Encrypted DNS weekly call

DNS4aLL Experimental Public Resolver by SIDN Labs

Marco Davids

February 3rd, 2025

@marcodavids

What (and what not) ?

- Public DNS resolver by SIDN Labs[1]
- Experimental
- Feature rich
- Anycast
- KinDNS - , RIPE-823[2] -, RFC8932- and
- GDPR compliant

- Not DNS4EU
- Not for production

1) https://www.sidnlabs.nl/en/news-and-blogs/dns4all-sidn-labs-experimental-public-dns-resolver
2) https://www.ripe.net/community/tf/dns-resolver-best-common-practice-task-force/

Why ?

- Running modern DNS (resolvers) is hard nowadays
- Many new (privacy) features added over the years
- ISPs are lagging behind, centralisation lurking around the corner
- We wanted to better understand
- And come up with a possible ‘blueprint’

By pure coincidence this happened during ‘DNS4EU’ call for tender (hence the wordplay)

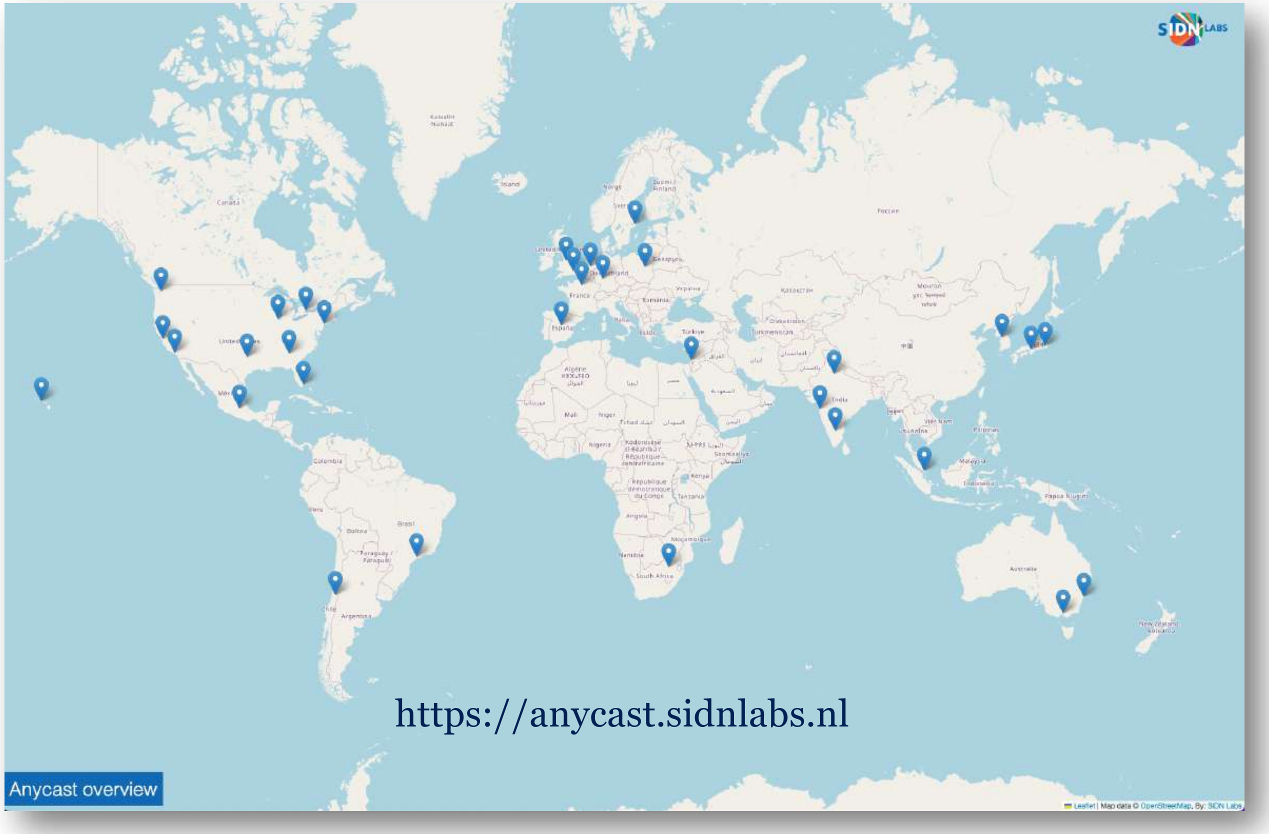
Some of the Features

- RFC6147: DNS64
- RFC7871: EDNS Client Subnet
- DoT, DoH, DoQ
- RFC8145: Trust Anchor Signalling
- RFC8198 Aggressive NSEC caching
- RFC8509: Root Key Trust Anchor Sentinel
- RFC8767: Serving Stale Data[1]
- RFC8914: Extended DNS Errors (subset)
- RFC8806: Local root (including ZONEMD, RFC8976)
- RFC9462: Discovery of Designated Resolvers
- RFC9606: RESINFO (are we the only ones?)
- RPZ: Response Policy Zones

