

Serverless DNS Analytics using ENTRADA 2.0

Moritz Müller | SIDN Connect 2019

28 november 2019



Remember ENTRADA?

- Open source tool that handles large amounts of DNS traffic
 - It processes, converts and enriches PCAP data
 - It stores the data
 - It provides interfaces for data analytics
- Deployed by multiple TLDs



What can you do with DNS traffic?

A First Look at QNAME Minimization in the Domain Name System

Wouter B. de Vries¹, Quirin Scheitle², Moritz Müller^{1,3}, Willem Toorop⁴,
Ralph Dolmans⁴, Roland van Rijswijk-Deij^{1,4}

¹University of Twente, ²TUM, ³SIDN Labs, ⁴NLnet Labs

Abstract. The Domain Name System (DNS) is a critical part of network and Internet infrastructure; DNS lookups precede almost any user request. DNS lookups may contain private information about the sites and services a user contacts, which has spawned efforts to protect privacy of users, such as transport encryption through DNS-over-TLS or DNS-over-HTTPS. In this work we provide a first look on the *resolver-side* techniques of query



What can you do with DNS traffic?

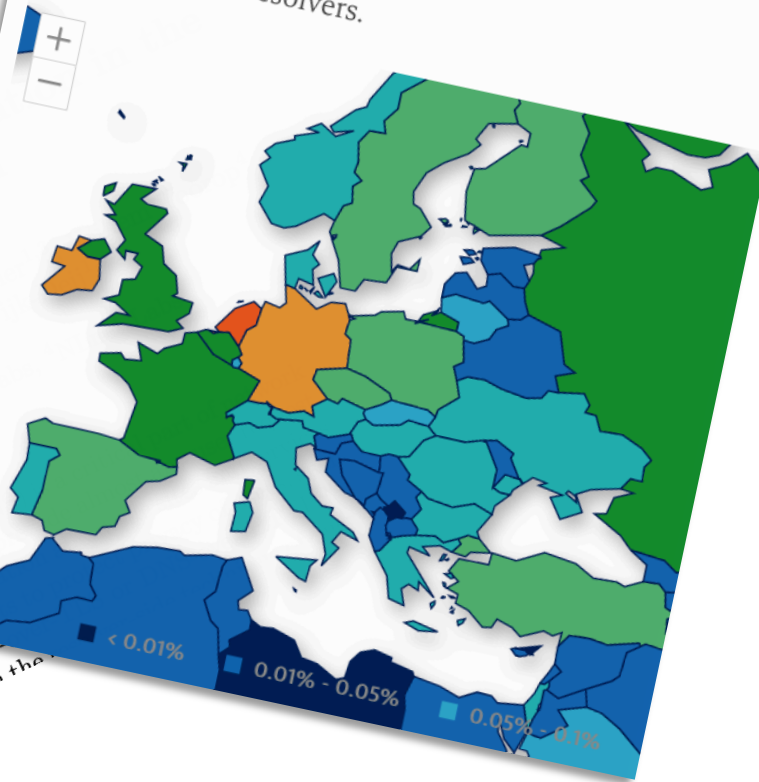
A First Look at QNAME Minimization in the Domain Name System

Wouter B. de Vries¹, Quirin Scheitle², Moritz
Ralph Dolmans⁴, Roland van
¹University of Twente, ²TUM, ³

Abstract. The Domain Name System and Internet infrastructure; DNS lookups may contain private user contacts, which has spawned as transport encryption through DNS. In this work we provide a first look on the

Resolverlocaties

Locaties van alle resolvers.



What can you do with DNS traffic?

