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

**Casey Deccio**, Robert Richardson, Nathaniel Bennett, Nathan Craddock

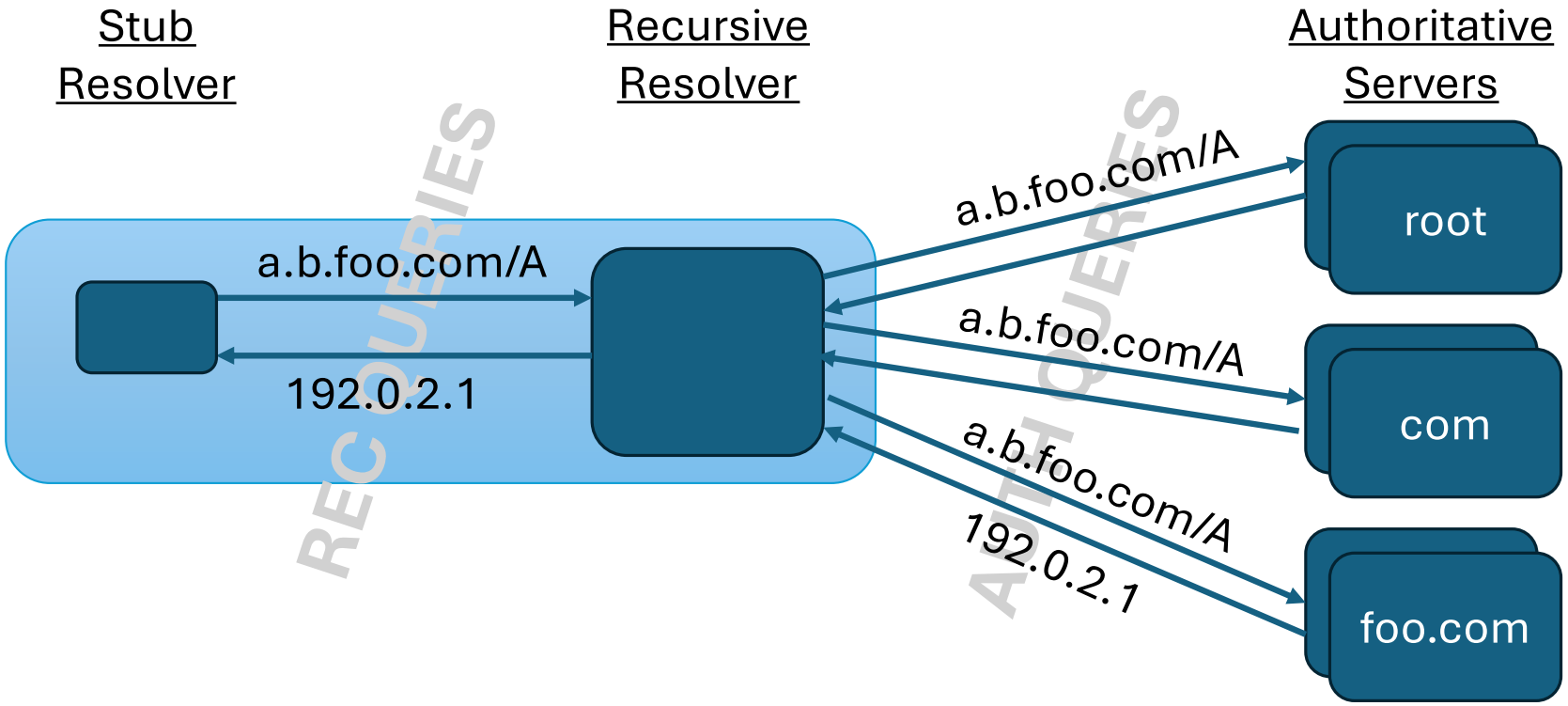
Brigham Young University

OARC 46

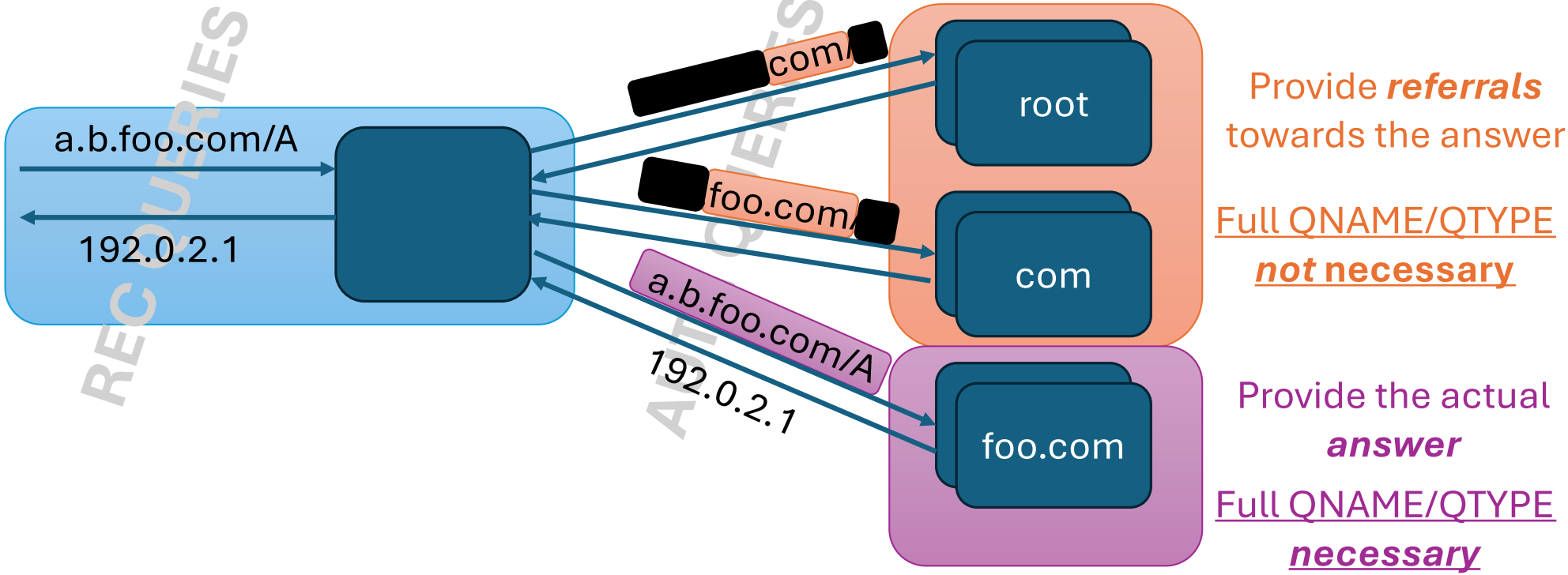