[1] Has some issues

Anycast

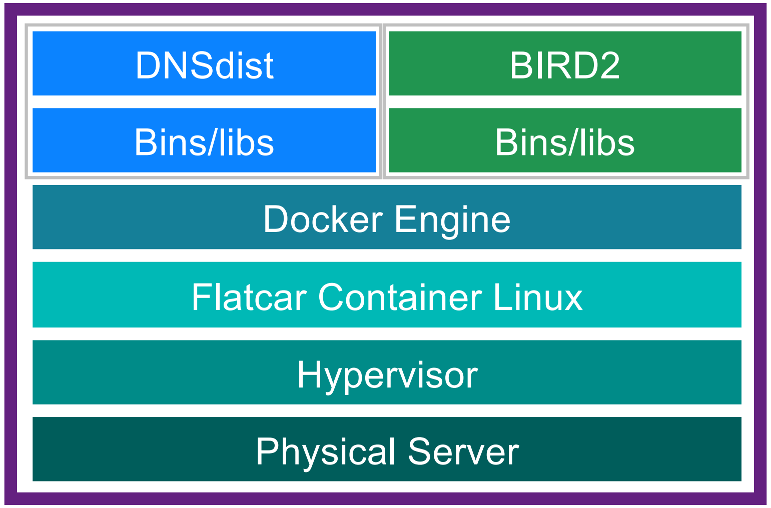
- We built in on top of our existing anycast testbed.



https://anycast.sidnlabs.nl

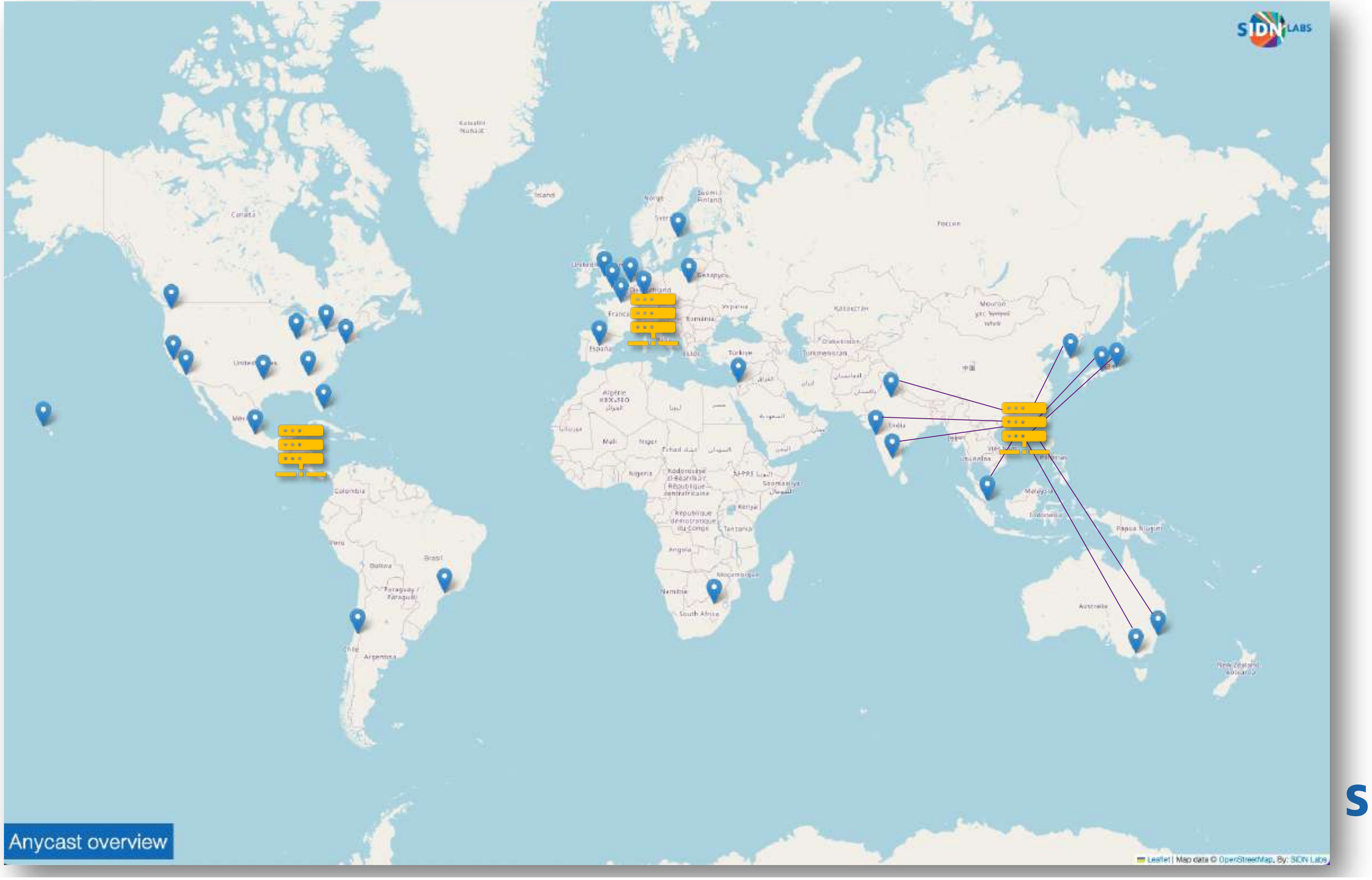
How ?

