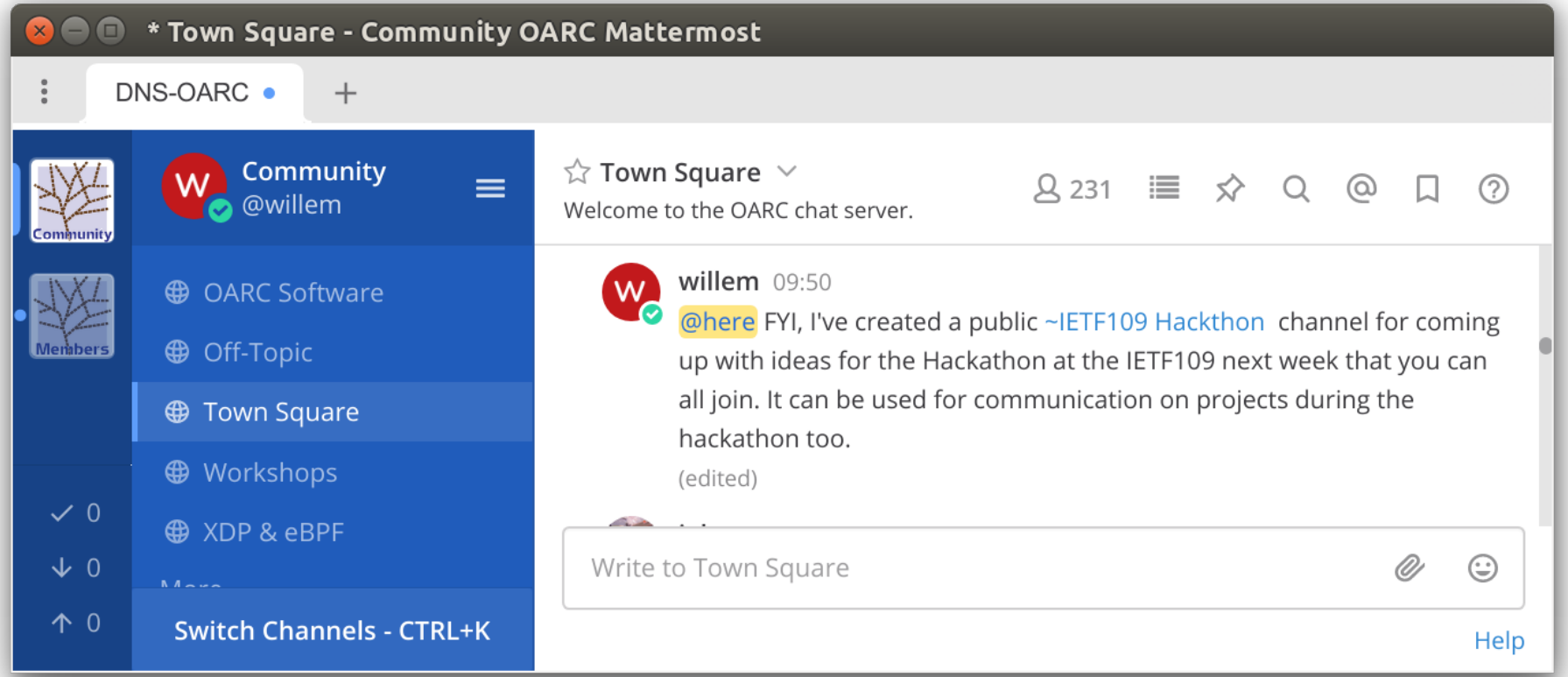
Results from project DNS

IETF 109
November 9-13, 2020
Online



14 signed up – but most(all) also still working as usual…

Hacks – DNS Error Reporting

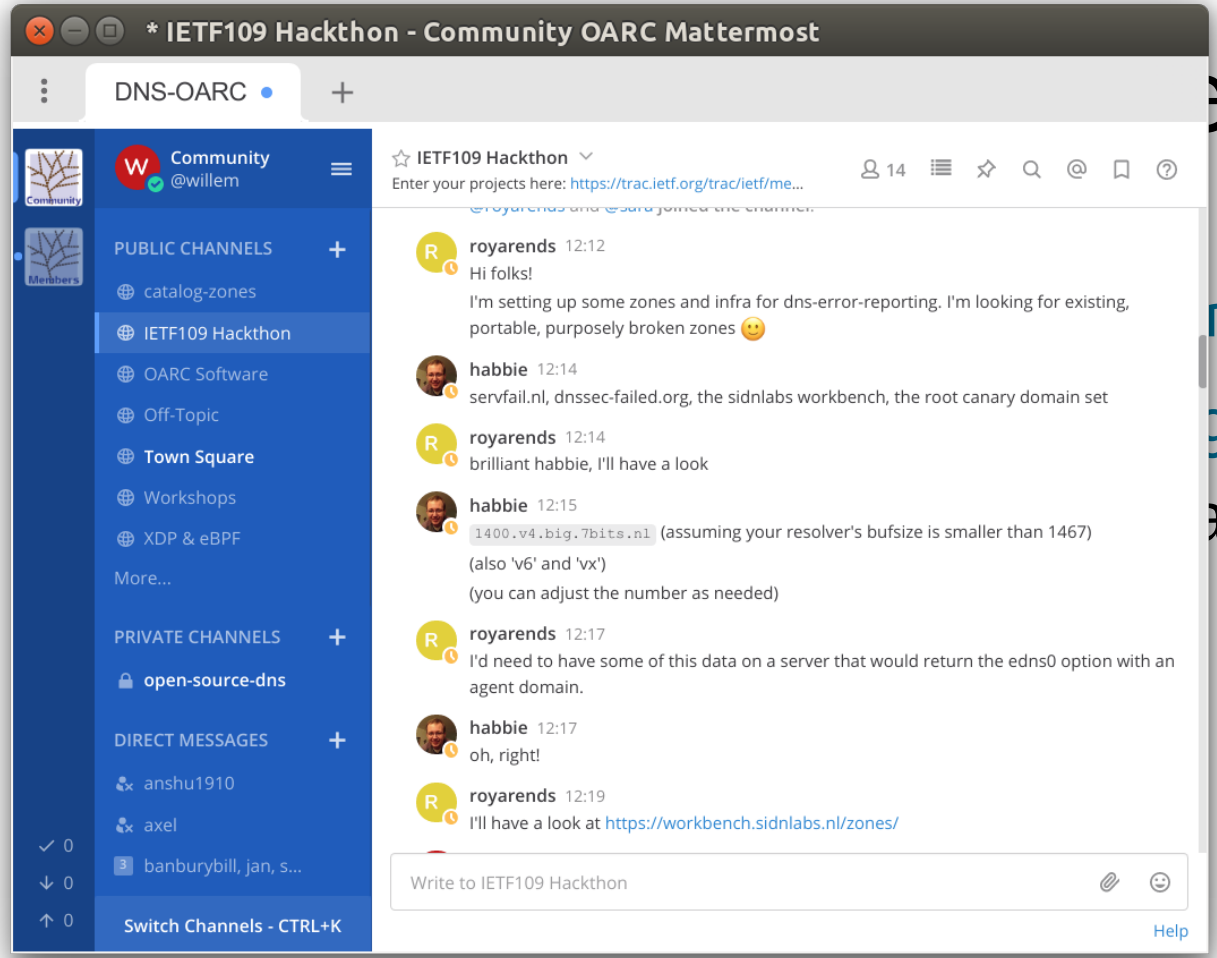
- `draft-arends-dns-error-reporting`
- Like Extended DNS Errors [RFC8914],
  but reporting to authoritative instead of querier

