Test sources:

- RIPE Atlas
- “Wild” Open Resolvers (found via DNS scans)
  (+ browsers, e.g., page load time)
- “Popular” Open Resolvers (e.g., from Wikipedia)

Things to test

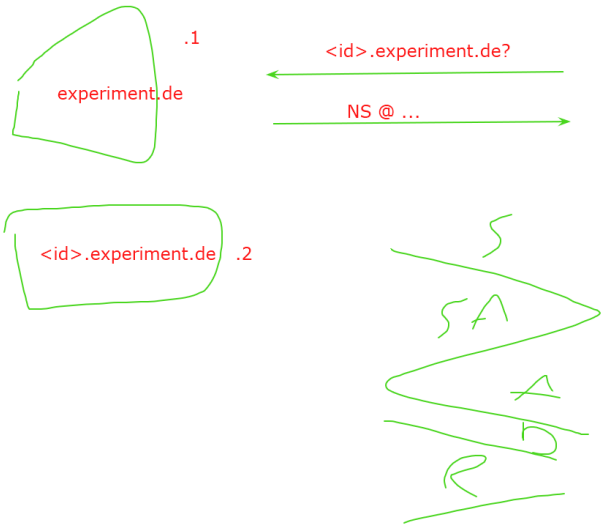
- Various rates of packet loss (10, 20, 40, 60, 80, 90, 95, 100)
- Truncation (switch to TCP)
- DNS Cookies
- RRL (no response vs. truncation)
- DNSSEC NSEC3 caching

Metrics of Attack Success

- DNS response failure rate (client side)
- DNS response rate (server side)
- DNS response latency
- Rate of stale records
- Name server migrations (and reasons thereof)
  - Multiple NS records
  - One NS with multiple A/AAAA records
  - (Anycast)
- Page load time (Web context)
- Attack amplification
  - Query duplicates
  - Switch-over rate to TCP

How to record traffic

- dnstap
- tcpdump -nn -s0 -w …
- dnscap


.1
experiment.de
<id>.experiment.de?
NS @ ...
<id>.experiment.de
.2

○