A Resolver Reputation System (ResRep)

June 4, 2014

CENTR Jamboree, R&D workshop

Marco Davids

SIDN labs
Internet Research & Innovation

The goal of the project:

- To investigate if assigning some sort of reputation to resolvers can help in mitigating abuse.

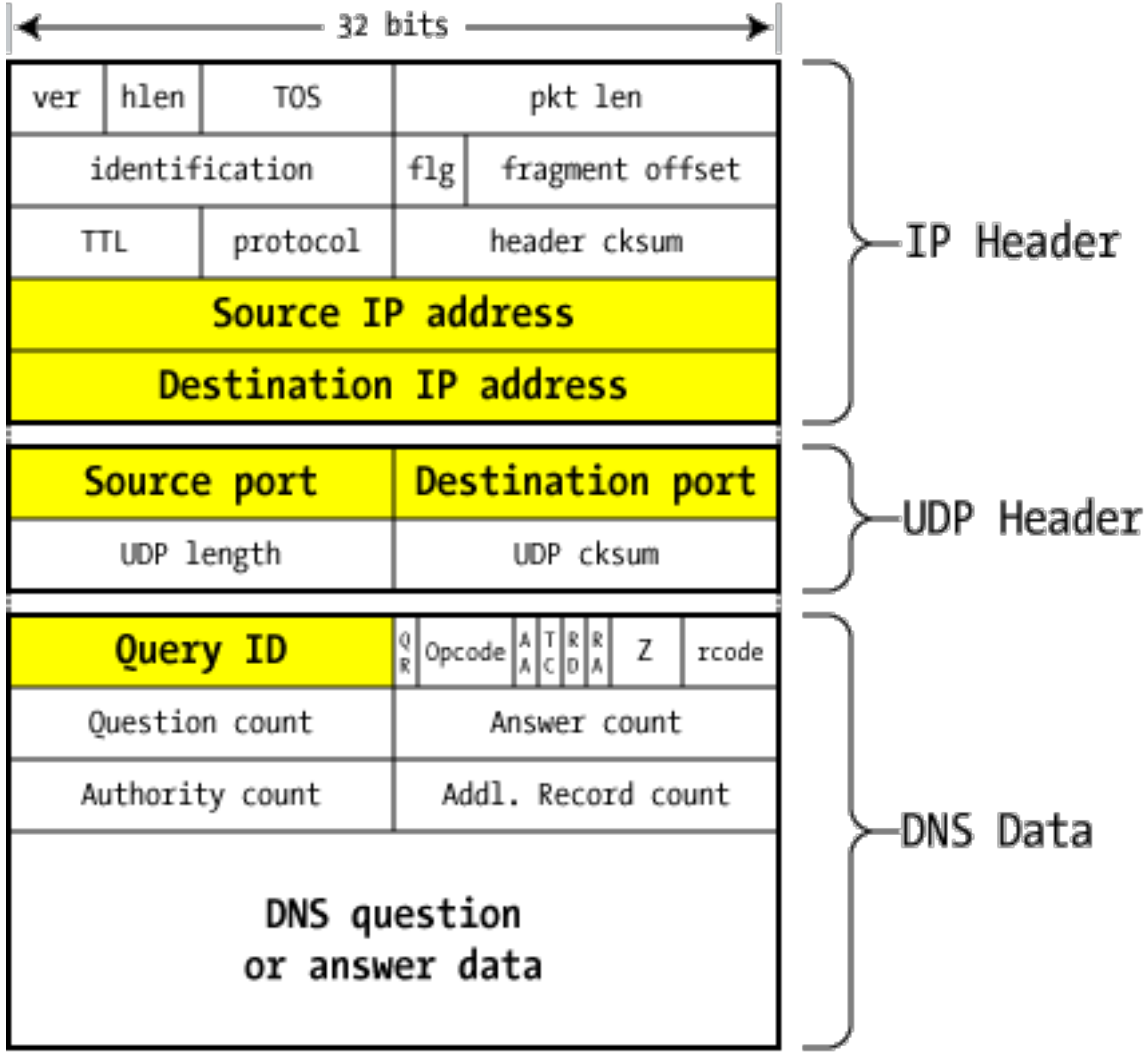
- To gather experience on data-science (analyzing ‘bigdata’).

SIDN labs
Internet Research & Innovation

SIDN

How?