Flatcar Container Linux, Docker, DNSdist, BIRDv2:



```
{
  "ignition": {
    "config": {
      "replace": {
        "source": "https://username:password@anycast.sidnlabs.nl/provisioning/flatcar/ignition.ign"
      }
    },
    "version": "3.4.0"
  }
}
```

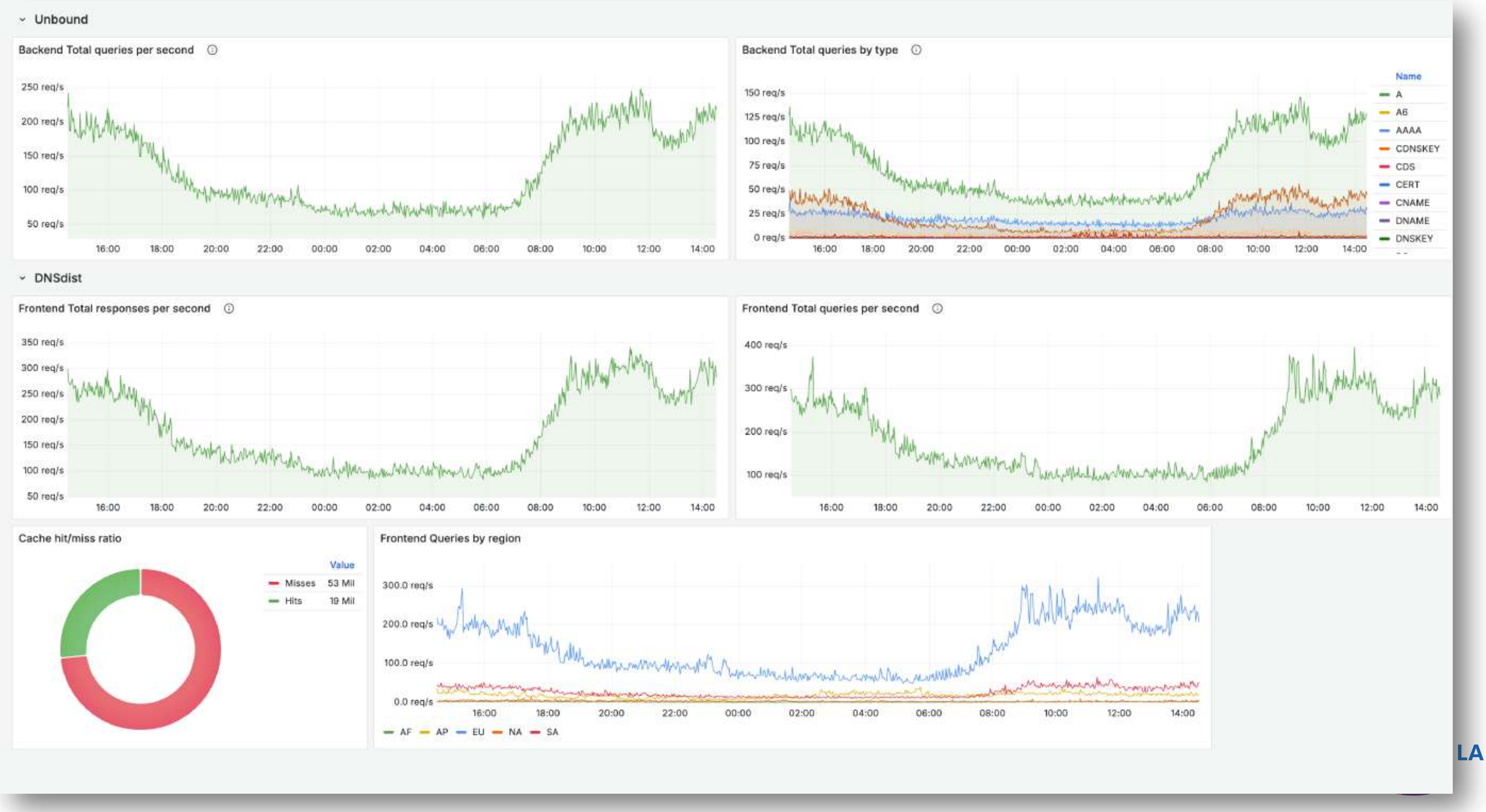
Bigger picture (with Unbound)



Nitty-gritty details

- Low-end VM’s from Vultr
- PROXYv2
  - For client IP addresses at resolver level
- Monitoring with Prometheus / Grafana
  - Including statistics on DoH/DoT/DoQ and IPv6 usage
- PQC for DoH and DoT
  - But not yet for DoQ
- Strict rate limiting (to be on the safe side)
- No ANY queries