Edinburgh, United Kingdom

May 16, 2026

# Background: DNS Name Resolution



# QNAME Minimization Principles



## Research Question

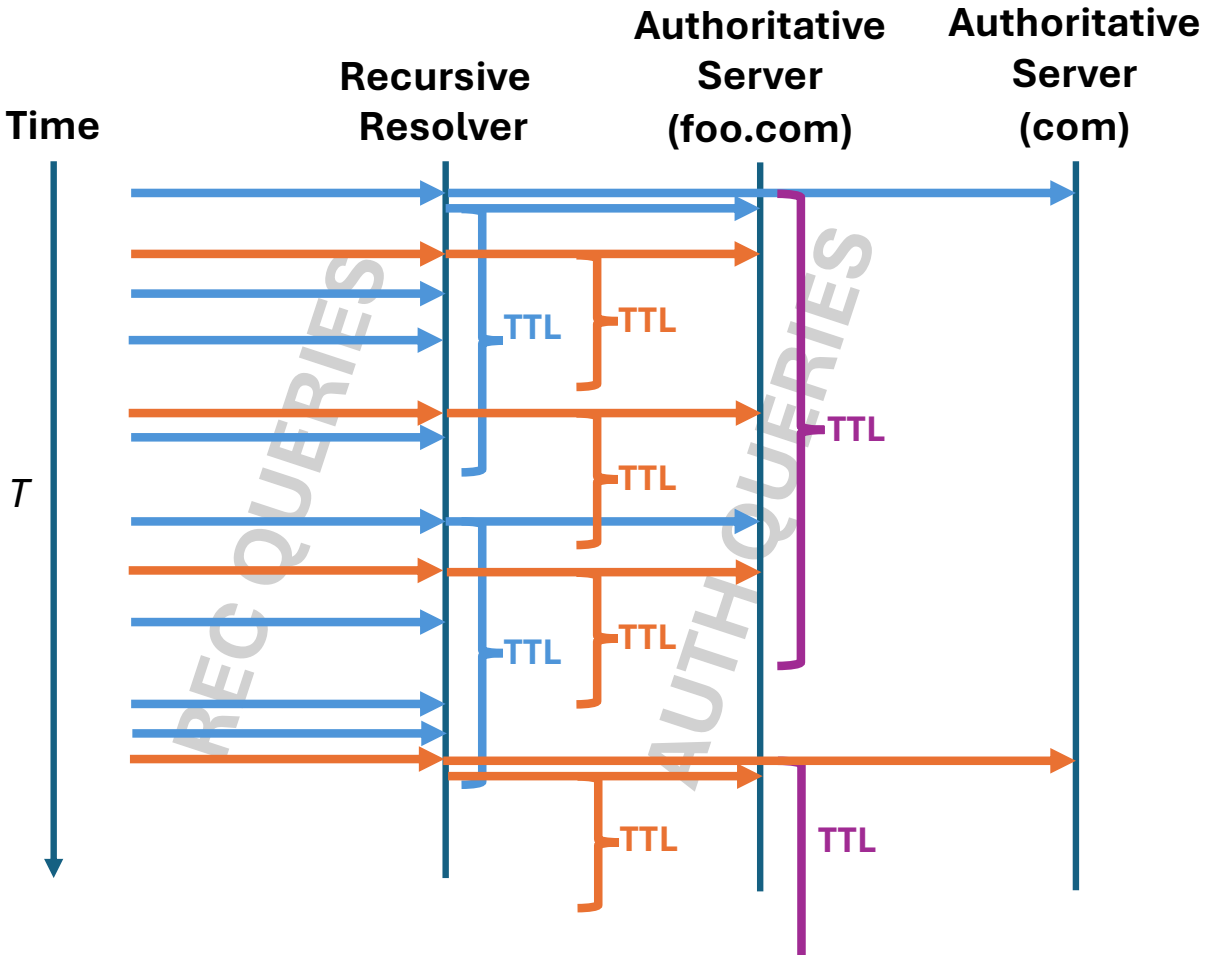
Can we quantify the utility of QNAME minimization?