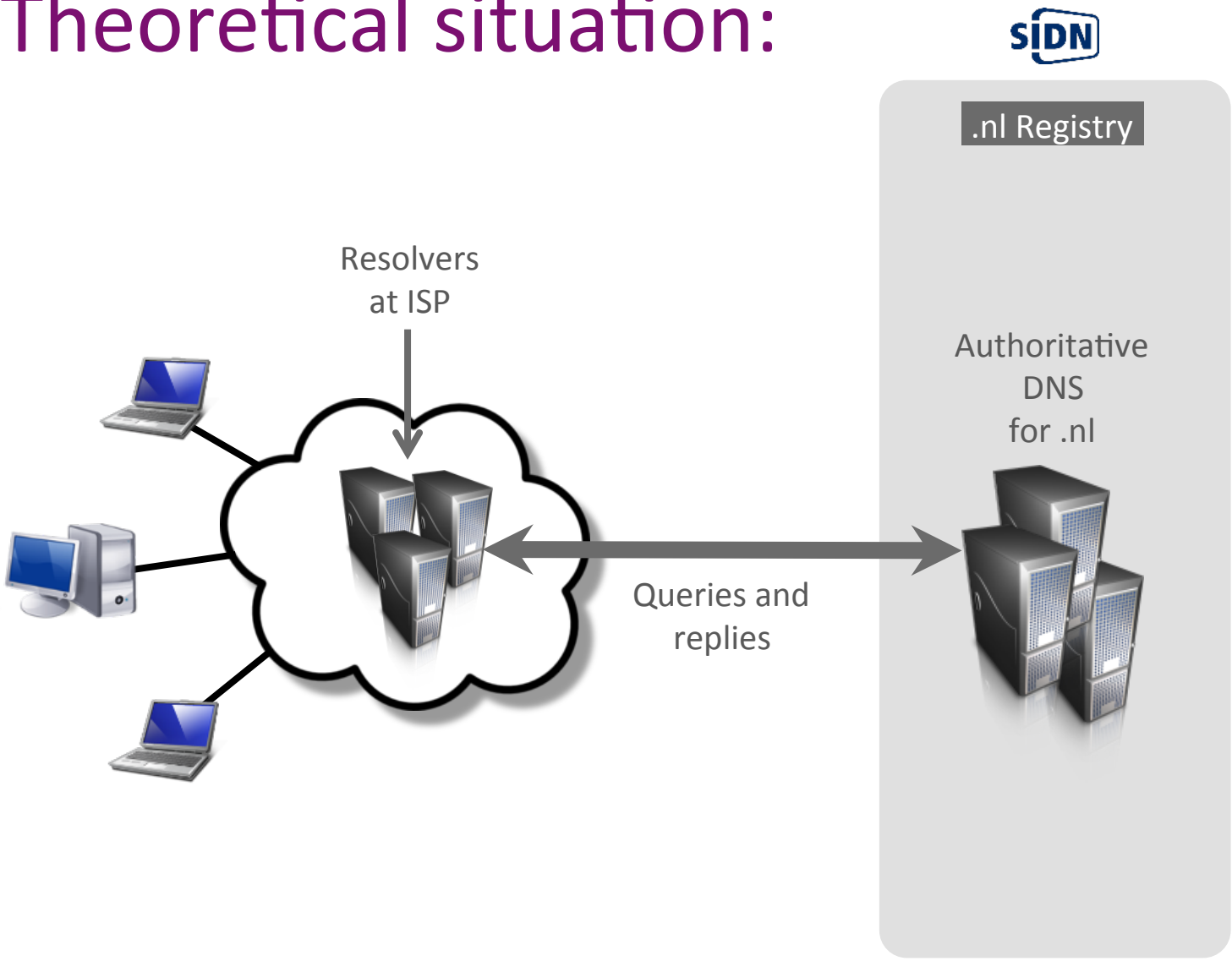
By ‘fingerprinting’ specific resolver-behavior.



