A Study of Unexpected DNS Queries at B-Root

Dipsy Desai, Jelena Mirkovic
USC/ISI

DINR 2024

Apr. 4, 2024

Hook

- > 50% of incoming queries are unexpected queries…

Introduction

- Why is Domain Name System important?
  - Core of Internet Architecture

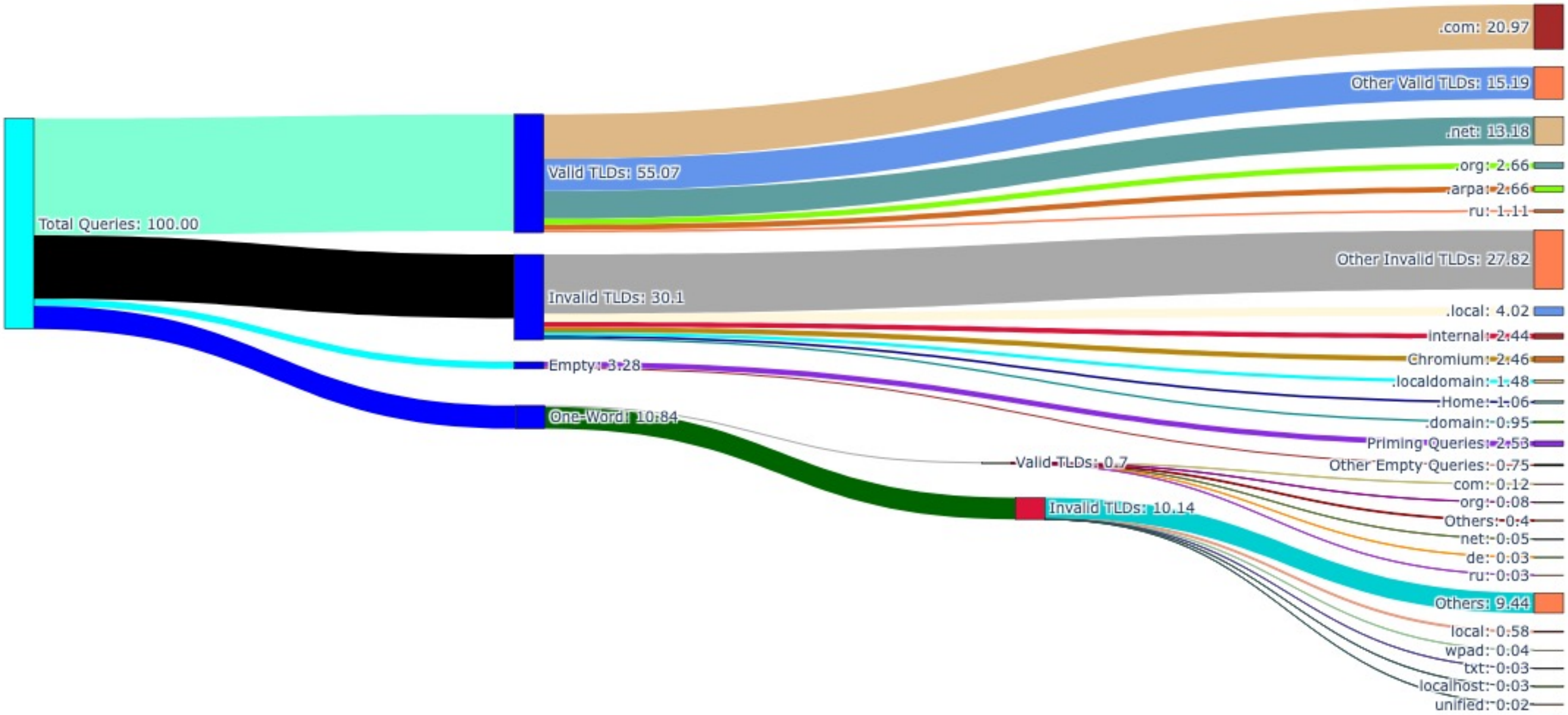
- B-Root Server
  - Billions of Queries

- Unexpected Queries
  - Malformed Queries
    - Non-printable characters, typos, PTR queries for private IP addresses, etc.
  - Repetitive Queries
    - Queries in quick succession for a www.example.com and www.noexample.com

