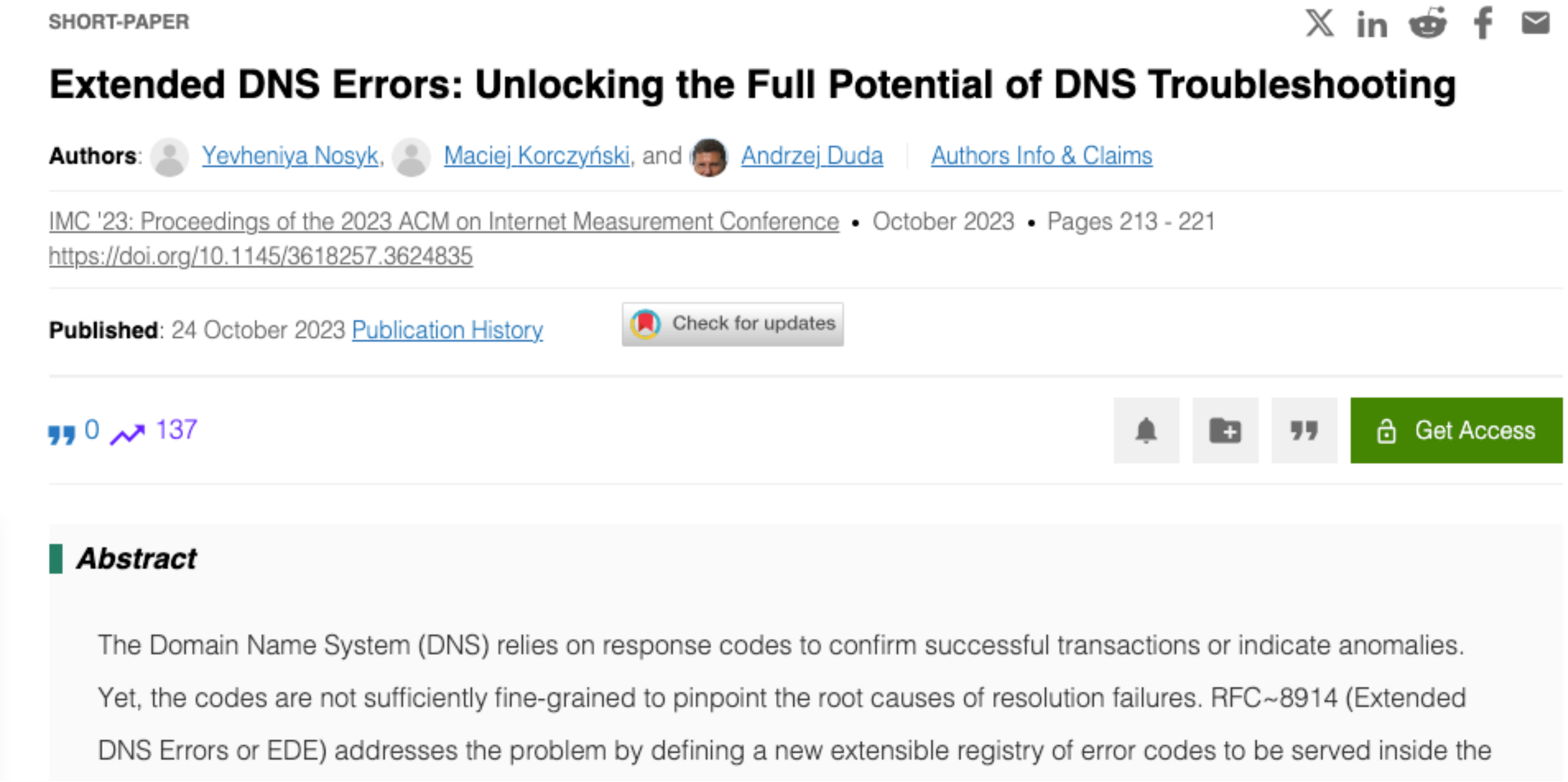
Extended DNS Errors: Unlocking the Full Potential of DNS Troubleshooting

Yevheniya Nosyk, Maciej Korczyński, Andrzej Duda
Université Grenoble Alpes (Grenoble, France)