## Methodology

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

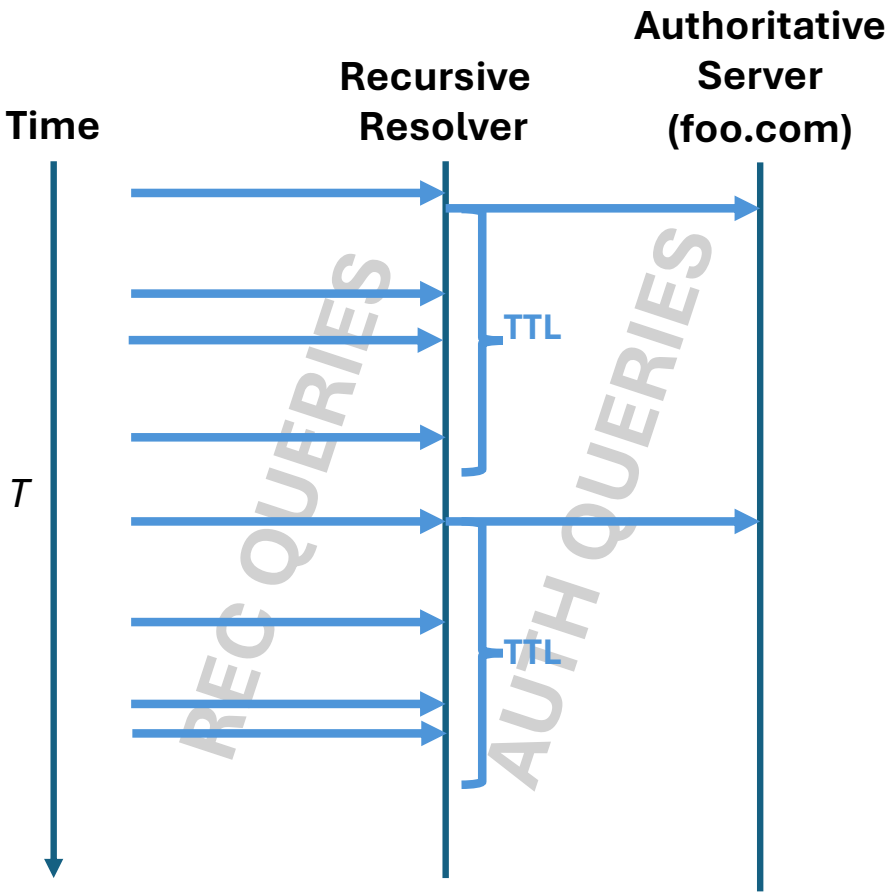
TTL for a.b.foo.com/A

Query for c.d.foo.com/A

TTL for c.d.foo.com/A

TTL for foo.com/NS

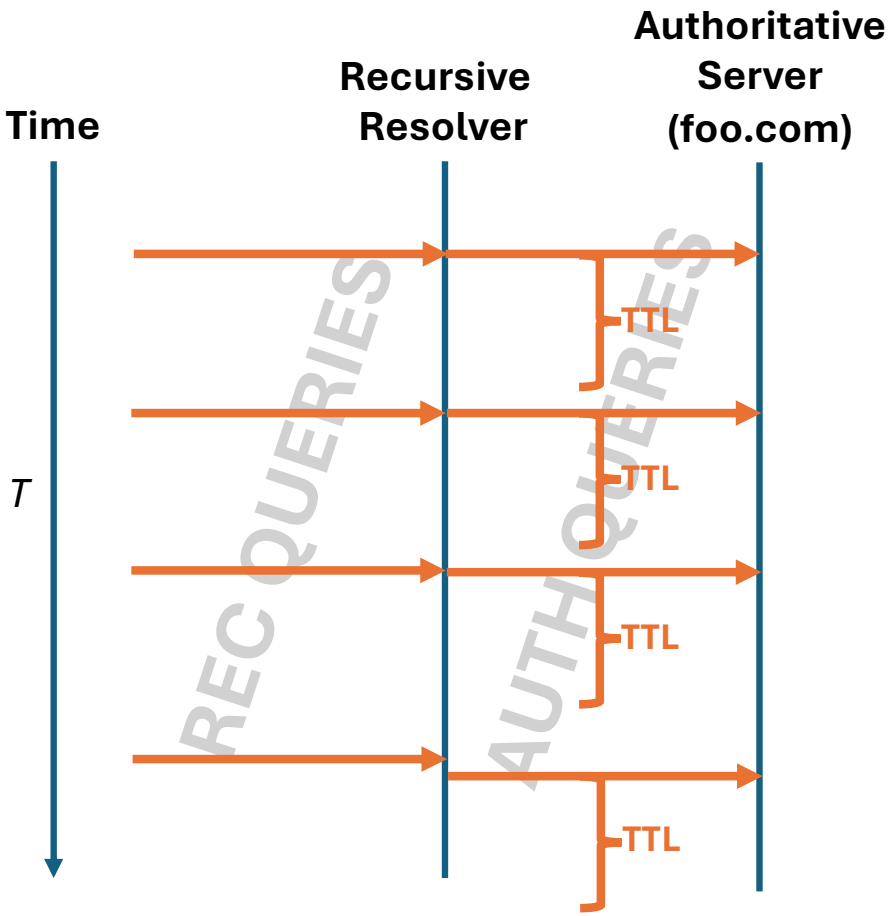
# Caching Dynamics - Observations




During Time Period *T*:

**When recursive queries > TTLs:**
auth queries = TTLs

# Caching Dynamics - Observations

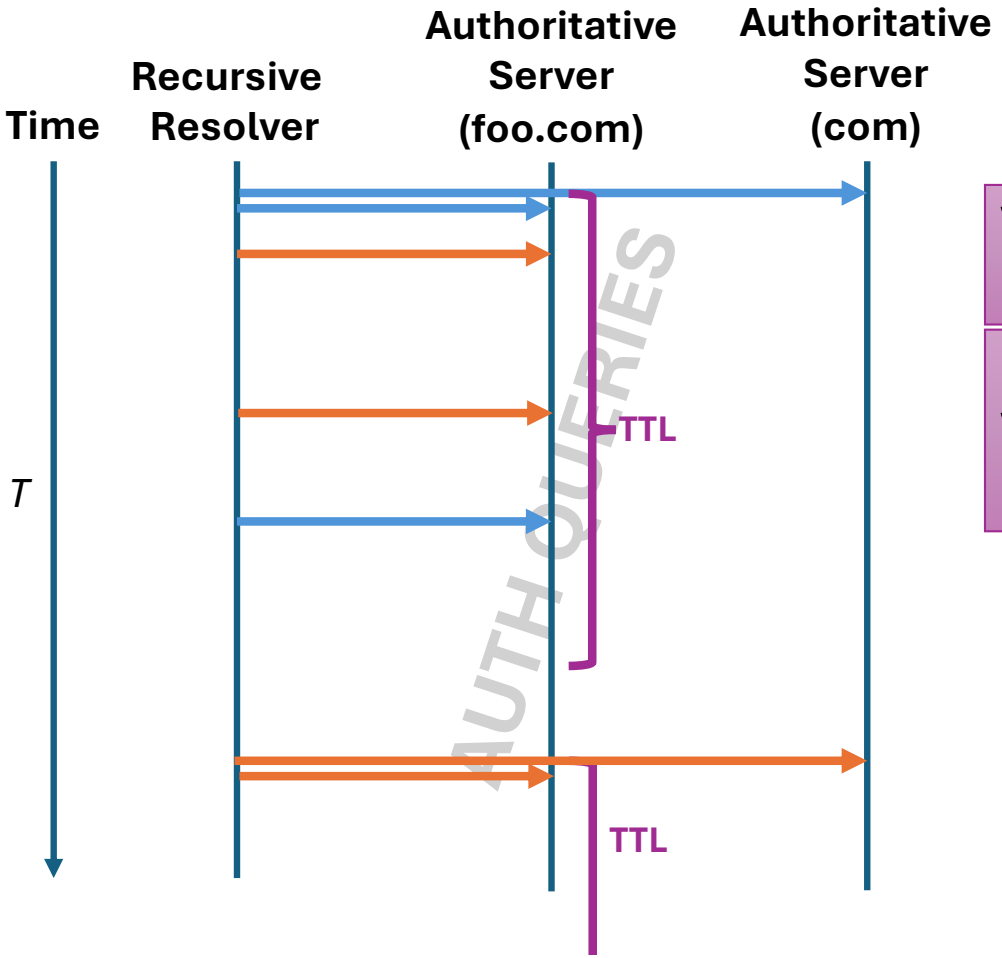



During Time Period *T*:

**When recursive queries > TTLs:**
auth queries = TTLs

**When recursive queries ≤ TTLs:**
auth queries = recursive queries

# Caching Dynamics - Observations

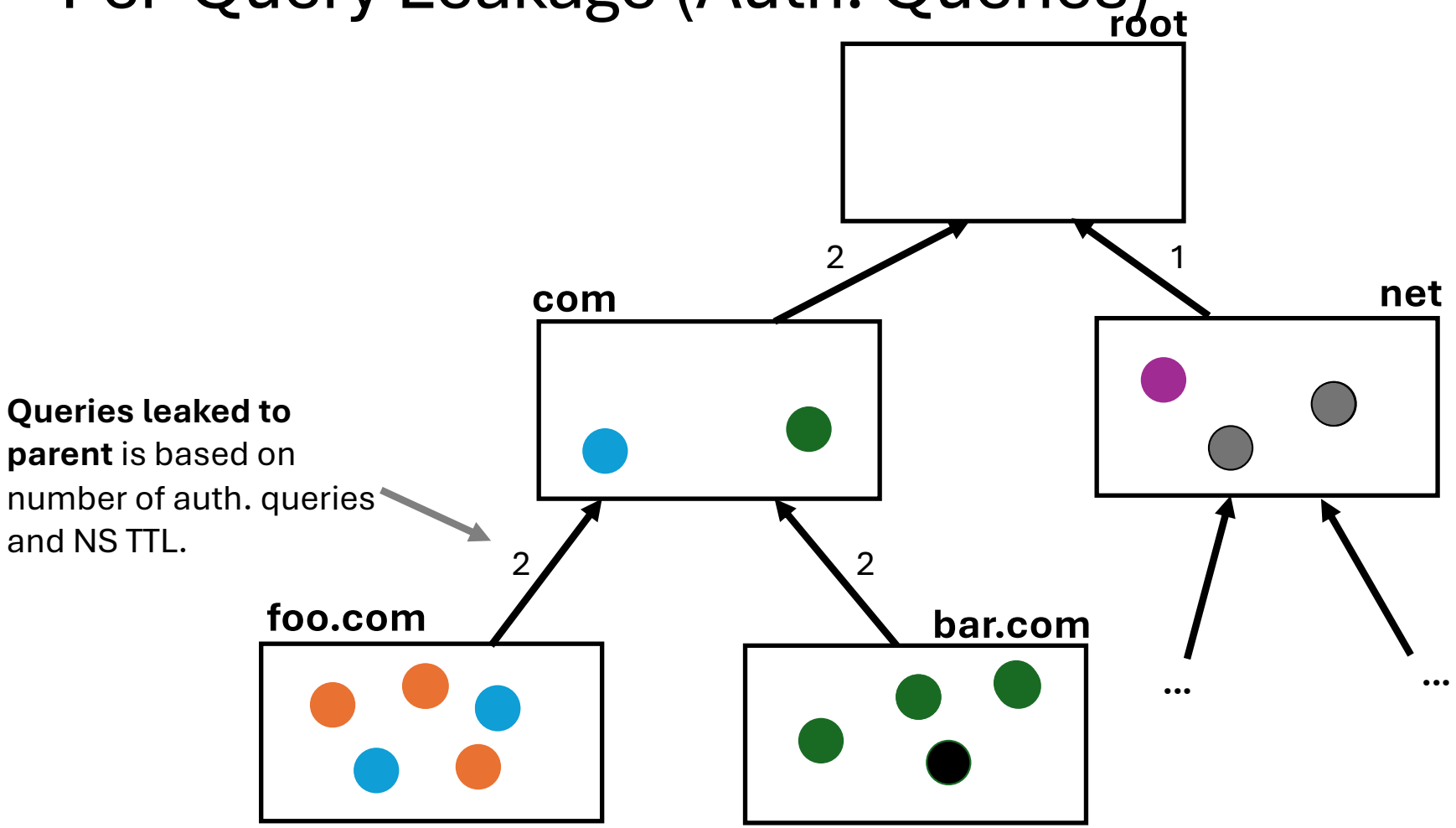



During Time Period *T*:

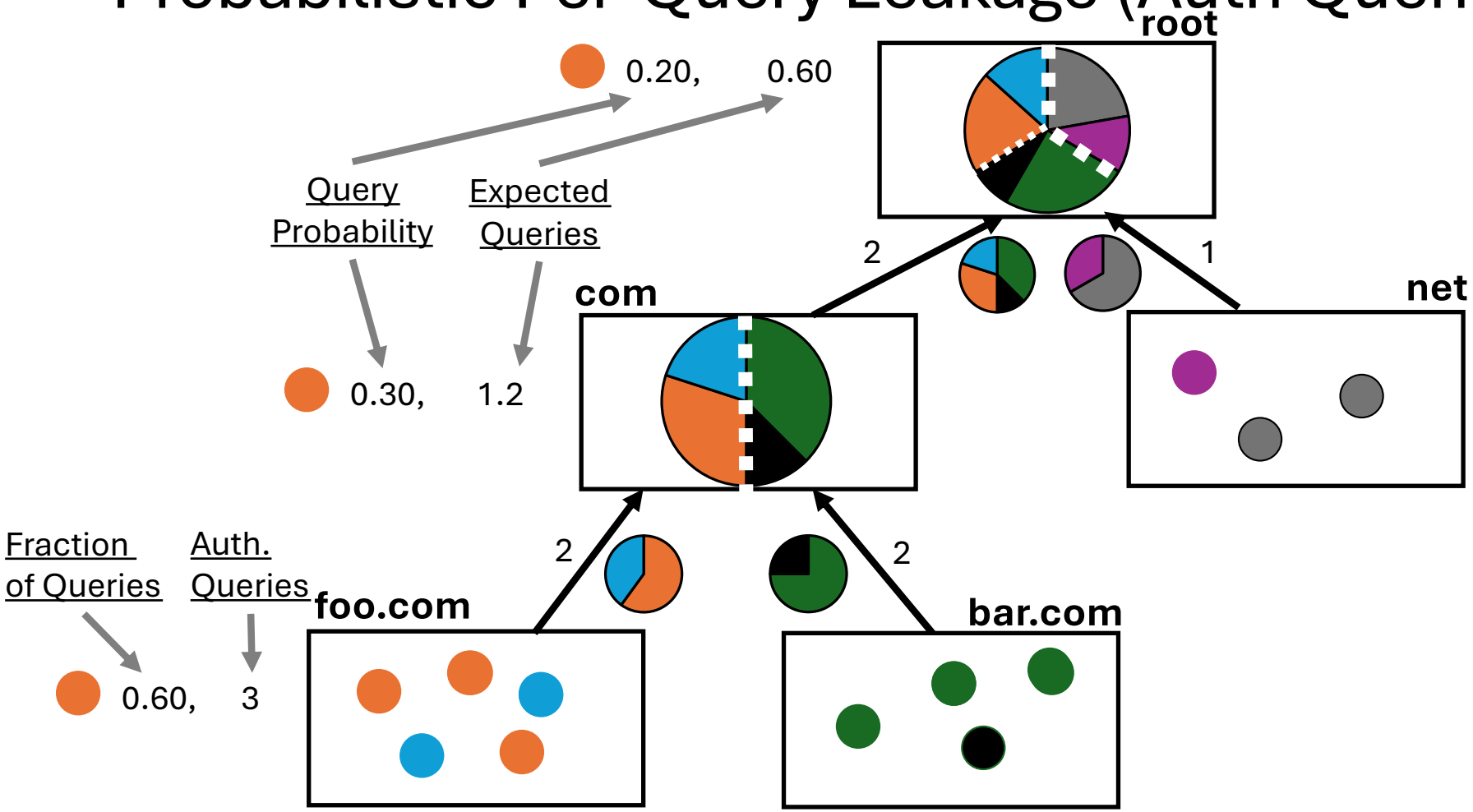
**When auth queries > NS TTLs:**
auth queries to parent = TTLs

