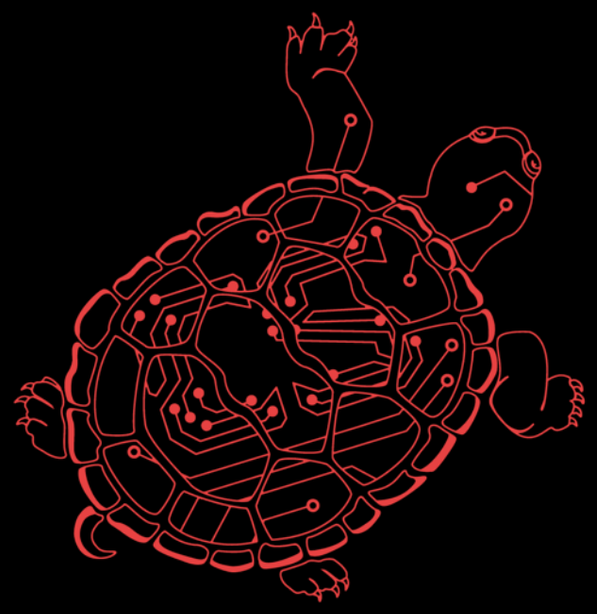
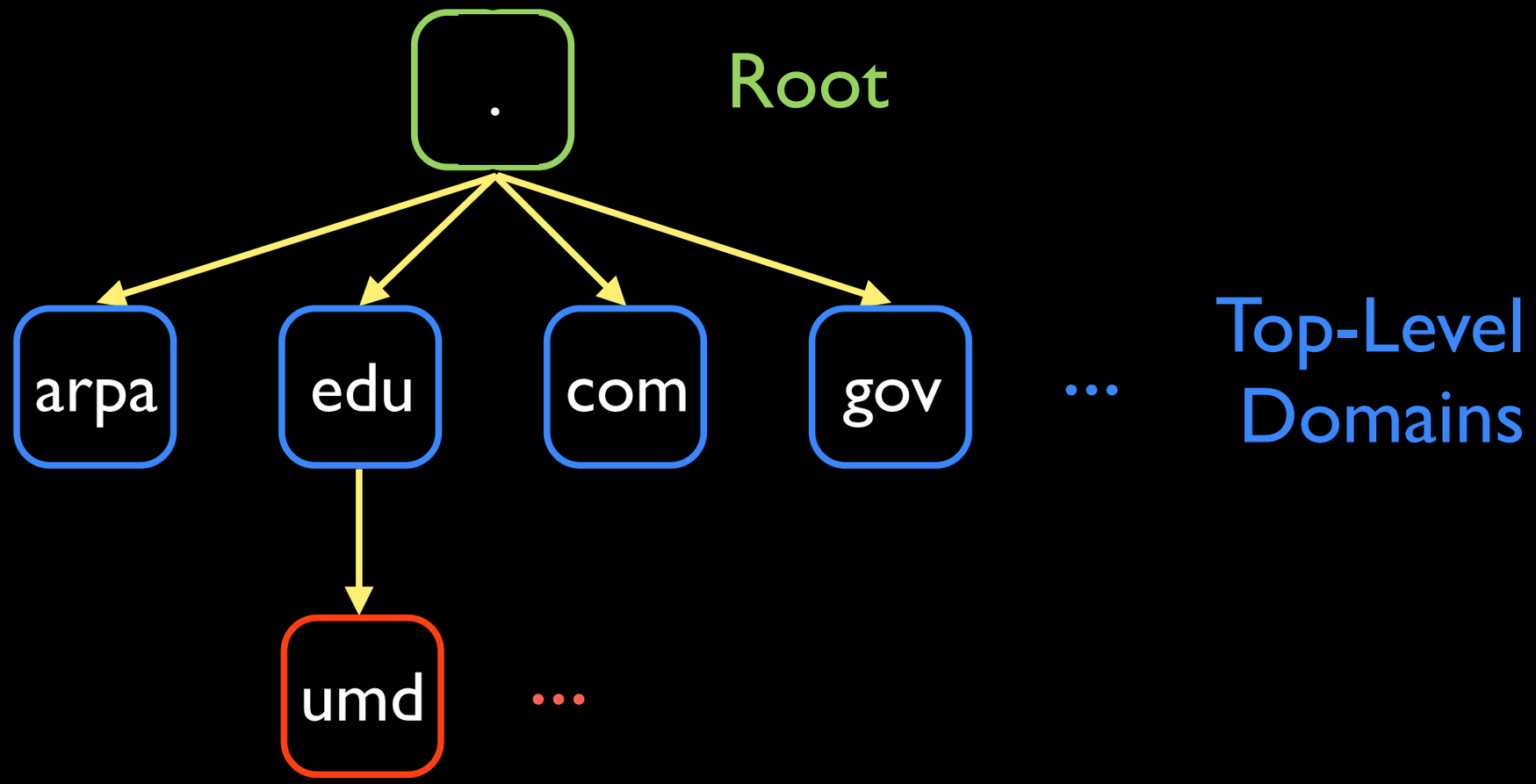
D-mystifying the D-Root Address Change

Matthew Lentz, Dave Levin, Jason Castonguay,
Neil Spring, Bobby Bhattacharjee

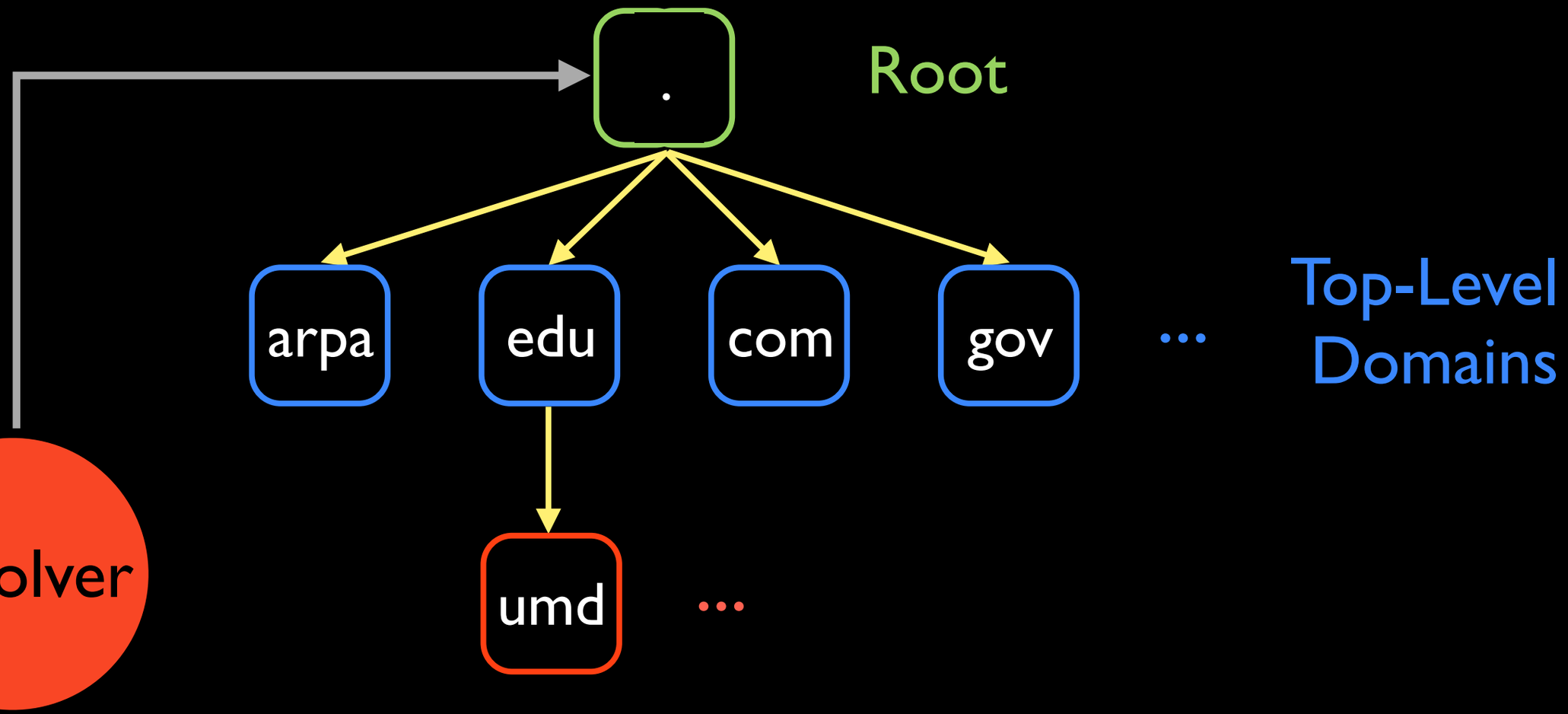
University of Maryland



Domain Name System (DNS)

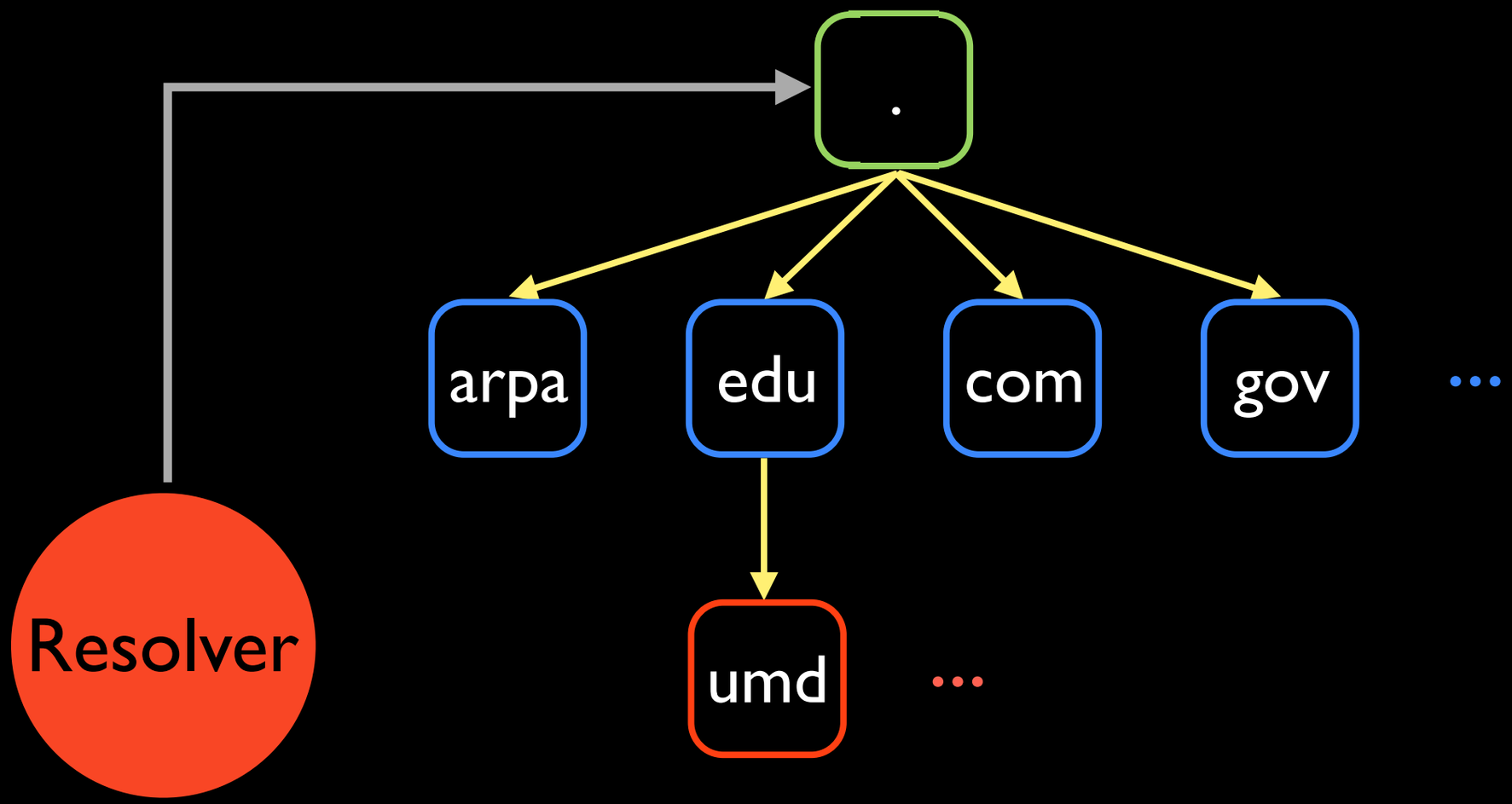


Domain Name System (DNS)



Q: www.umd.edu.

Domain Name System (DNS)



Q: www.umd.edu.

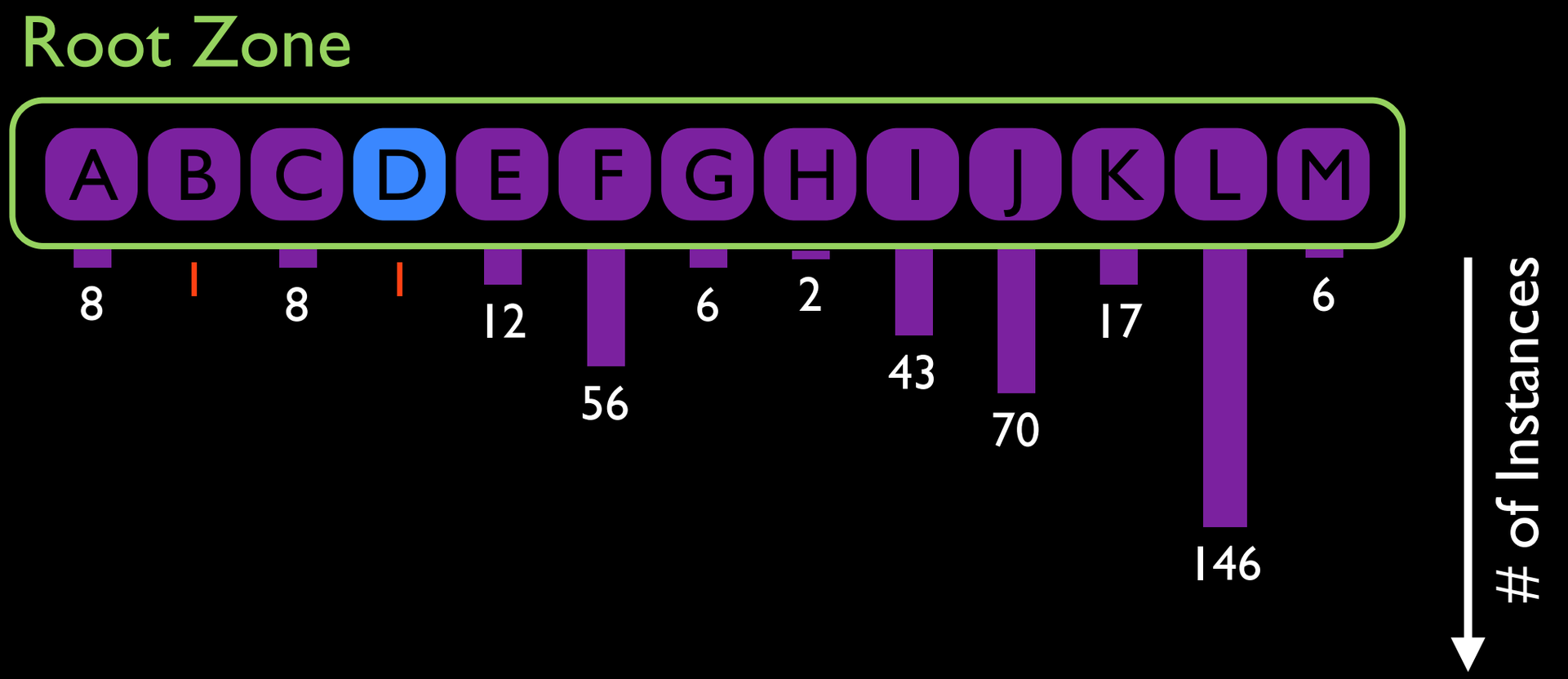
Domain Name System (DNS)

