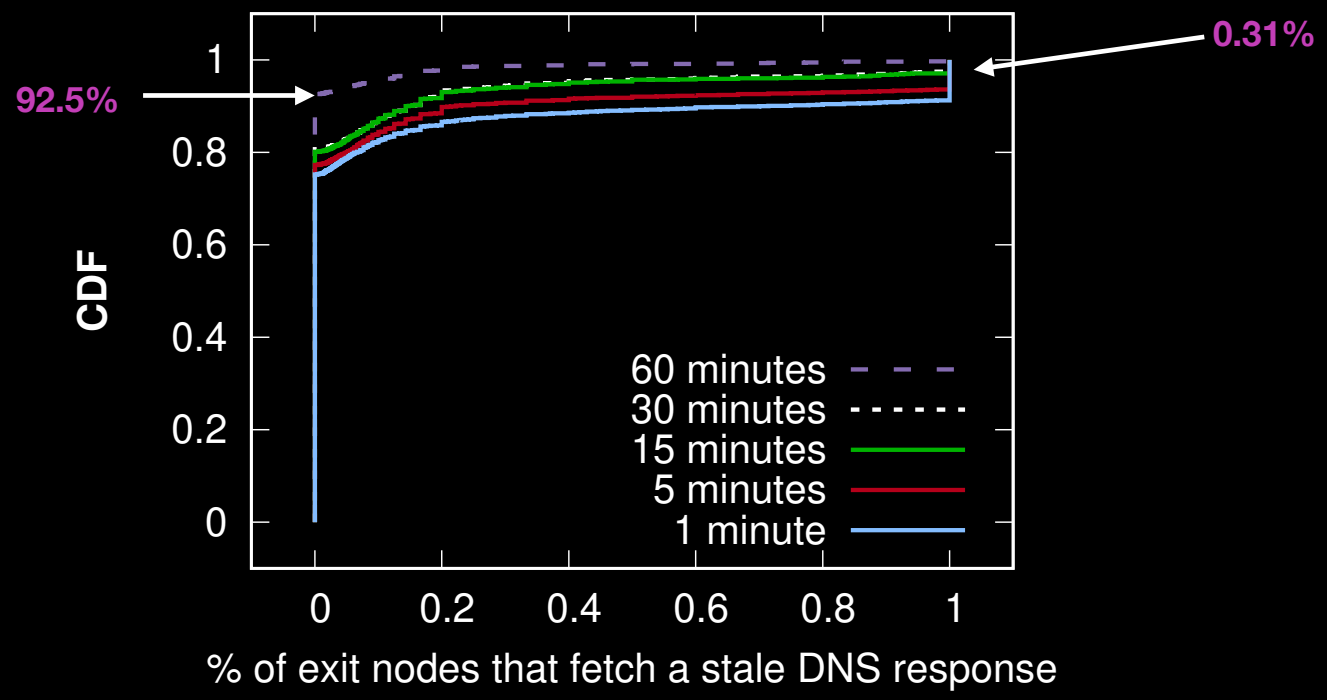
VIRGINIA TECH

Measurement Data

HTTP Queries		2M
Exit Nodes	**Unique IDs**	274,570
	ASes	9,514
	Countries	220

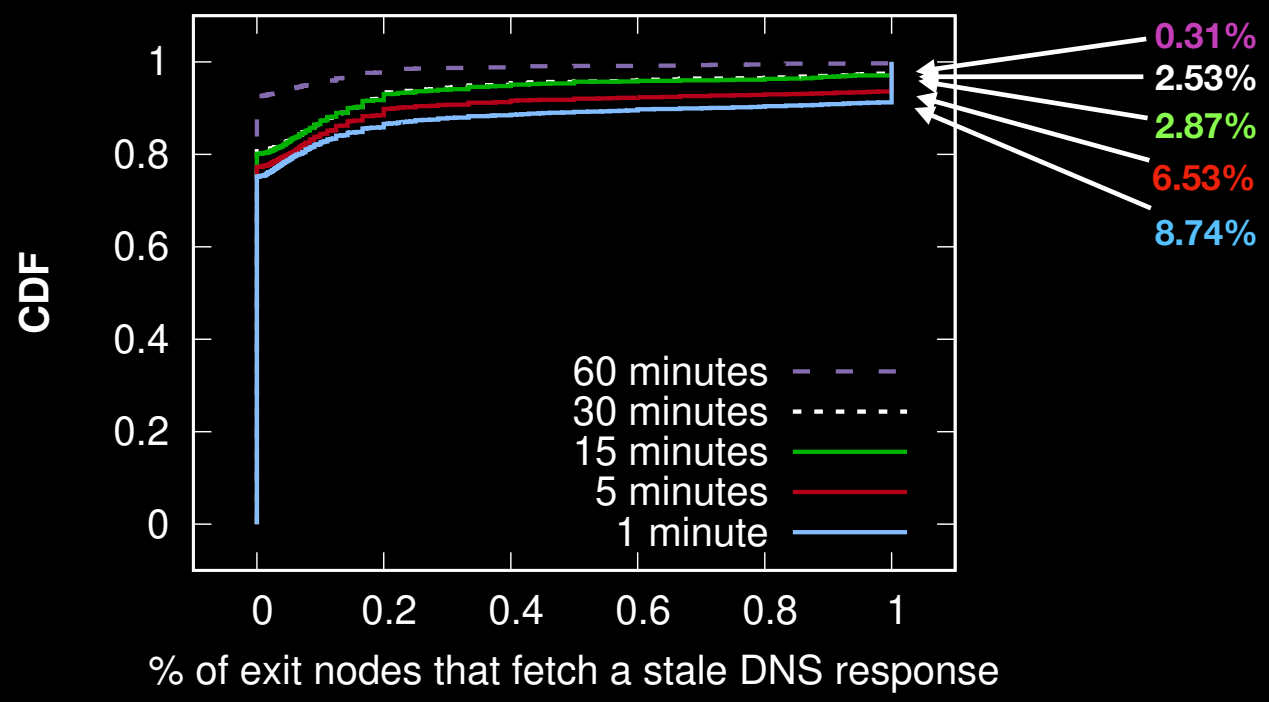
VIRGINIA TECH

Measurement Result



VIRGINIA TECH

Measurement Result



VIRGINIA TECH

Cross-validation

		Our methodology	
		Honoring	Extending
Direct Scan	Honor	197	0
	Extending	0	16

Cross-validation

		Our methodology	
		Honoring	Extending
Direct Scan	Honor	197	0
	Extending	0	16
Exit Nodes	Honor	381	1
	Extending	0	62

Country-level Results

Rank	Country	Exit nodes		Ratio
		TTL-extended	Total	
1	Togo	91	106	85.8%
2	China	1,514	2,425	62.4%
3	Reunion (France)	112	189	59.3%
4	Jamaica	175	481	36.4%
5	Sint Maaten	137	455	30.1%
6	France	81	329	24.6%
7	Côte d'Ivoire	68	288	23.6%
8	Cayman Island	105	461	22.8%
9	Ireland	347	1,726	20.1%
10	Switzerland	141	704	20.0%