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

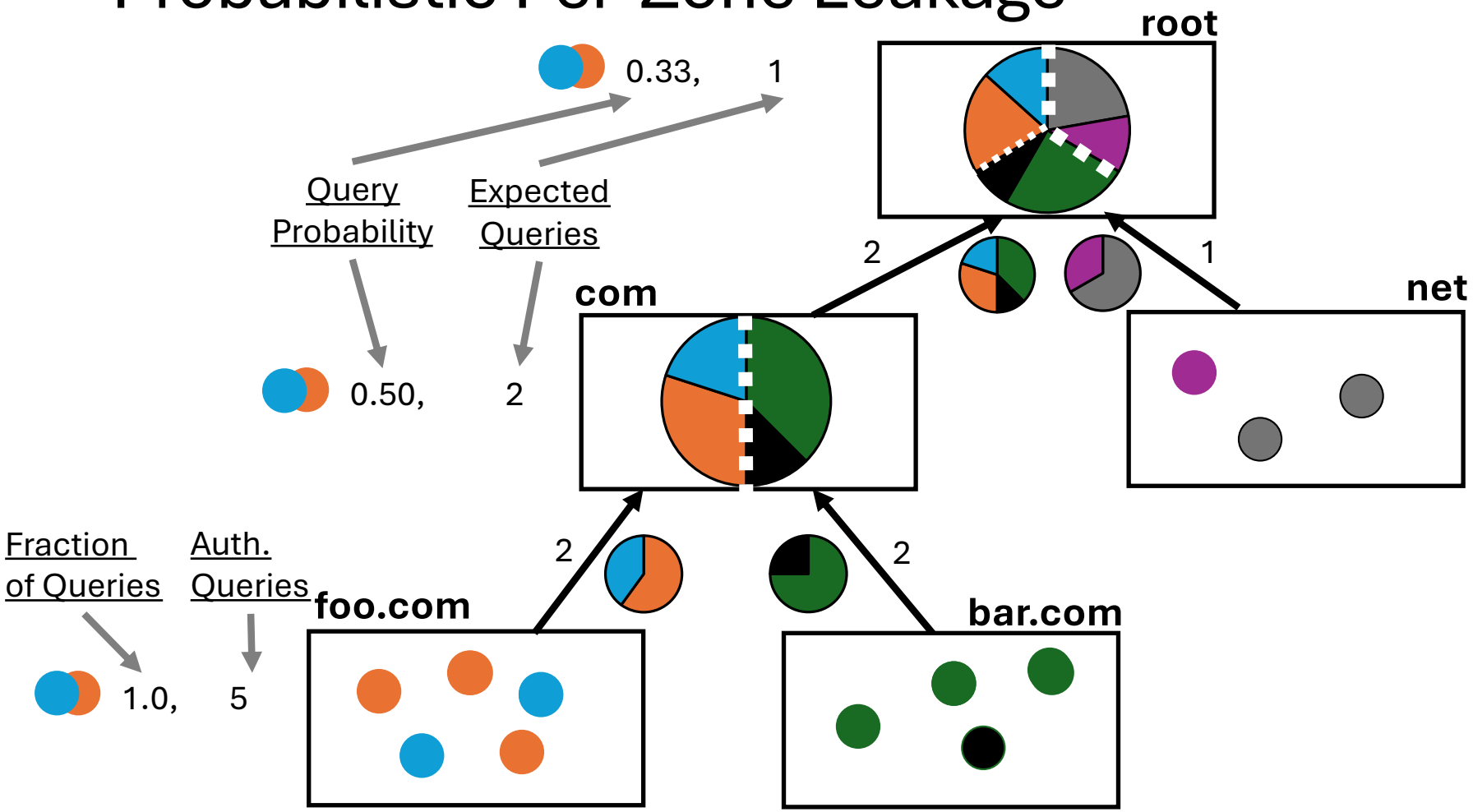
# Per-Query Leakage (Auth. Queries)



