Modeling DNS Queries and Caching to Evaluate the Merits of QNAME Minimization

Casey Deccio, Robert Richardson, Nathaniel Bennett, Nathan Craddock

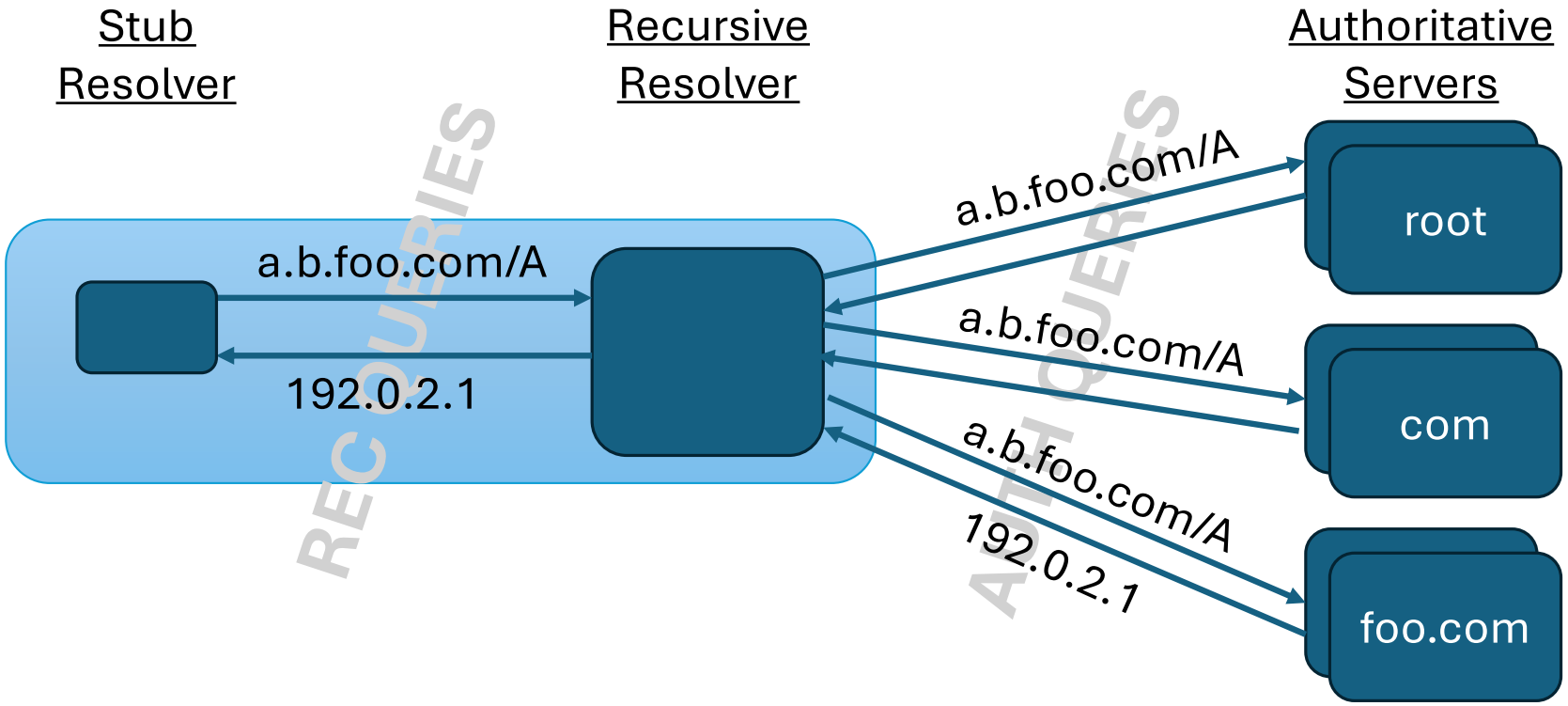
Brigham Young University

OARC 46