ISP-level Results

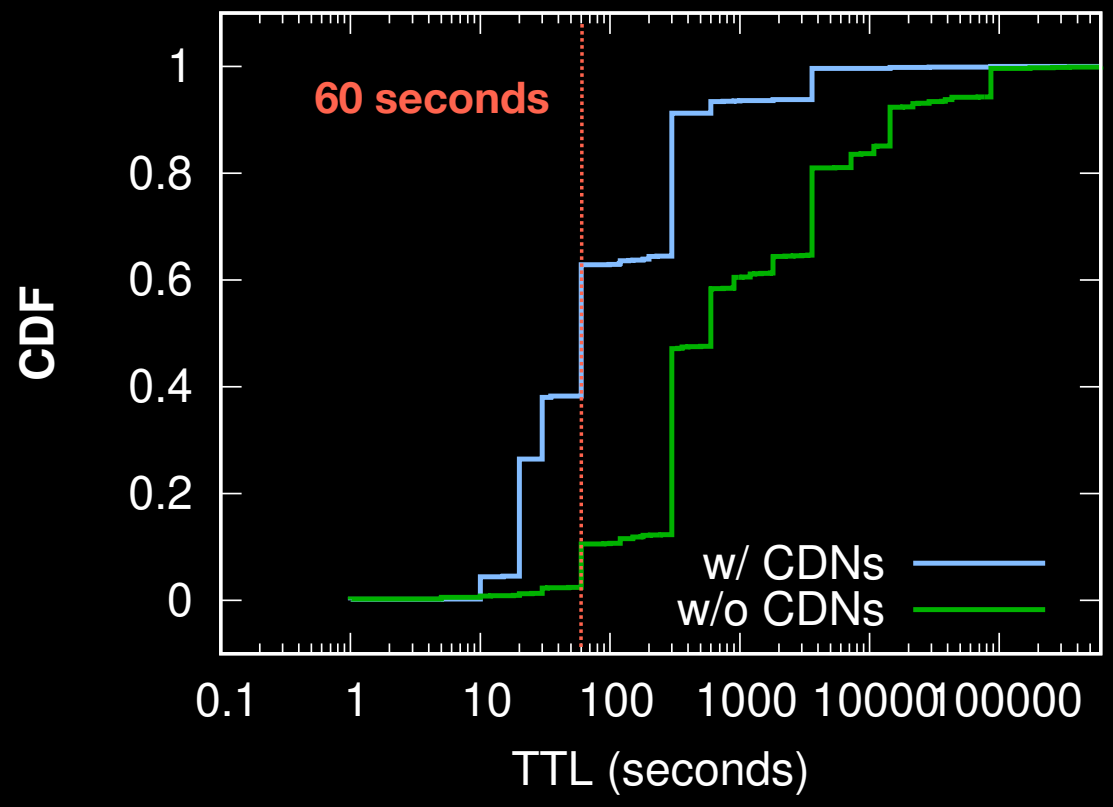
Country	ISP	DNS Resolvers	Exit Nodes
Russia	PSJC Vimpelcom	16	366
	PSJC Rotelecom	12	124
	Net By Net	8	58
	TIS Dialog	6	108
	MTS PSJC	4	69
	MSK-IX	4	36
China	China Telecom	13	125
	China Mobile	7	39
	Tianjin Provincial	5	50
	China Unicom	4	27