IETF 120, IRTF Open Meeting (Vancouver, Canada)
July 22, 2024

The paper



SHORT-PAPER

Extended DNS Errors: Unlocking the Full Potential of DNS Troubleshooting

Authors: Yevheniya Nosyk, Maciej Korczyński, and Andrzej Duda | Authors Info & Claims

IMC '23: Proceedings of the 2023 ACM on Internet Measurement Conference • October 2023 • Pages 213 - 221
https://doi.org/10.1145/3618257.3624835

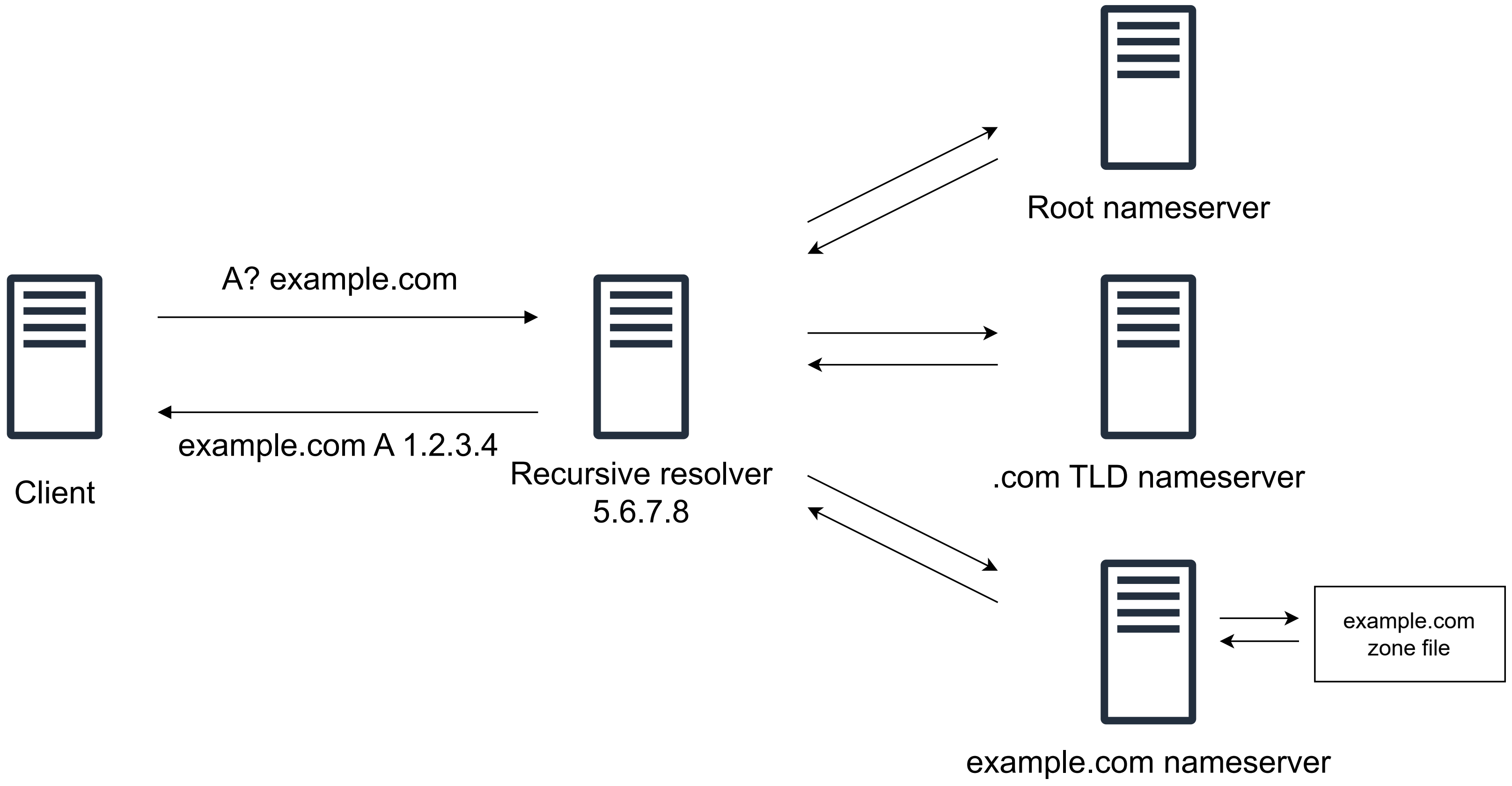
Published: 24 October 2023 Publication History