Need

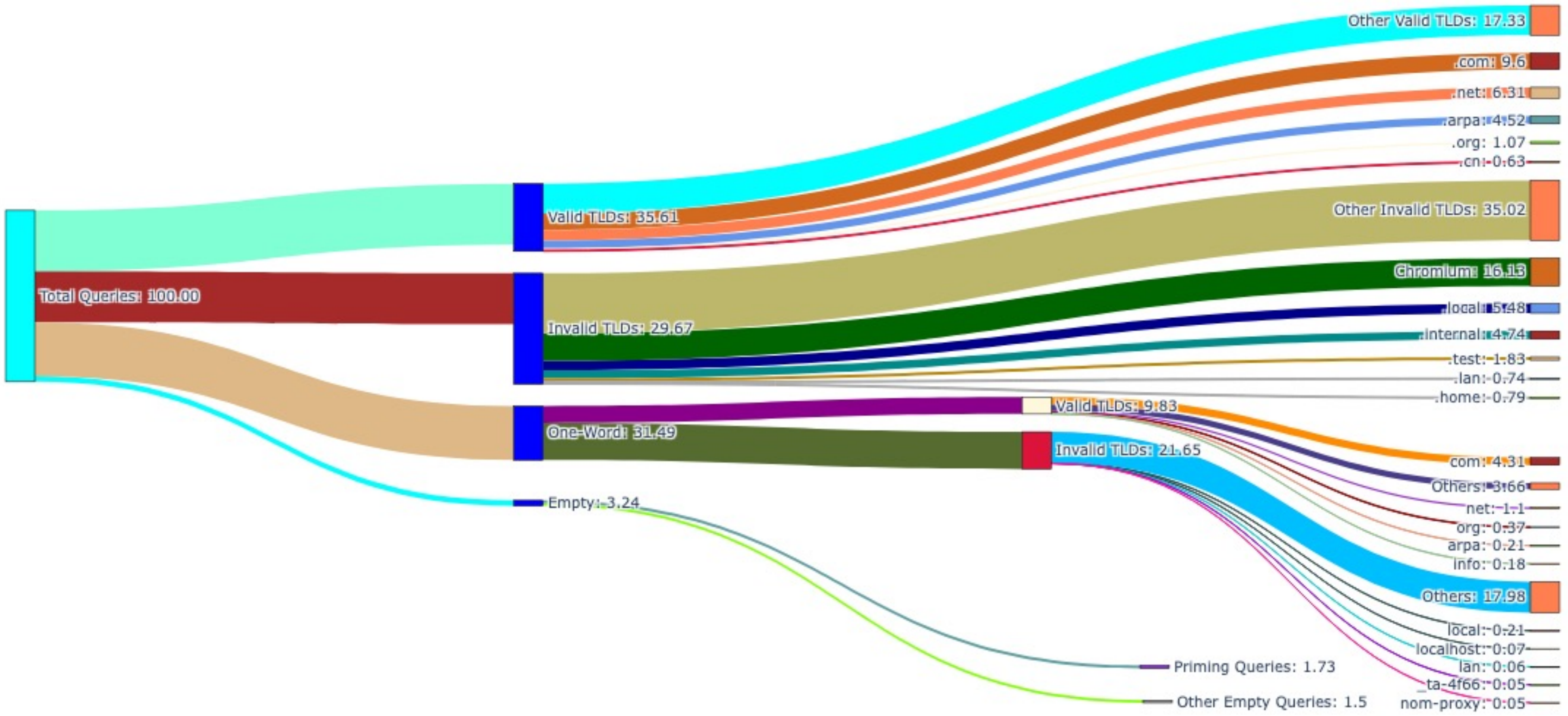
- A comprehensive analysis of incoming queries will help …
  - Find the source and probable cause
  - Malicious or Accidental ?
  - Improve efficiency of the root-server