# Probabilistic Per-Query Leakage (Auth Queries)

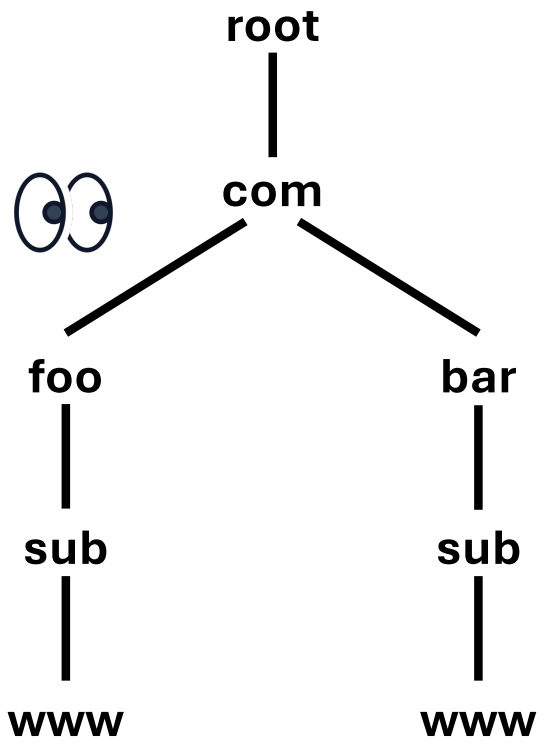


# Probabilistic Per-Zone Leakage



# Privacy Boundaries - Principle

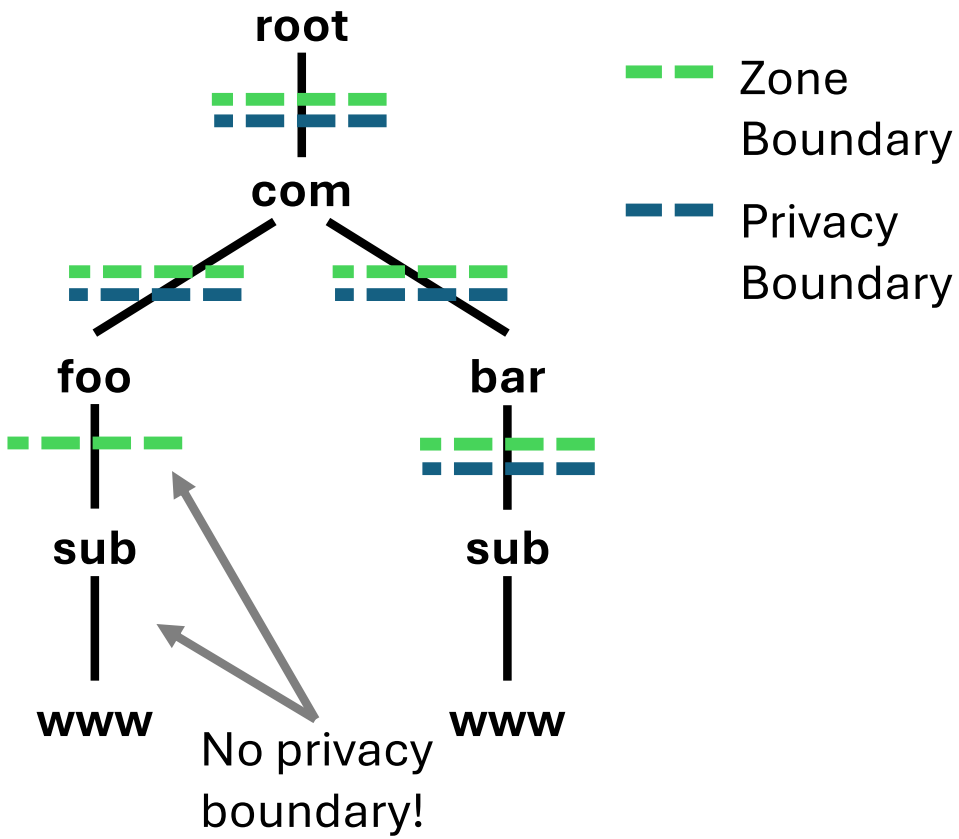
Leakage across boundary must suggest that a new entity can observe queries.




https://www.flaticon.com/free-icon/eyes_7835667

# Privacy Boundaries – Implemented Heuristic

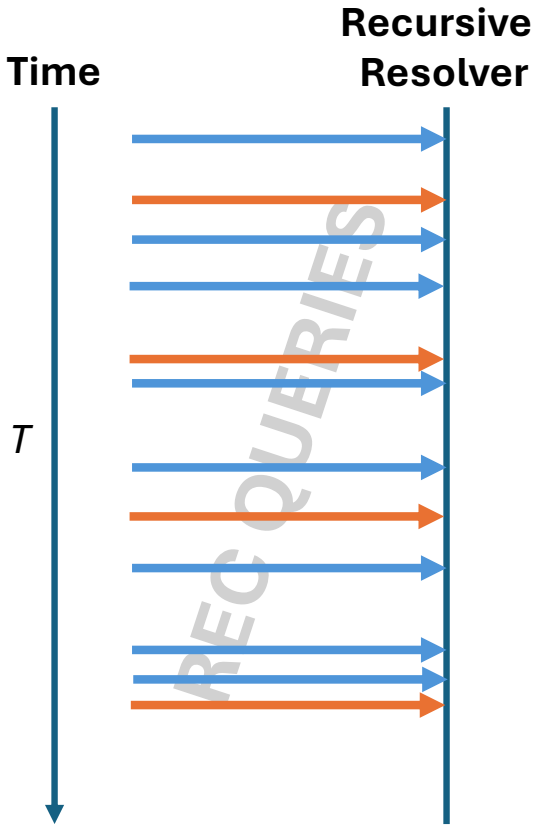
1. Zone boundary must exist.
2. Set of ASes for parent (NS) servers includes at least one AS that is distinct from the set of ASes for child (NS) servers.



# Measurement Dataset

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

| | |
|---|---|
| Recursive Queries | 5.0B |
| QNAME-QTYPE Pairs | 5.8M |
| QNAMEs | 3.5M |
| DNS Zones | 347K |
| Privacy Boundary Groups | 290K |
| Parent Domain is root | 492 (0.2%) |
| Parent Domain is TLD | 254K (87%) |
| Parent Domain is below TLD | 36K (12%) |



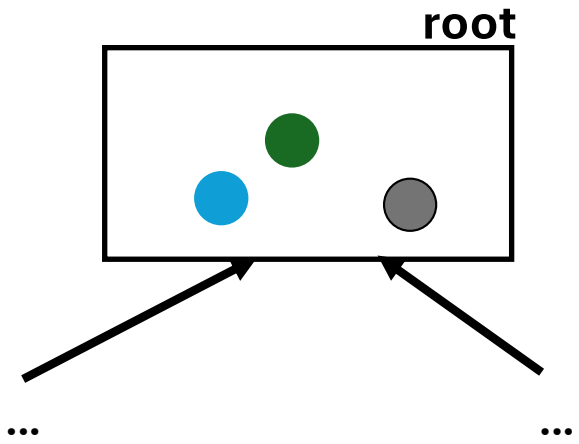
# Results (Yay! and meh.)

- For 87% of privacy domains (96% of queries) the parent 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 privacy domains, *all QNAMEs are leaked* to parent.
  - Yay! QNAME minimization keeps QNAMEs to minimal disclosure.
  - Meh. 74% of QNAMEs are associated with fewer than five recursive queries
  - Meh. For 98% of privacy domains, only 10 or fewer QNAMEs leaked to parent.
- For 99% of privacy domains, QNAME leakage rate to root is ≤65%
  - Yay! QNAME minimization keeps the root from seeing these queries.
  - Meh. For half of privacy domains, only a single QNAME is represented
  - Meh. Only 1.7% of privacy domains leak one or more QNAMEs to root servers.