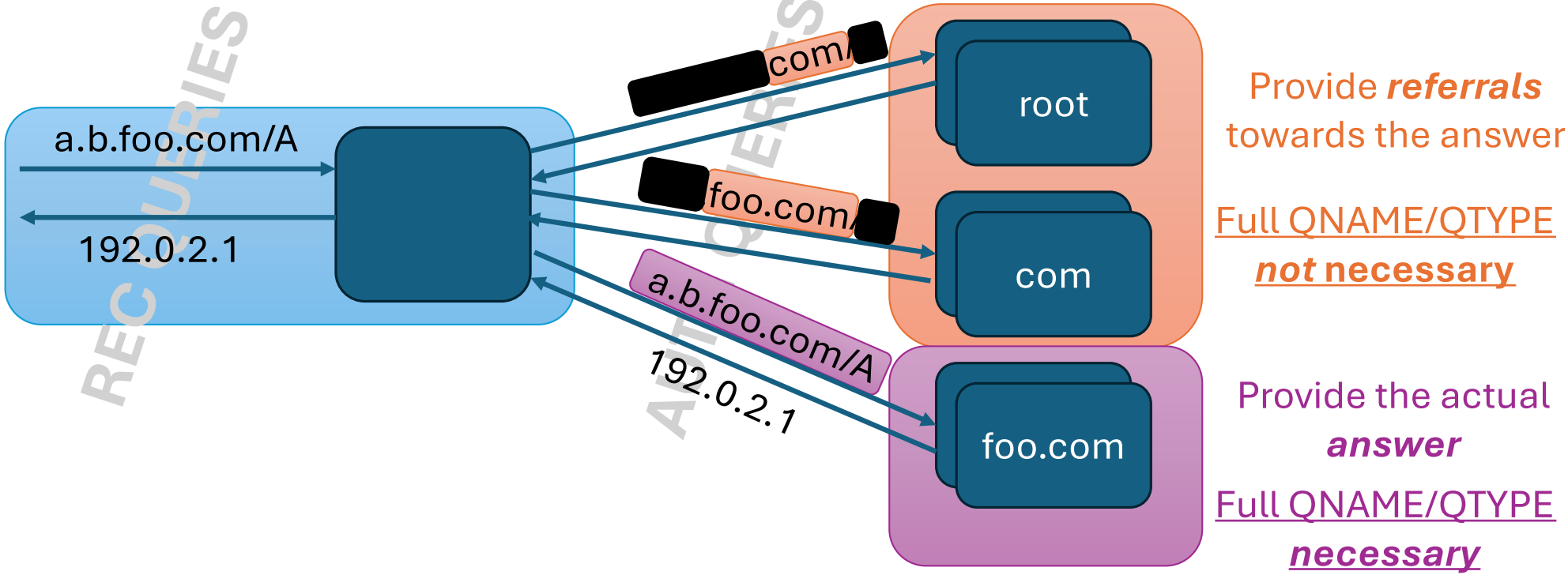
Edinburgh, United Kingdom

May 16, 2026

Background: DNS Name Resolution



QNAME Minimization Principles



Research Question

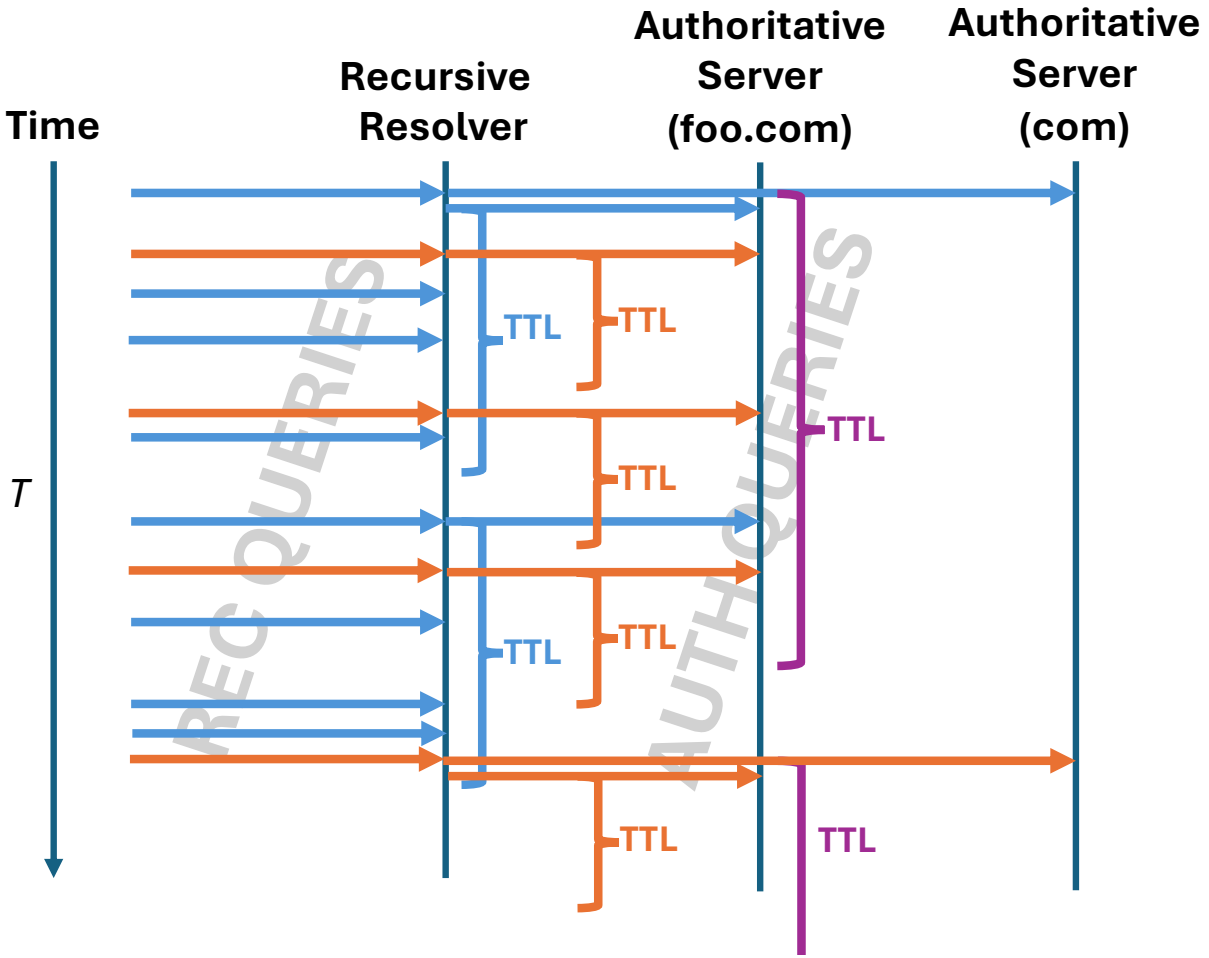
Can we quantify the utility of QNAME minimization?