SIDN labs
Internet Research & Innovation

SIDN

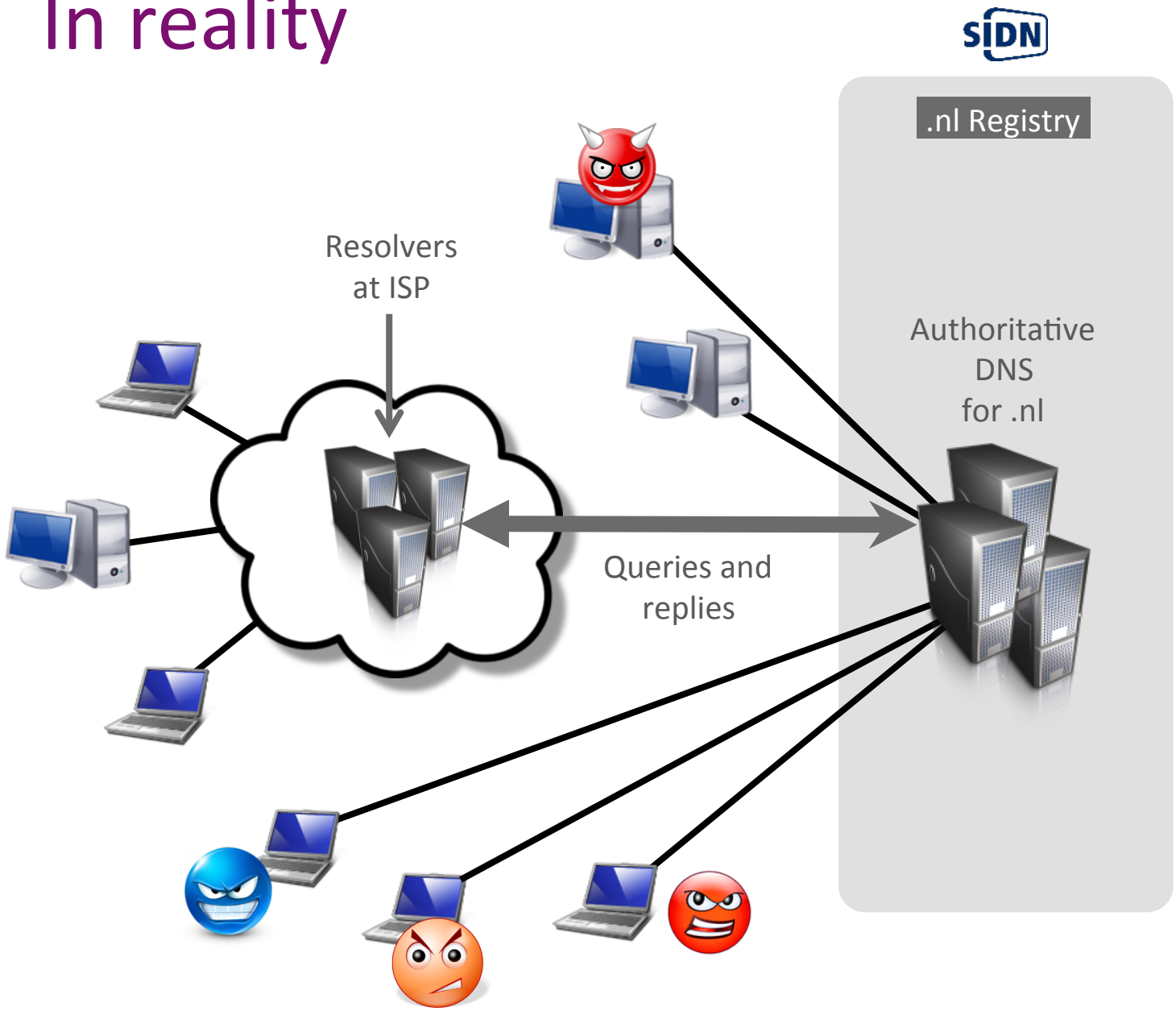
Theoretical situation:



Normal resolvers:

- Large ISP's.
- Home users (privacy-issue).
- 'Domainers' (on the edge).
- Validating (or not).
- In sensor-networks (RIPE Atlas DNSmon etc.).

In reality



Malicious systems:

- Spam-runs.
- Cutwail and other spambotnets.
- DNS-amplification DDoS with *spoofed* addresses.
- Open resolvers.

But also:

- Legacy software, or poorly configured software.
- Things we do not yet fully understand.

SIDN labs
Internet Research & Innovation

SIDN

Some examples of what we look at…

- Ratio between ANY / non-ANY queries.
- REFUSED (asking for .com for example).
- Only asking second-level.
- Triggering TC-bit (RRL truncated answers).
- Only use TCP.
- Relatively many NXDOMAIN’s.