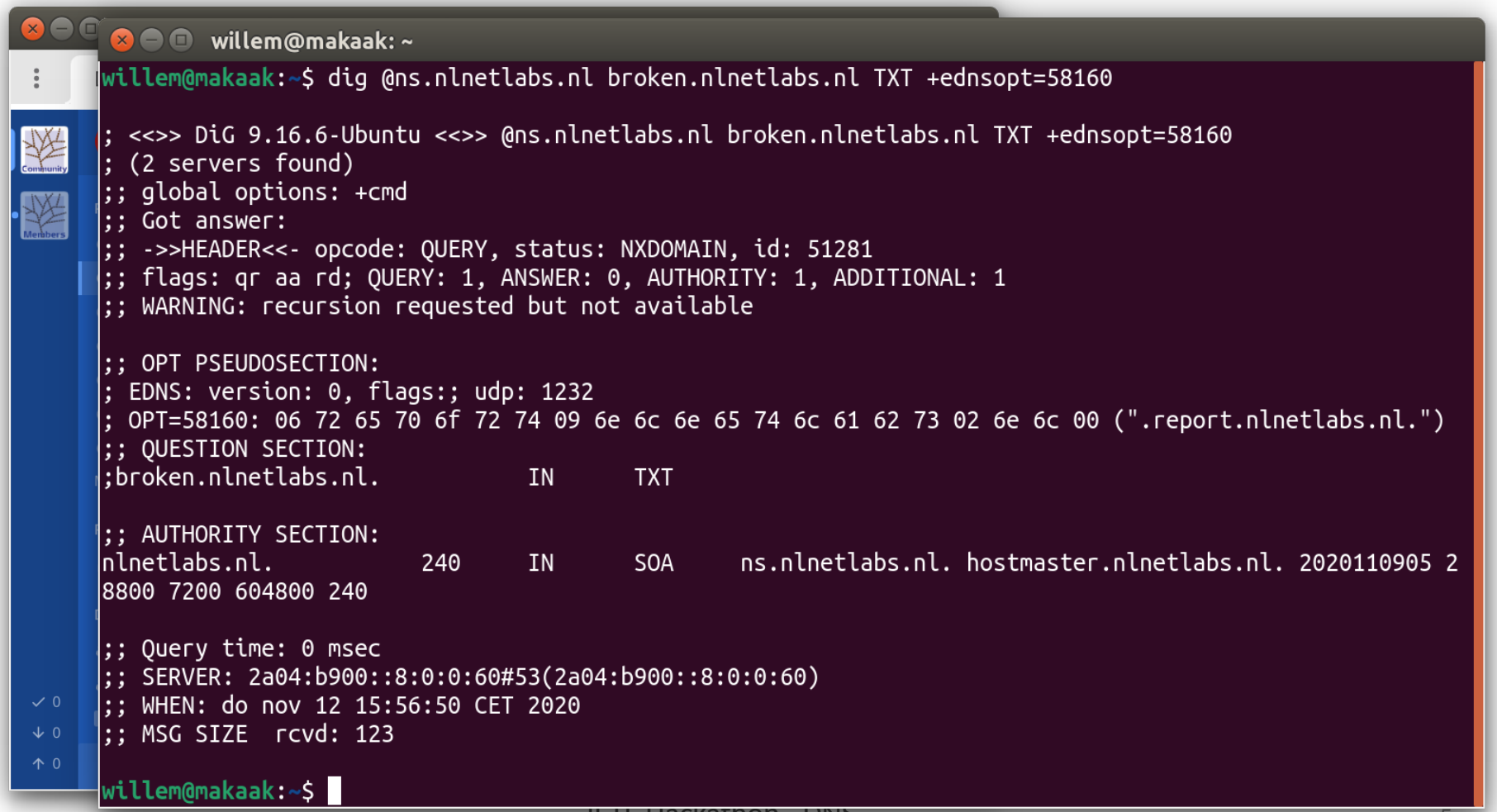
eporting

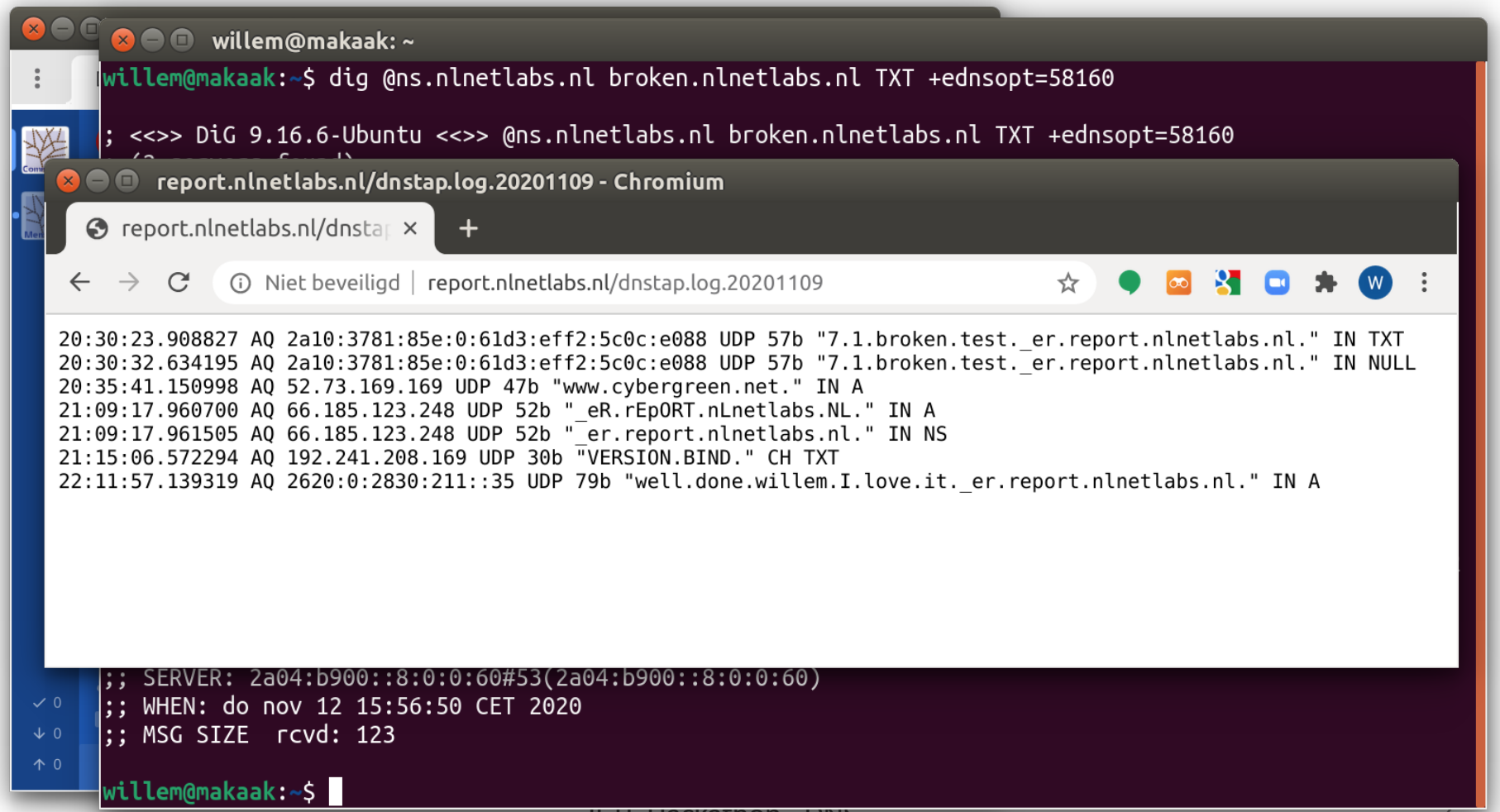
ng

914],

ad of querier




willem@makaak: ~
willem@makaak:~$ dig @ns.nlnetlabs.nl broken.nlnetlabs.nl TXT +ednsopt=58160
; <<>> DiG 9.16.6-Ubuntu <<>> @ns.nlnetlabs.nl broken.nlnetlabs.nl TXT +ednsopt=58160
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 51281
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; OPT=58160: 06 72 65 70 6f 72 74 09 6e 6c 6e 65 74 6c 61 62 73 02 6e 6c 00 (".report.nlnetlabs.nl.")
;; QUESTION SECTION:
;broken.nlnetlabs.nl. IN TXT
;; AUTHORITY SECTION:
nlnetlabs.nl. 240 IN SOA ns.nlnetlabs.nl. hostmaster.nlnetlabs.nl. 2020110905 2
8800 7200 604800 240
;; Query time: 0 msec
;; SERVER: 2a04:b900::8:0:0:60#53(2a04:b900::8:0:0:60)
;; WHEN: do nov 12 15:56:50 CET 2020
;; MSG SIZE rcvd: 123
willem@makaak:~$