Case-Study

Case-Study of CDNs

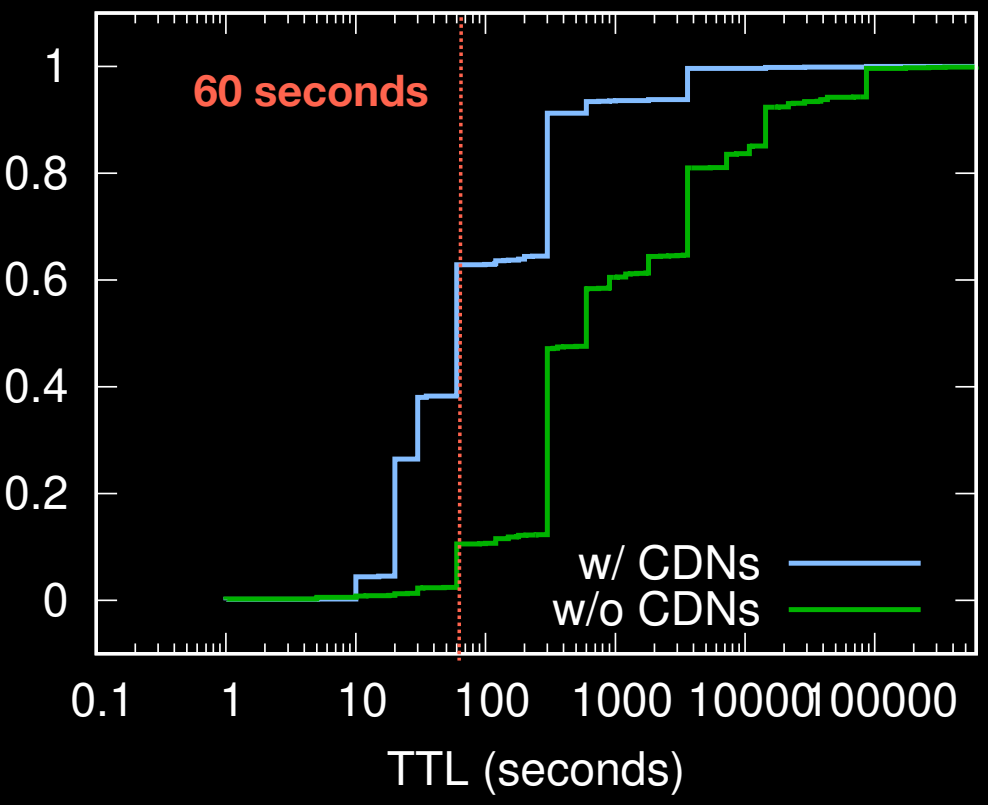
```
$ dig www.reddit.com
...
;; ANSWER SECTION:
www.reddit.com.          3600      IN  CNAME   reddit.map.fastly.net.
reddit.map.fastly.net    60           IN  A              151.101.1.140
```

