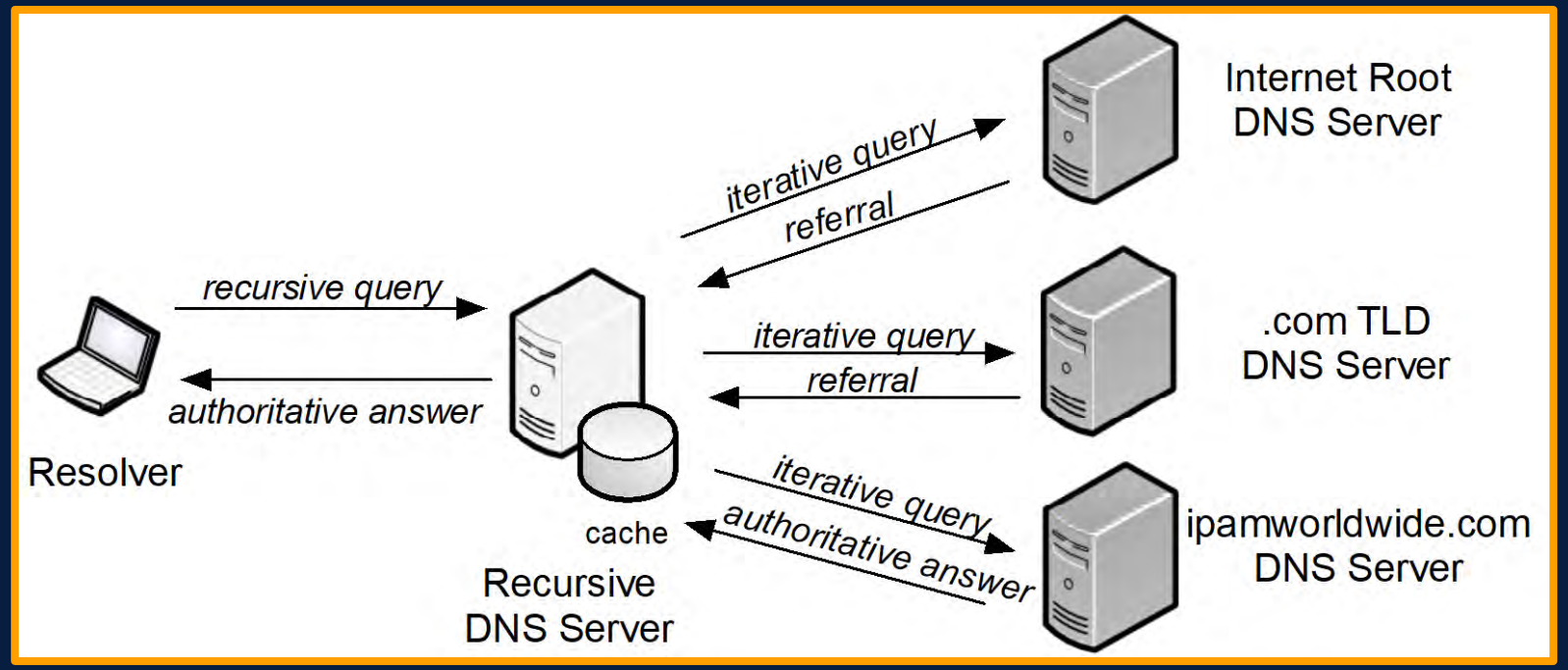
Extended DNS Errors

N3K Expert Webinar Series

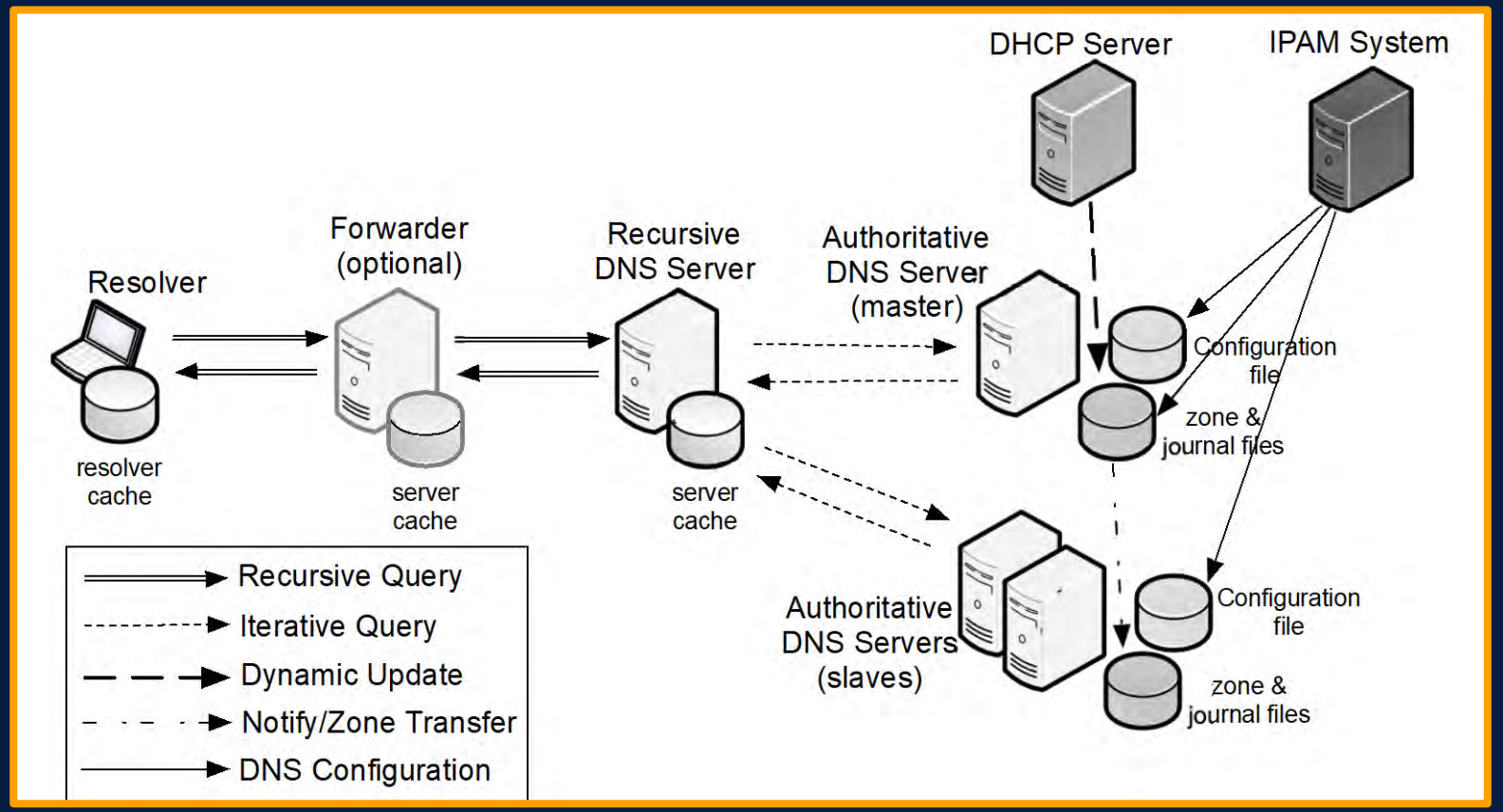
Andreas Taudte
Principal DDI Consultant

Last updated March 2023

Why not just use ping?



Why not just use ping?