Some statistics



Unbound

Backend Total queries per second

Backend Total queries by type

DNSdist

Frontend Total responses per second

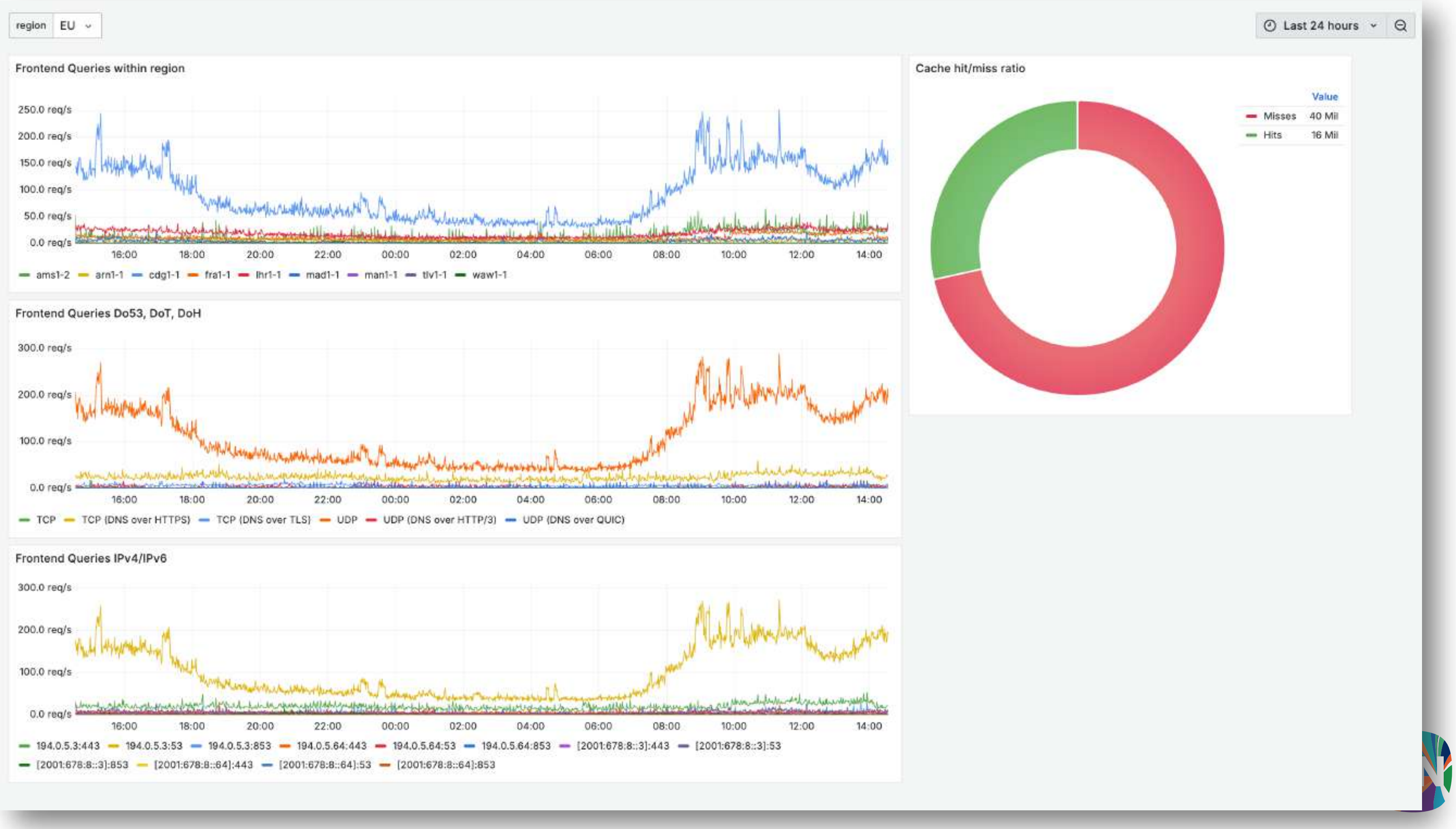
Frontend Total queries per second

Cache hit/miss ratio

	Value
Misses	53 Mil
Hits	19 Mil

Frontend Queries by region