Classification of Incoming Queries to B-Root in 2013



Total Queries ≈ 2.45 B

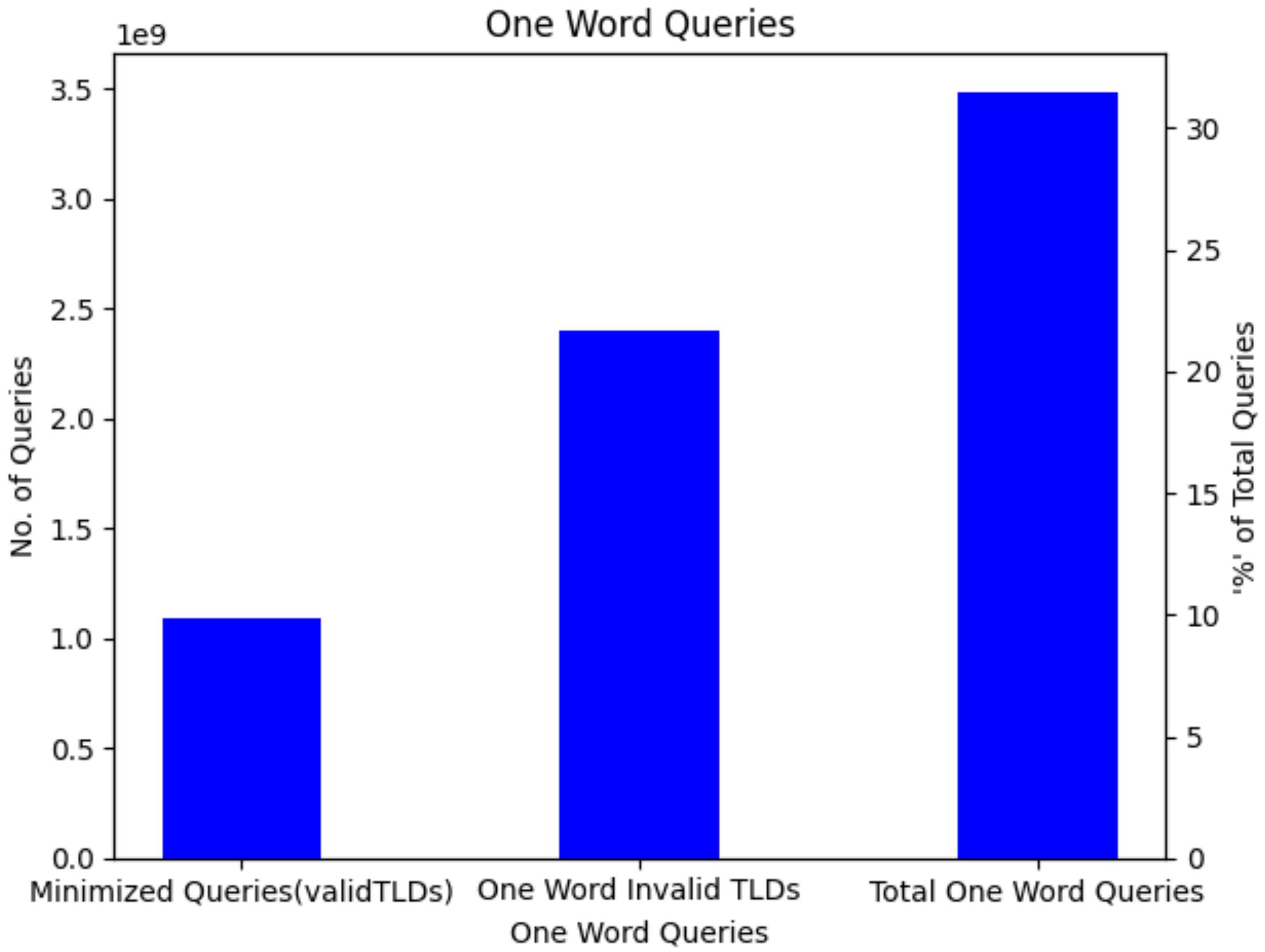
Classification of Incoming Queries to B-Root in 2023