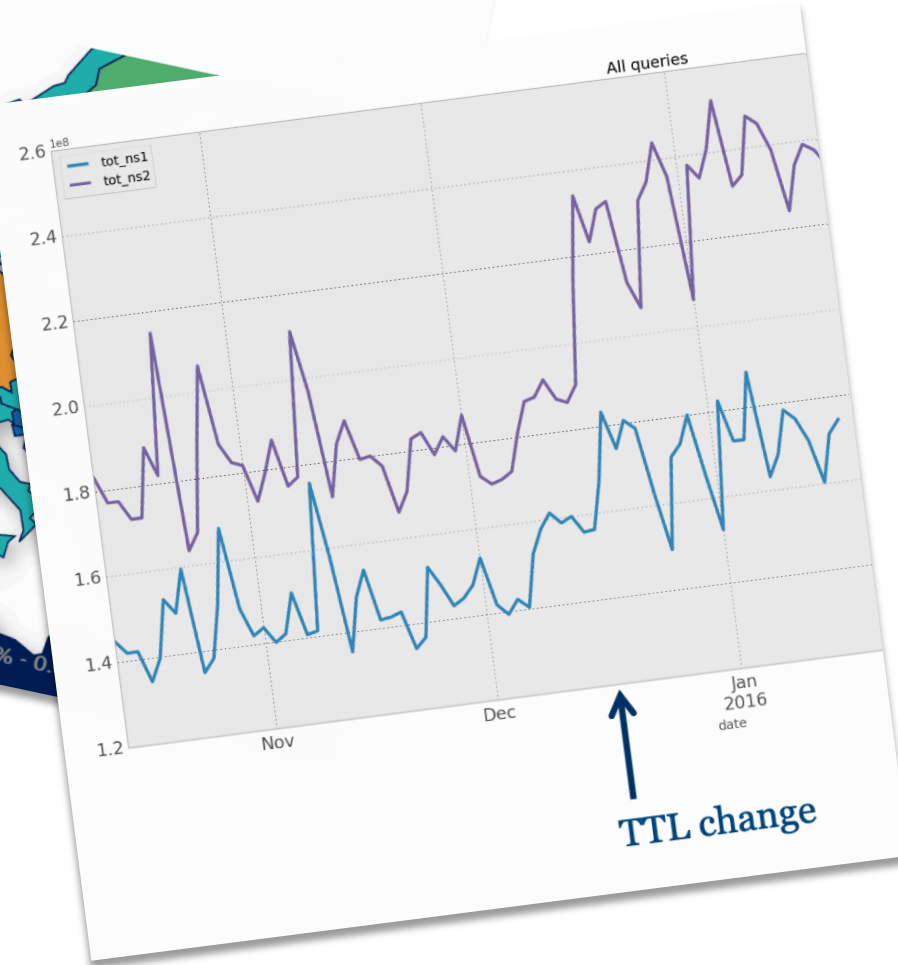
A First Look at QNAME Minimization in the Domain Name System

Wouter B. de Vries¹, Quirin Scheitle², Moritz
Ralph Dolmans⁴, Roland van
¹University of Twente, ²TUM, ³

Abstract. The Domain Name System and Internet infrastructure; DNS lookups may contain private user contacts, which has spawned a user contacts encryption through DNS as transport encryption through DNS. In this work we provide a first look on the

Resolverlocaties

Locaties van alle resolvers.



What can you do with DNS traffic?