SIDN labs
Internet Research & Innovation

SIDN

As well as…

- Relatively many MX-queries?
- Are they large resolvers?
- Do they visit us regularly?
- Are they home-resolvers (exclude them for privacy reasons).
- Are they validating?
- Do they respect our TTL?
- Do they only use source port 53?

Etc.

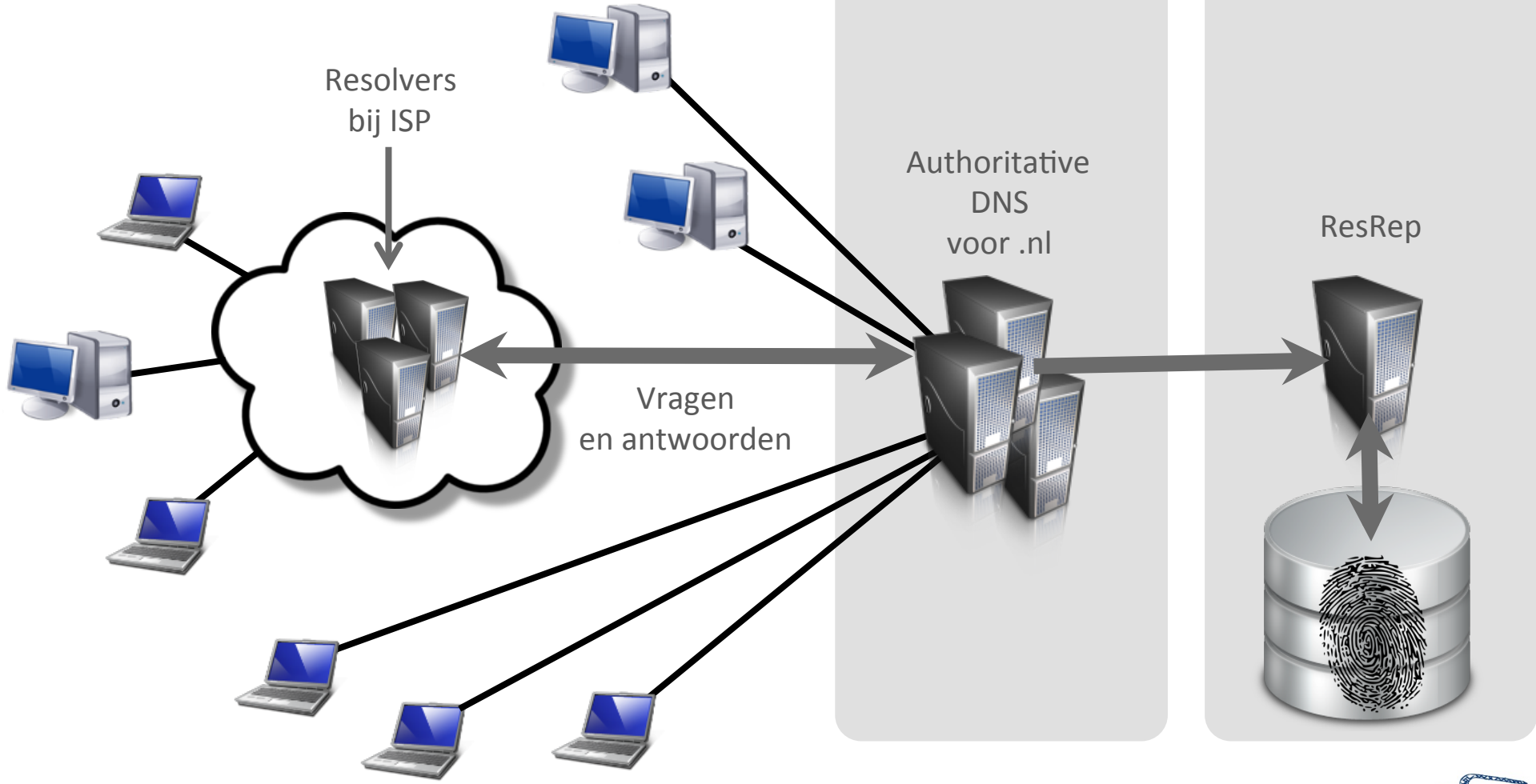
SIDN labs
Internet Research & Innovation