DNS Response Codes

- **NOERROR** - No Error
- **FORMERR** - Format Error
- **SERVFAIL** - Server or Feature Problem
- **NXDOMAIN** - FQDN doesn’t exist
- **NOTIMPL** - Not implemented
- **REFUSED** - Action refused
- **NotAuth** - Server not authoritative for Zone
- **NotZone** - Name not contained in Zone
- **prereq** - YXDomain, YXRRSet, NXRRSet

Extended DNS Erros (EDE)

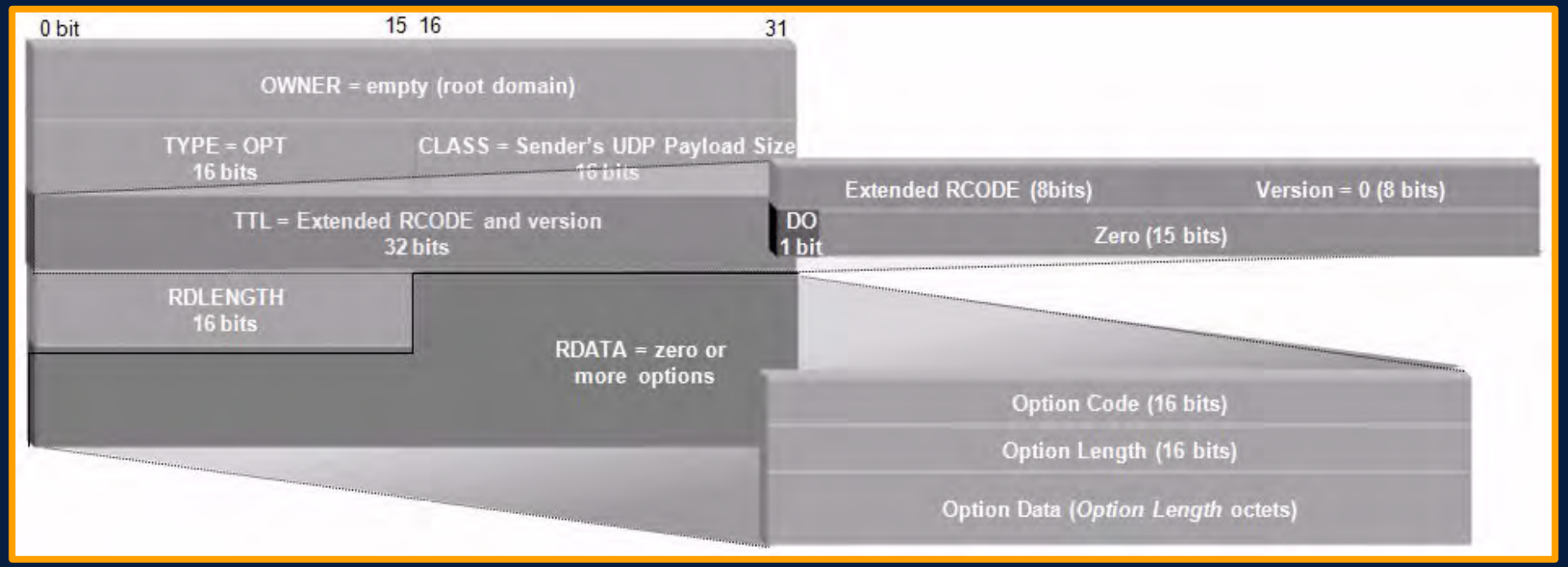
- Defines Variety of new Error Messages[1] in DNS
- Extends **SERVFAIL** and **REFUSED** with Details about the Cause
- Reduces Complexity of Diagnosing DNS Issues (the fun is lost)
- Does not affect Processing of Response Codes (**RCODE**)
- Uses EDNS0 Option to include extended Information
- Unauthenticated unless secured by Transaction (such as TSIG[2], DoH[3] or DoQ[4])

[1]https://www.rfc- editor.org/info/rfc8914
[2]https://www.rfc- editor.org/info/rfc8945
[3]https://www.rfc- editor.org/info/rfc8484
[4]https://www.rfc- editor.org/info/rfc9250