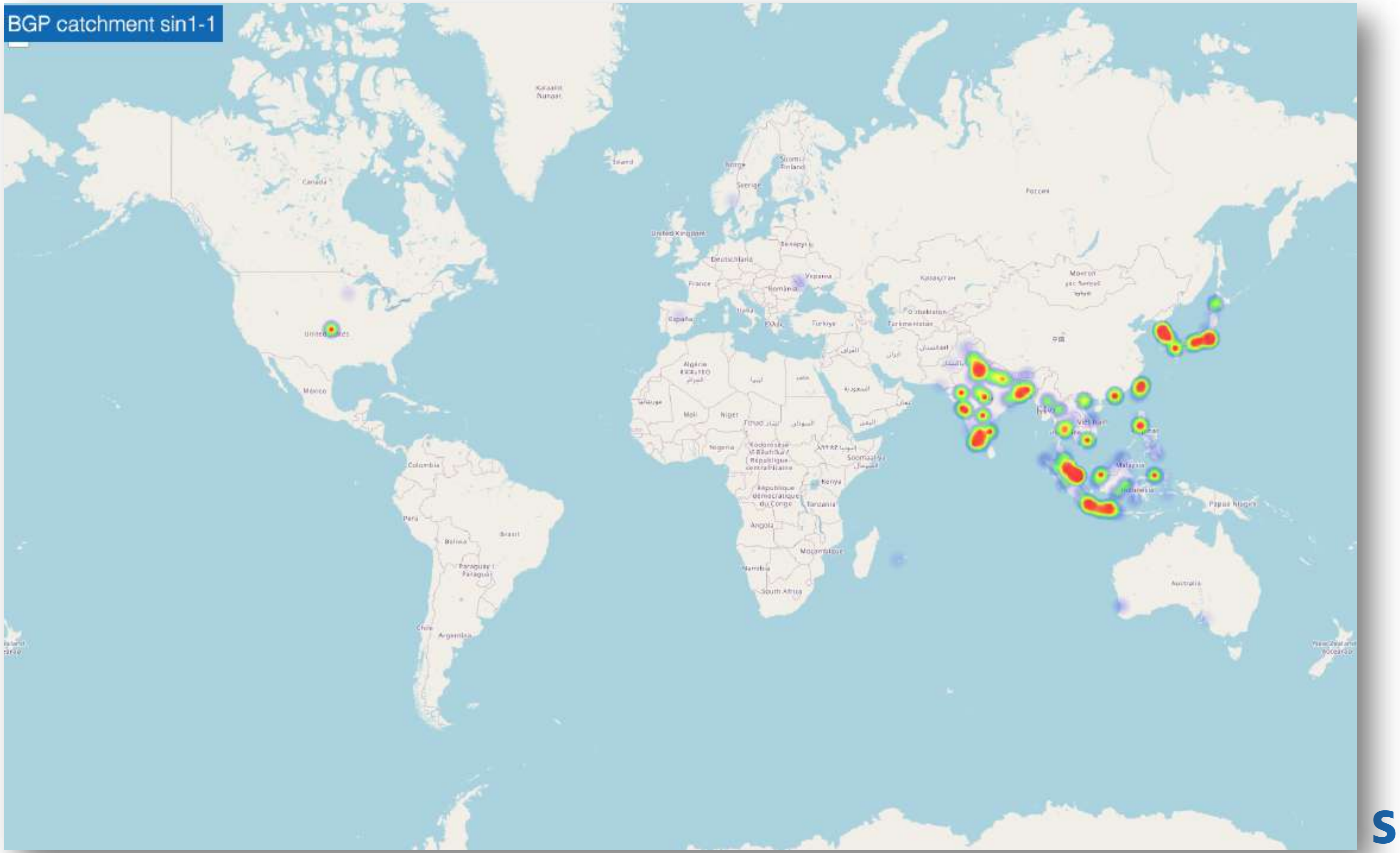
Some statistics



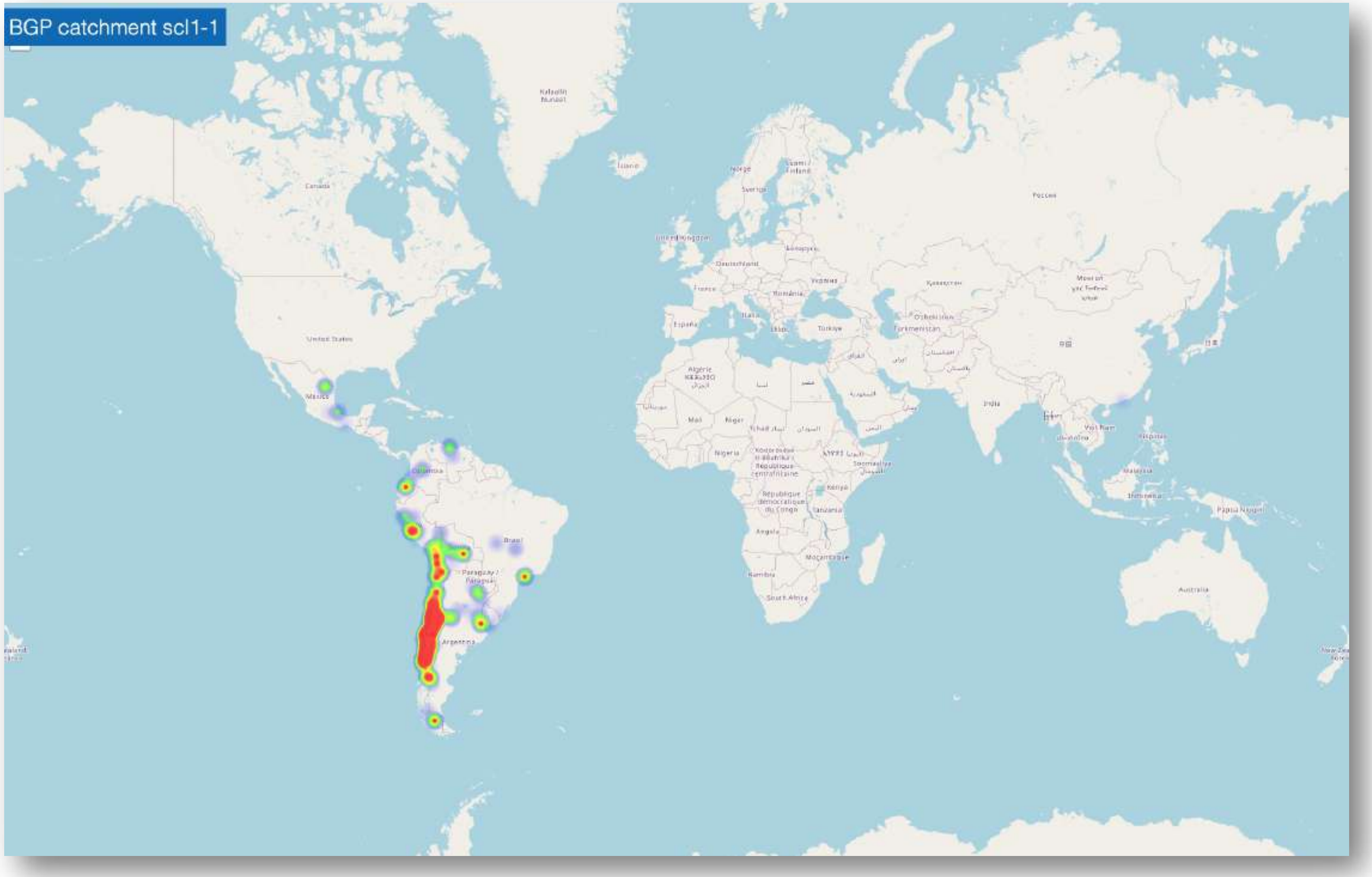
region EU

Last 24 hours

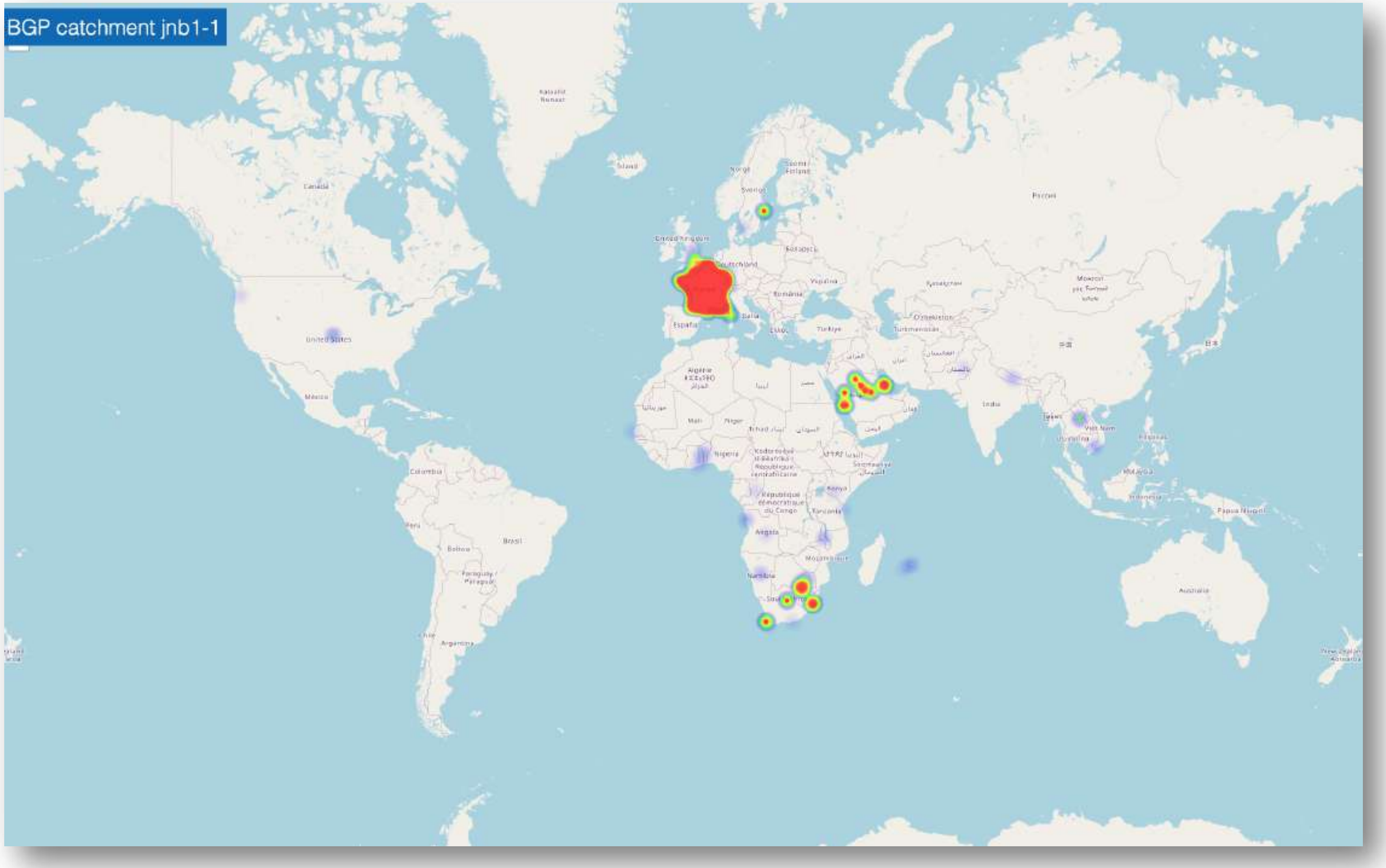
Catchment



Catchment

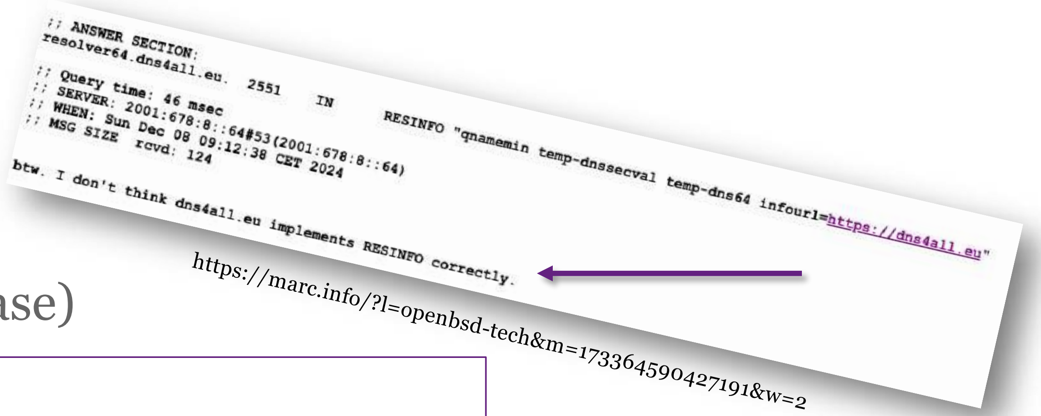

BGP catchment scl1-1
Kalaallit Nunaat
Canada
United States
México
Colombia
Brasil
Paraguay
Argentina
Ísland
United Kingdom
Norge
Sverige
France
España
Deutschland
Italia
Türkiye
Россия
Қазақстан
India
Algérie
Mali
Niger
Nigeria
Angola
Namibia
South Africa
Moçambique
Tanzania
Kenya
Australia
Papua Niugini
Indonesia
Malaysia
Pilipinas
Việt Nam
Монгол улс
日本
中国