Total Queries ≈ 11.07 B

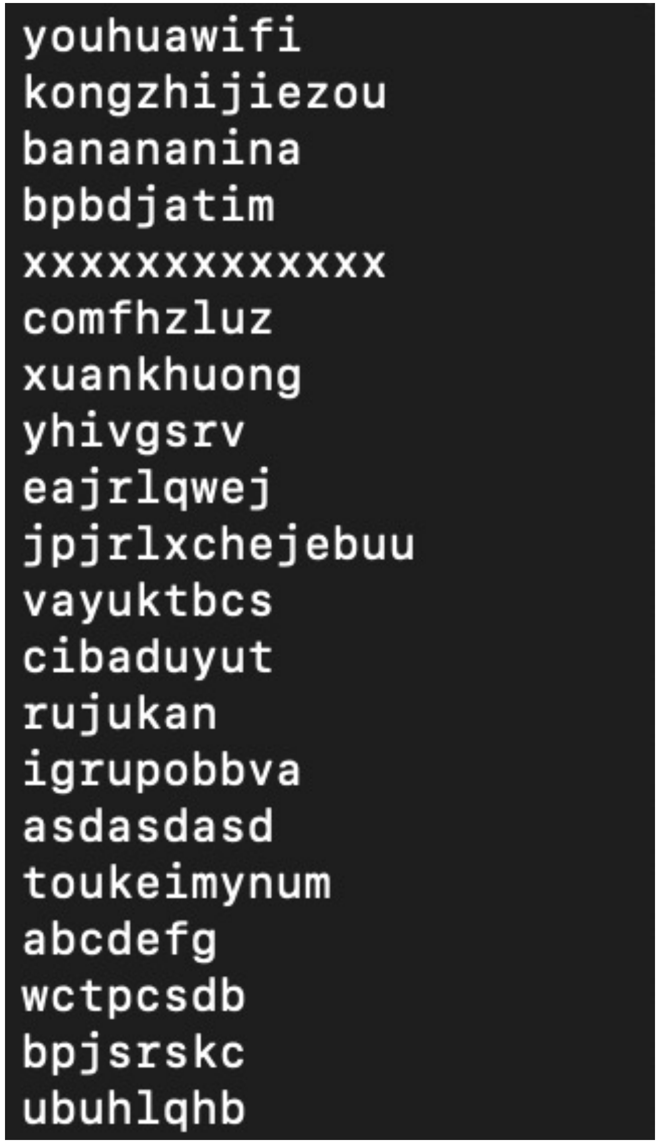
Approach contd.

- One-word Queries
  - Query Minimization
    - RFC 7816
    - com ← www.amazon.com
    - edu ← www.usc.edu



Approach contd.