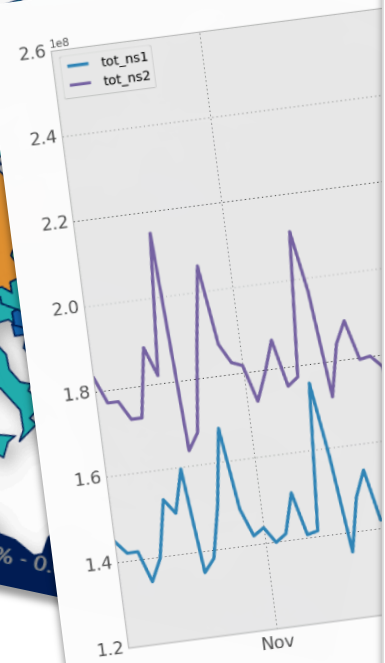
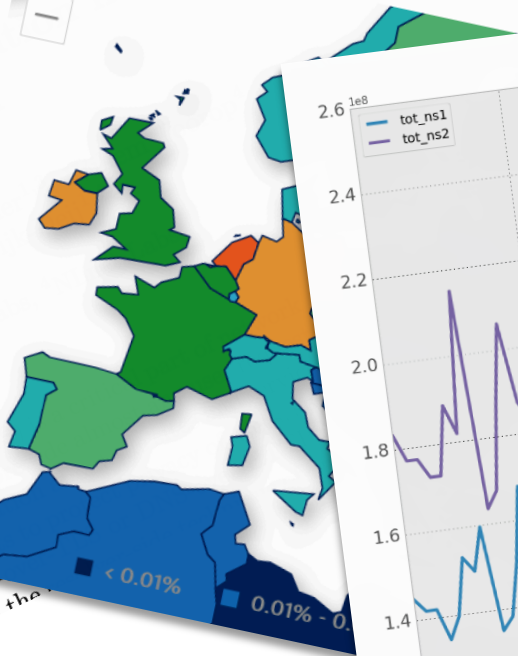
A First Look at QNAME Minimization in the Domain Name System

Wouter B. de Vries¹, Quirin Scheitle², Moritz
Ralph Dolmans⁴, Roland van
¹University of Twente, ²TUM, ³

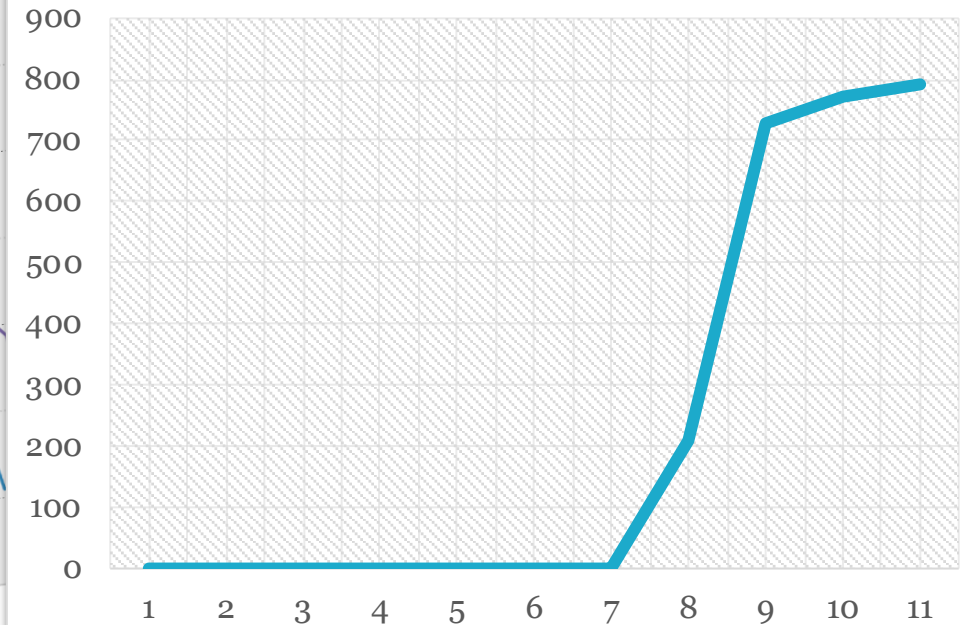
Abstract. The Domain Name System and Internet infrastructure; DNS lookups may contain private user contacts, which has spawned as transport encryption through DNS. In this work we provide a first look on the

Resolverlocaties

Locaties van alle resolvers.



Queries www.rabobank.vervang-service.nl.