Root Zone

Root Server Anycasting

Root Zone

Root Server Anycasting



Anycasting enables global server replication

Root Server Anycasting

Anycasting enables global server replication

Root Server Anycasting

Anycasting enables global server replication

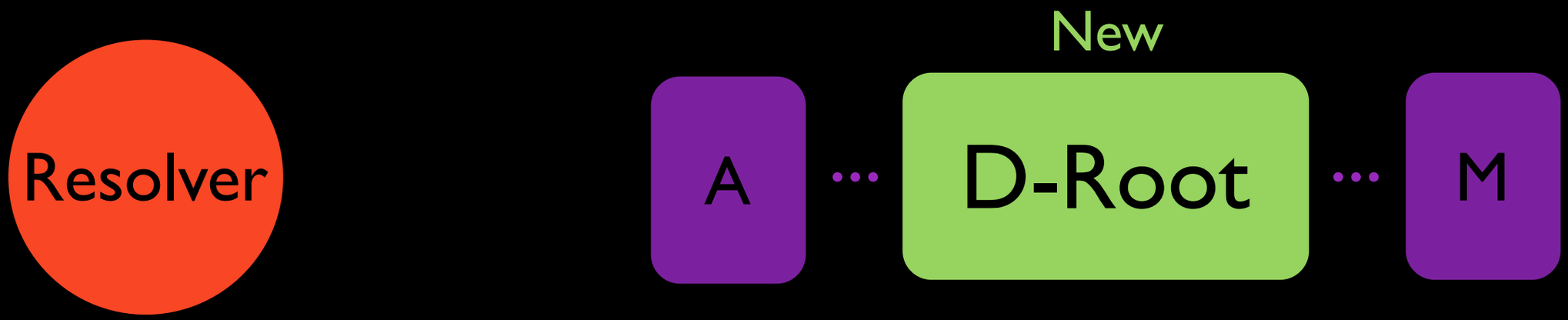
Root Server Anycasting

Anycasting enables global server replication

D-Root required IP address change

Root Server Anycasting

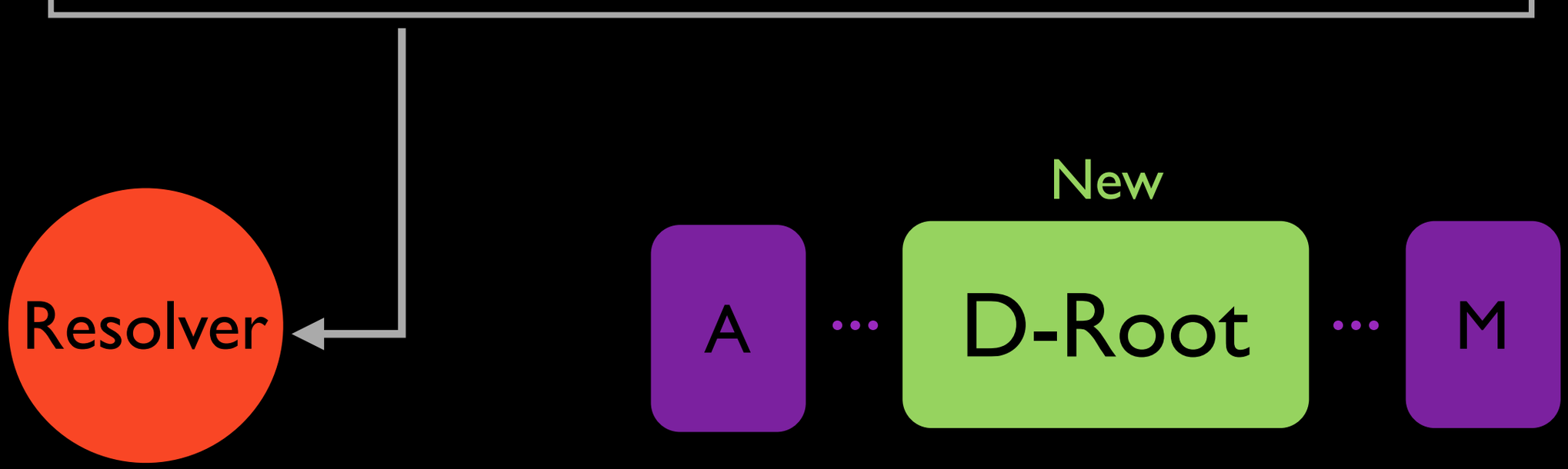
Updating Resolvers: Out-of-Band



Updating Resolvers: Out-of-Band

1. Obtain the root hints file

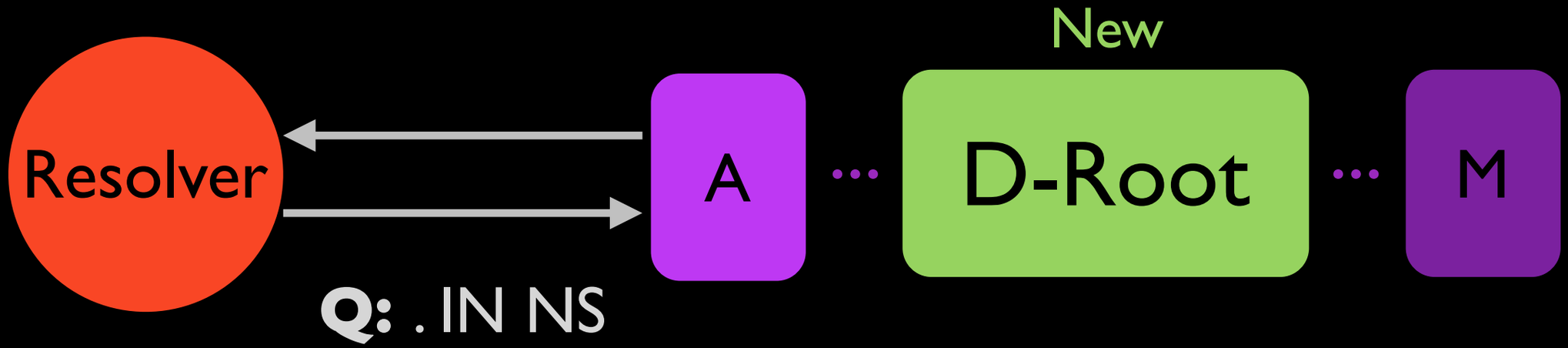
```
.                        3600000    NS      D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000    A       199.7.91.13
D.ROOT-SERVERS.NET.      3600000    AAAA    2001:500:2D::D
                                ...
```



Updating Resolvers: In-Band

2. Issue priming query to known root server

```
;; ANSWER SECTION:
.                       518400  IN    NS    d.root-servers.net.
;; ADDITIONAL SECTION:
d.root-servers.net.   3600000 IN    A     199.7.91.13
                                ...
```

