Serverless DNS Analytics using ENTRADA 2.0

Moritz Müller | SIDN Connect 2019

28 november 2019

SIDN LABS

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

Photo by Sharon McCutcheon on Unsplash

What can you do with DNS traffic?

A First Look at QNAME Minimization in the Domain Name System

Wouter B. de Vries[1], Quirin Scheitle[2], Moritz Müller[1,3], Willem Toorop[4], Ralph Dolmans[4], Roland van Rijswijk-Deij[1,4]

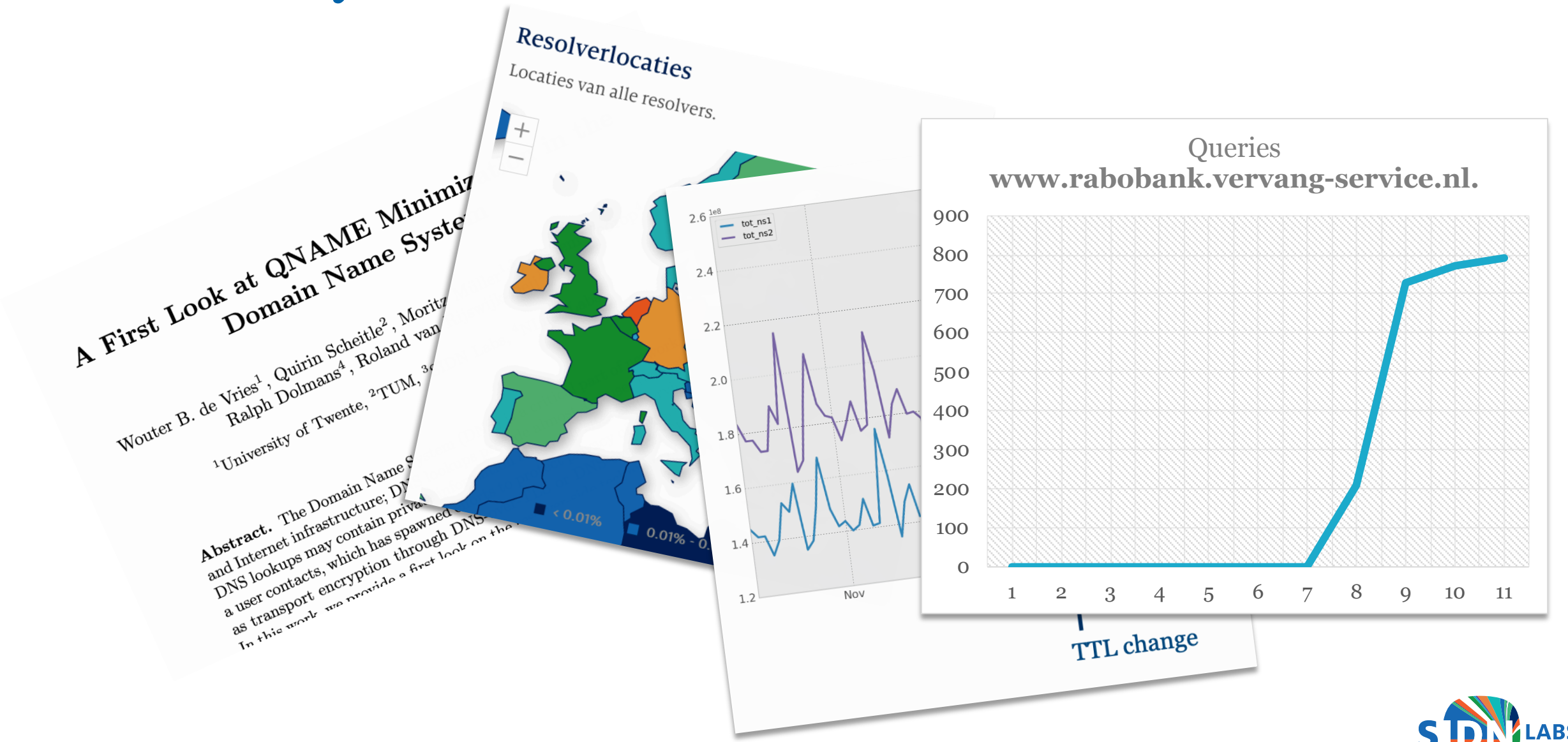
[1]University of Twente, [2]TUM, [3]SIDN Labs, [4]NLnet Labs

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 technique of query

What can you do with DNS traffic?

What can you do with DNS traffic?

What can you do with DNS traffic?



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

SIDN LABS

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?