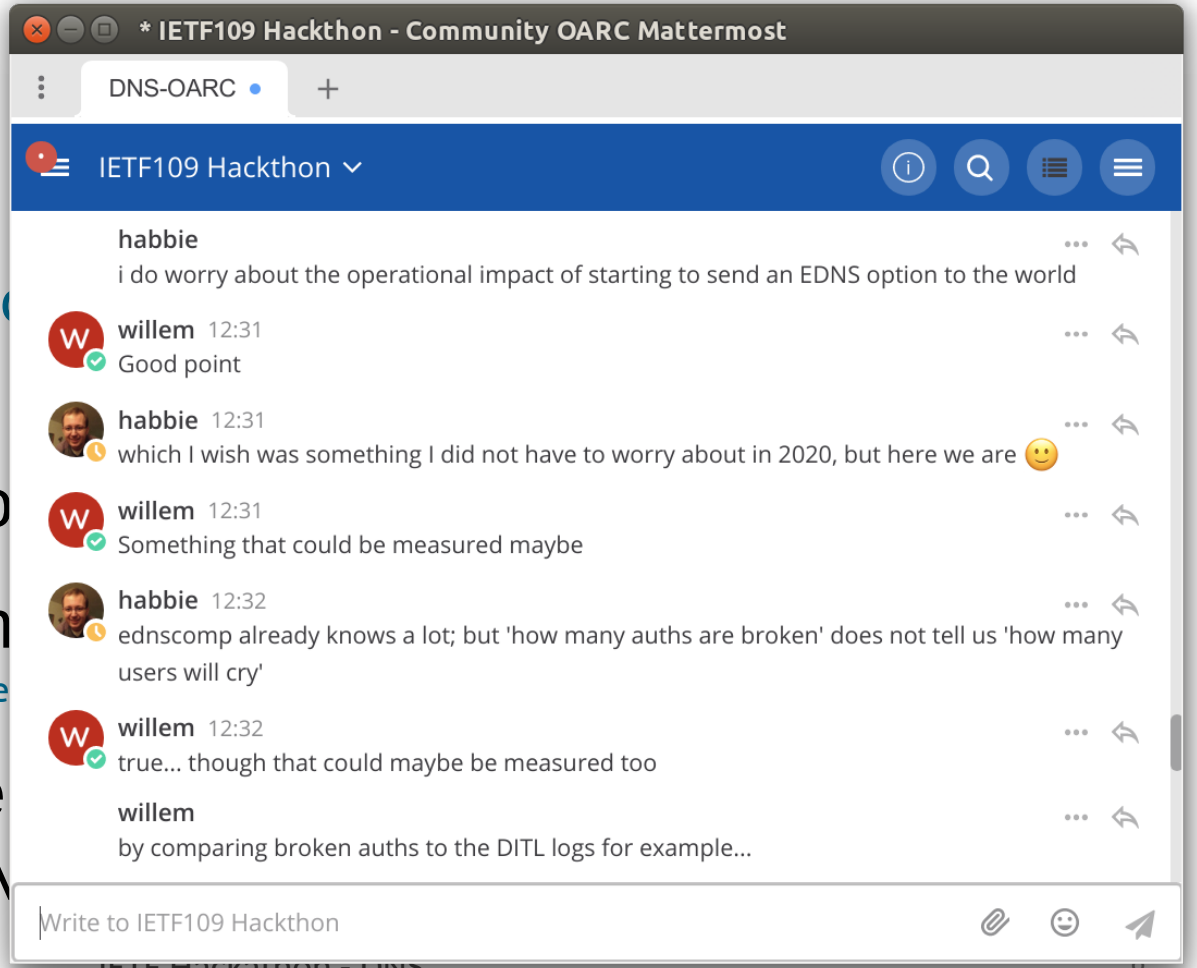

willem@makaak: ~
willem@makaak:~$ dig @ns.nlnetlabs.nl broken.nlnetlabs.nl TXT +ednsopt=58160
; <<>> DiG 9.16.6-Ubuntu <<>> @ns.nlnetlabs.nl broken.nlnetlabs.nl TXT +ednsopt=58160
report.nlnetlabs.nl/dnstap.log.20201109 - Chromium
report.nlnetlabs.nl/dnsta
Niet beveiligd | report.nlnetlabs.nl/dnstap.log.20201109
20:30:23.908827 AQ 2a10:3781:85e:0:61d3:eff2:5c0c:e088 UDP 57b "7.1.broken.test._er.report.nlnetlabs.nl." IN TXT
20:30:32.634195 AQ 2a10:3781:85e:0:61d3:eff2:5c0c:e088 UDP 57b "7.1.broken.test._er.report.nlnetlabs.nl." IN NULL
20:35:41.150998 AQ 52.73.169.169 UDP 47b "www.cybergreen.net." IN A
21:09:17.960700 AQ 66.185.123.248 UDP 52b "_eR.rEpORT.nLnetlabs.NL." IN A
21:09:17.961505 AQ 66.185.123.248 UDP 52b "_er.report.nlnetlabs.nl." IN NS
21:15:06.572294 AQ 192.241.208.169 UDP 30b "VERSION.BIND." CH TXT
22:11:57.139319 AQ 2620:0:2830:211::35 UDP 79b "well.done.willem.I.love.it._er.report.nlnetlabs.nl." IN A
;; SERVER: 2a04:b900::8:0:0:60#53(2a04:b900::8:0:0:60)
;; WHEN: do nov 12 15:56:50 CET 2020
;; MSG SIZE rcvd: 123
willem@makaak:~$

Hacks – DNS Error Reporting

- draft-arends-dns-error-reporting
- Like Extended DNS Errors [RFC8914],
  but reporting to authoritative instead of querier
- Testing environment & 1 auth implementation ready
  https://github.com/NLnetLabs/nsd/tree/features/draft-arends-dns-error-reporting
- Resolver implementations coming soon…
  Knot, PowerDNS, Unbound all have EDE branches