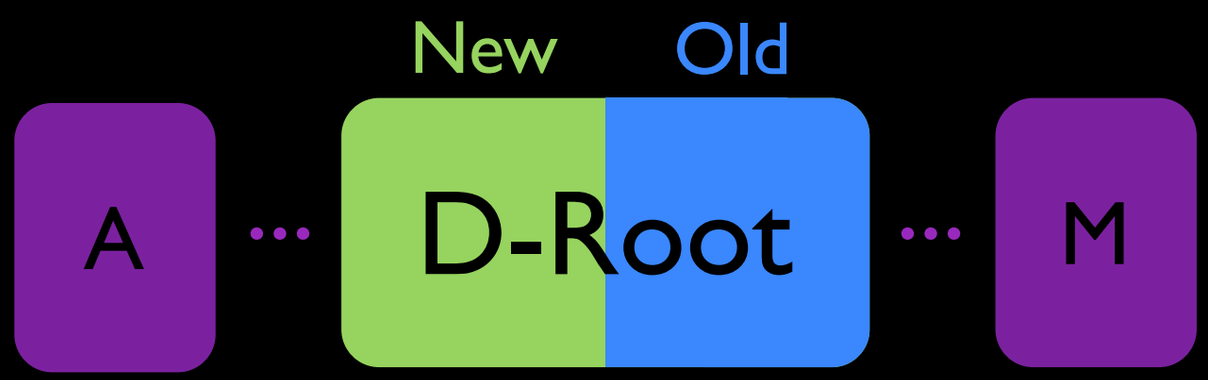


Updating Resolvers: In-Band

D-Root Address Change

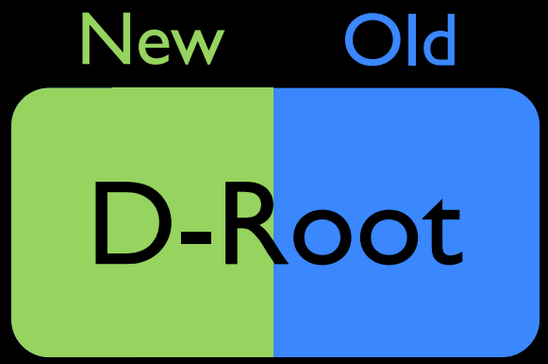
New

D-Root Address Change

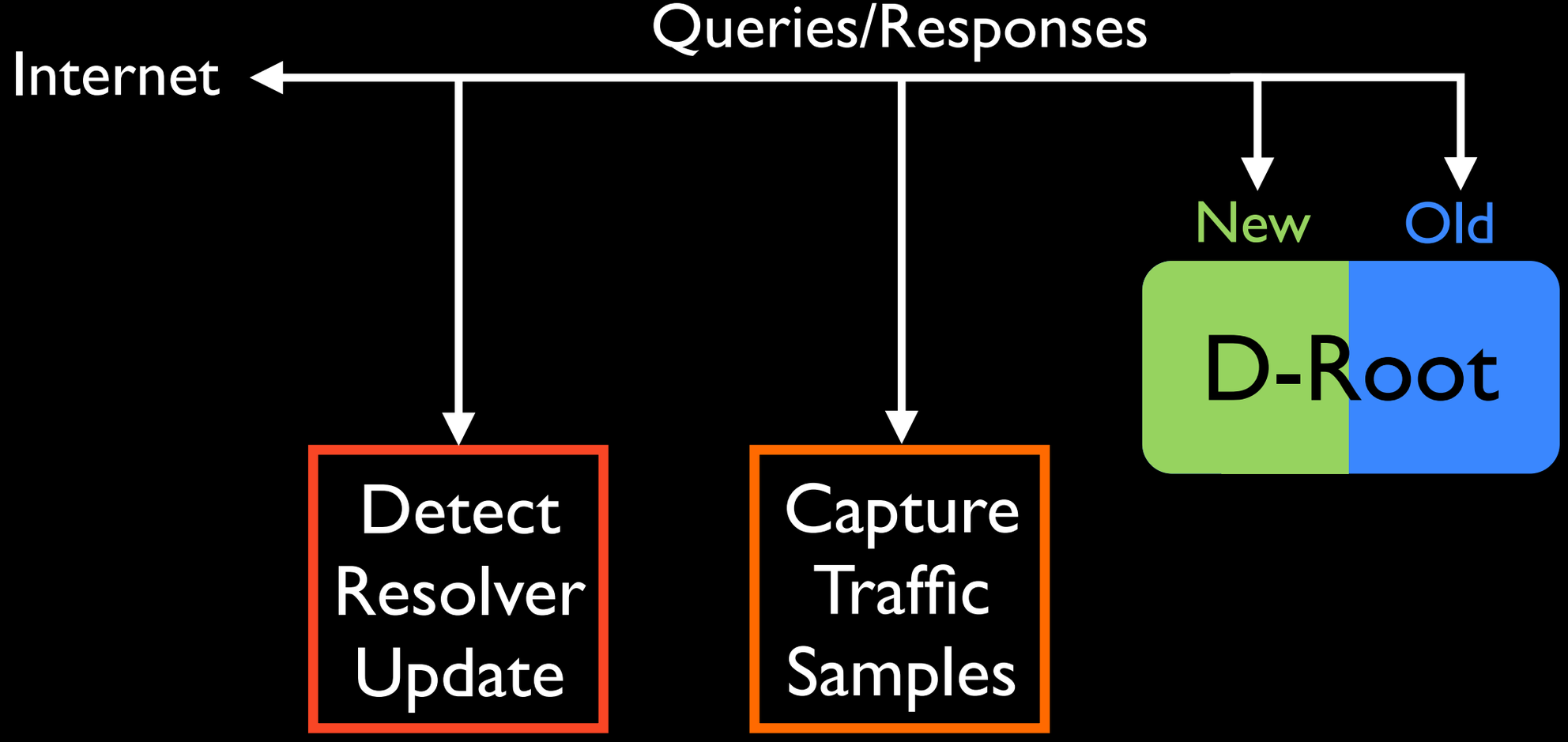


Serves queries on both addresses

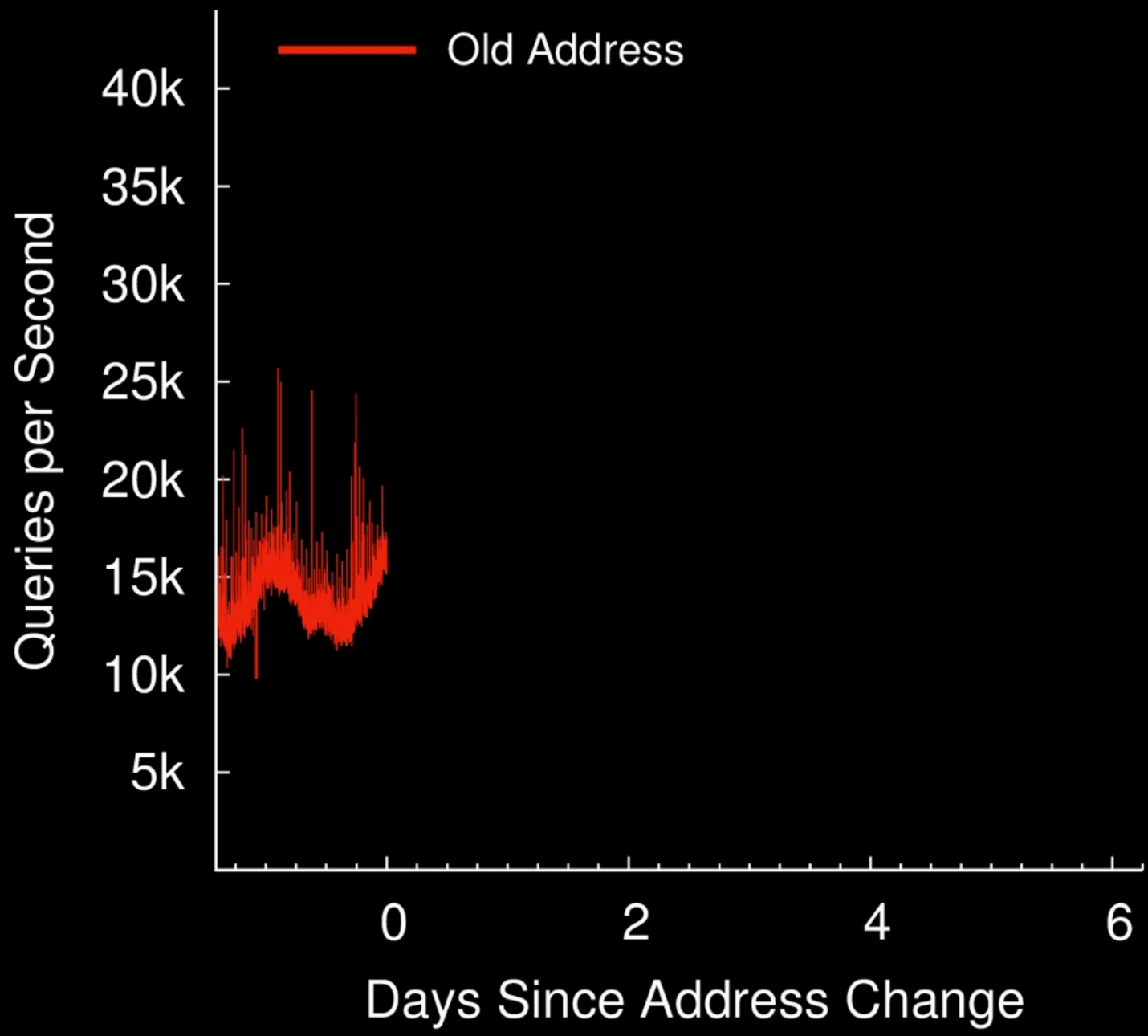
Experimental Setup



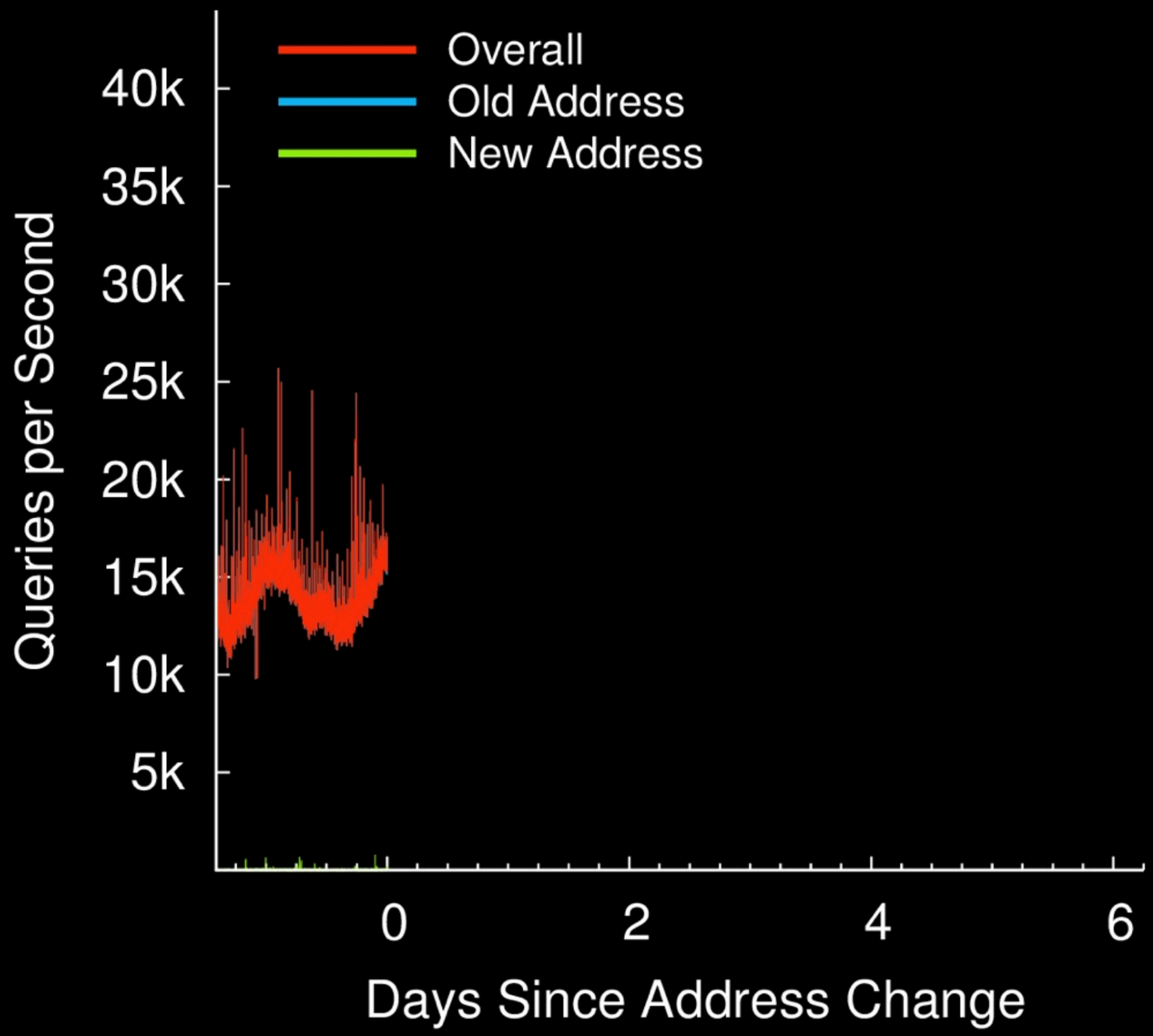
Experimental Setup



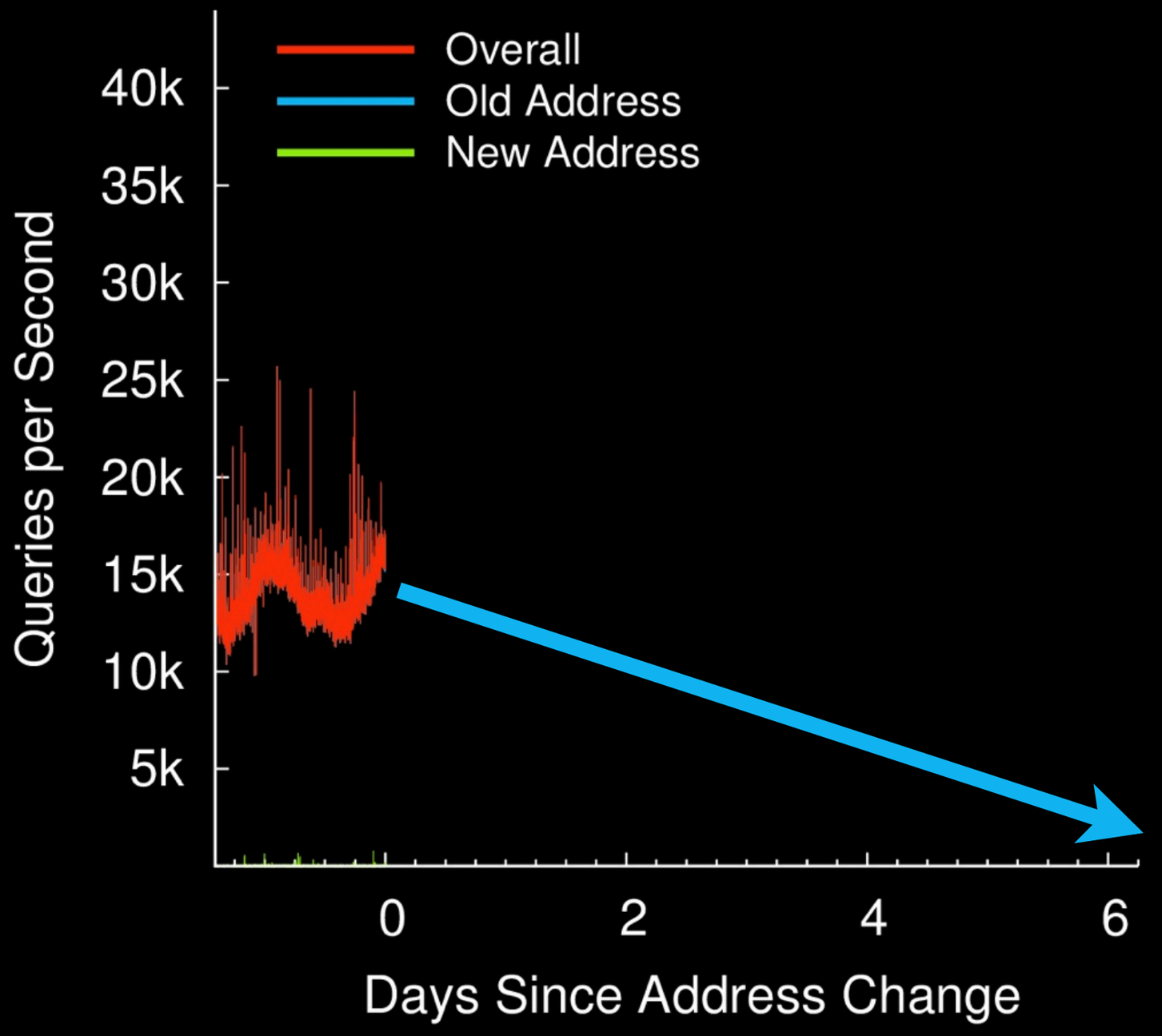
The Changeover



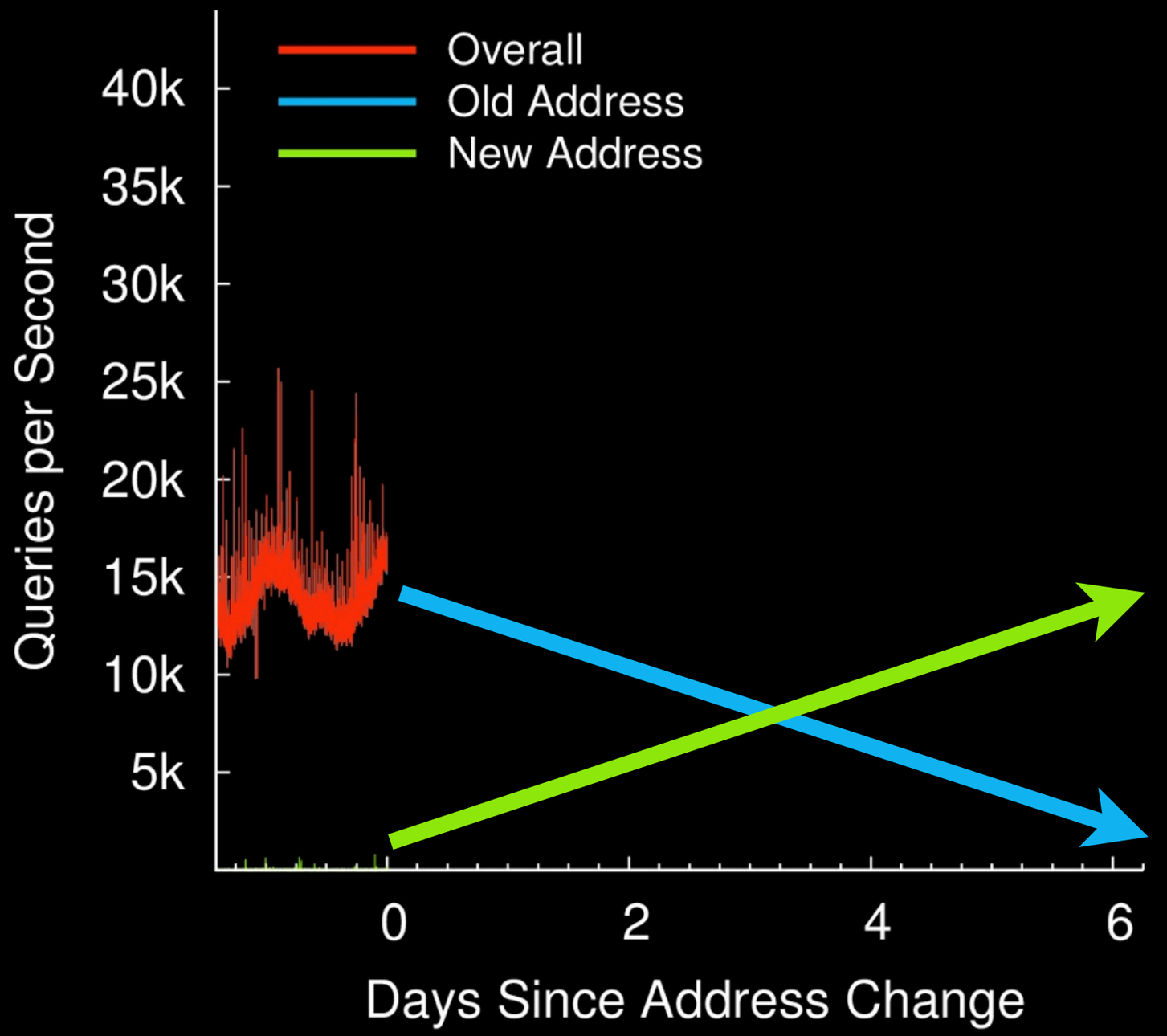
Expected Behavior



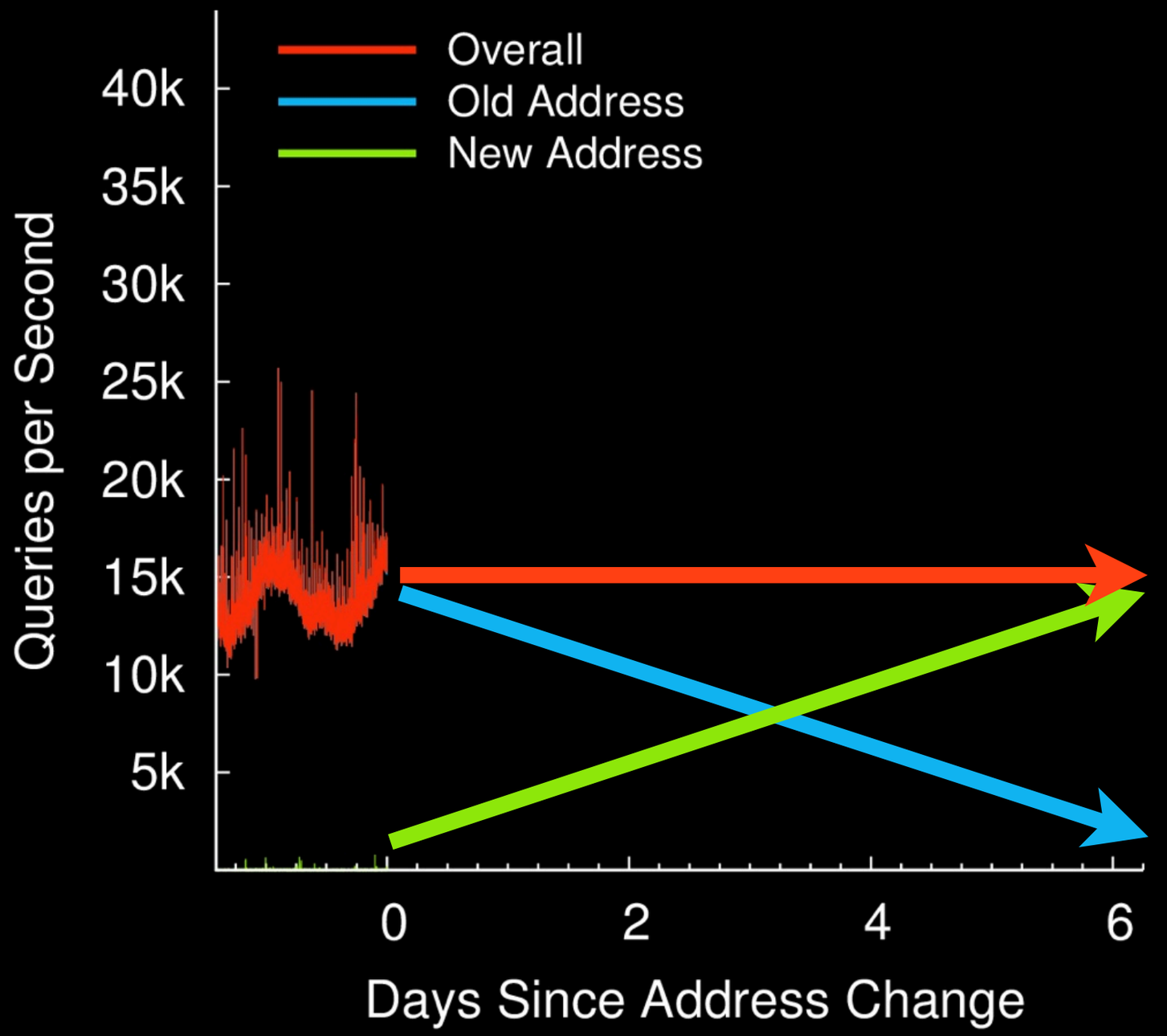
Expected Behavior



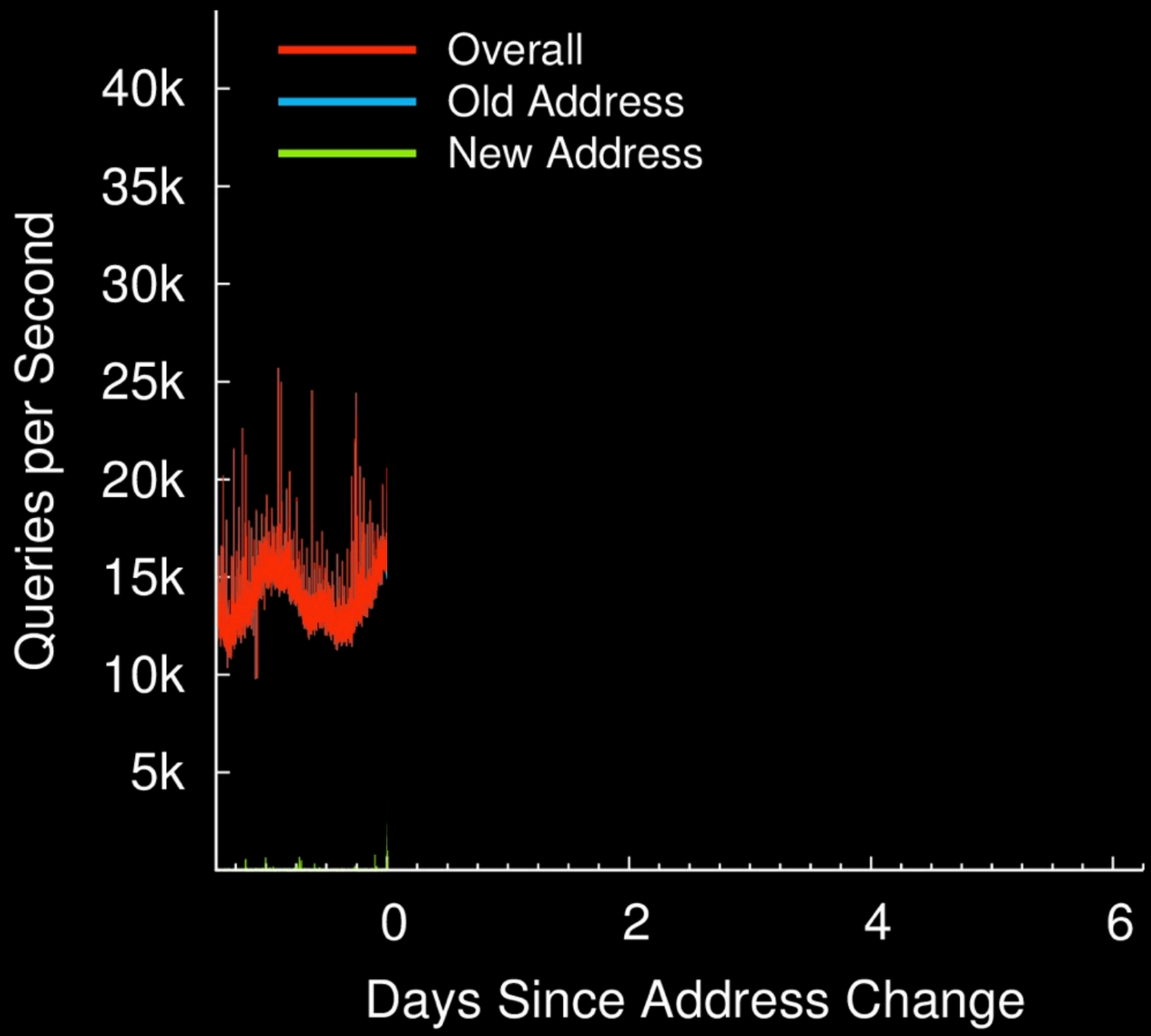
