A Study of Unwanted DNS Traffic at b-root.server

Dipsy Desai,
University of Southern California

Joint work with Prof. Jelena Mirkovic

ICANN 82

8-13 March 2025

USC Viterbi School of Engineering

USC INFORMATION SCIENCES INSTITUTE

Hook 

> 70% of all incoming queries to root-servers are unwanted!

Introduction

- Domain Name System (DNS)
  - Phonebook of the Internet
  - Crucial for navigating the Internet without memorizing numbers
  - Structured hierarchically for efficient management

- Root Servers
  - At the top of DNS hierarchy – processing billions of queries every day
  - Authoritative for managing Top-Level Domains (TLDs) like ‘.com’, ‘.net’, etc.
  - 13 unique root-servers, named ‘a’ through ‘m’

Need

- A comprehensive analysis of incoming queries
  - Understand root causes of queries
    - Resolver software
    - Applications
    - User behavior
  - Identify sources responsible for unwanted traffic

Approach

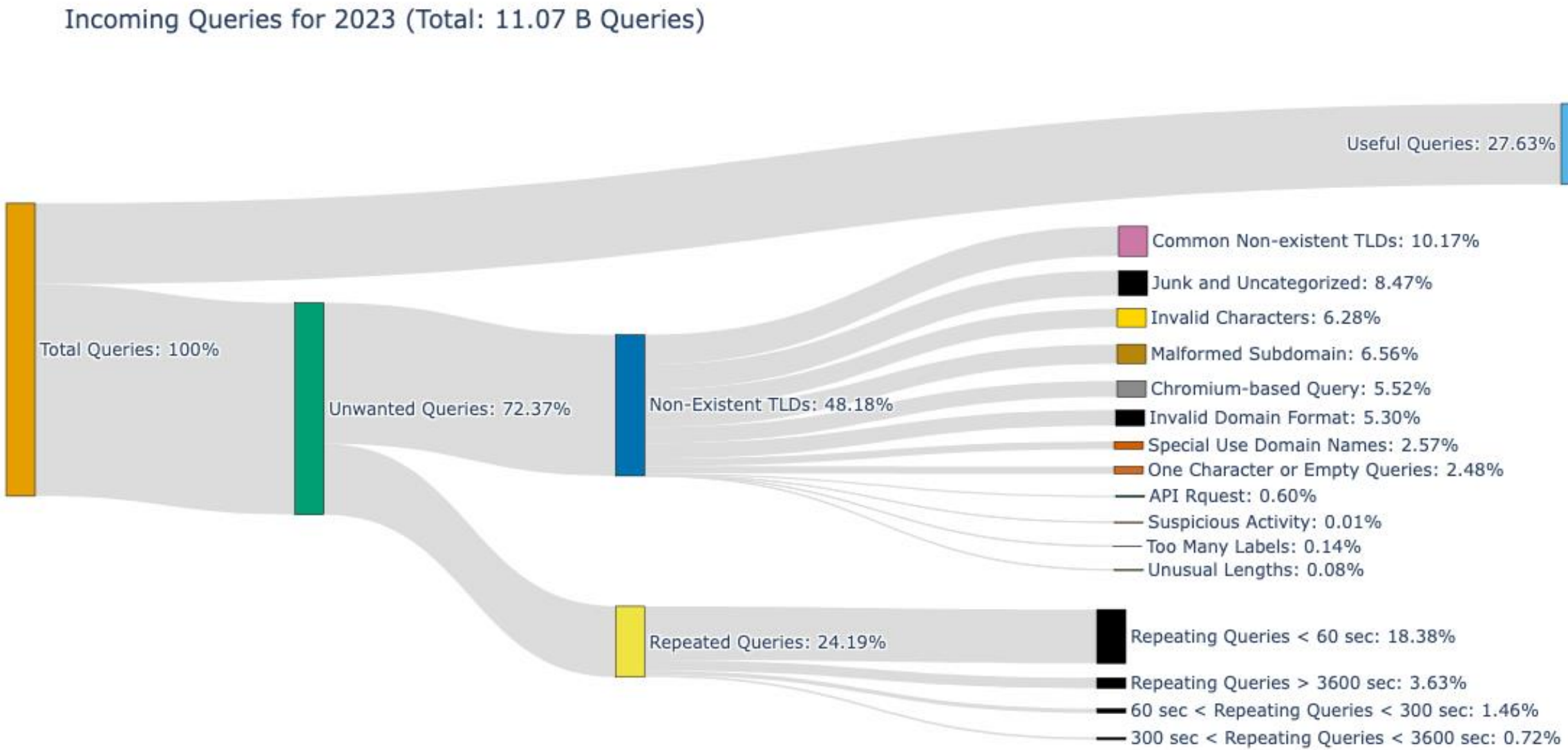
- Longitudinal Analysis
  - DNS OARC facilitates collection of Day-In-The-Life of the Internet (DITL) data
    - Gathered over a 48-hour period each year
  - b.root-server's DITL data has been collected annually since 2013
    - Our research utilizes DITL data for 11 years (2013 – 2023)

- Query parameters
  - timestamp - time at which a query arrived (Ex: Epoch time - 1618311662)
  - srcIP - IP address that sent the query (Ex: 68.181.75.207)
  - name - content of the query (Ex: www.isi.edu)
  - qtype - type of query (Ex: A, AAAA, MX, NS)

Approach contd.

- Repetitive Queries
  - Absence of caching mechanism, independent sources (non-resolver devices)
  - Bias in caching towards specific QTYPEs

- Queries to Unallocated TLDs
  - Misconfigurations, default forwarding policy
  - Lack of mechanisms to handle non-existent TLDs, software bugs
  - Open-source router software, older versions of DNS software
  - Chromium-based queries, domain-generation algorithms
  - Misconfigured web applications, inadequate validation checks



Benefits

- Identifying Unwanted Queries
  - Thoroughly dealing with them at the source
- Detailed Categorization can help identify
  - Possible misconfigured DNS resolvers
  - Suggest changes to querying mechanisms
- Repetitive Queries
  - Identify optimum TTL value

Competition/Challenges

- Analysis of wide-area name server traffic (SIGCOMM 1992)
  - Seminal work on classifying unwanted DNS traffic
- Is you caching resolver polluting the internet (SIGCOMM 2004 Workshop)
  - Reasons for bogus traffic reaching root-servers
- A Day at the Root of the Internet (SIGCOMM 2008)
  - Study on DITL dataset from 8 root-servers – 98% of unwanted traffic
- Unwanted DNS traffic still exists!

Conclusion

- Comprehensive analysis on incoming queries to b.root-server
- Identify the root cause of each category of unwanted queries
- Improve efficiency of the root-servers – save computational and operational resources
- Enhances the sanity of DNS ecosystem

Questions?

Get in touch!

USC Viterbi School of Engineering

USC INFORMATION SCIENCES INSTITUTE