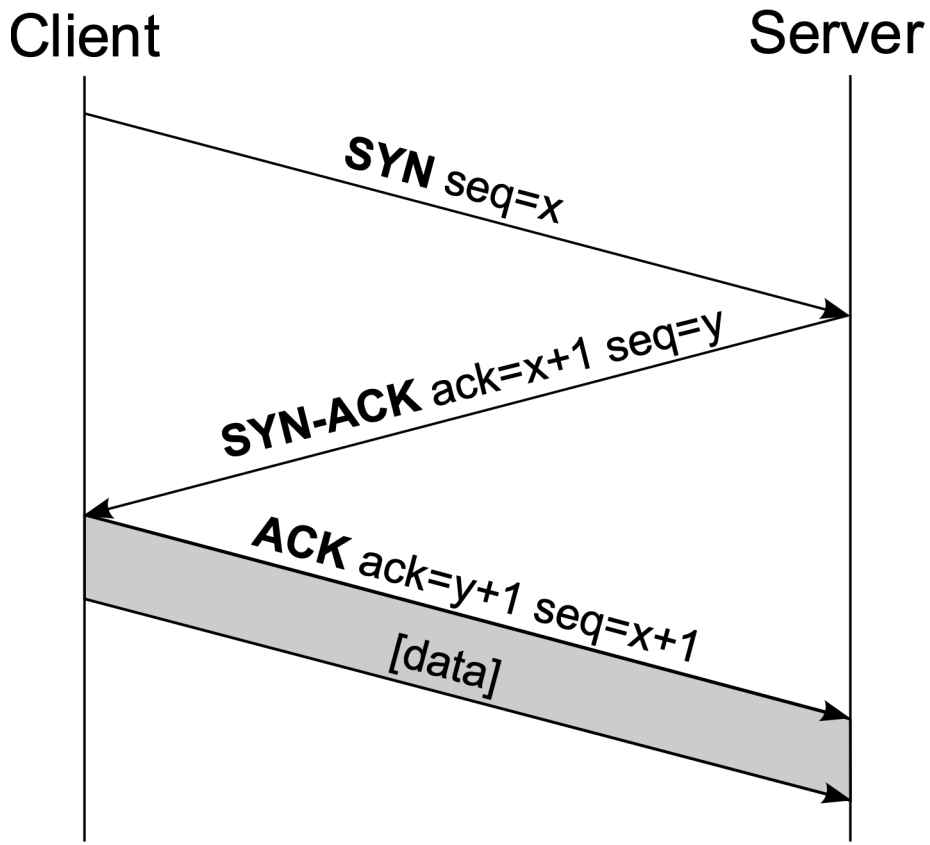
Photo by Icons8 Team on Unsplash

Quality of Service Monitoring

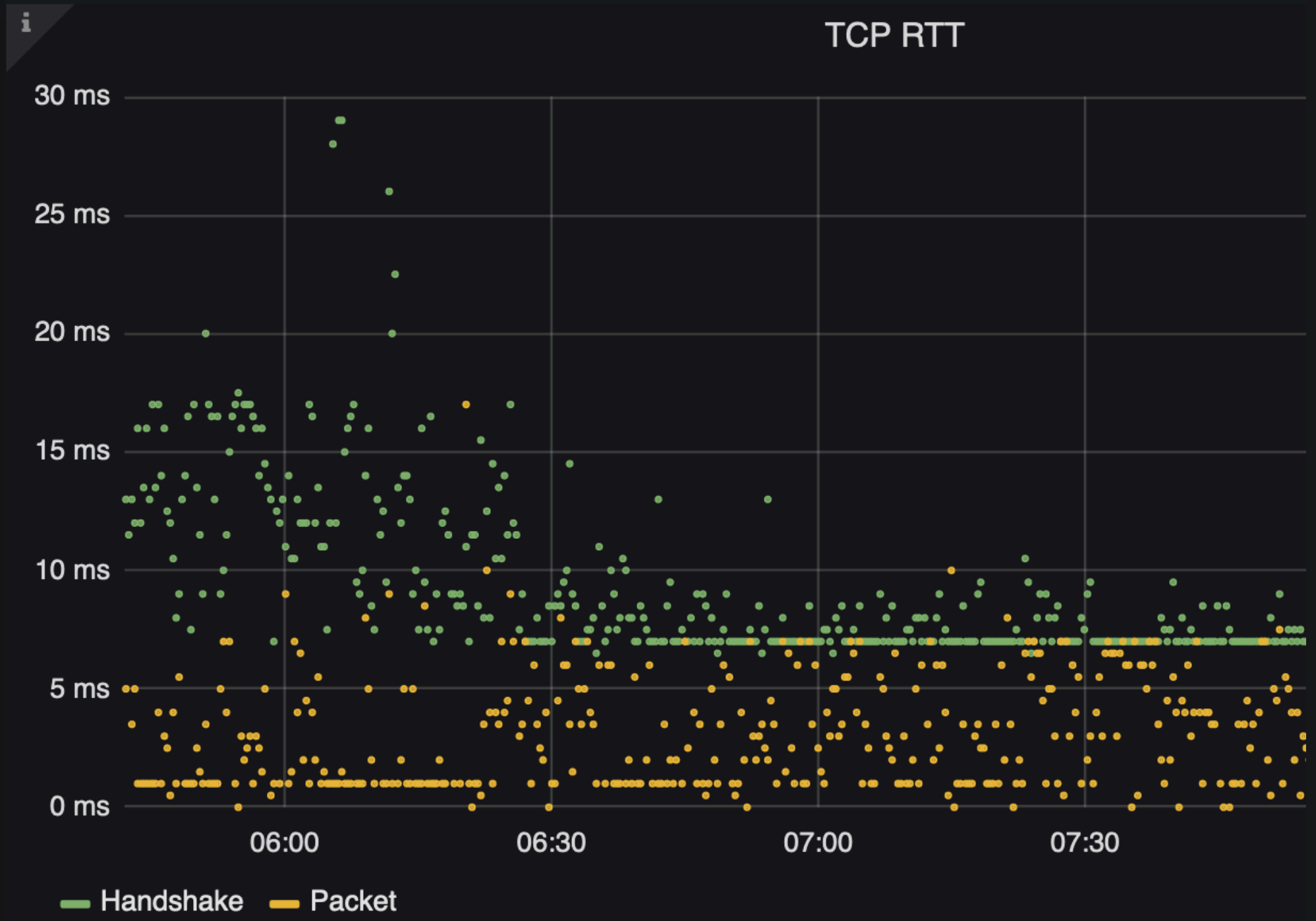
- External monitoring platforms exist, but:
  - they often cost money
  - they don’t reflect your real clients
  - they don’t provide easy to interpret interfaces

SDN LABS

Quality of Service Monitoring with TCP



dif(SYN ACK – ACK) = RTT


TCP RTT
30 ms
25 ms
20 ms
15 ms
10 ms
5 ms
0 ms
06:00
06:30
07:00
07:30
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)