Expected Behavior



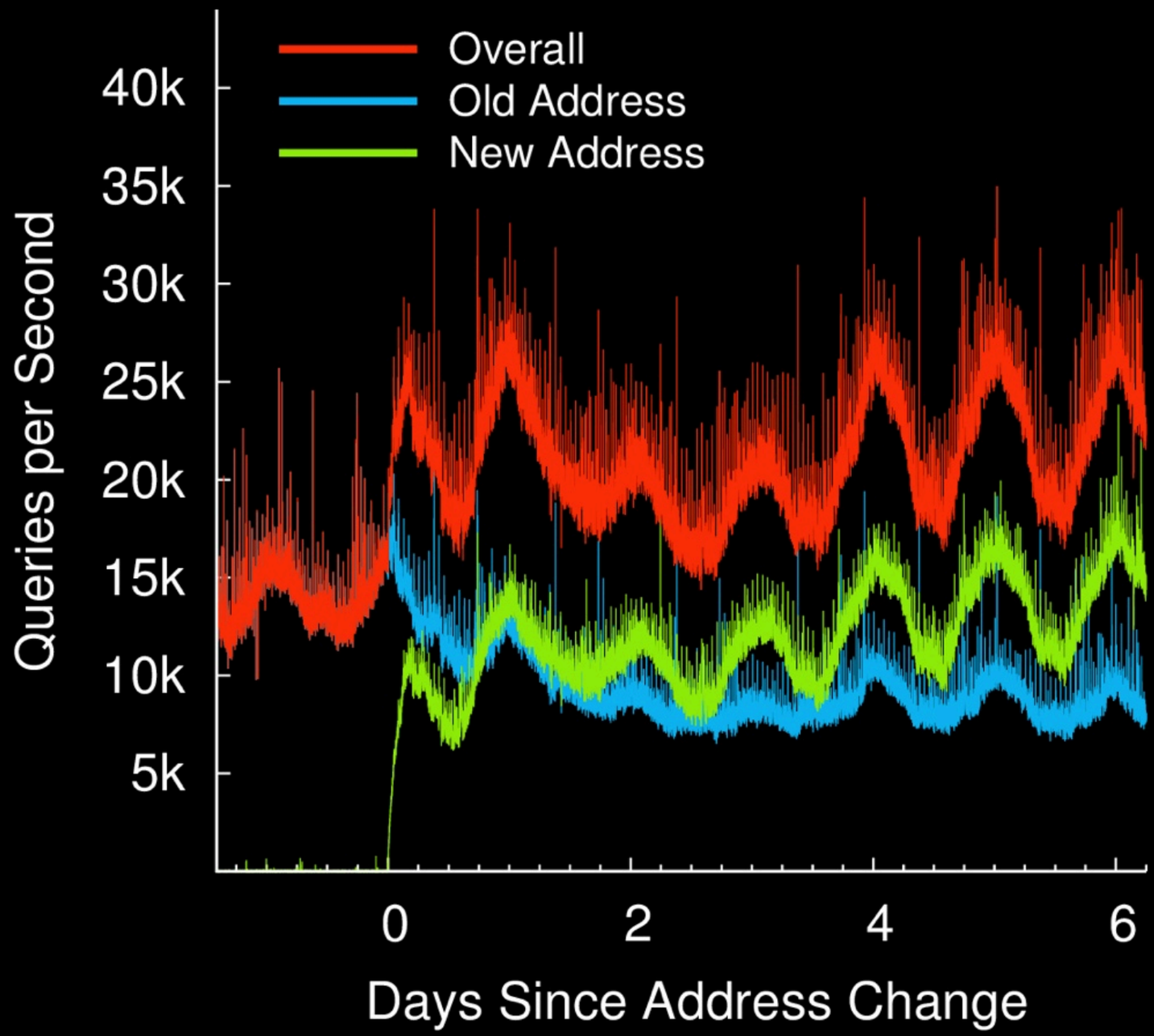
Expected Behavior



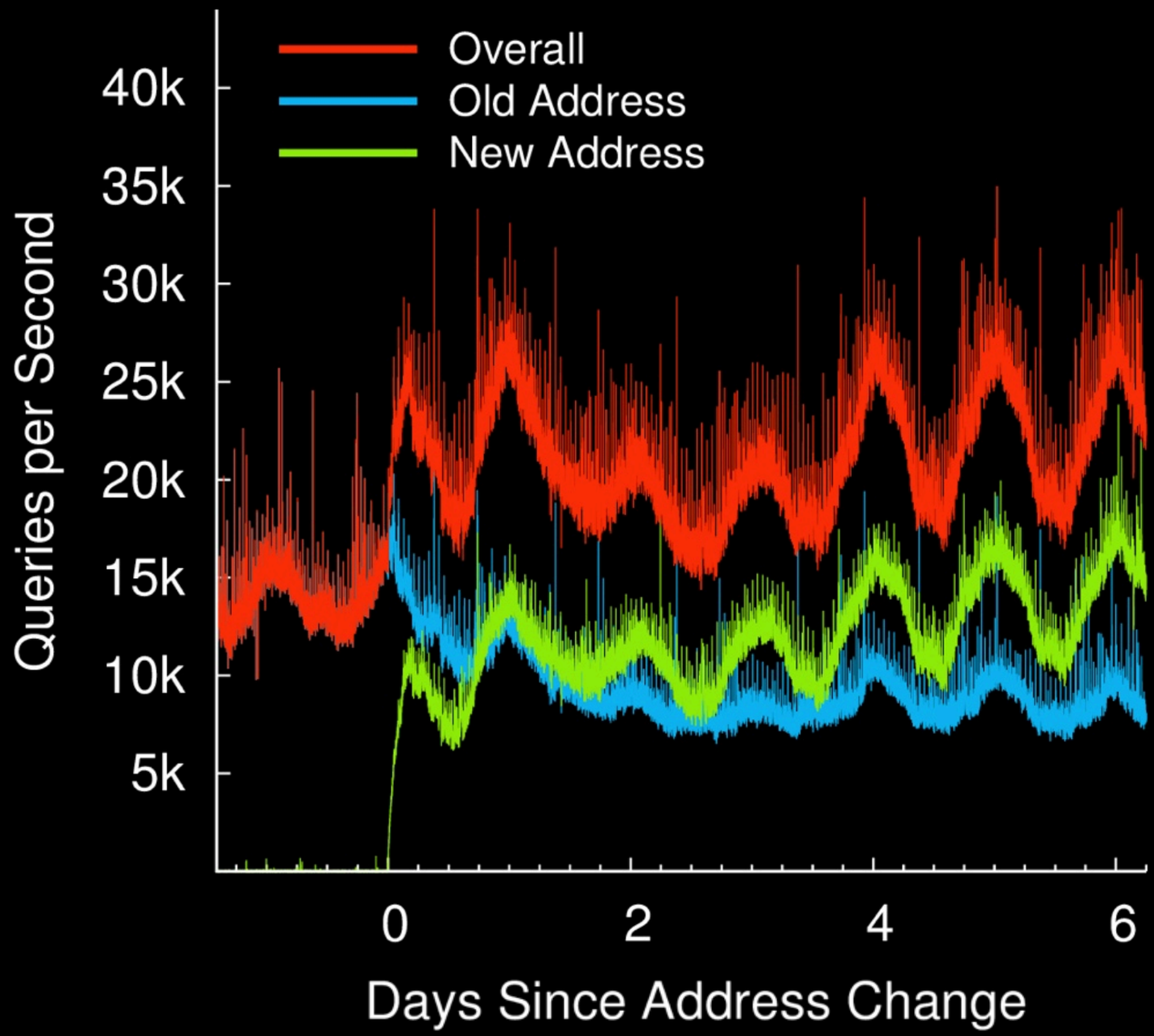
Reality


Overall
Old Address
New Address
40k
35k
30k
25k
20k
15k
10k
5k
Queries per Second
0
2
4
6
Days Since Address Change

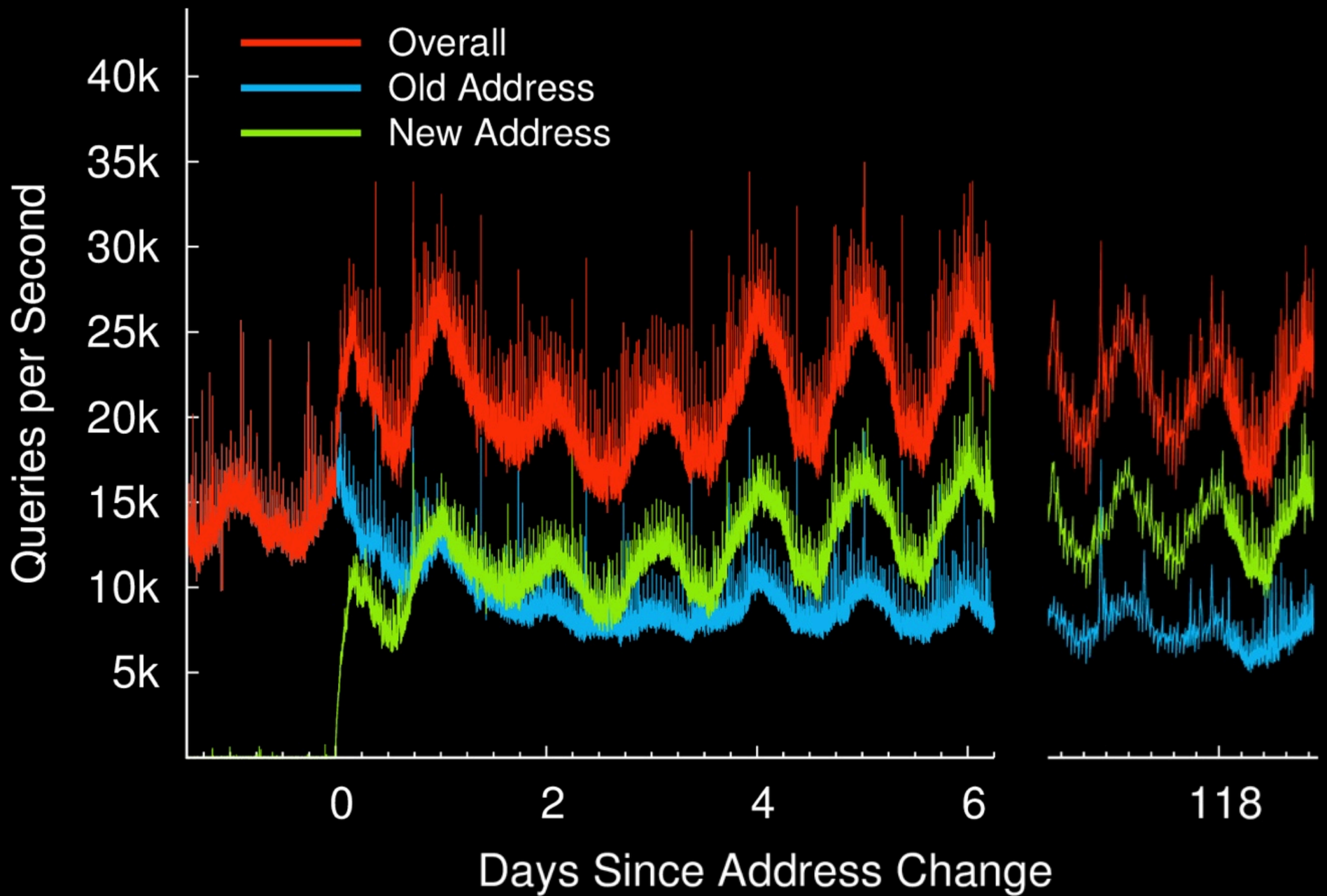
Reality


Overall
Old Address
New Address
40k
35k
30k
25k
20k
15k
10k
5k
Queries per Second
0
2
4
6
Days Since Address Change

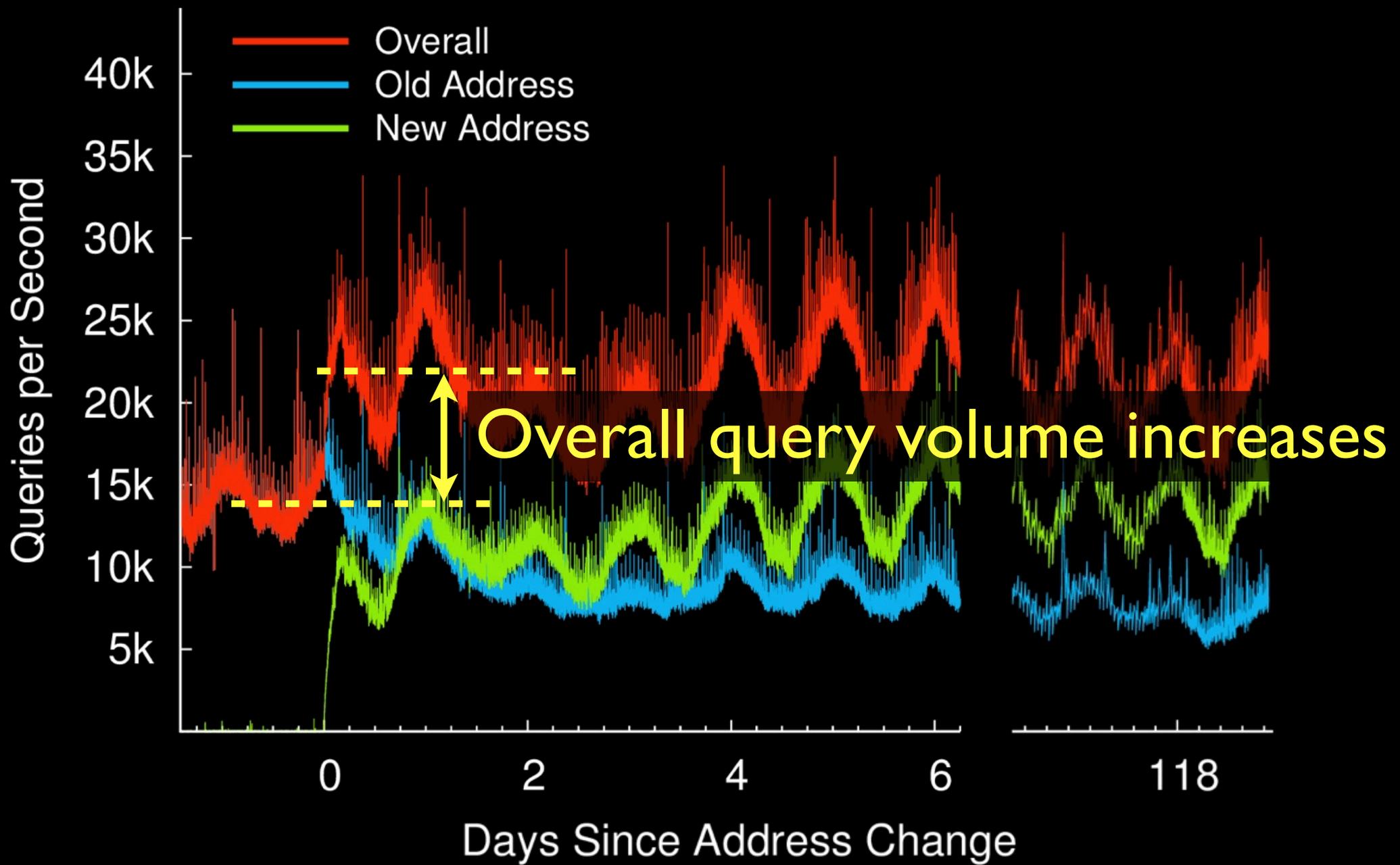
Reality


Overall
Old Address
New Address
40k
35k
30k
25k
20k
15k
10k
5k
Queries per Second
0
2
4
6
Days Since Address Change