Hacks –

- draft-arends-
- Like Extended
  but reporting to
- Testing environ
  https://github.com/NLne
- Resolver imple
  Knot, PowerDN



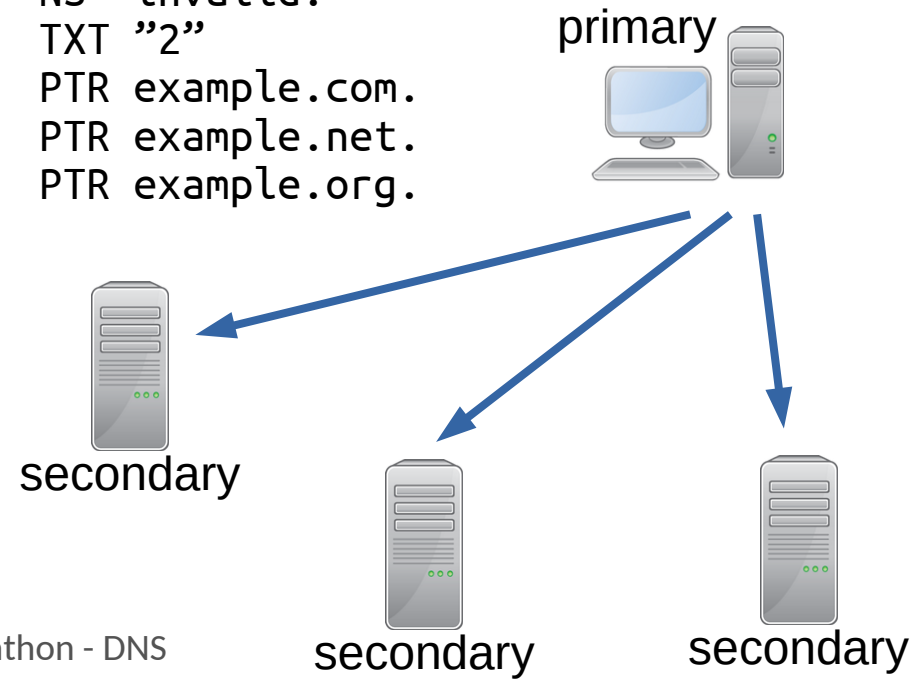
Hacks – Message Digest for DNS Zones

- `draft-ietf-dnsop-dns-zone-digest`
- DNSSEC : Integrity and Authenticity for RRsets
- ZONEMD: Integrity and Authenticity for complete zones
- PoC ldns tool existed, but was a bit cumbersome to sign:
  → add ZONEMD RR with tool
  → ldns-signzone
  → run tool again to equip and sign the ZONEMD RR
- Now, do all this at once with new -z option to `ldns-signzone`
- `https://github.com/NLnetLabs/ldns/tree/features/draft-ietf-dnsop-dns-zone-digest`

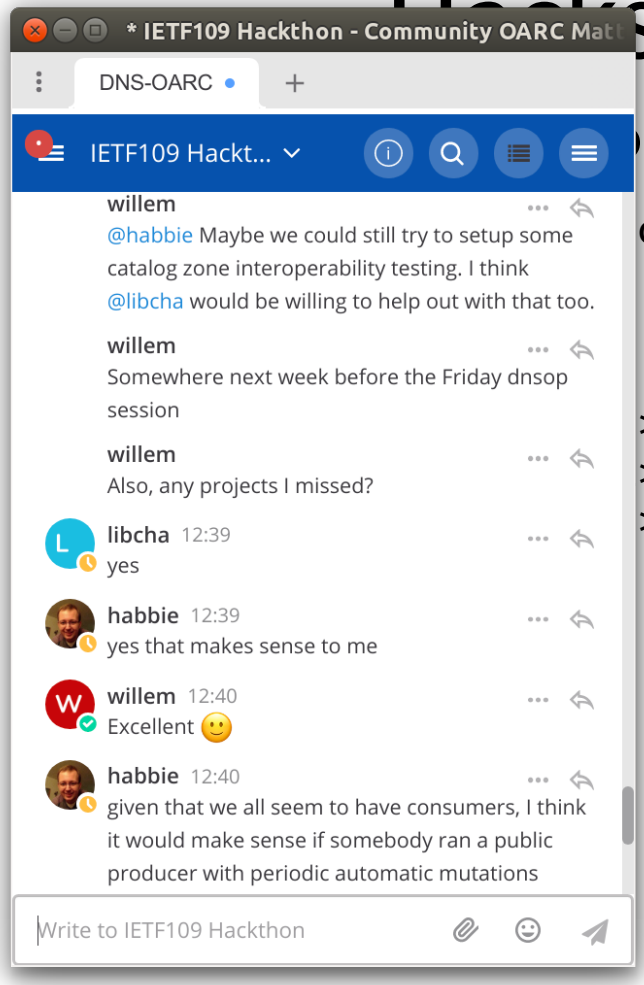
Hacks – Catalog Zones

- draft-toorop-dnsop-dns-catalog-zones

```
$ORIGIN catzone.
@                       IN  SOA . . 1552507036 86400 14400 86400 0
@                       IN  NS  invalid.
version                 IN  TXT ”2”
<unique-id-1>.zones IN  PTR example.com.
<unique-id-2>.zones IN  PTR example.net.
<unique-id-3>.zones IN  PTR example.org.
```