Catchment 🤔



Some observations

- Setup works!
  - We learned a lot but is is also fun
- RFC ambiguity (RESINFO in this case)



```
;; ANSWER SECTION:
resolver64.dns4all.eu.  2551    IN      RESINFO "qnamemin temp-dnssecval temp-dns64 infourl=https://dns4all.eu"

;; Query time: 46 msec
;; SERVER: 2001:678:8::64#53(2001:678:8::64)
;; WHEN: Sun Dec 08 09:12:38 CET 2024
;; MSG SIZE  rcvd: 124

btw. I don't think dns4all.eu implements RESINFO correctly.
```

https://marc.info/?l=openbsd-tech&m=173364590427191&w=2

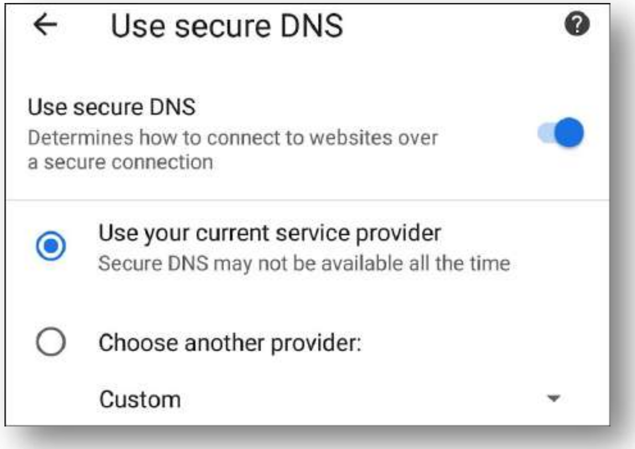
```
;; QUESTION SECTION:
;resolver.arpa.                      IN RESINFO

;; ANSWER SECTION:
resolver.arpa.                      0 IN RESINFO "qnamemin" "temp-dnssecval" "infourl=https://dns4all.eu"
```

- Many RFC9640 HTTPS queries (iOS?)
  - not so many sites using them (Cloudflare, mostly)
  - What happens if the ipv[46] hints are not updated?

```
;; ANSWER SECTION:
example.nl.             3600        IN          HTTPS       1 . alpn="h2" ipv4hint=94.198.159.35 ipv6hint=2a00:d78:0:712:94:198:159:35
```

Some observations

- DDR does not work for us?
  - Why not?
  - Perhaps we do not fully understand the concept
  - How to test? (https://info.dns4all.eu)
  - IP addresses in SAN not trivial (is it needed?)*
  - DoH usage is low because of this?



Use secure DNS

Use secure DNS
Determines how to connect to websites over a secure connection

● Use your current service provider
Secure DNS may not be available all the time

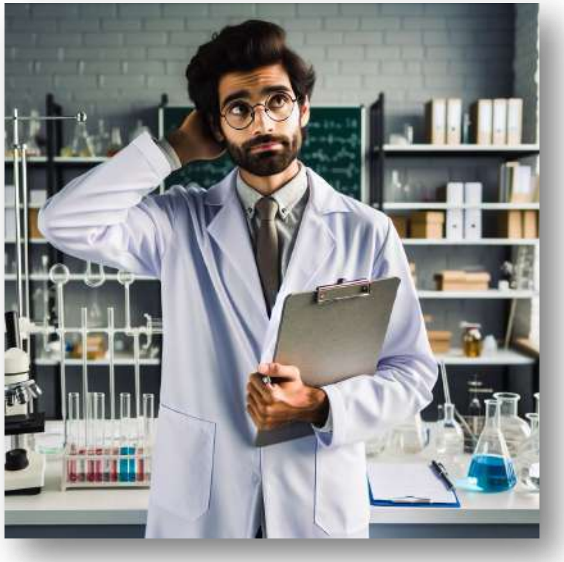
○ Choose another provider:
Custom

```
;; QUESTION SECTION:
;_dns.resolver.arpa.       IN SVCB

;; ANSWER SECTION:
_dns.resolver.arpa.        3600 IN       SVCB 1 resolver.dns4all.eu. alpn="dot,doq" port=853 ipv4hint=194.0.5.3 ipv6hint=2001:678:8::3
_dns.resolver.arpa.        3600 IN       SVCB 1 resolver.dns4all.eu. alpn="h2,h3" port=443 ipv4hint=194.0.5.3 ipv6hint=2001:678:8::3 key7="/dns-query{?dns}"
```