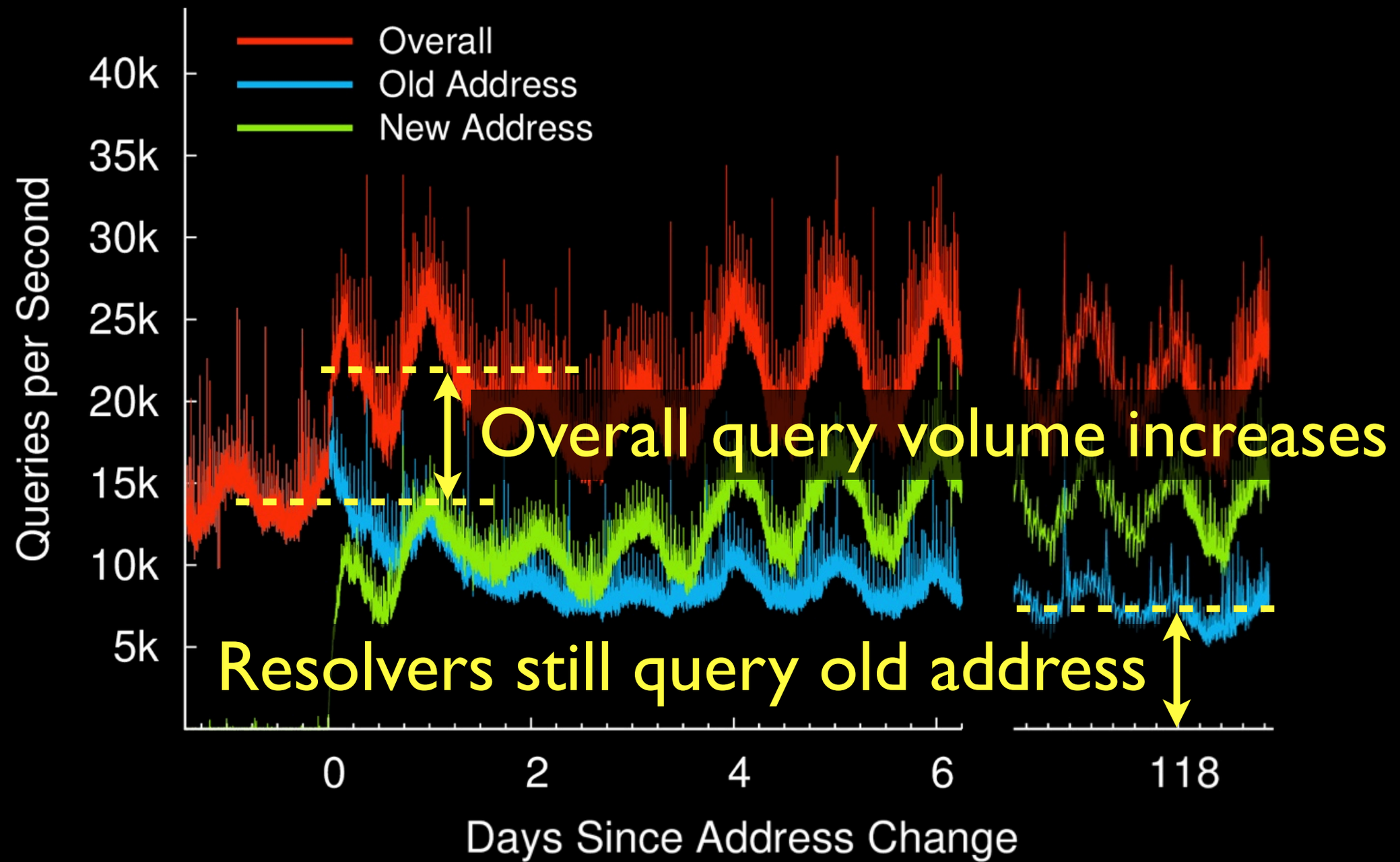
Reality


Overall
Old Address
New Address
40k
35k
30k
25k
20k
15k
10k
5k
Queries per Second
0
2
4
6
118
Days Since Address Change

Reality


Overall
Old Address
New Address
40k
35k
30k
25k
20k
15k
10k
5k
Queries per Second
Overall query volume increases
0
2
4
6
118
Days Since Address Change

Reality


Overall
Old Address
New Address
40k
35k
30k
25k
20k
15k
10k
5k
Queries per Second
Overall query volume increases
Resolvers still query old address
0
2
4
6
118
Days Since Address Change

Reality

Overall query volume increases

Resolvers still query old address

Reality

Overall query volume increases

Resolvers still query old address

Reality

Overall query volume increases

Resolvers still query old address

Queries to old address fail less often

Why ... ?

Overall query volume increases

Resolvers still query old address

Queries to old address fail less often

Why ... ?

Overall query volume increases

Resolvers still query old address

Queries to old address fail less often

Why does query volume increase?

New Resolvers

and/or

More Queries

Why does query volume increase?