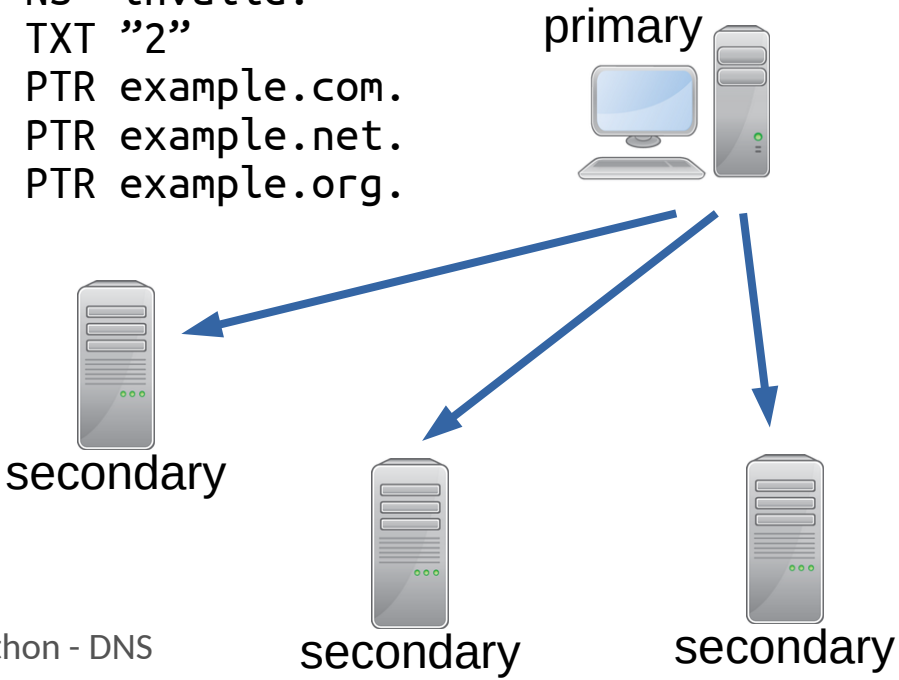


Hacks – Catalog Zones



draft-**p**-dns-catalog-zones

```
one.
        IN  SOA . . 1552507036 86400 14400 86400 0
        IN  NS  invalid.
        IN  TXT "2"
>.zones IN  PTR example.com.
>.zones IN  PTR example.net.
>.zones IN  PTR example.org.
```



Hacks – Catalog Zones

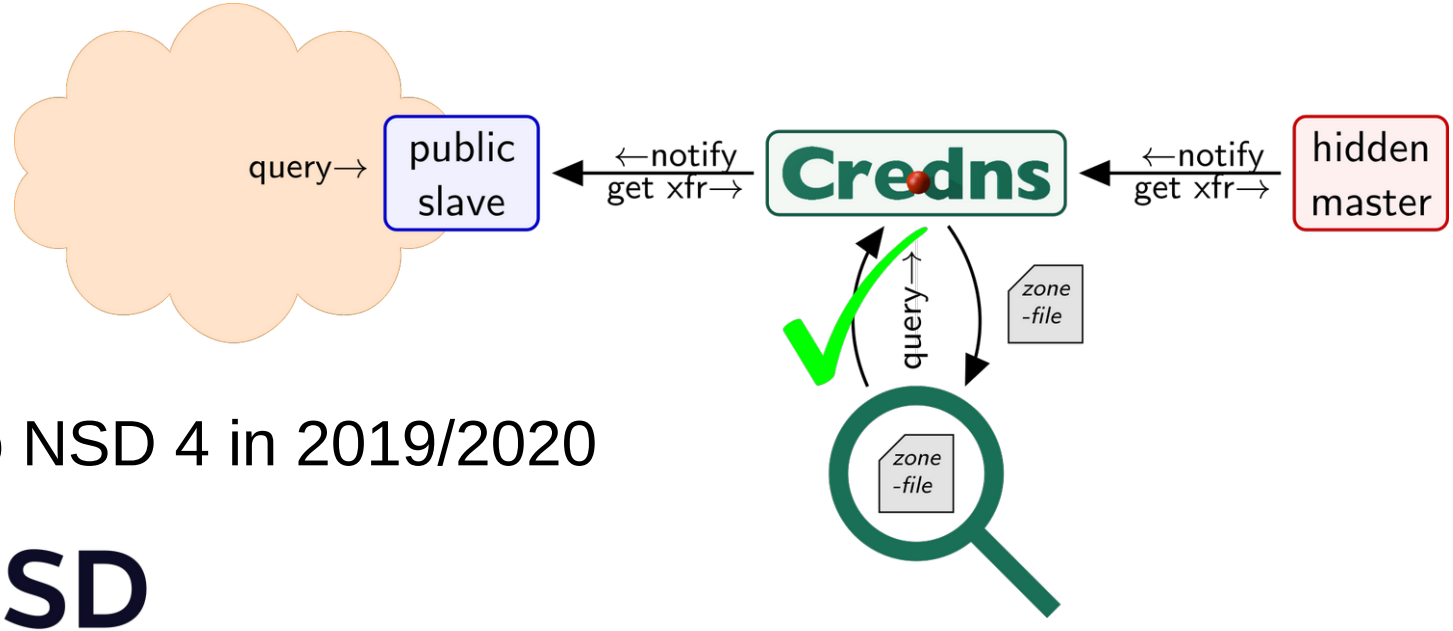
- `draft-toorop-dnsop-dns-catalog-zones`
- Interoperability testing

- Consumes version 2 Catalog Zones since version 3.0.0 *(September 2020)*
- Producer in the make