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

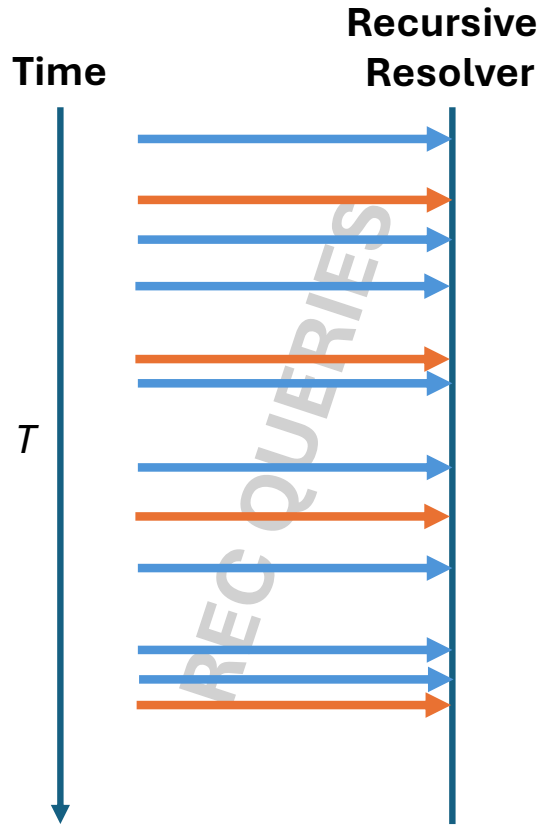
# Other QNAME Minimization Costs

- 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].



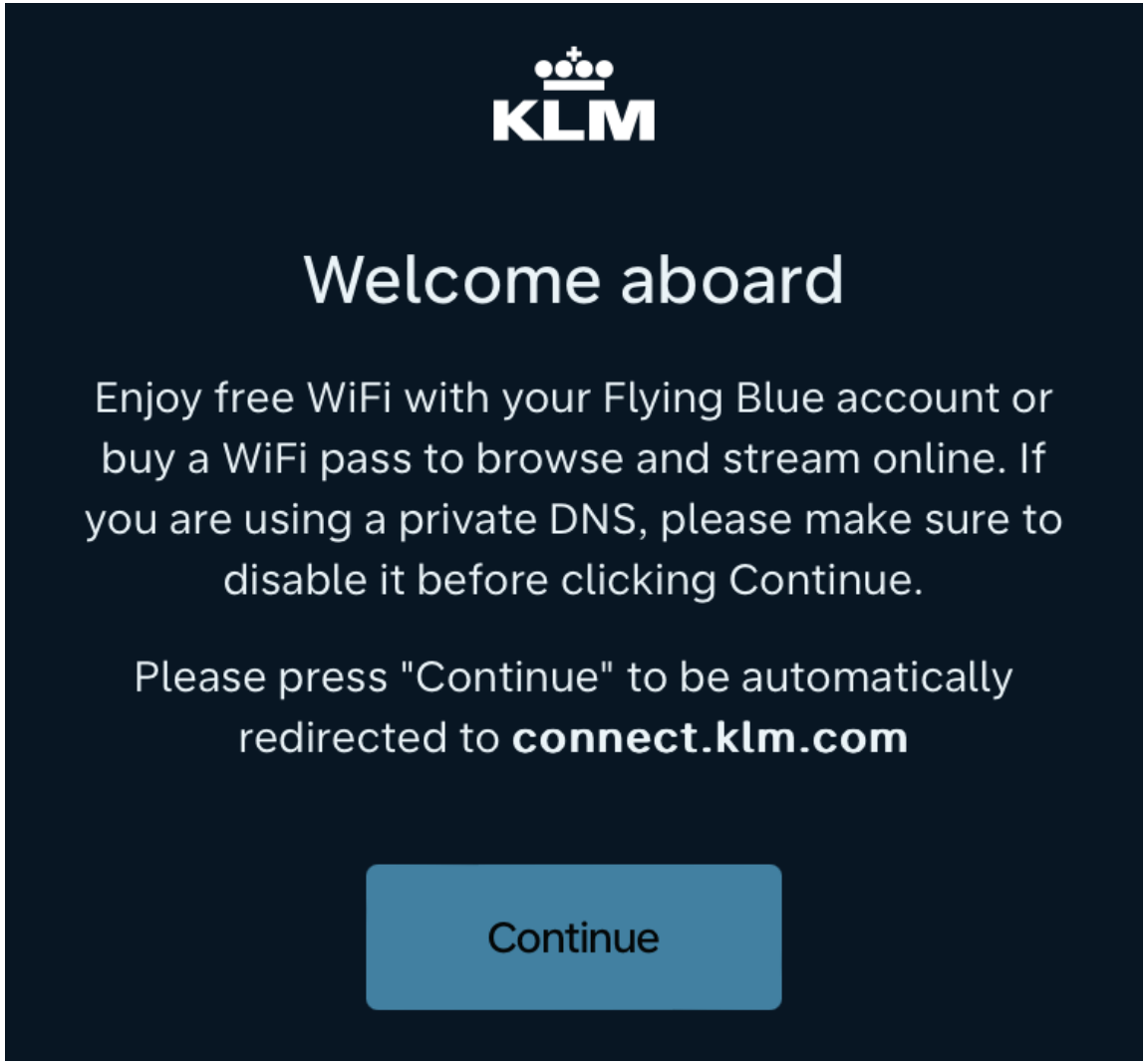
# Summary

- 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



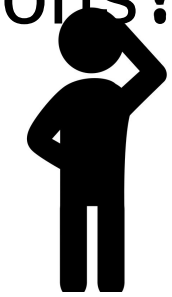
# Hard Questions

- Do organizations understand the costs and benefits of QNAME minimization?
- Did organizations ask for QNAME minimization?
- Is this something that organizations are enabling or disabling explicitly?  Or is it typically based on default configuration behavior?
- What do organizations gain or lose by continuing the practice?
- Who controls the destiny of QNAME minimization?




“If you are using a private DNS, please make sure to disable it…”

Questions?



casey@byu.edu

BYU