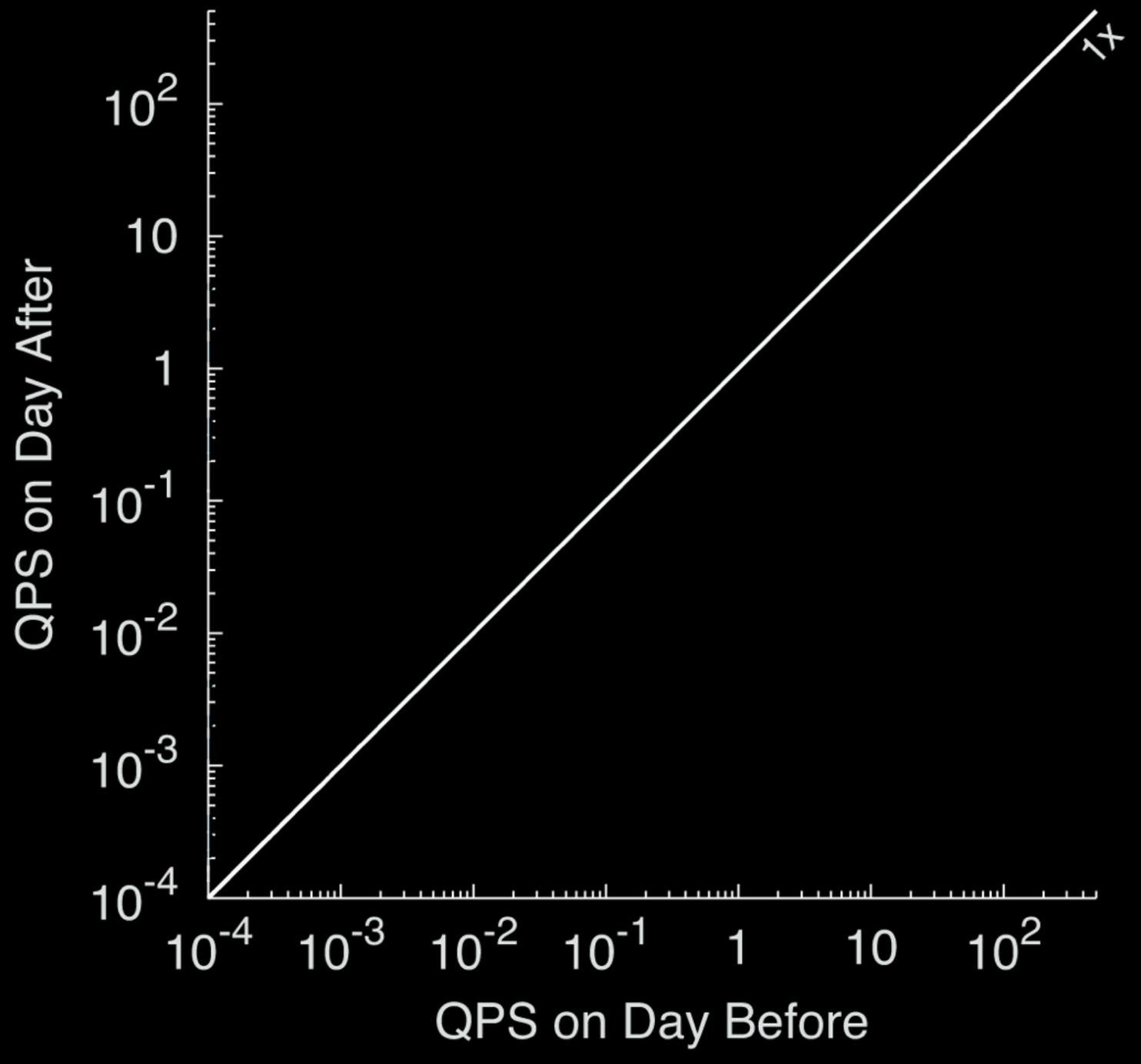
New Resolvers

and/or

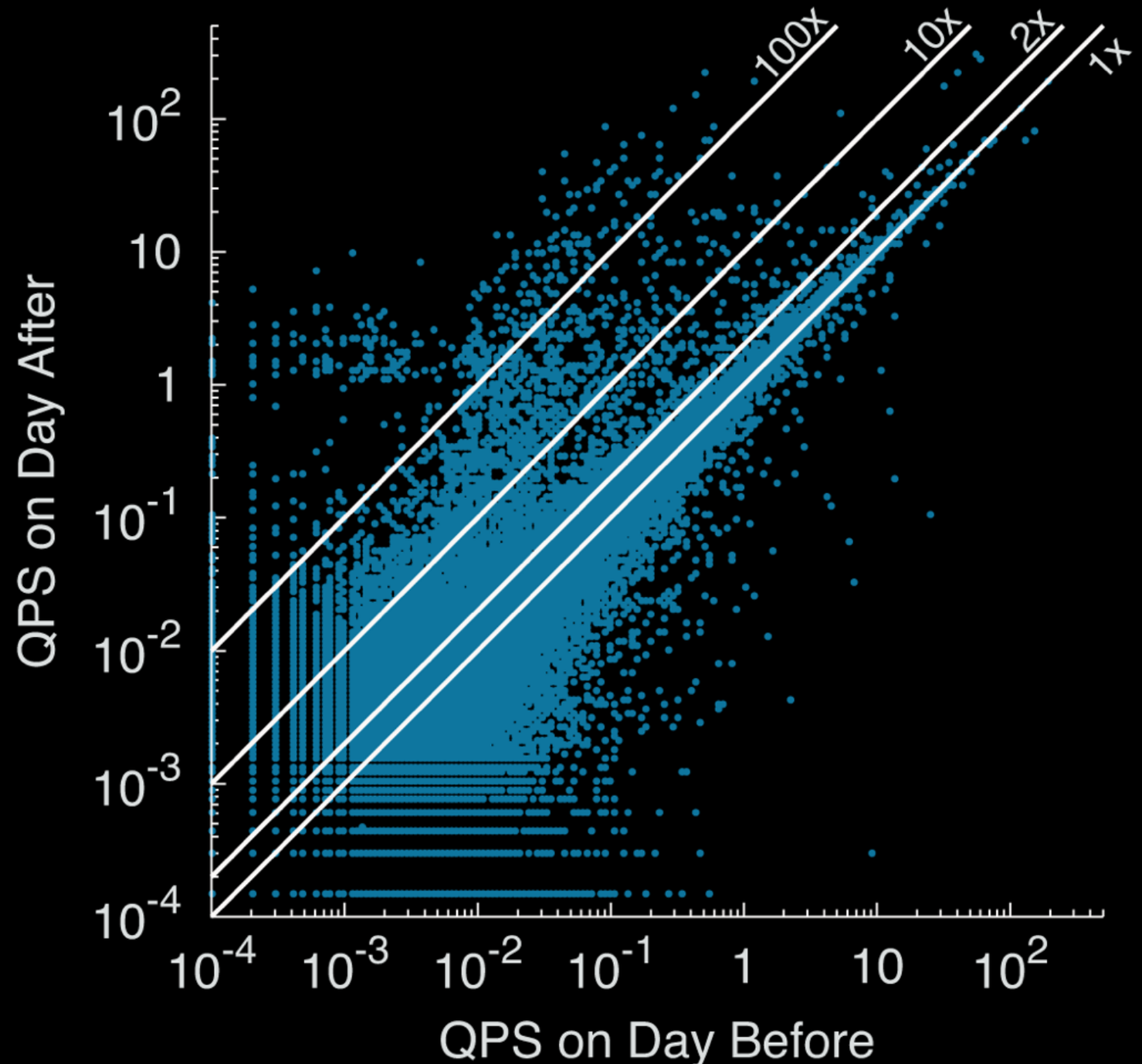
More Queries

Actually, unique resolvers decreased

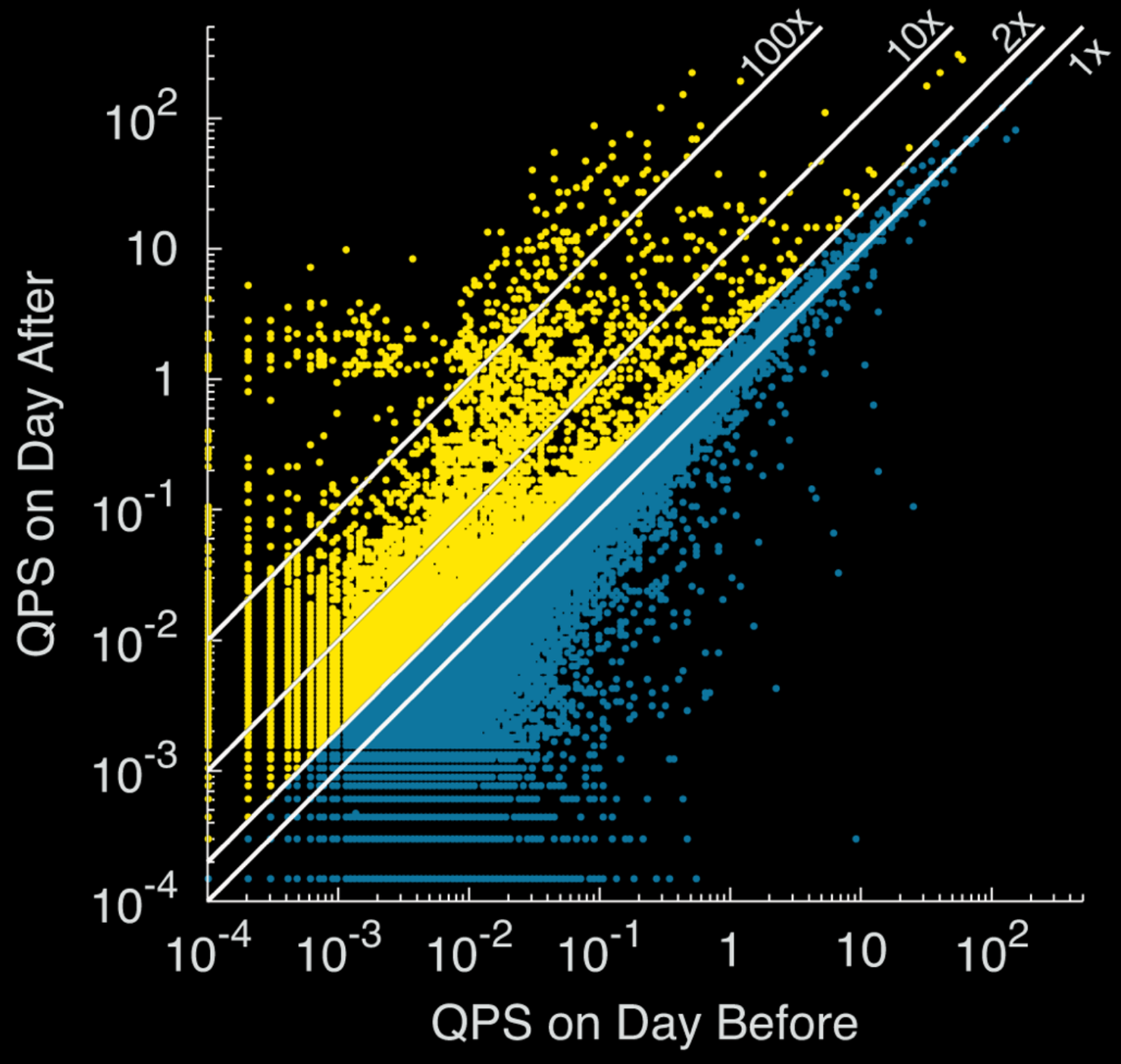
QPS - 24 Hours Before/After



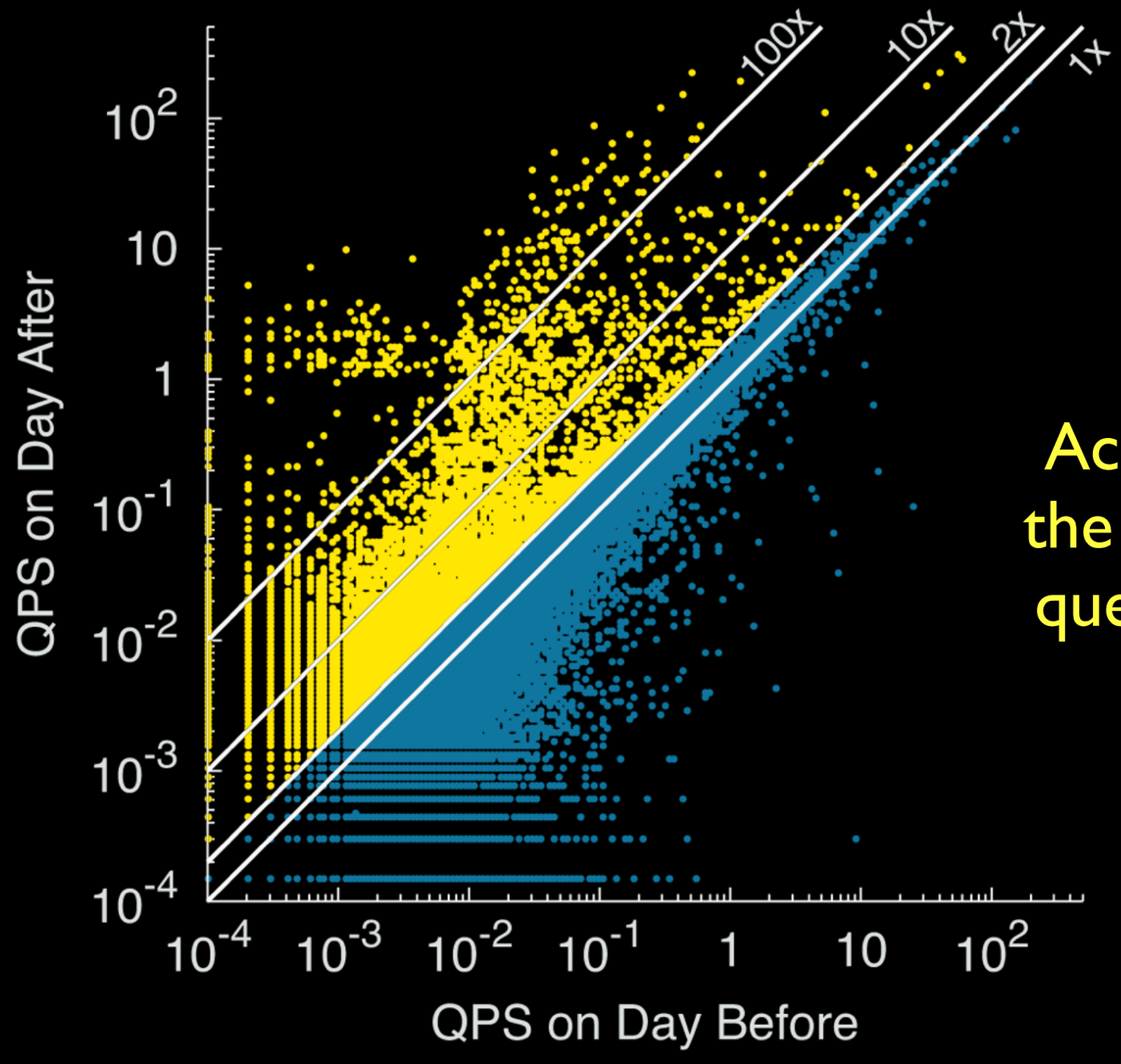
QPS - 24 Hours Before/After



Excitables


100x
10x
2x
1x
10^2
10
1
10^{-1}
10^{-2}
10^{-3}
10^{-4}
QPS on Day After
10^{-4}
10^{-3}
10^{-2}
10^{-1}
1
10
10^2
QPS on Day Before

Excitables



Accounts for the increase in query volume

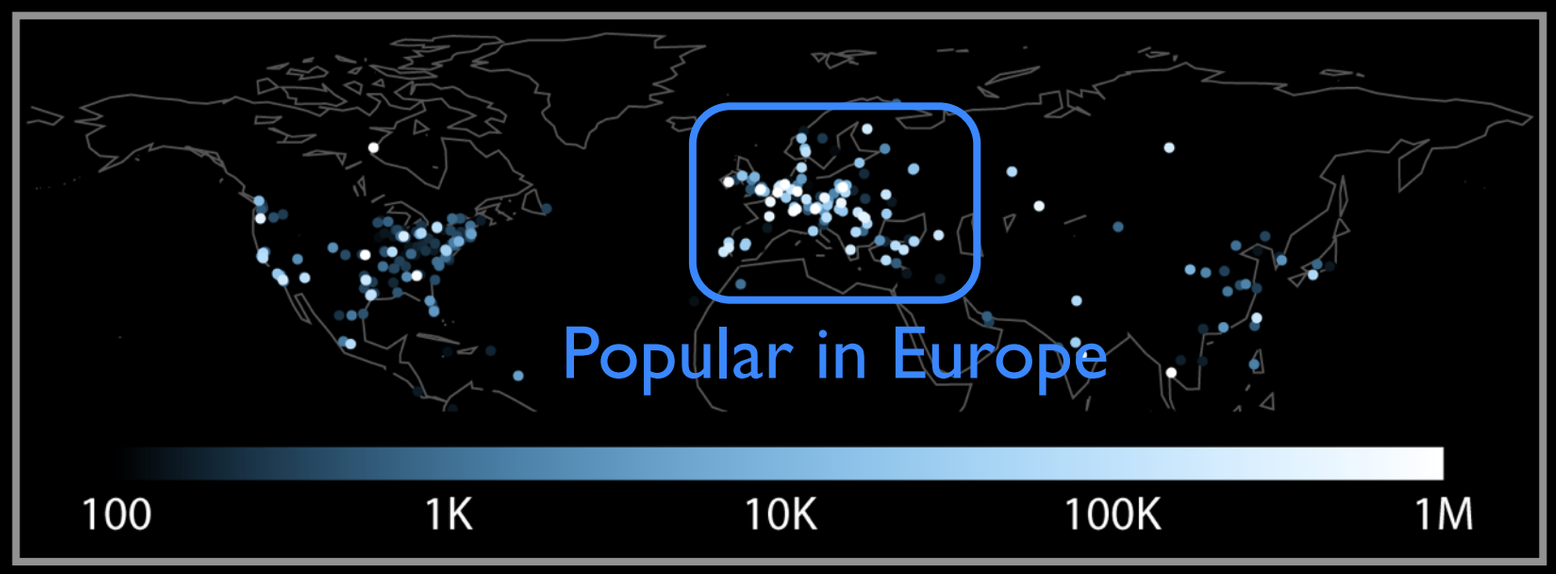
Excitables Explained by ... ?

Excitables Explained by ... ?

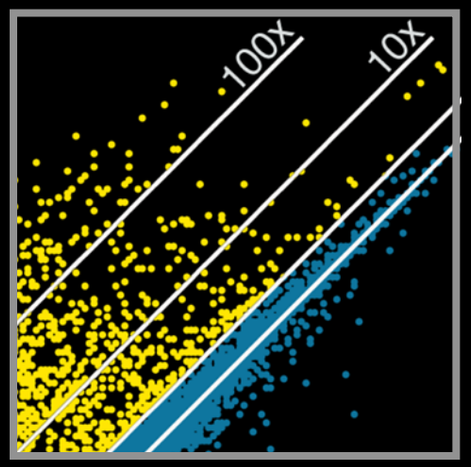
Couldn't
Fingerprint

Excitables Explained by ... ?

Couldn't
Fingerprint

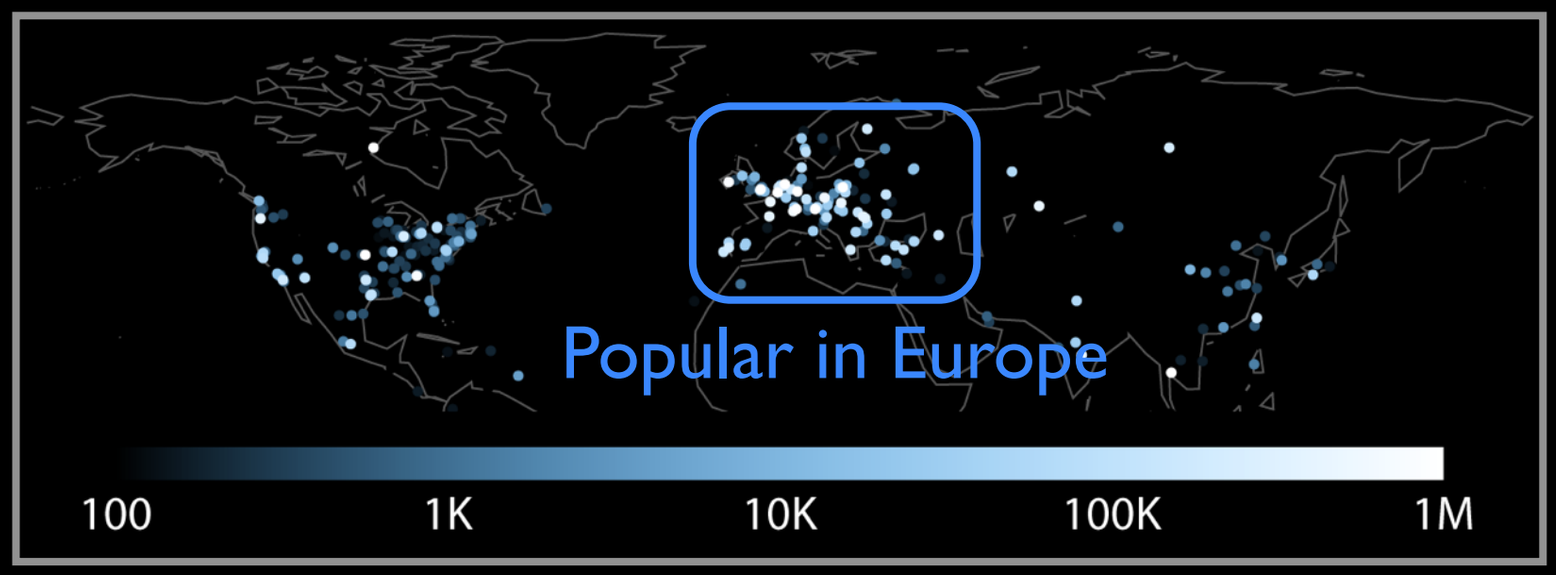


Excitables Explained by ... ?

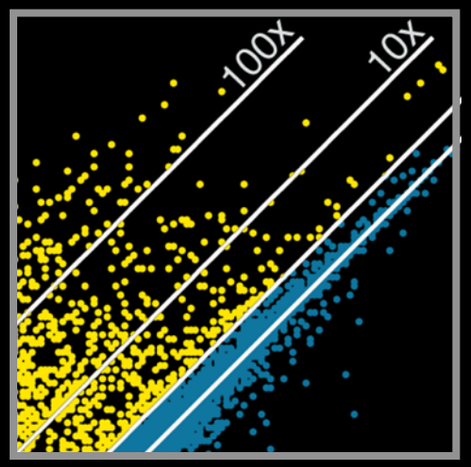


"Spike" Query Distribution

Couldn't Fingerprint

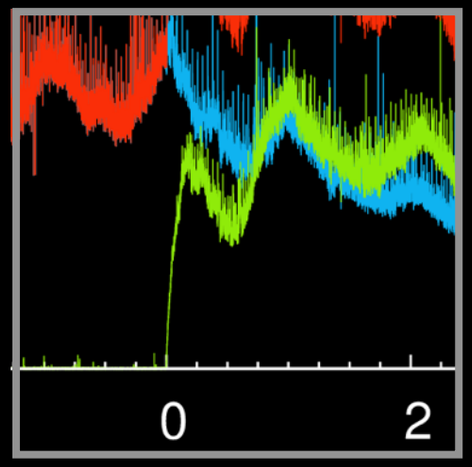


Excitables Explained by ... ?

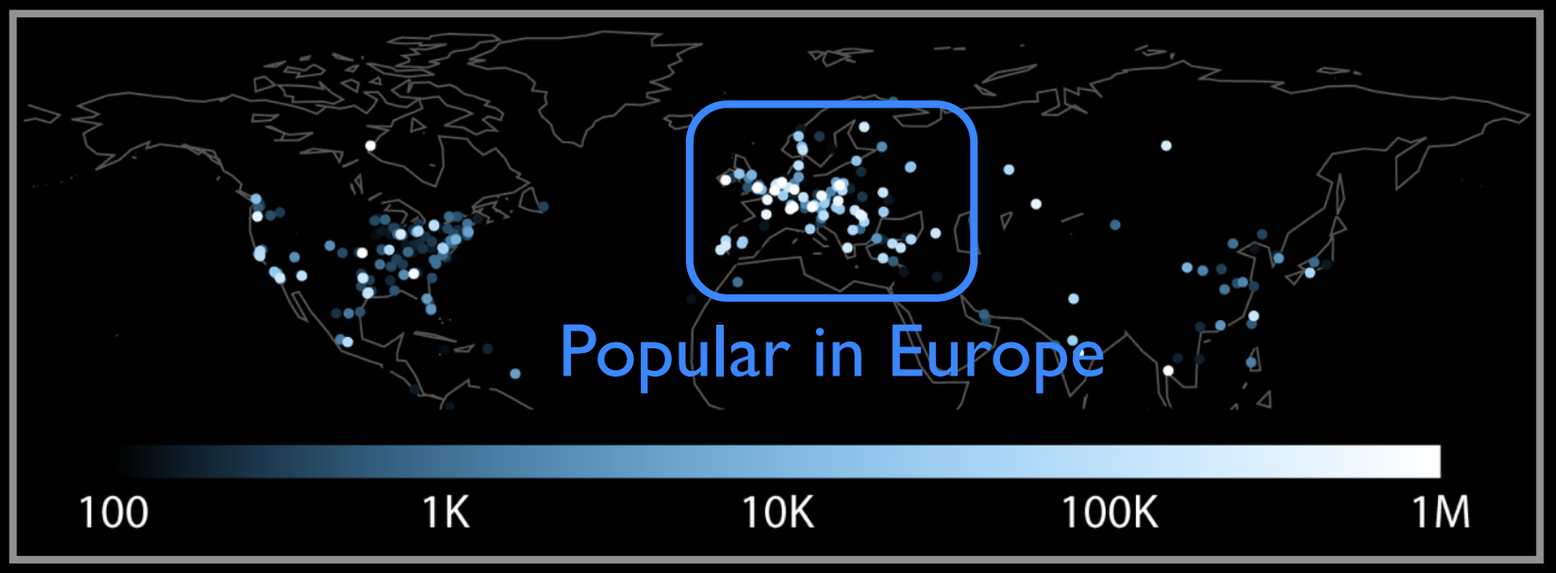


"Spike" Query Distribution

Couldn't Fingerprint



Frequently Re-Primes



Why ... ?

Overall query volume increases

Resolvers still query old address

Queries to old address fail less often

Why ... ?

Overall query volume increases

Excitables pointed to bug in PowerDNS

Resolvers still query old address

Queries to old address fail less often

Why ... ?

Overall query volume increases

Excitables pointed to bug in PowerDNS

Resolvers still query old address

Queries to old address fail less often

Who's still using the old address?

Expect most resolvers to update correctly

Who's still using the old address?

Expect most resolvers to update correctly

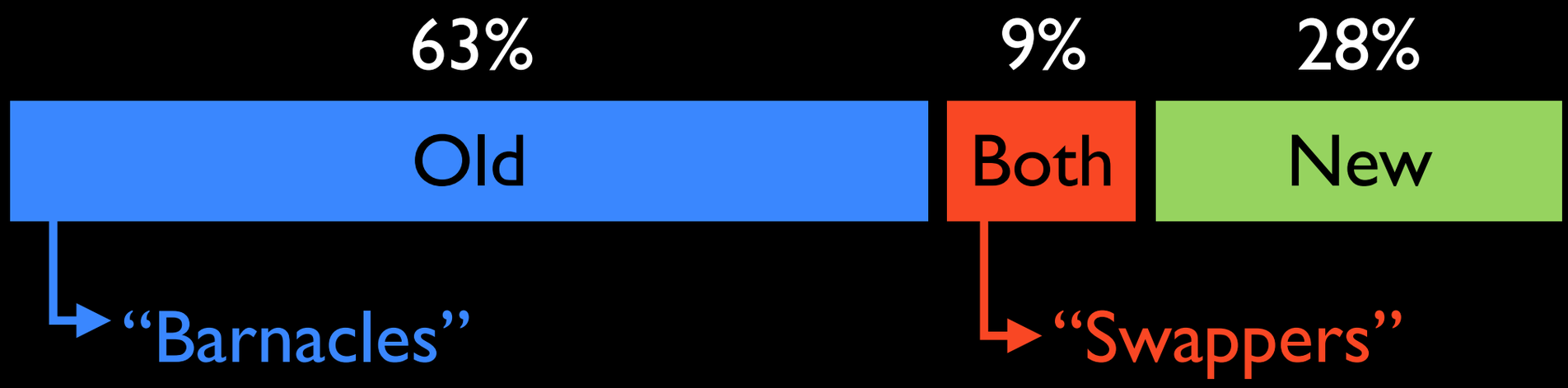
New

Who's still using the old address?