*) https://datatracker.ietf.org/doc/html/rfc9462#name-certificate-management

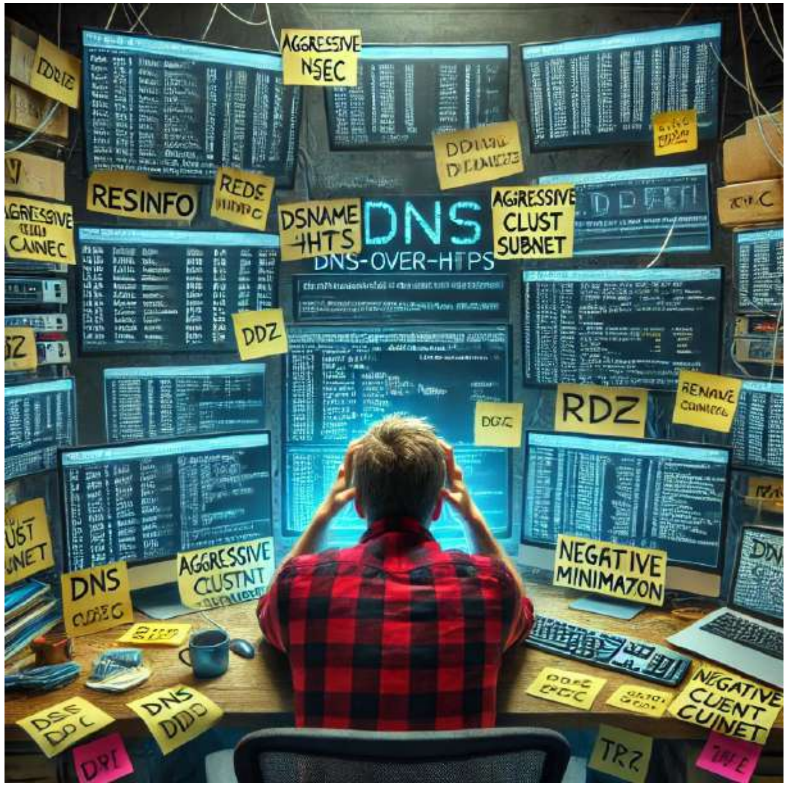
What’s next ?

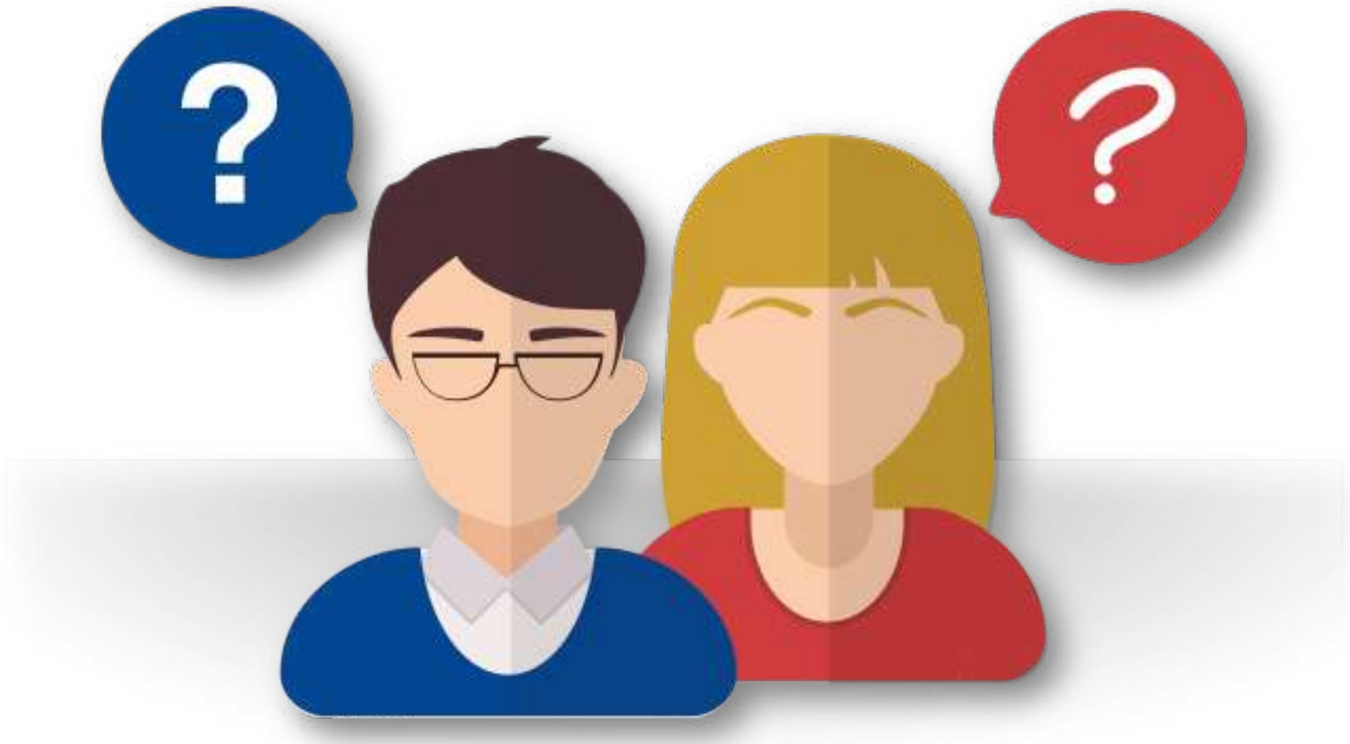
- Keep it like it is for now and continue to explore
- But what if people actually start using it…? 🫣



Summarizing

- Fun project!
- Modern resolvers are complicated
  - No news, but still…
- What should we do?
  - KinDNS, RIPE-823, RFC8932 ?
  - Cookbooks, blueprints?
  - Or just don’t care…





Thank you!!