- Proof of Concept hack: PowerCATZ *(October 2016)*

Hacks – Catalog Zones

- Interoperability testing

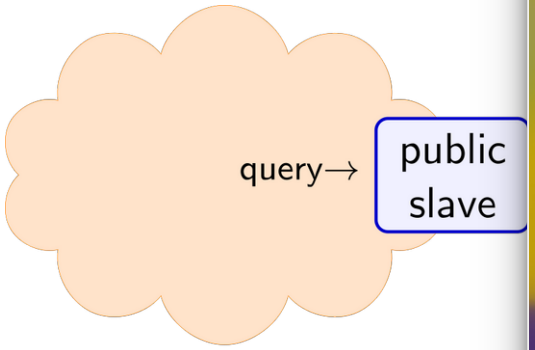


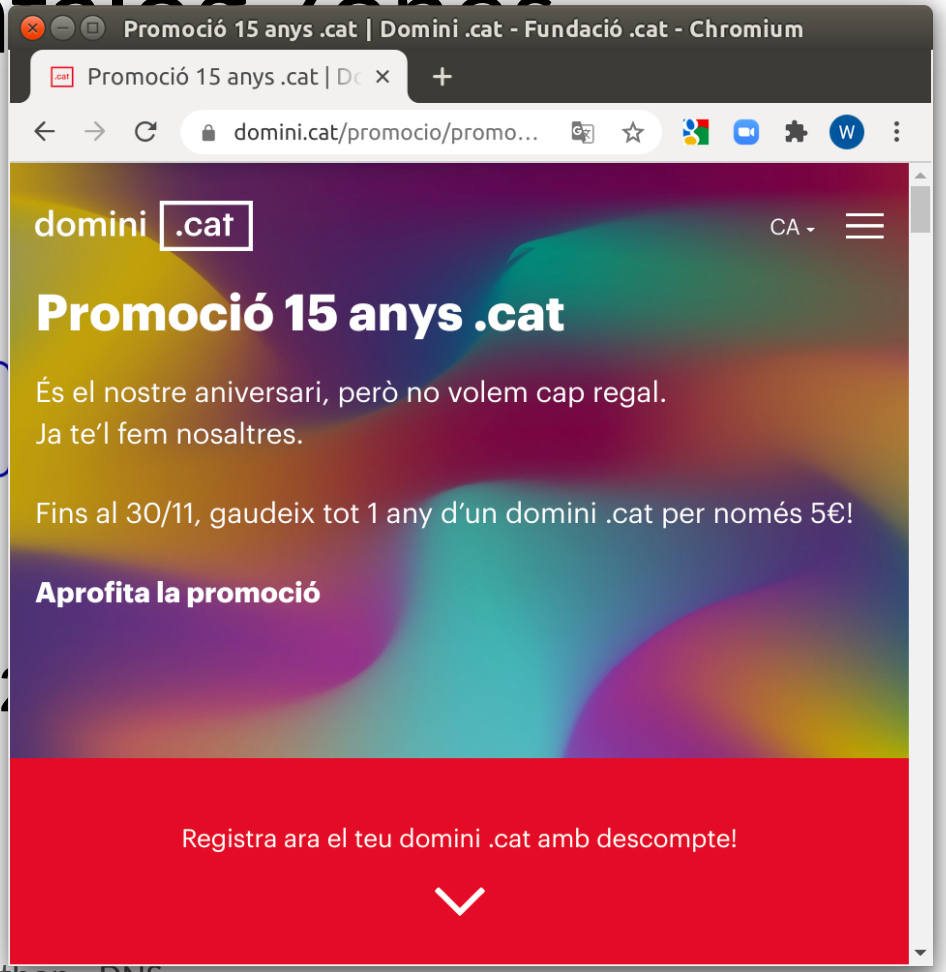
- Ported to NSD 4 in 2019/2020

NSD

Hacks – Catalog Zones

- Interoperability testing

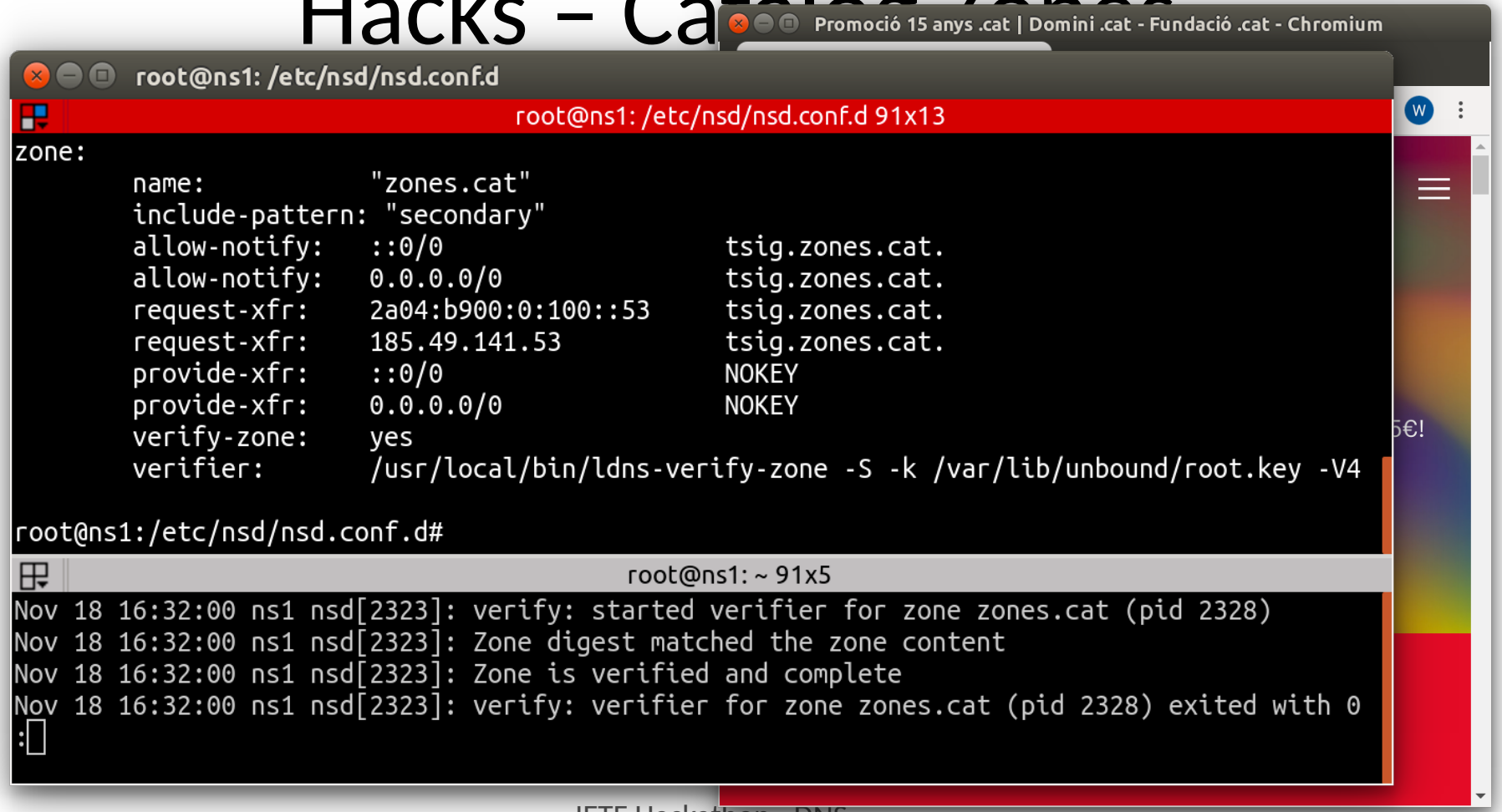




- Ported to NSD 4 in 2019/20

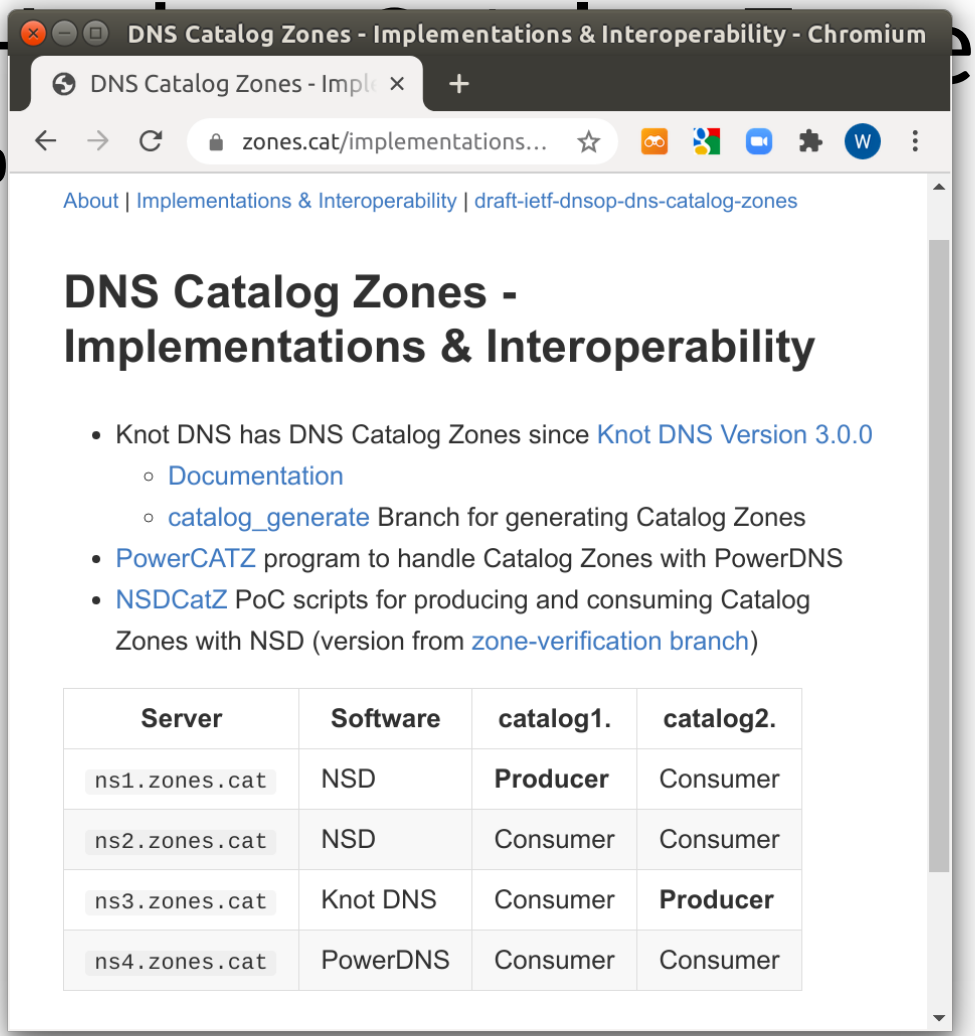
NSD

Hacks – Catalog Zones



H…es

- Interoperab…



What we learned

- I miss the in-person hackathon & meeting!
  - better ad-hoc conversations & social interaction
  - dedicated time-slot
- Online hackathon still worth it, because
  - implementers focus on new ideas and standards
  - still good input for the workgroup

What we learned

- I miss the in-person hackathon & meeting!
  - better ad-hoc conversations & social inte
  - dedicated time-slot
- Online hackathon still worth it, because
  - implementers focus on new ideas and st
  - still good input for the workgroup