Expect most resolvers to update correctly

Who's still using the old address?

Expect most resolvers to update correctly



Barnacles: Feature Selection

kp8goqfsz2skj.sukaxdmziq
gfpb4fimbreso.qlbkgxsnue
...

210.33.31.50.bl.spamcop.net
85.180.105.46.zen.spamhaus.org
...

Barnacles: Feature Selection

kp8goqfsz2skj.sukaxdmziq
gfpb4fimbreso.qlbkgxsnue
...

Random

Always Fail

210.33.31.50.bl.spamcop.net
85.180.105.46.zen.spamhaus.org
...

Barnacles: Feature Selection

kp8goqfsz2skj.sukaxdmziq
gfpb4fimbreso.qlbkgxsnue
...

Random

Always Fail

210.33.31.50.bl.spamcop.net
85.180.105.46.zen.spamhaus.org
...

DNSBLs

Always Succeed

Barnacles: Feature Selection

kp8goqfsz2skj.sukaxdmziq
gfpb4fimbreso.qlbkgxsnue
...

Random

Always Fail

210.33.31.50.bl.spamcop.net
85.180.105.46.zen.spamhaus.org
...

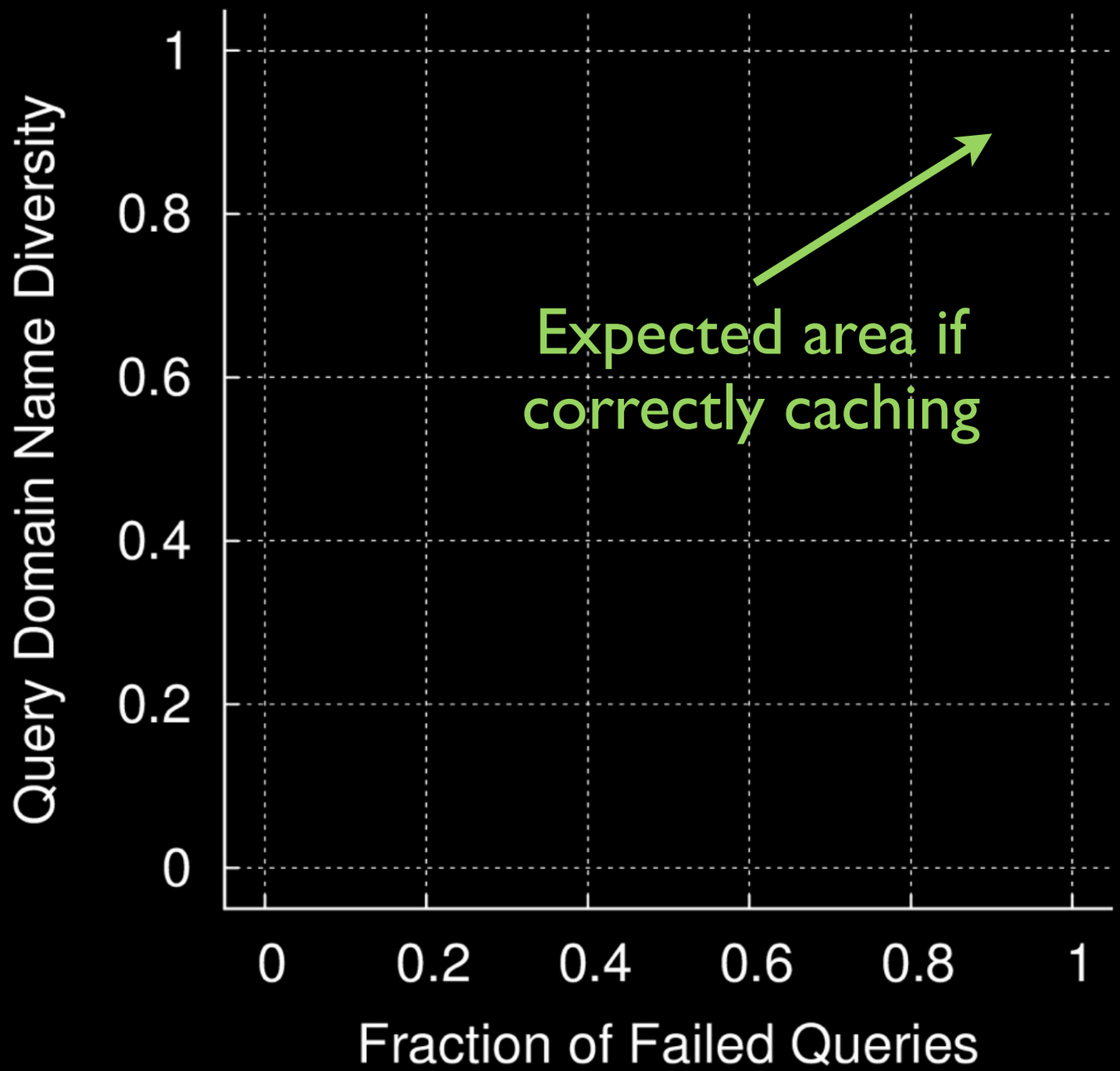
DNSBLs

Always Succeed

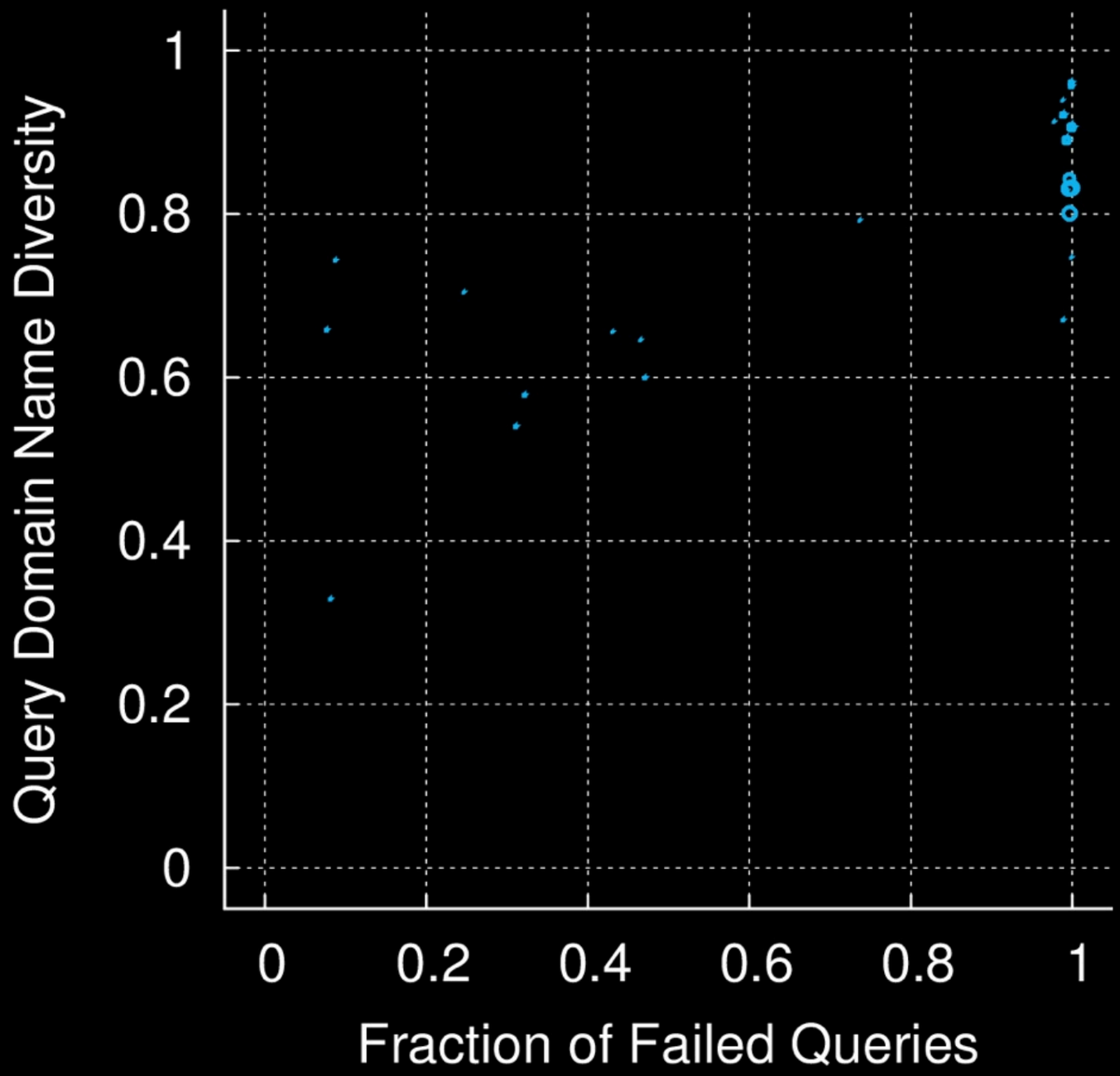
Query Diversity

Failure Rate

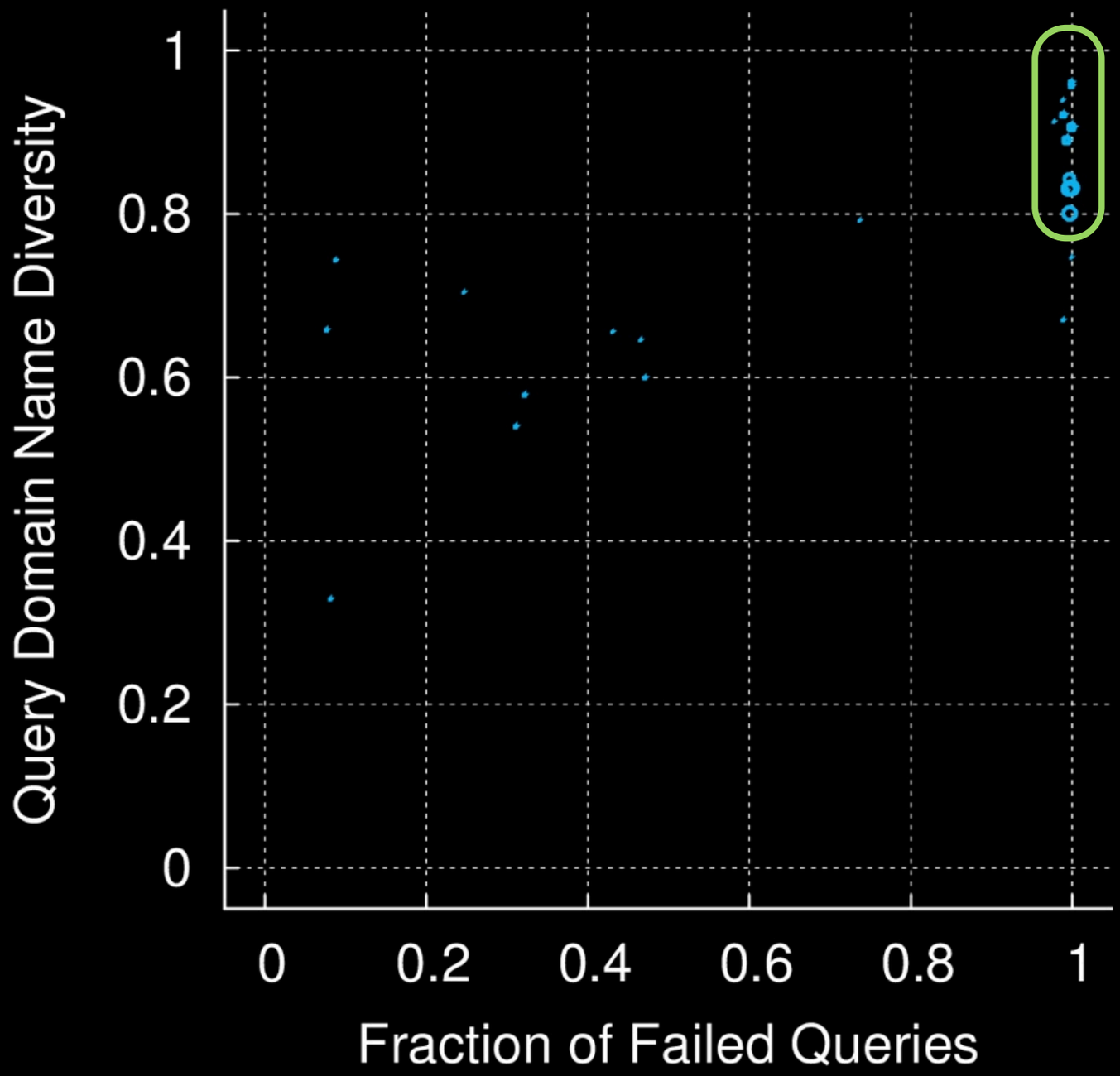
What should root servers expect?



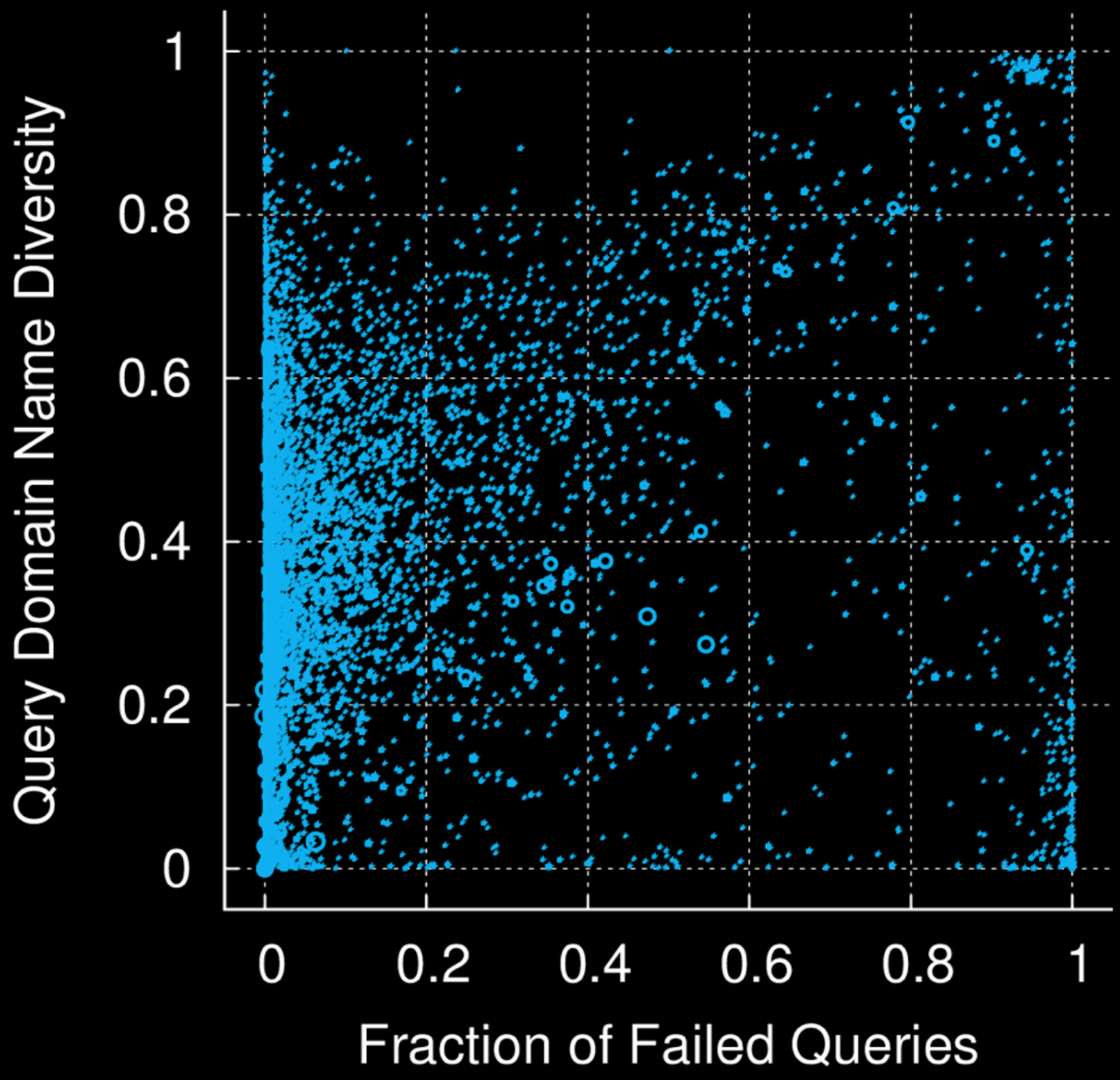
Classifying "Normals"