Extension Mechanisms for DNS

- DNS Responses typically small in Size (less than 512 Bytes)
- Version 0 (EDNS0) defines OPT Pseudo Record Record
  - Used to advertise Capabilities of Sender
  - Placed in **`ADDITIONAL SECTION`** by Resolver or Server
  - UDP-based DNS Message of up to 4096 Bytes
- Required for Features like
  - DNSSEC validation,
  - DNS COOKIE option or
  - Name Server Identifier (NSID)

EDNSo Format



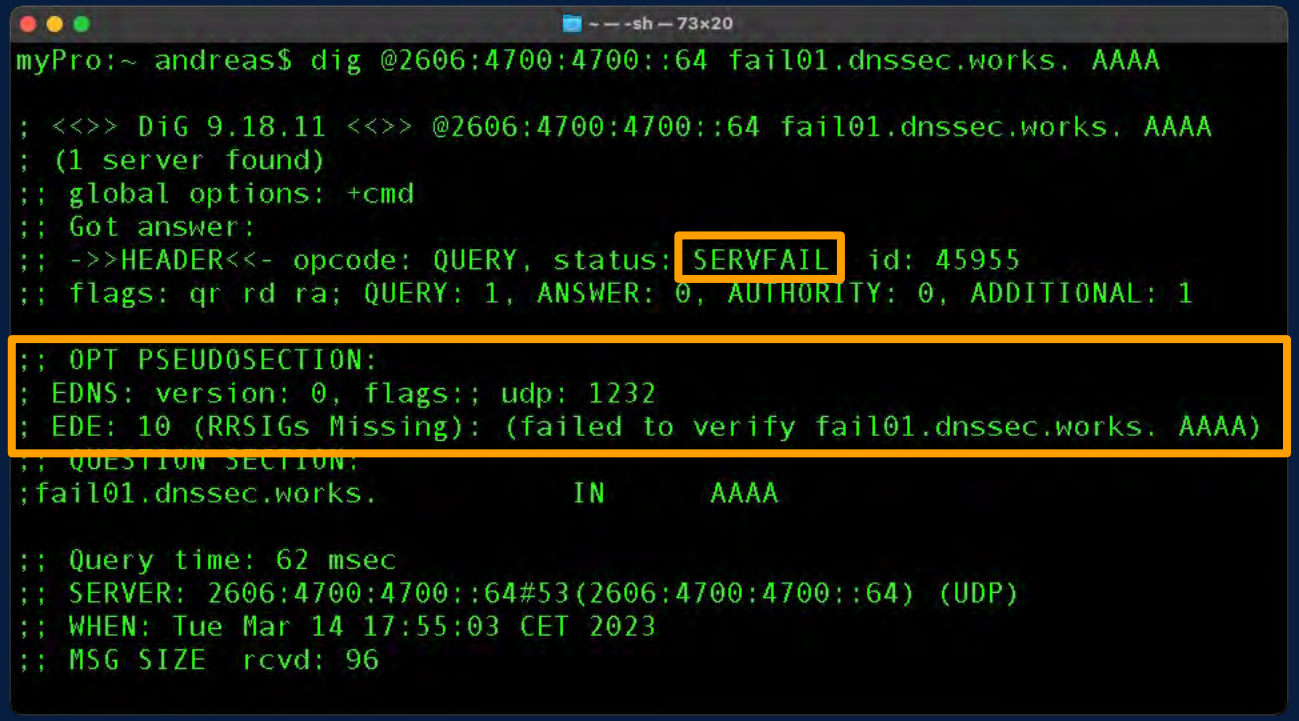
Testing EDNS Compatibility

https://kb.isc.org/docs/edns-compatibility-dig-queries
https://ednscomp.isc.org/ednscomp/