SIDN

Example:

170	0ill69fqh.nl.	11
171	7nvg0ei3767675.nl.	11
172	7koi83.nl.	11
173	7io3k704uwt12.nl.	11
174	0hzs32a.nl.	11
175	7b8pk10022j21z.nl.	11
176	785o56a3p1.nl.	11
177	99u9xh6z7a2e7.nl.	11
178	7q9h3.nl.	11
179	0jxetc86hg4oxh.nl.	11
180	0n5hf0770wsa9.nl.	11
181	0i39d.nl.	11
182	7k7zv.nl.	11
183	7n4dmq91i1ia4.nl.	11
184	794j2q8n.nl.	11
185	0k3yl8.nl.	11
186	77r0vvg4.nl.	11
187	7dt80.nl.	11
188	7ew5140.nl.	11
189	99w1dx335rp.nl.	11

Resolver Reputation System:



Example of first prototype

```
SELECT * , SUM( qps_refused ) AS sum_refused
FROM `resolvers_daily`
WHERE qps_refused <>0
AND qps_refused = qps_tot
GROUP BY ip
ORDER BY sum_refused DESC
LIMIT 0 , 30
```

Profiling [Rechtstreeks] [Wijz

Paginanummer: 1 > >>

Toon : 30 rij(en) beginnend bij 30 in horizontaal modus en herhaal kopregels na 100 cellen

Sorteren op sleutel: Geen

+ Opties

batch	ip	qps_tot	qps_a	qps_aaaa	qps_mx	qps_any	qps_nx	qps_tc	qps_rd	qps_refused	qps_no3rdlvl	sum_refused
1395745508	217.12	0.0283333	0.0283333	0	0	0	0	0	0.0283333	0.0283333	0	10.309996260330081
1395747308	93.171	0.0233333	0.0216667	0	0	0	0	0	0	0.0233333	0.0216667	0.8566664725076407
1395747308	64.140	0.0166667	0.0166667	0	0	0	0	0	0.0166667	0.0166667	0	0.6800001533702016
1395747308	63.142	0.00666667	0.00666667	0	0	0	0	0	0.00666667	0.00666667	0	0.5549998548813164
1395746108	69.76.	0.00166667	0.00166667	0	0	0	0	0	0.00166667	0.00166667	0	0.5400001718662679
1395746708	78.93.	0.0283333	0.0283333	0	0	0	0	0	0.0283333	0.0283333	0	0.5399998284410685
1395746708	75.184	0.0316667	0.0316667	0	0	0	0	0	0.0316667	0.0316667	0	0.5333334659226239
1395745508	24.67.	0.0266667	0.0266667	0	0	0	0	0	0.0266667	0.0266667	0	0.5283333696424961
1395756608	105.22	0.01	0.01	0	0	0	0	0	0.01	0.01	0	0.5183334478642792
1395749708	92.13.	0.00833333	0.00833333	0	0	0	0	0	0.00833333	0.00833333	0	0.5066665562335402
1395746108	91.183	0.00666667	0.00666667	0	0	0	0	0	0.00666667	0.00666667	0	0.4916675587184727
1395747980	173.12	0.05	0.05	0	0	0	0	0	0.05	0.05	0	0.4566664000600576
1395746108	196.20	0.015	0.015	0	0	0	0	0	0.015	0.015	0	0.4550009367242455
1395745508	92.45.	0.035	0.035	0	0	0	0	0	0.035	0.035	0	0.4549999495223165
1395745508	139.22	0.00833333	0.00833333	0	0	0	0	0	0.00833333	0.00833333	0	0.4399999009910971
1395746708	105.22	0.0166667	0.0166667	0	0	0	0	0	0.0166667	0.0166667	0	0.4249999003484845
1395753007	190.16	0.015	0.015	0	0	0	0	0	0.015	0.015	0	0.4166667622048408
1395746108	94.140	0.035	0.035	0	0	0	0	0	0.035	0.035	0	0.3966677243076265
1395745508	83.110	0.0216667	0.0216667	0	0	0	0	0	0.0216667	0.0216667	0	0.3950000887271017
1395745508	105.22	0.0116667	0.0116667	0	0	0	0	0	0.0116667	0.0116667	0	0.39333350863307714