Case-Study of CDNs



VIRGINIA TECH

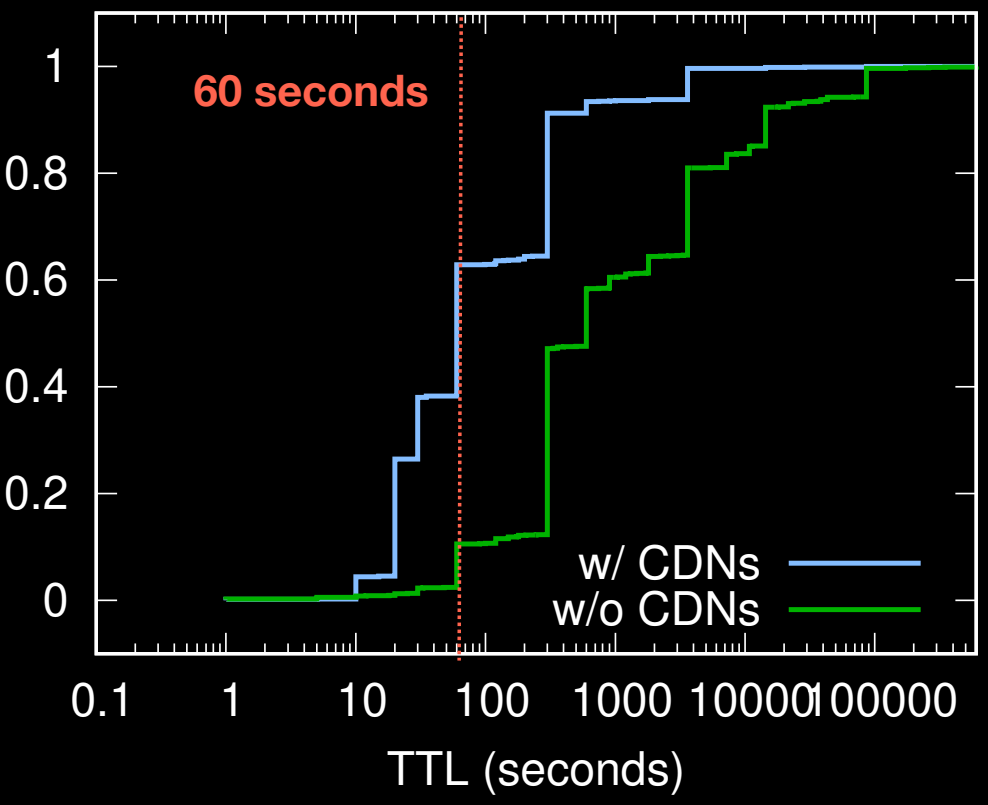
Case-Study of CDNs



CDN	TTL	Domains
Akamai	20	12,247 (99.9%)
Cloudflare	300	10,736 (98.7%)
Cloudfront	60	9,642 (99.8%)
Fastly	30	6,237 (98.6%)
Google	300	2,759 (98.8%)
Azure	10	2,536 (47.0%)
Netlify	20	1,531 (98.2%)
XCDN	20	99 (47.8%)
Alibaba	150	91 (58.7%)
CDN77	15	68 (91.8%)

VIRGINIA TECH

Case-Study of CDNs

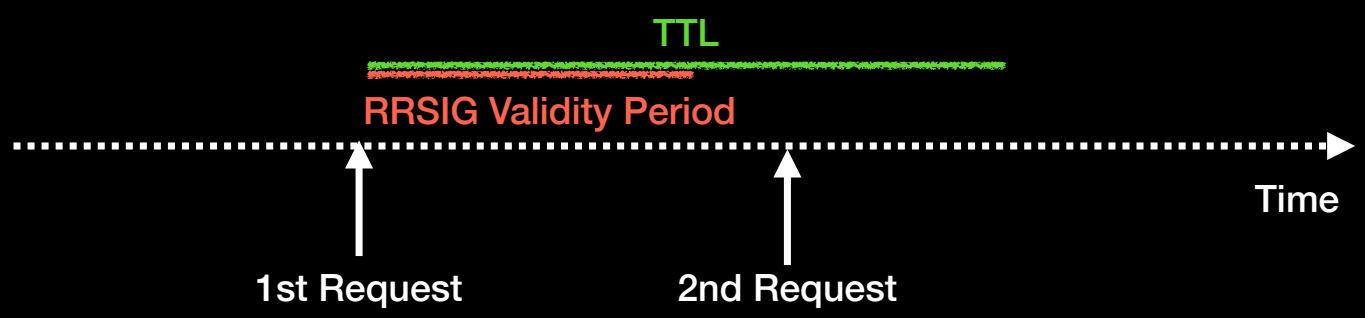


CDN	TTL	Domains
Akamai	20	12,247 (99.9%)
Cloudflare	300	10,736 (98.7%)
Cloudfront	60	9,642 (99.8%)
Fastly	30	6,237 (98.6%)
Google	300	2,759 (98.8%)
Azure	10	2,536 (47.0%)
Netlify	20	1,531 (98.2%)
XCDN	20	99 (47.8%)
Alibaba	150	91 (58.7%)
CDN77	15	68 (91.8%)

VIRGINIA TECH

TTL Violation in DNSSEC

- Background
  - DNSSEC Signature carries inception and expiration date
  - Resolvers must evict DNS responses where RRSIGs are expired from the cahce even if their TTL is not expired yet
- Our experiment setting
  - TTL to 60 minutes for A records, but the signature expires in 30 minutes



VIRGINIA TECH

TTL Violation in DNSSEC

- Background
  - DNSSEC Signature carries inception and expiration date
  - Resolvers must evict DNS responses where RRSIGs are expired from the cahce even if their TTL is not expired yet