TTL change

Drawbacks of ENTRADA 1.0

ENTRADA 1.0 runs on Hadoop

- Setup and maintenance costs time and money
- Requires knowledge of Hadoop
- Requires hardware or software cluster



This is why we introduce: ENTRADA 2.0

New Features

- Serverless DNS analytics
- Support for multiple SQL query engines
- Quality of Services Monitoring, round-trip time (RTT) analysis
- Easier deployment using Docker

Serverless DNS analytics

~~Serverless DNS analytics~~

DNS analytics on the computer of someone else

~~Serverless DNS analytics~~

DNS analytics on the computer of someone else

- No need to deploy any server
- No hardware/network maintenance cost
- Only pay for amount of data analysed

ENTRADA will:

- Create database schema
- Convert, upload and optimize data

DNS analytics on the computers of Amazon

Support for Amazon Web Services (AWS)

- S3 storage
- Athena SQL-query engine
- Pricing; \$5 per TB of scanned data



Quality of Service Monitoring

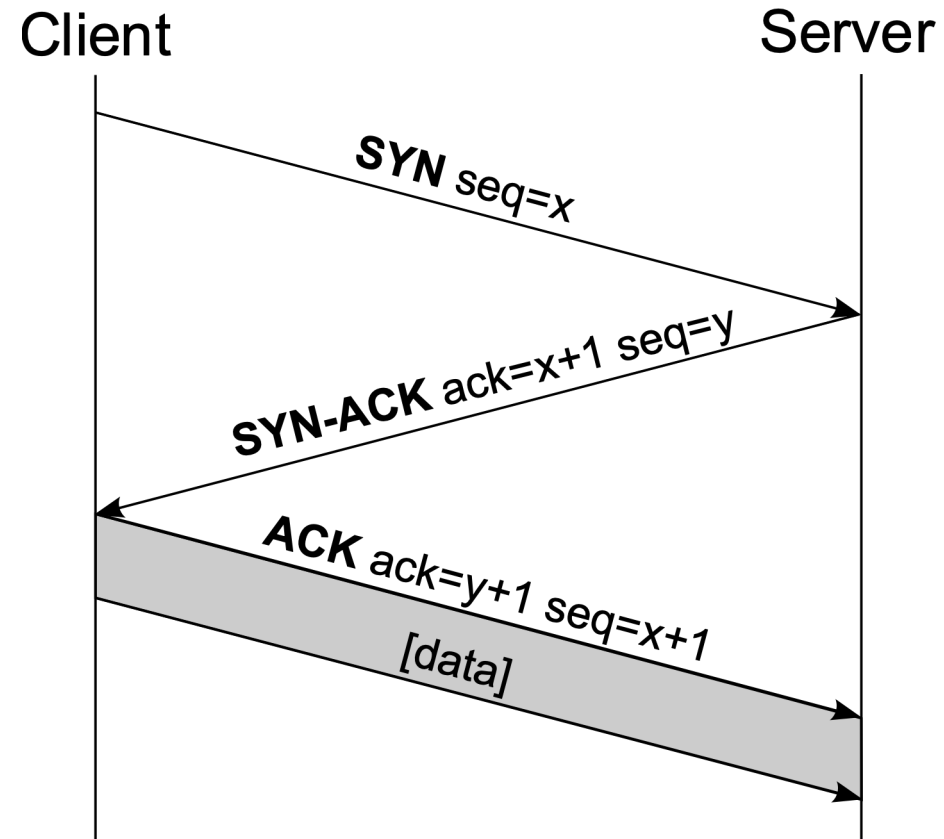
- Understanding how clients perceive your DNS service is crucial for measuring reliability, e.g.:
 - are there issues with my uplink?
 - are there issues with my routing/anycast?
 - are there issues with my client?



Quality of Service Monitoring

- External monitoring platforms exist, but:
 - they often cost money
 - they don't reflect your real clients
 - they don't provide easy to interpret interfaces