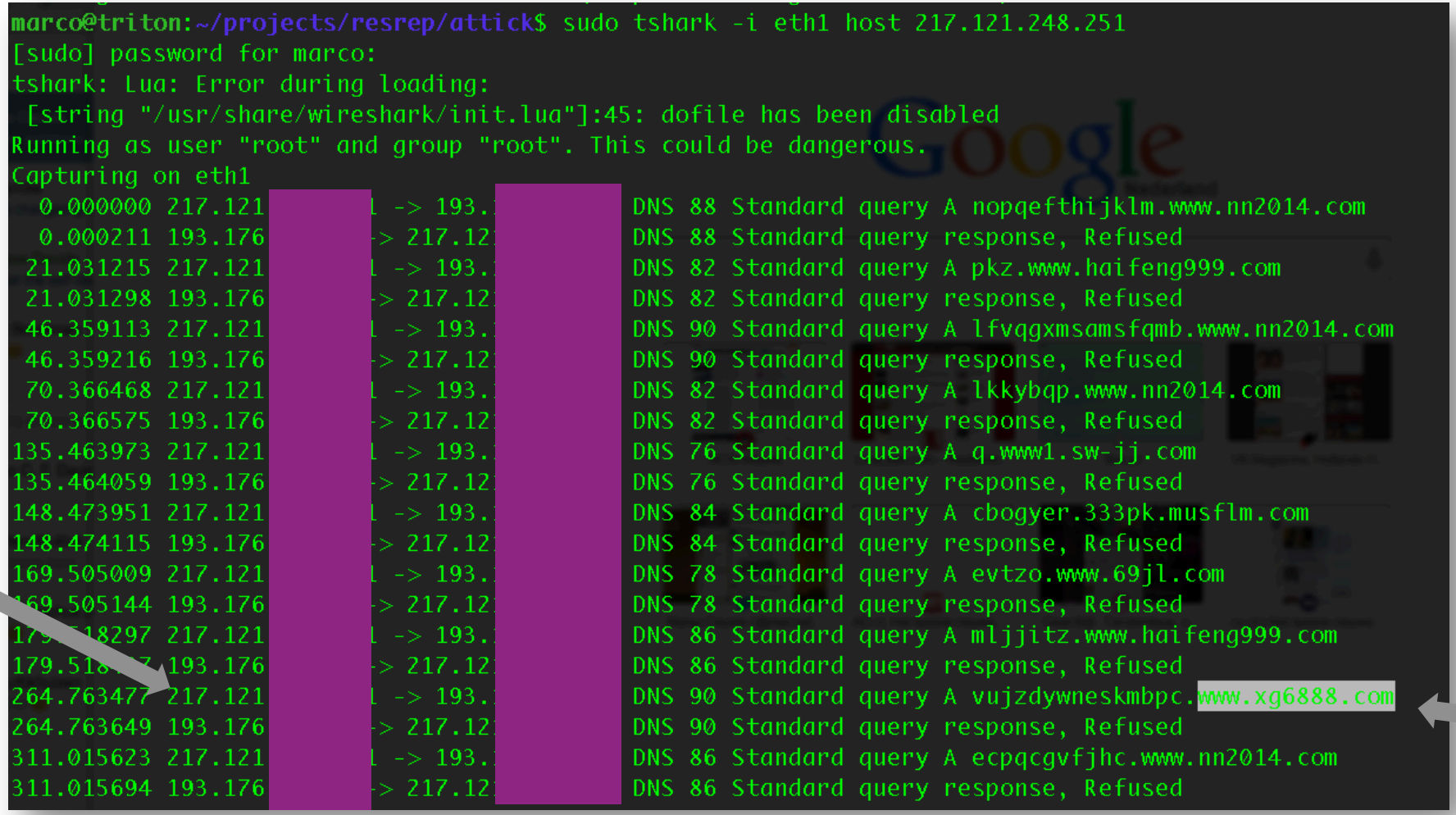
labs Research & Innovation

SIDN

Looking closer

Ziggo

Example of ongoing attack

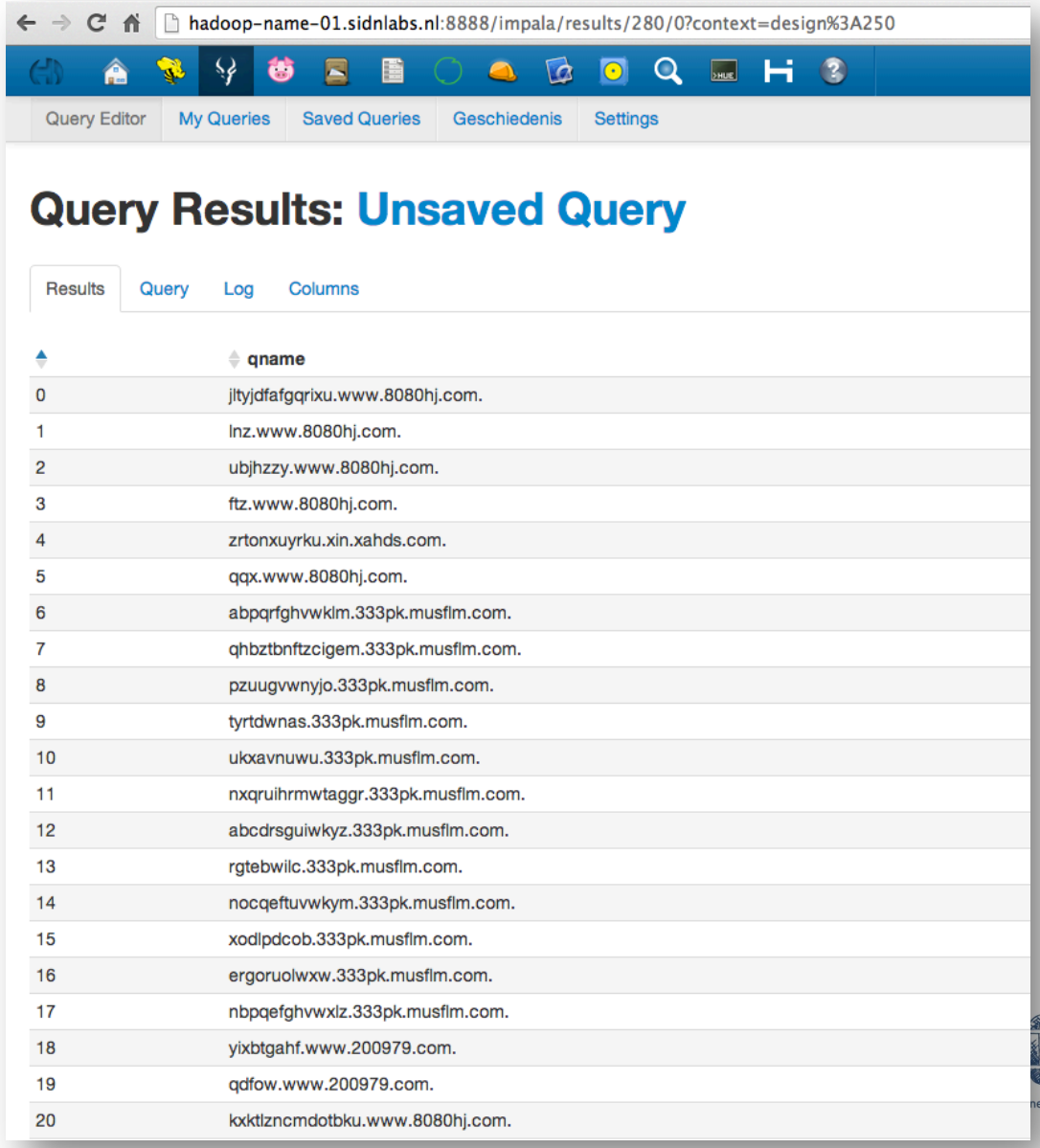


SIDN labs
Internet Research & Innovation

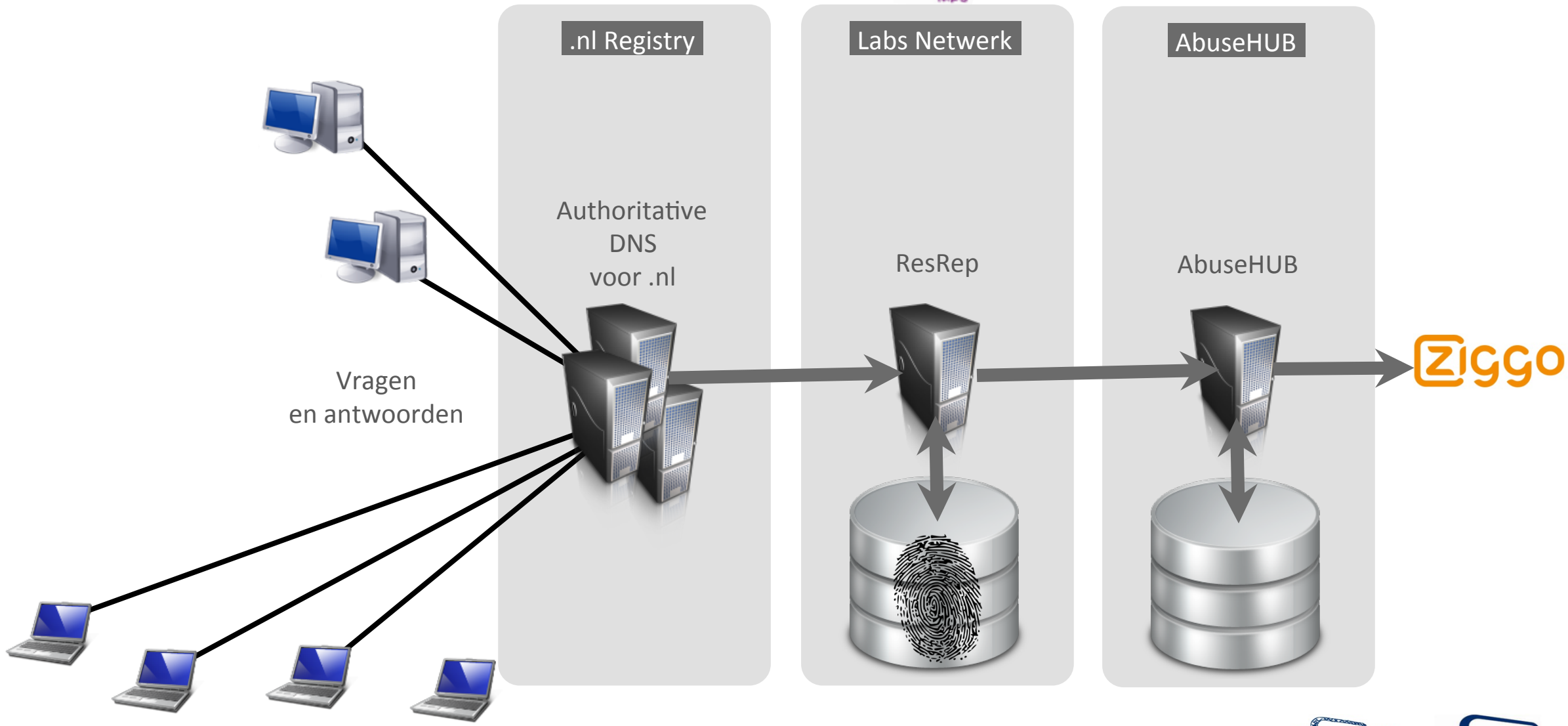
SIDN

In retrospective

```
select qname from dns.packet
where src="217.121.XXX.XXX"
limit 500
```



Ultimate situation:



Internet Research & Innovation

What have we found so far…

- More ‘resolvers’ than anticipated (~4 million).
- ~750000 seem ‘suspicious’ (possibly only tip of the iceberg).
- Various remarkable findings.
  - botnets sending spam, DDoS-traffic, a number of unknown phenomenon's.
- Also some things we hoped for, but didn’t encounter.

Lessons learned:

- Profiling and defining ‘security metrics’ is quite complicated.
  - But can produce interesting results (needle in the haystack).
- Derived behavior, there’s a fair change of false positives.
  - Results so far are probably only complementary on other measurements, but we would like more.
- We see only systems that are contacting our DNS, obviously.

SIDN labs
Internet Research & Innovation

SIDN

Tell me please:

- Are you involved in similar projects?
- Do you have any opinions about this project?
- Any other feedback, suggestions, proposals?

SIDN labs
Internet Research & Innovation

SIDN

Thank you!

Marco Davids

marco.davids@sidn.nl

@marcodavids

sidn.nl | sidnlabs.nl

SIDN labs
Internet Research & Innovation

SIDN