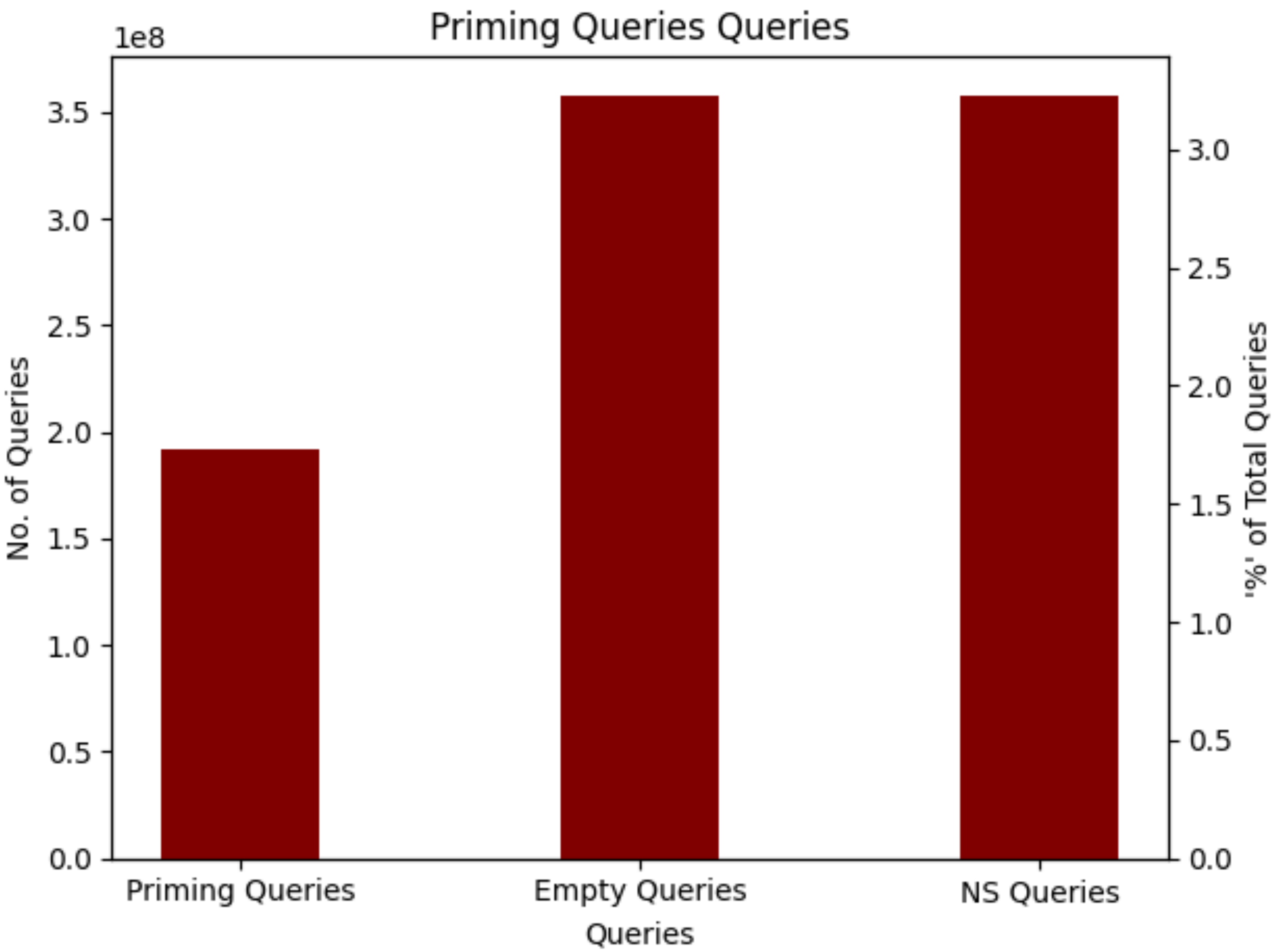
- Invalid TLDs
  - Chromium-based
  - Ex: bananaina, asdasdasd



```
youhuawifi
kongzhijiezou
banananina
bpbdjatim
xxxxxxxxxxxxx
comfhzluz
xuankhuong
yhivgsrv
eajrlqwej
jpjrlxchejebuu
vayuktbcs
cibaduyut
rujukan
igrupobbva
asdasdasd
toukeimynum
abcdefg
wctpcsdb
bpjsrskc
ubuhlqhb
```