Methodology

1. Develop a model of queries, caching, and leakage
2. Apply the model to a set of queries

https://www.vectorstock.com/royalty-free-vector/man-with-question-mark-flat-icon-pictogram-vector-4920218

Caching Dynamics



Query for a.b.foo.com/A

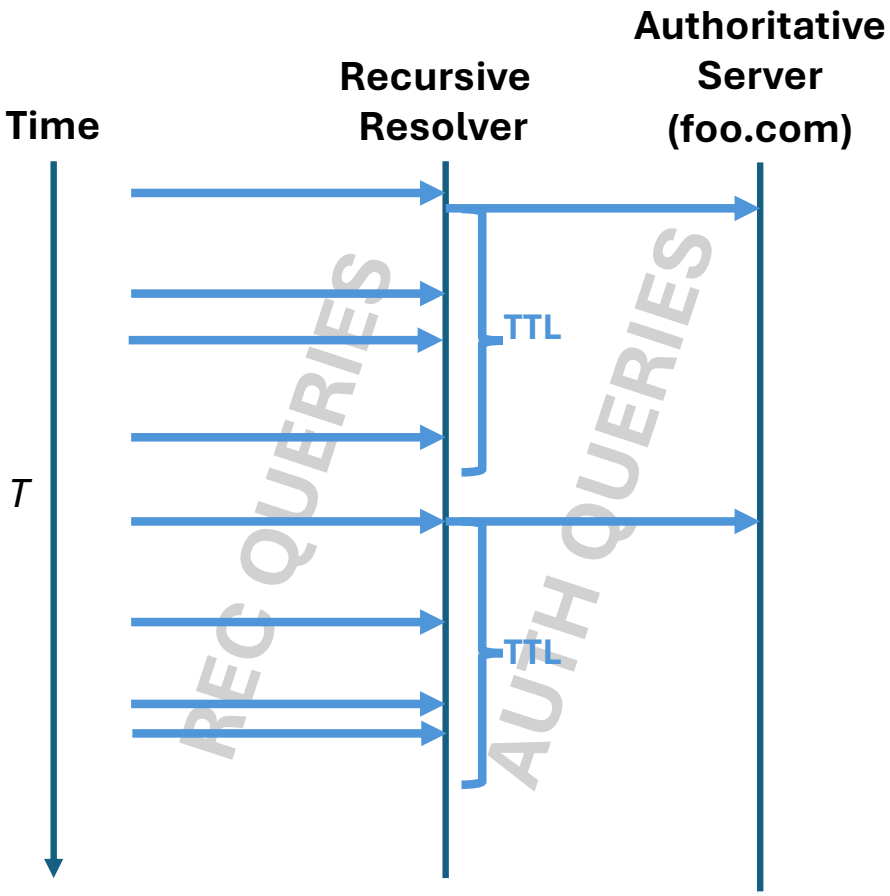
TTL for a.b.foo.com/A

Query for c.d.foo.com/A

TTL for c.d.foo.com/A

TTL for foo.com/NS

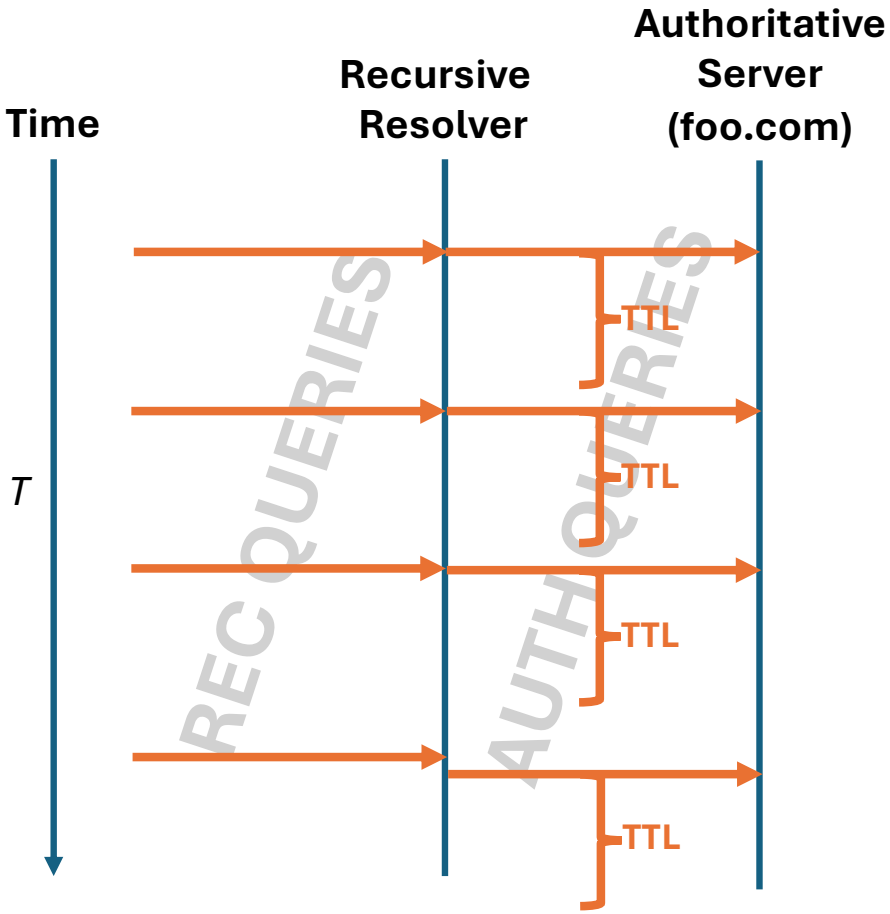
Caching Dynamics - Observations



During Time Period *T*:

When # recursive queries > # TTLs:
auth. queries = # TTLs

Caching Dynamics - Observations

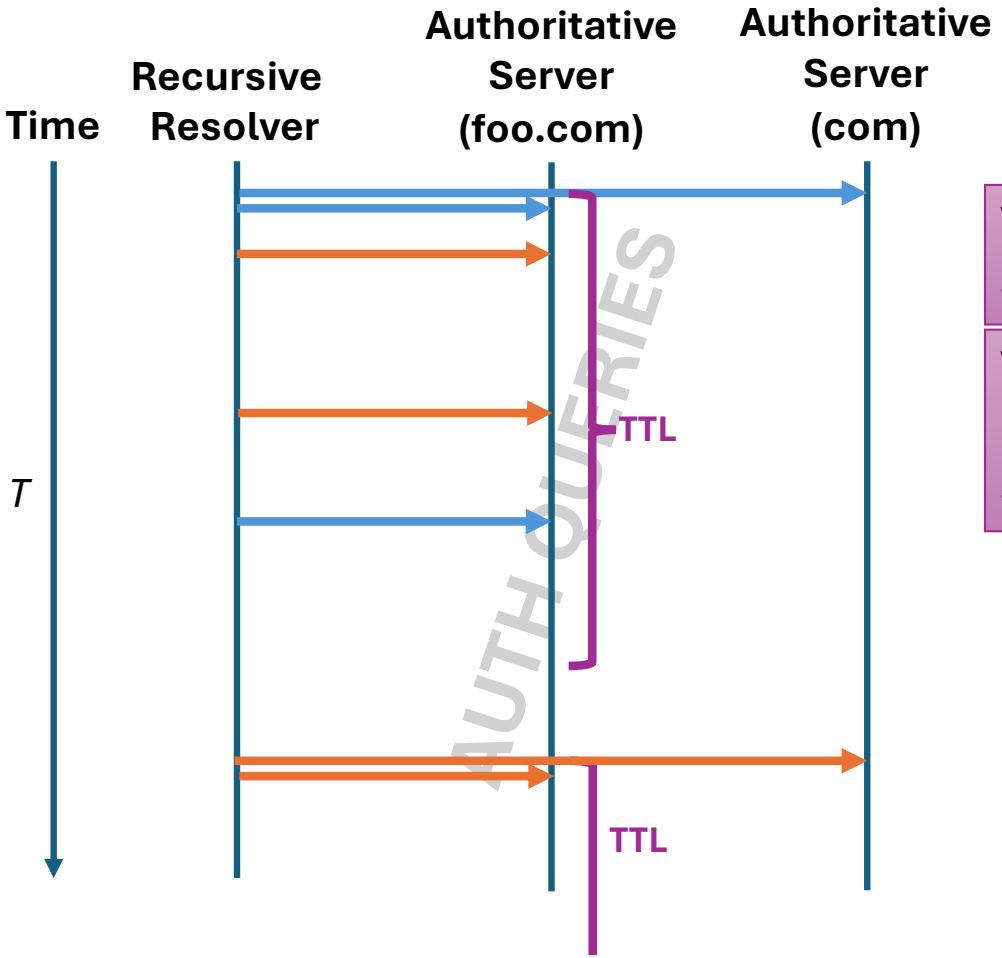


During Time Period *T*:

When # recursive queries > # TTLs:
auth. queries = # TTLs

When # recursive queries ≤ # TTLs:
auth. queries = # recursive queries

Caching Dynamics - Observations

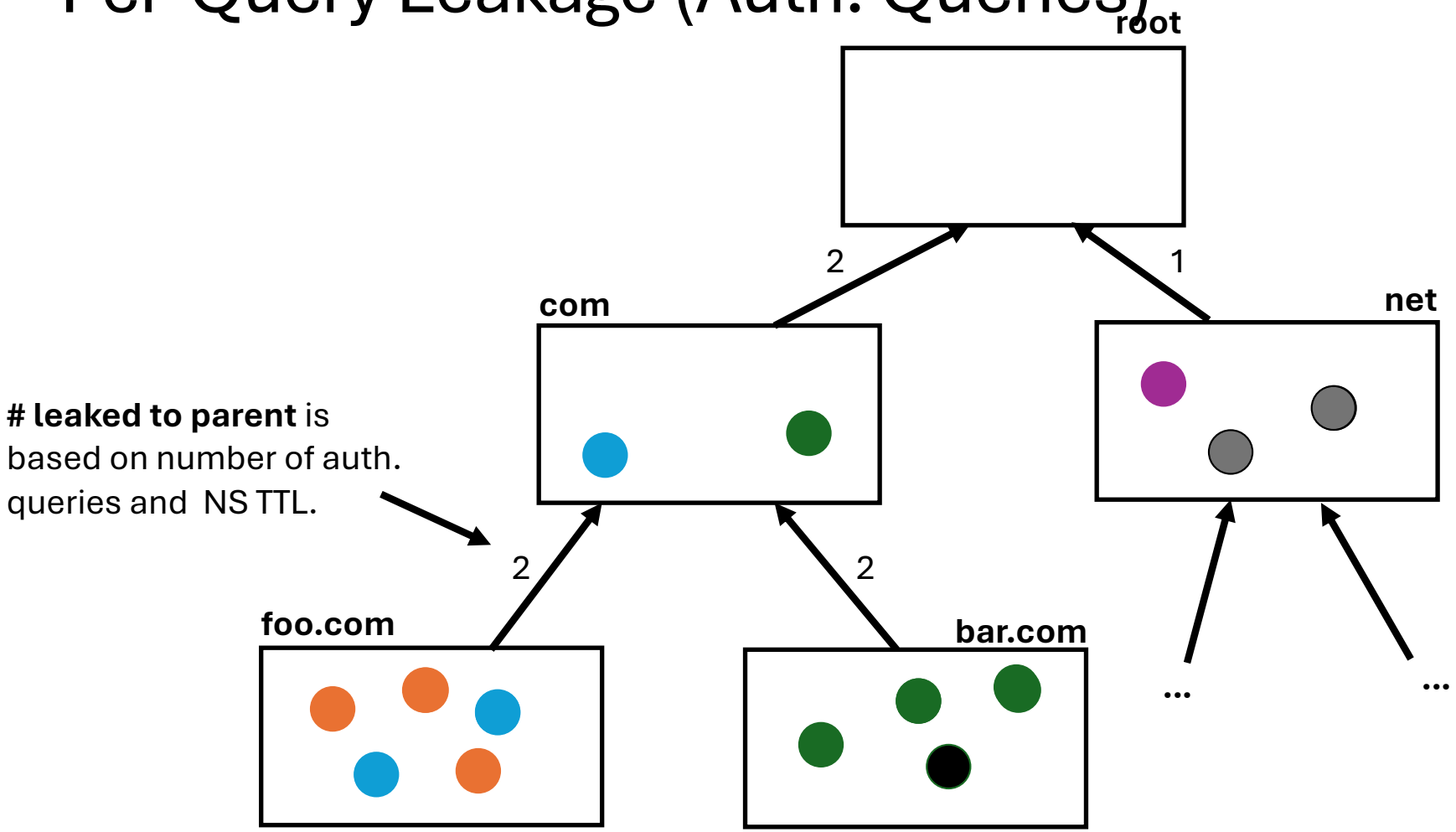


During Time Period *T*:

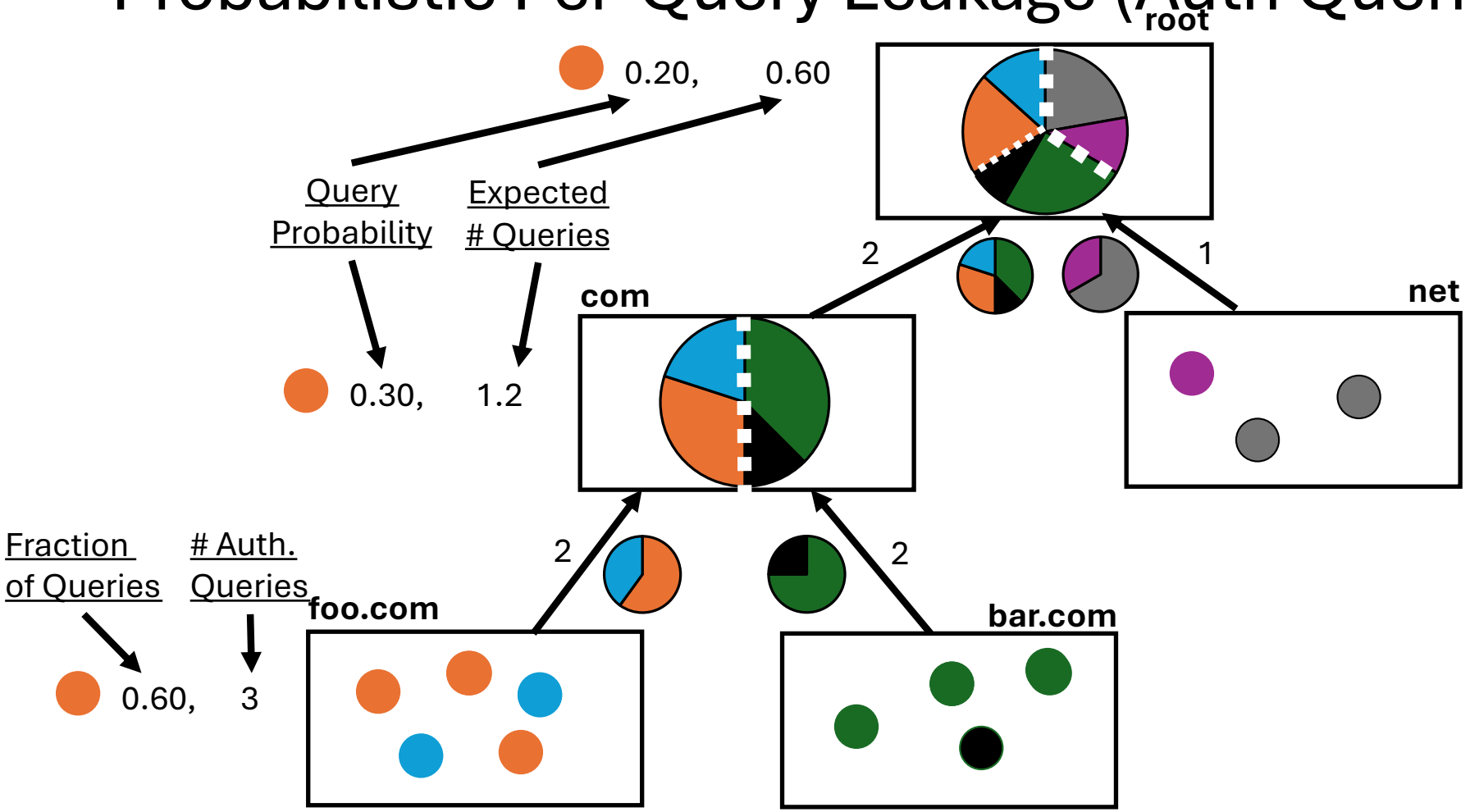
When # auth queries > # NS TTLs:
auth queries to parent = # TTLs

When # auth queries ≤ # NS TTLs (not shown):
auth queries to parent = # auth queries