Classifying "Normals"

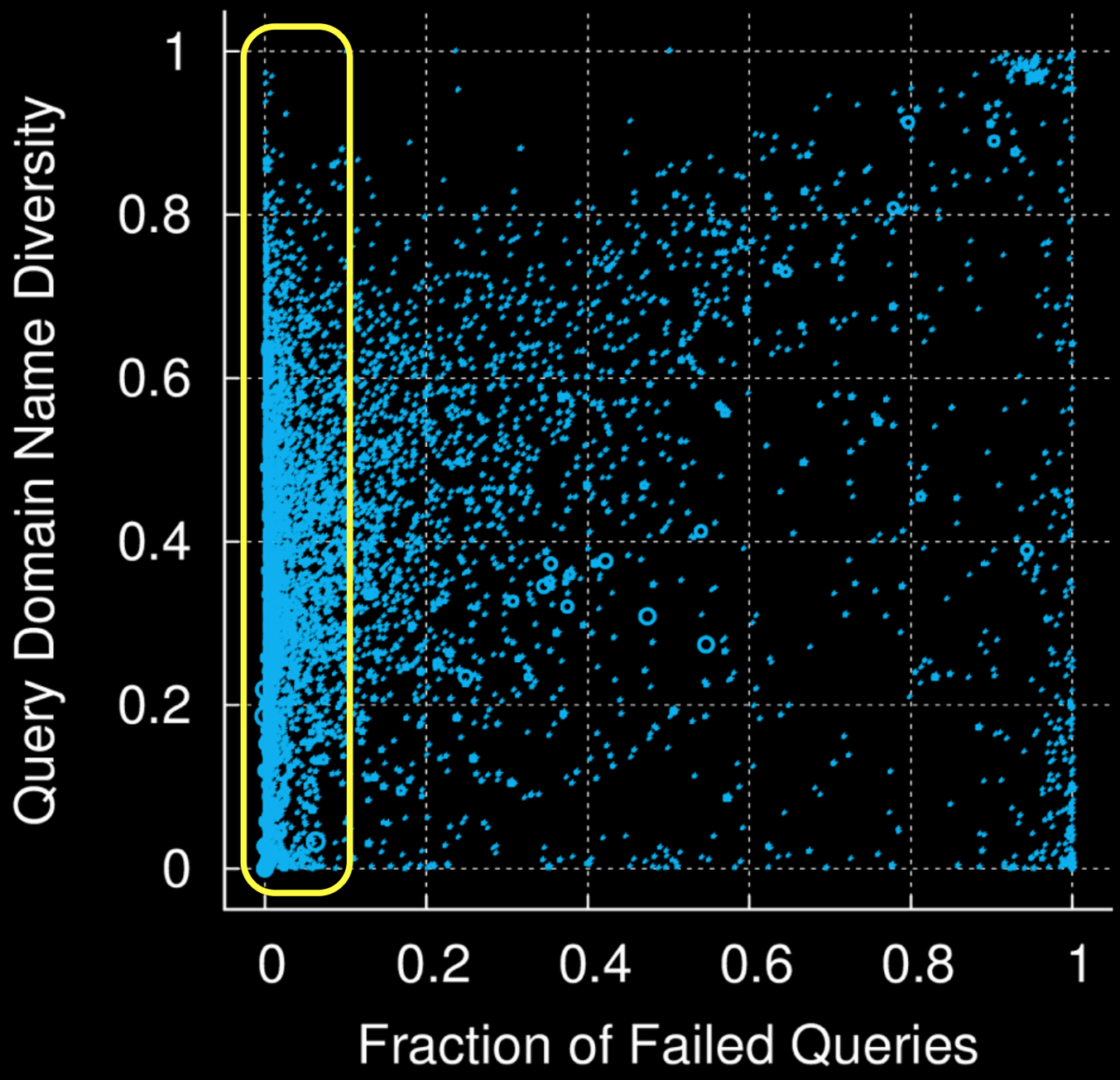


Classifying "Barnacles"



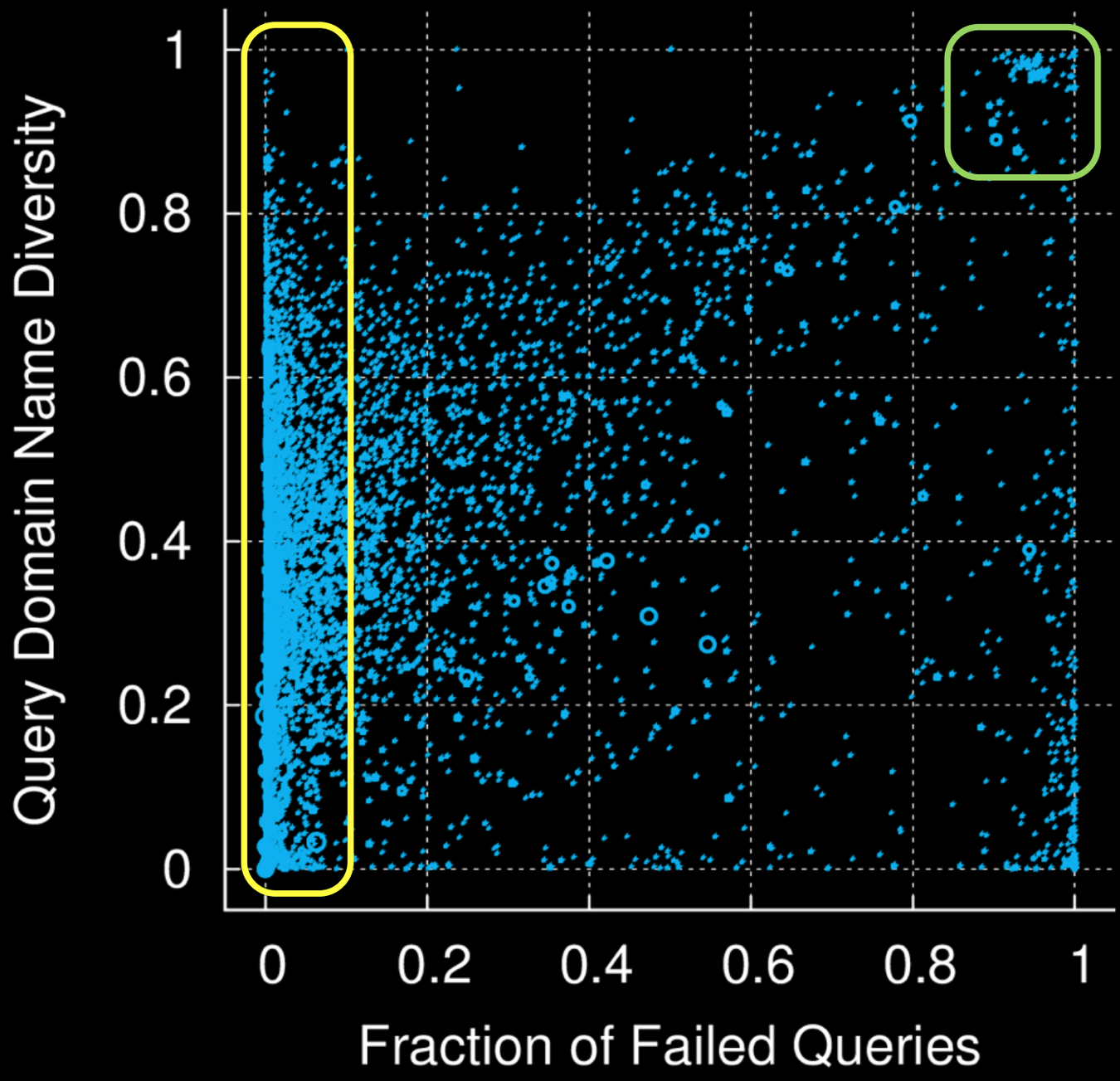
Classifying "Barnacles"

Majority have <10% failures



Classifying "Barnacles"

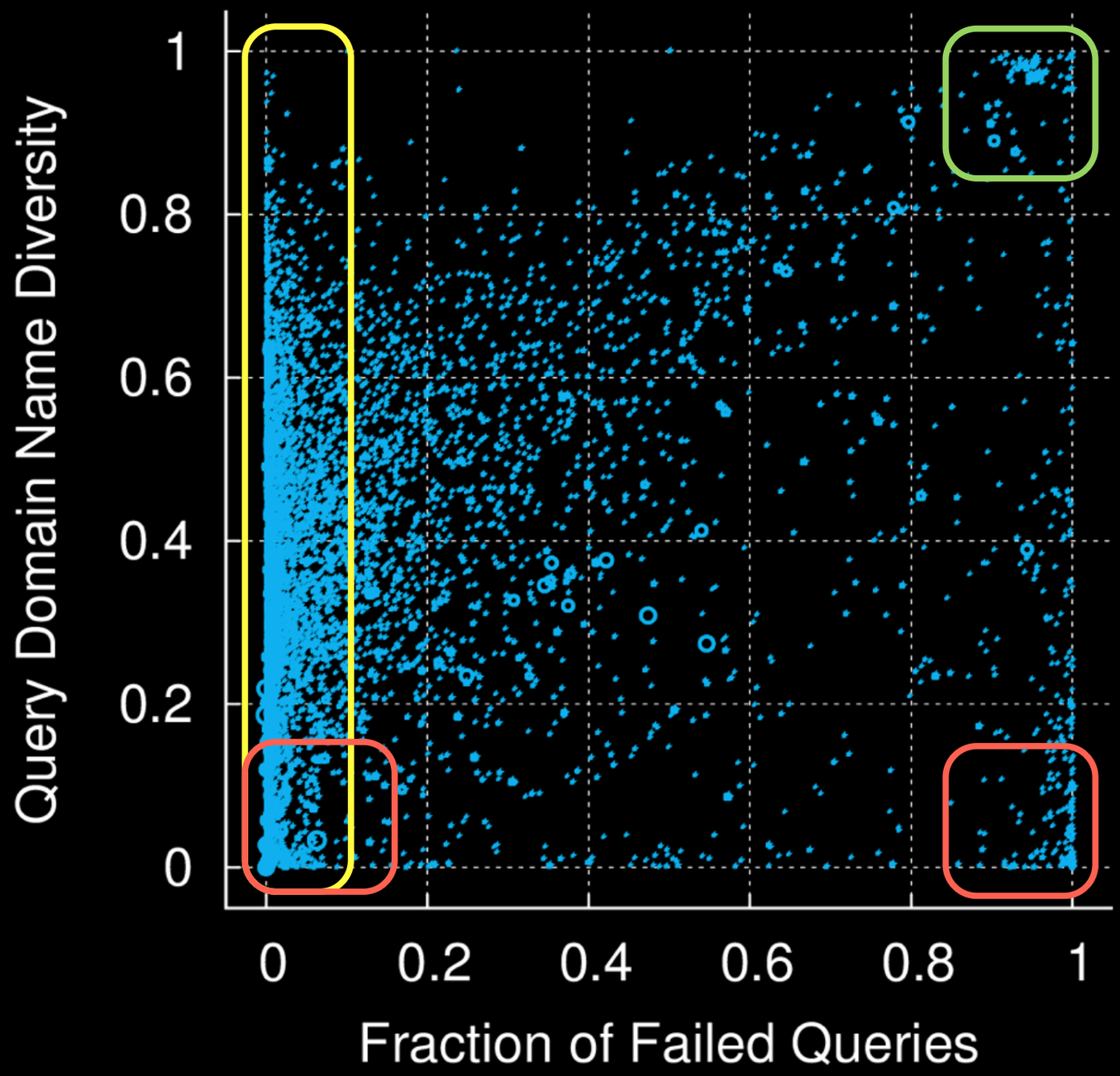
Majority have <10% failures



Like "Normals", but do not prime

Classifying "Barnacles"

Majority have <10% failures



Like "Normals", but do not prime

Queries from a small set

Why ... ?

Overall query volume increases

Excitables pointed to bug in PowerDNS

Resolvers still query old address

Queries to old address fail less often

Why ... ?

Overall query volume increases

Excitables pointed to bug in PowerDNS

Resolvers still query old address

Queries to old address fail less often

Barnacles due to misconfigurations, bugs, scanners, etc

Summary

Overall query volume increases

Excitables pointed to bug in PowerDNS

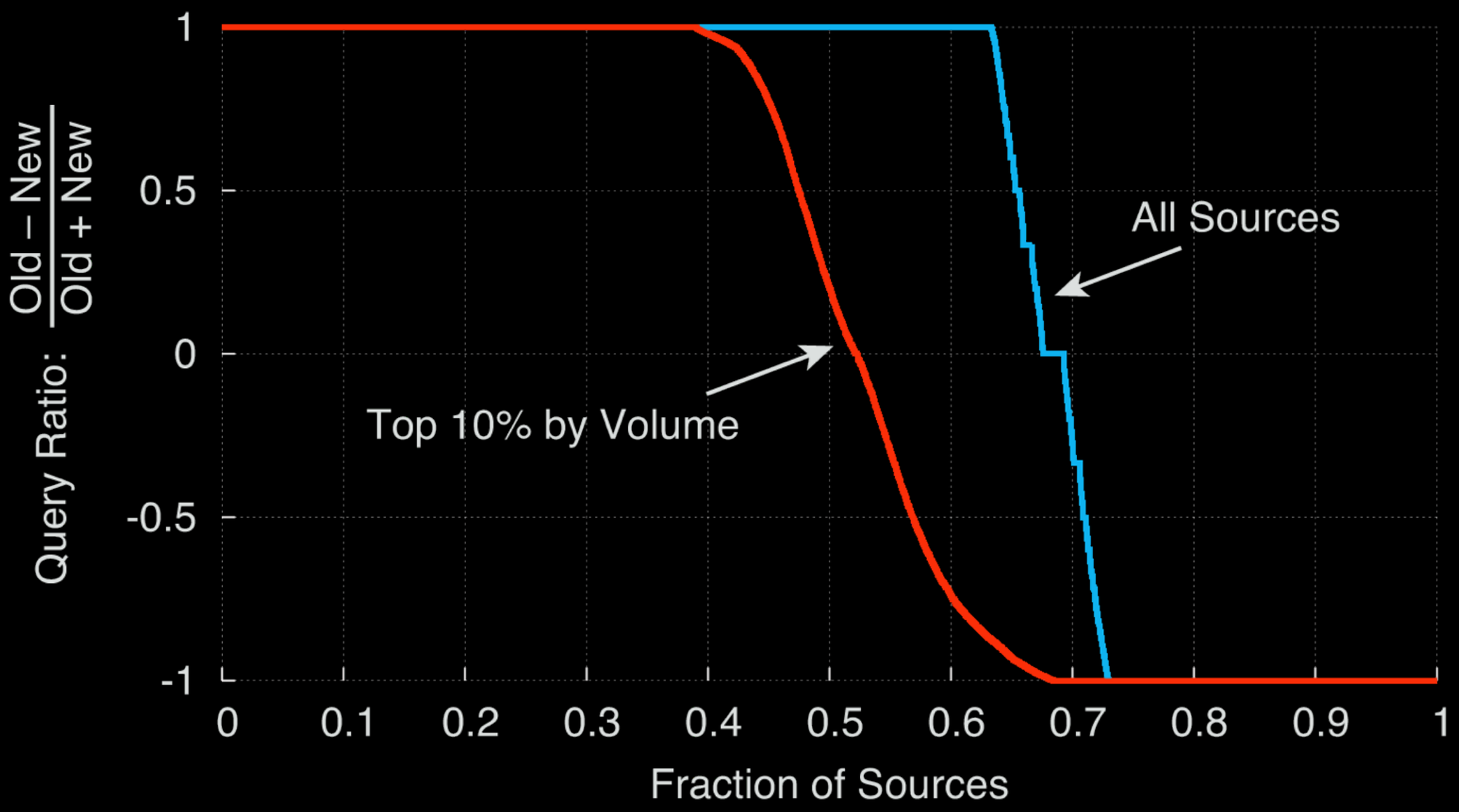
Resolvers still query old address

Queries to old address fail less often

Barnacles due to misconfigurations, bugs, scanners, etc

http://www.cs.umd.edu/projects/droot

Resolver Query Ratio



Classifying "Swappers"