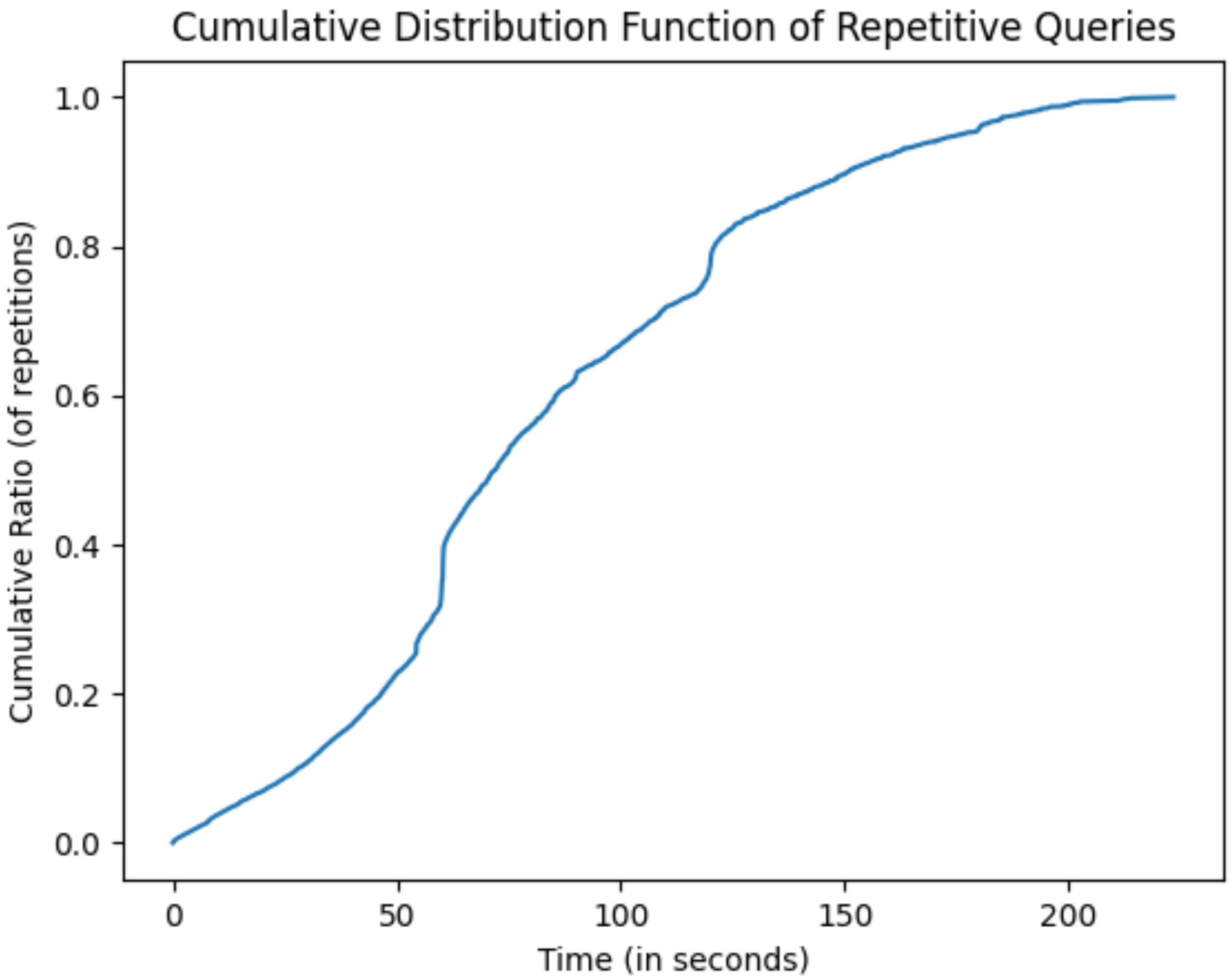
Approach contd.

- Empty Queries
  - Priming Queries
    - RFC 8109
    - QTYPE = NS, QNAME = .



Approach contd.

- Repetitive Queries
  - Varying TTL cache
- From Bogon IP ranges
  - Mostly IoT devices



Benefits

- Improve the efficiency of B-Root Server
  - Thoroughly dealing with unexpected queries

- Identify Frequent Senders
  - Possible misconfigured DNS resolvers
  - Suggest changes to querying mechanisms

- Repetitive Queries
  - Identify optimum TTL value

Competition/Challenges

- Study on DITL dataset from 8 root-servers
  - Castro et al. (ACM SIGCOMM 2008)

- Study on Chromium based queries
  - Verisign (K-Root server)
    - Prompted Chromium to change their querying mechanism

- Identifying the need to deal with unexpected queries
  - Save computational and operational resources
  - Increase the performance of the server

Conclusion

- Comprehensive analysis on incoming queries to B-Root
- Assist in identifying repeated senders
- Improve Efficiency of the root server

Questions?