RESOLVER TRAFFIC: WHAT DOES IT LOOK LIKE?

João Damas
Mónica Cortés Sack
We look a lot at traffic between resolvers and authoritative servers.

and very little at traffic between recursive resolvers and their clients.

Is it still the Internet? or maybe something similar to the Internet?
What traffic we are looking at
Where is the data?

- Hard to get a hold of this sort of traffic
- Concerns about PII, exposing customer issues, etc
How to look at the data

• PacketQ is an excellent tool
  • no longer maintained as open source but works for 90% of your needs
• Additional home-grown software to do the remaining analysis
The sample
RCODE distribution
Infrastructure domains
Infrastructure domains
zoom
CDNs
ADs
Entertainment sites
wtf sites
Security services
Social
Main domains
EDNS usage
DNSSEC - do
DNSSEC - dnskey
What now?

- Study how parameter changes at resolves affect their behaviour towards clients

- Followup work: study impact of changes in server configuration and actions on load handling
  - how does min_ttl help/harm
  - can prefetch help? When and how?
Acknowledgements

This study was sponsored by a Comcast research grant
Questions?