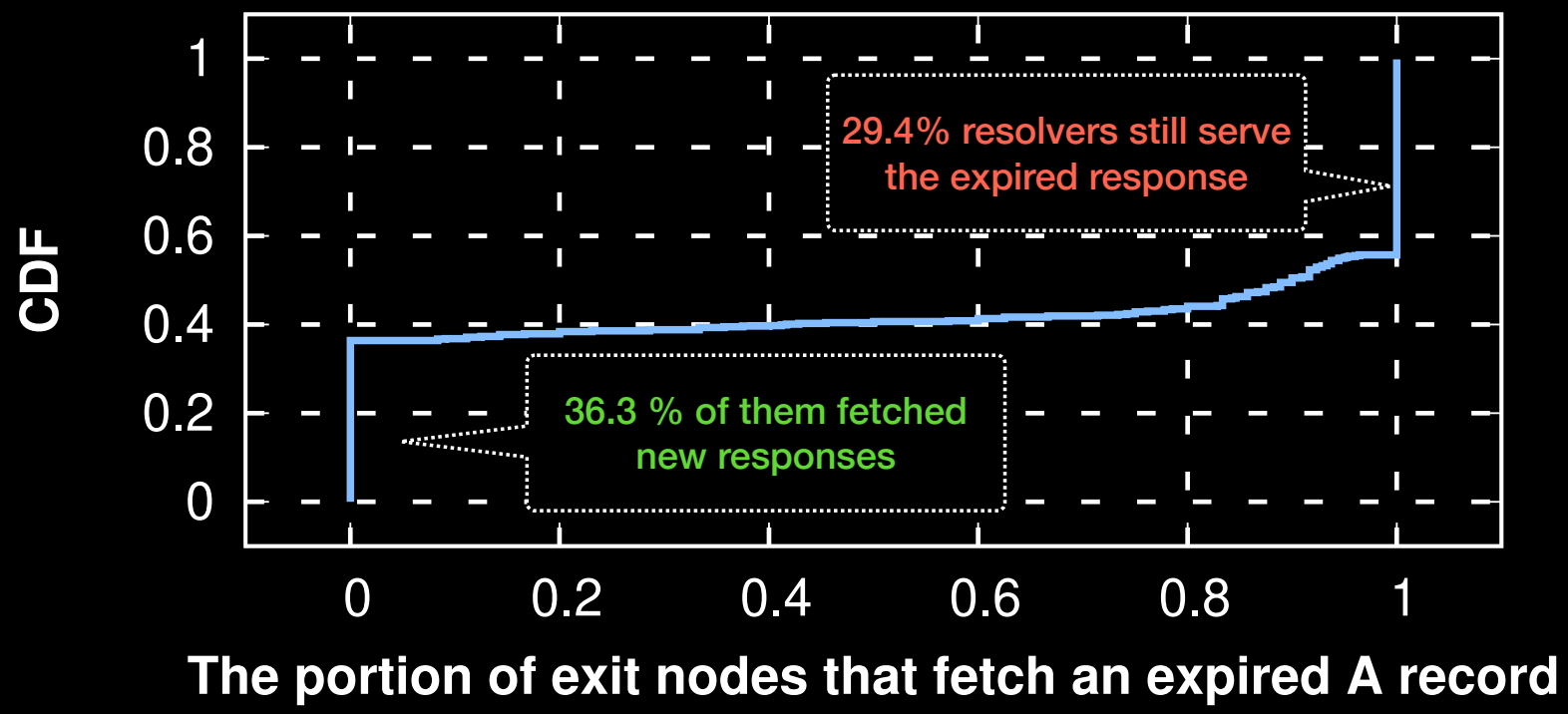
Pre-processing

	Filtering resolvers (# of exit nodes < 5)	DO Bit Enabled	Validates RRSIGs
exit nodes	91,637	75,684 (82.6%)	71,242 (94%)	6,001 (8.4%)
DNS resolvers	12,679	5,274 (38.5%)	4,917 (93.2%)	646 (13.1%)

93.2% of resolvers seem to support DNSSEC,
but only 13.1% validates the DNSSEC response

VIRGINIA TECH

Results



VIRGINIA TECH

Limitation and Discussion

- Can’t measure a multi-layer distributed caching infrastructure
  - Can only measure the backend caching DNS resolvers because we can only monitor the incoming DNS requests to the authoritative server.
  - Thus, we focused the only resolvers that we can measure at least from five different exit nodes
- Datasets and source codes are
  - https://ttl-violation-study.github.io

Questions