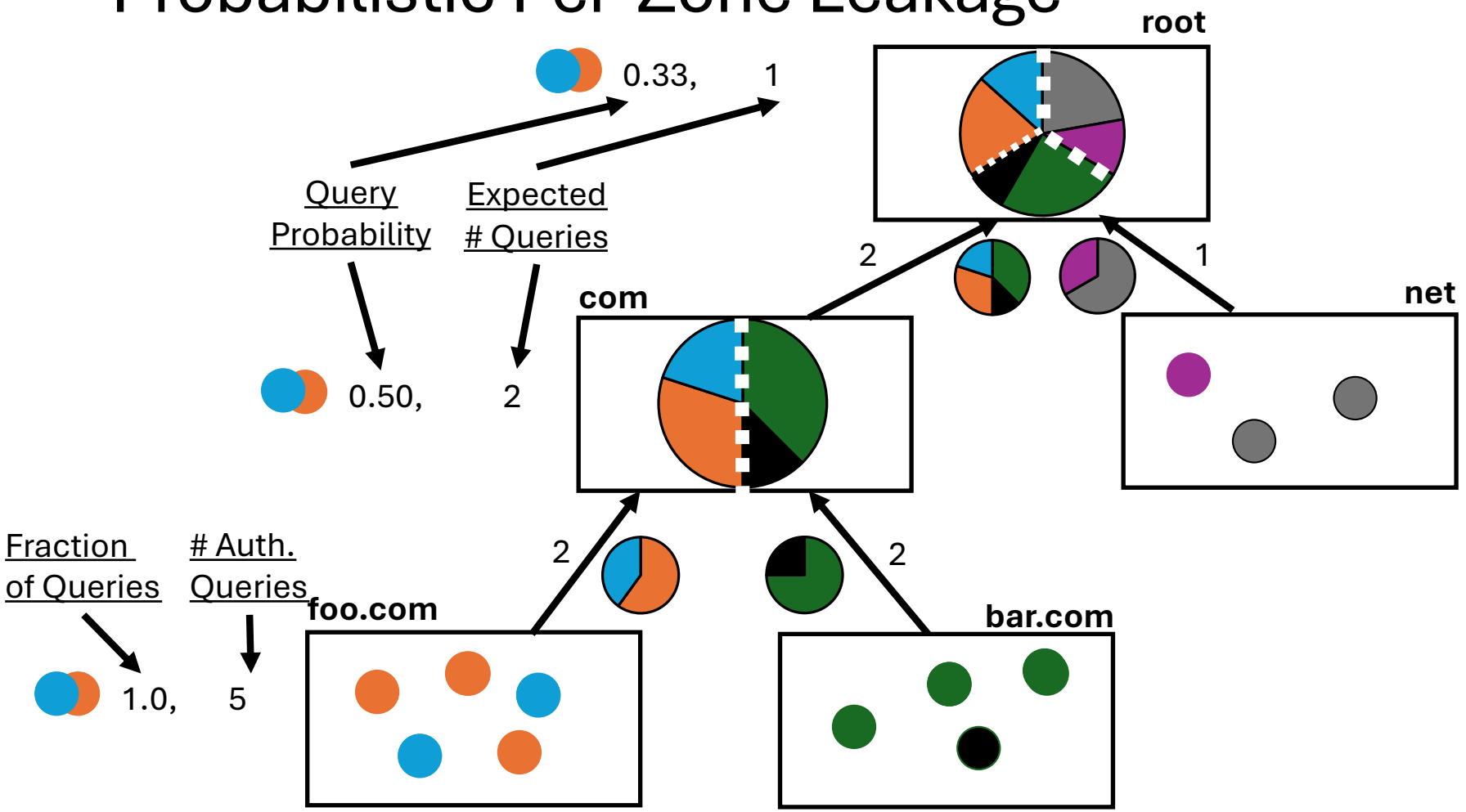
Per-Query Leakage (Auth. Queries)



Probabilistic Per-Query Leakage (Auth Queries)

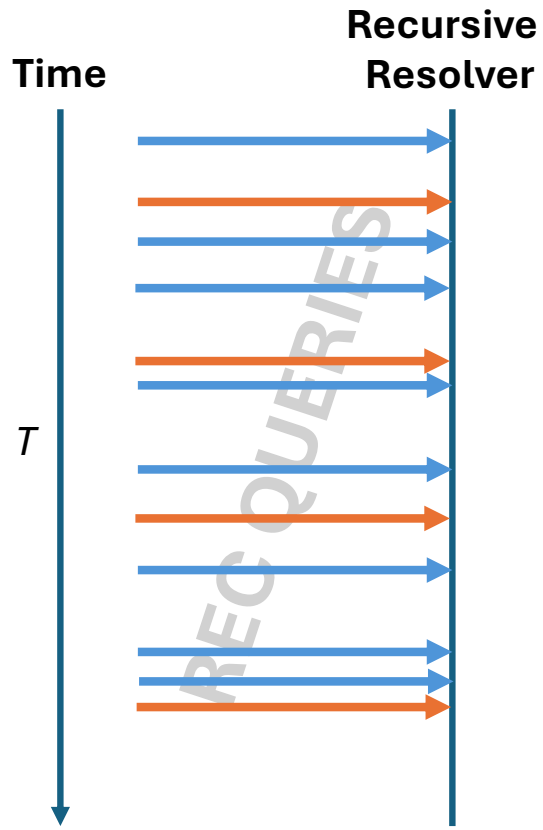


Probabilistic Per-Zone Leakage



Dataset

- One week of recursive queries from BYU's campus network.
- Queries anonymized to preserve privacy.