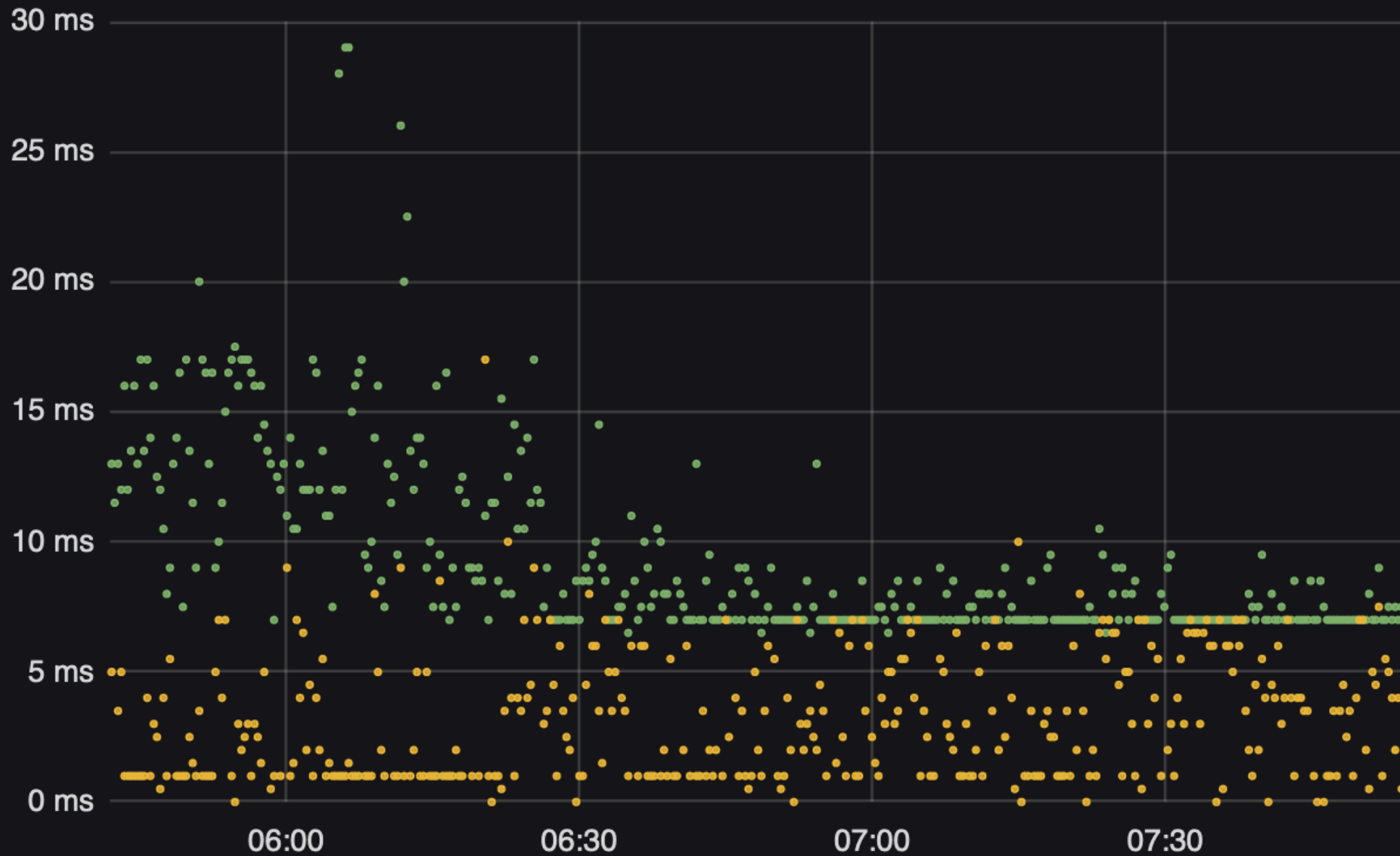
Quality of Service Monitoring with TCP



$$\text{dif}(\text{SYN ACK} - \text{ACK}) = \text{RTT}$$

i

TCP RTT



— Handshake — Packet

Links

- Introduction: <https://www.sidnlabs.nl/nieuws-en-blogs/tijd-voor-entrada-2-0>
- Documentation: <https://entrada.sidnlabs.nl/>
- Source Code: <https://github.com/SIDN/entrada>

- Contact:
 - Maarten Wullink (marten.wullink.sidn.nl)
 - Moritz Müller (moritz.muller@sidn.nl)