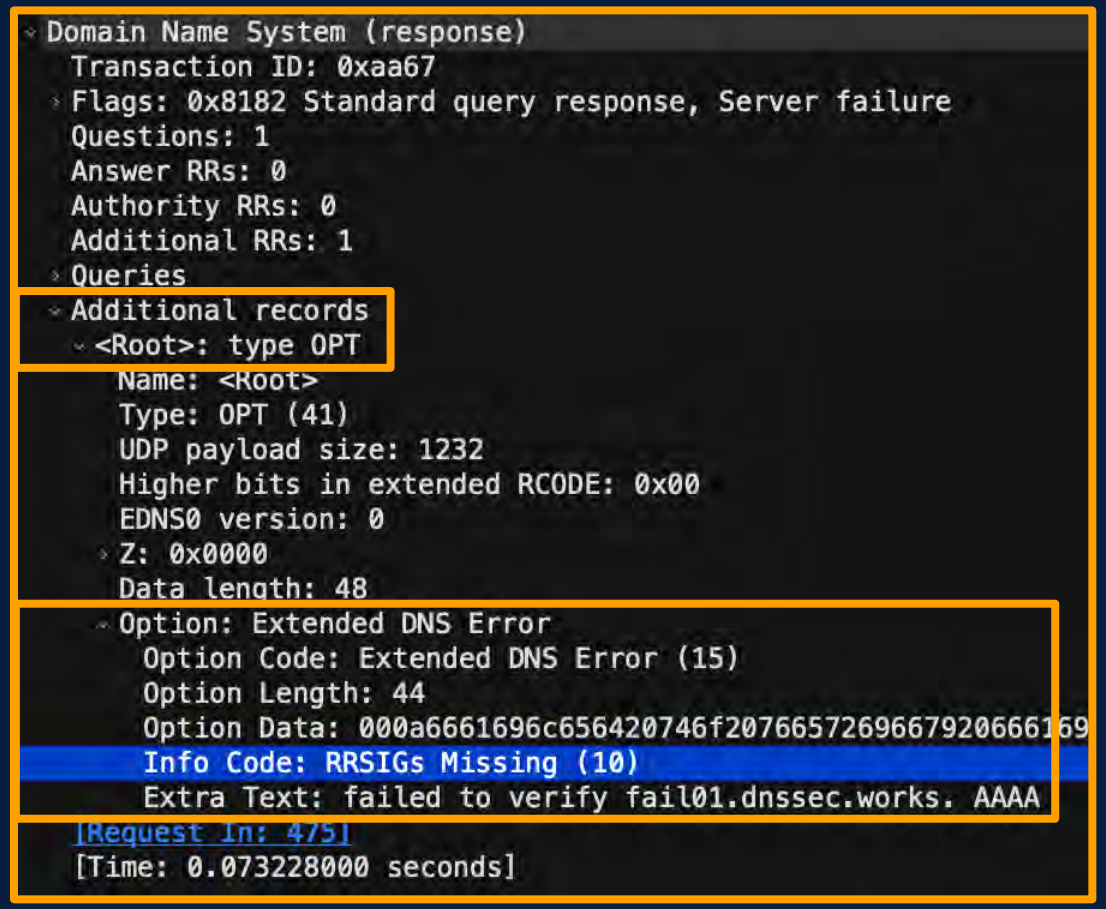
Initially Defined Extended DNS Errors

0	Other
1	Unsupported DNSKEY Algorithm
2	Unsupported DS Digest Type
3	Stale Answer
4	Forged Answer
5	DNSSEC Indeterminate
6	DNSSEC Bogus
7	Signature Expired
8	Signature Not Yet Valid
9	DNSKEY Missing
10	RRSIGs Missing
11	No Zone Key Bit Set
12	NSEC Missing
13	Cached Error
14	Not Ready
15	Blocked
16	Censored
17	Filtered
18	Prohibited
19	Stale NXDOMAIN Answer
20	Not Authoritative
21	Not Supported
22	No Reachable Authority
23	Network Error
24	Invalid Data