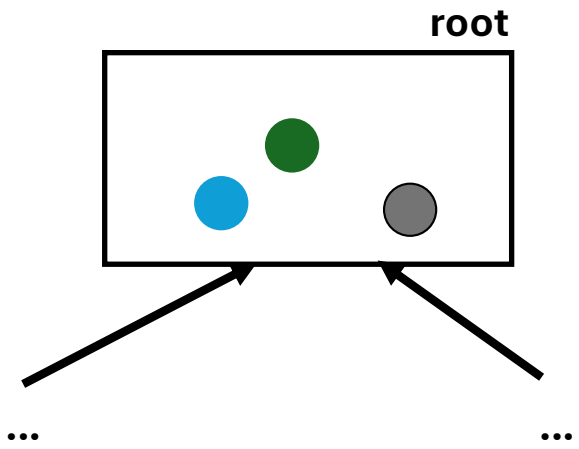
Results (Yay! and meh.)

- For 87% of domains, representing 96% of queries, the parent domain is a TLD.
  - Yay! 😆 TLDs could be considered potential aggregators of query info.
  - Meh. 😕 Parent domains always see the QNAME's domain anyway.
- For half (50%) of domains, *all QNAMEs are leaked* to parent domain.
  - Yay! 😆 QNAME minimization keeps QNAMEs to minimal disclosure.
  - Meh. 😕 74% of QNAMEs are associated with fewer than five recursive queries.
- For 99% of domains, the QNAME leakage rate to root servers is 65% or less.
  - Yay! 😆 QNAME minimization keeps the root from seeing these queries.
  - Meh. 😕 For half of domains, only a single QNAME is represented in queries.

https://www.flaticon.com/free-icons/excited https://www.flaticon.com/free-icons/bored

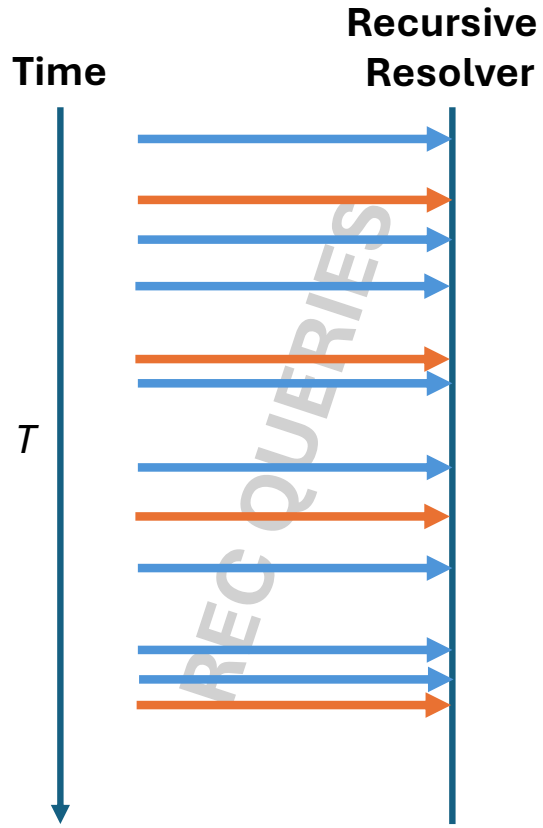
Other QNAME Minimization Costs

- Root server queries provide a rich data source to the Internet community (DITL).
  - Queries at root represent a sample of recursive queries issued.
  - Value diminished by QNAME minimization.
- QNAME minimization has been a contributor to attacks.
  - “CAMP: Compositional amplification attacks against DNS” [Duan, USENIX Security 2024].

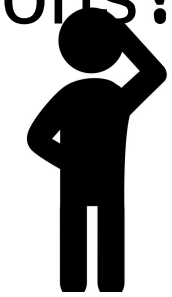


Summary

- Caching and leakage can be modeled.
- There are pros and cons to QNAME minimization.
  - **Pro:** modest privacy gains
  - **Con:** decreased utility of internet community datasets



Questions?



casey@byu.edu

BYU