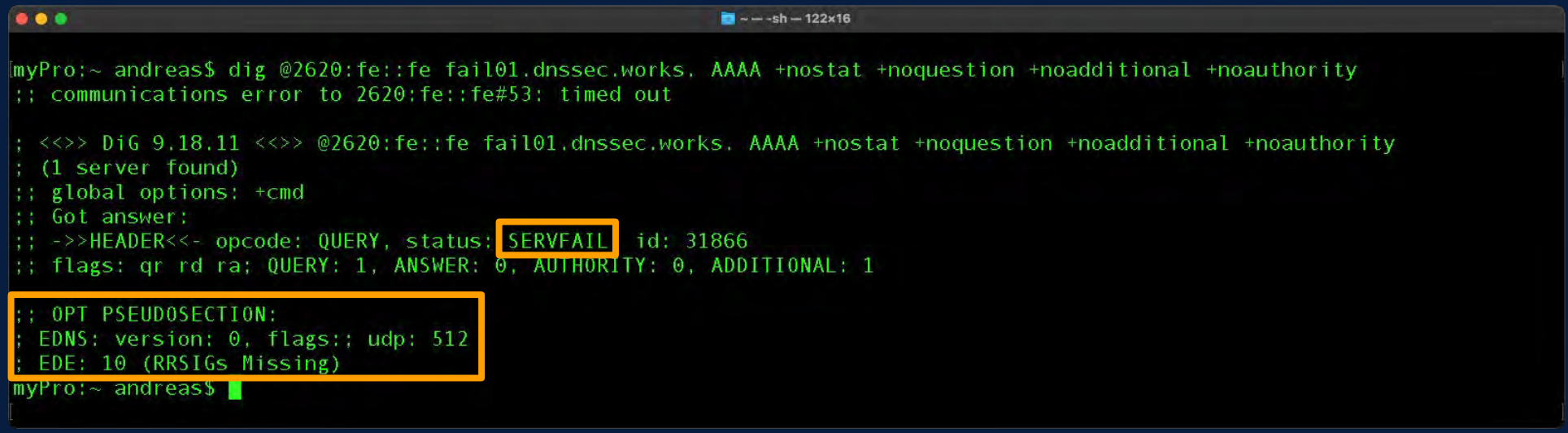
EDE on the Wire

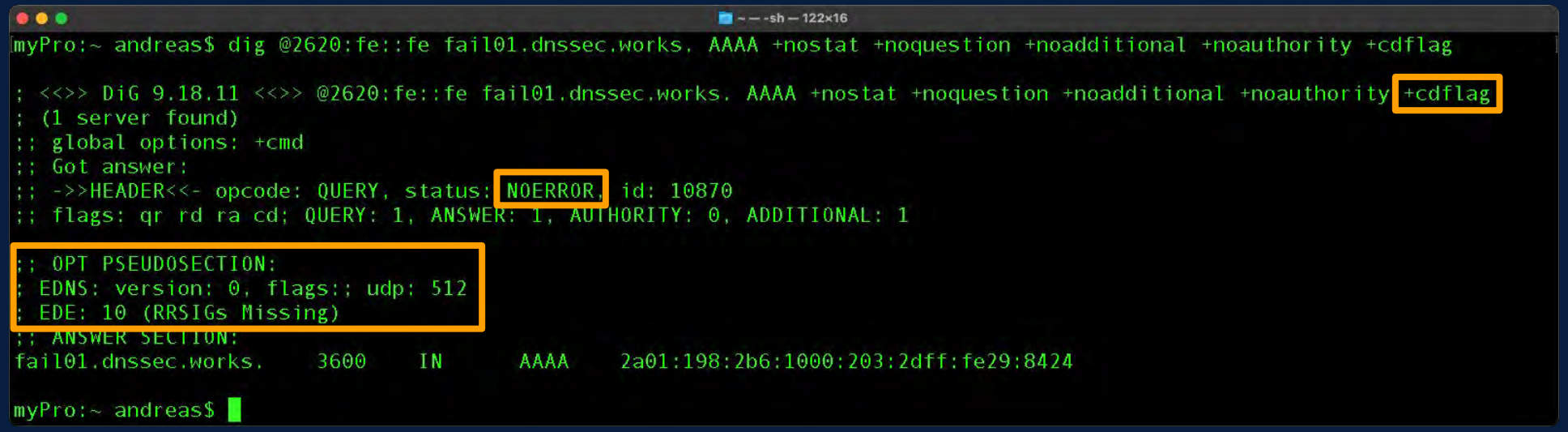


EDE on the Wire

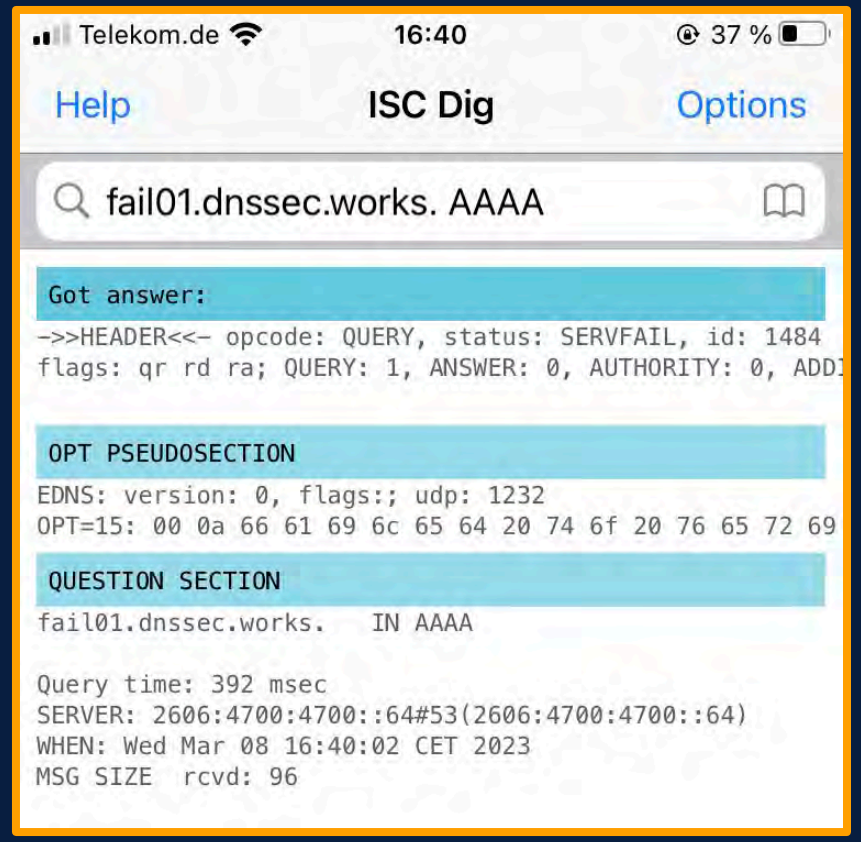


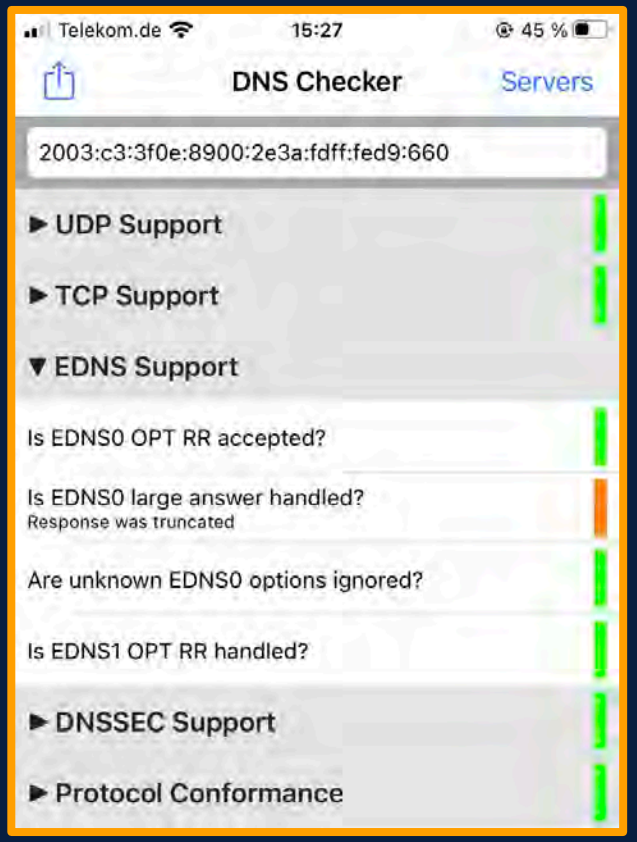
Digging Broken DNSSEC





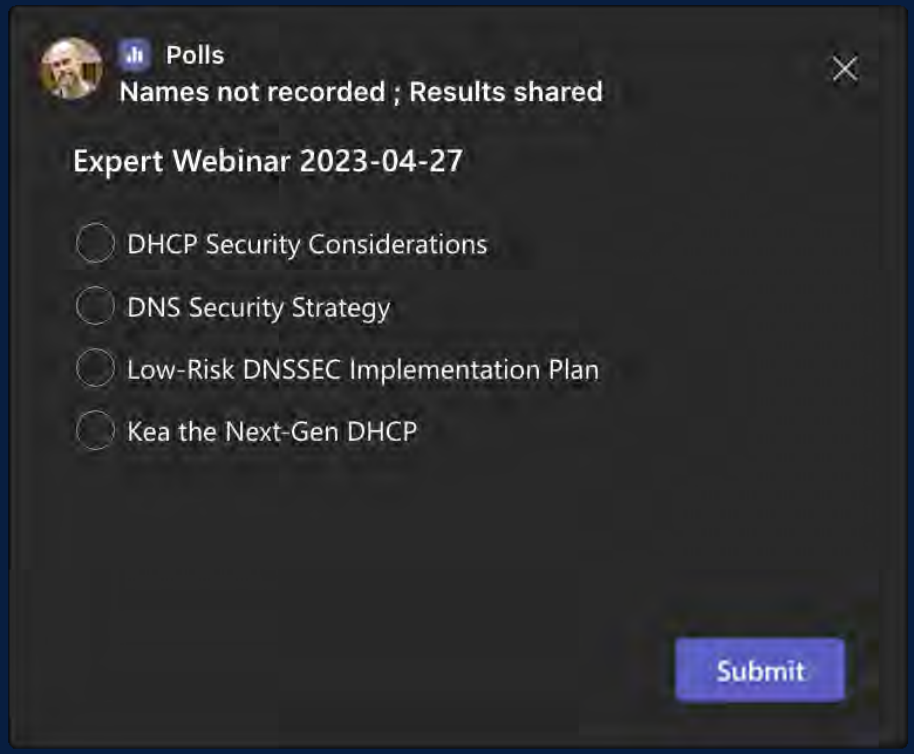
Digging on the Phone





https://apps.apple.com/us/app/isc-dig/id1115648880
https://apps.apple.com/de/app/isc-dns-checker/id1141834002

What's next?


Polls
Names not recorded ; Results shared
Expert Webinar 2023-04-27
DHCP Security Considerations
DNS Security Strategy
Low-Risk DNSSEC Implementation Plan
Kea the Next-Gen DHCP
Submit

Greedy for more?

https://ddiug.de

https://www.n3k.com/en/services/trainings

Thank you for your Time.

N3K Network Systems
Ferdinand-Braun-Straße 2/1 | 74074 Heilbronn
+49 7131 594 95 0
info@n3k.de