Abstract

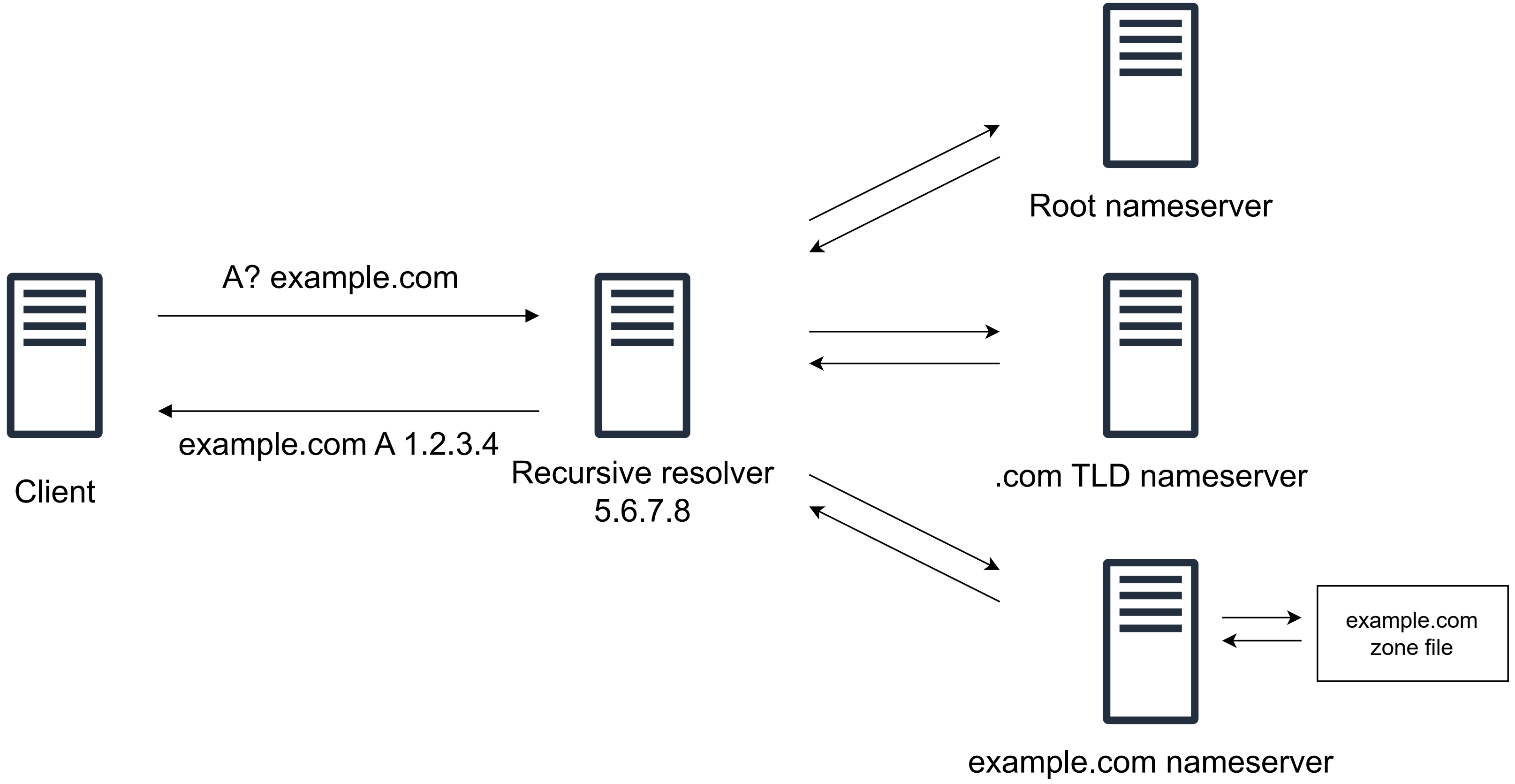
The Domain Name System (DNS) relies on response codes to confirm successful transactions or indicate anomalies. Yet, the codes are not sufficiently fine-grained to pinpoint the root causes of resolution failures. RFC~8914 (Extended DNS Errors or EDE) addresses the problem by defining a new extensible registry of error codes to be served inside the

Source: https://dl.acm.org/doi/10.1145/3618257.3624835

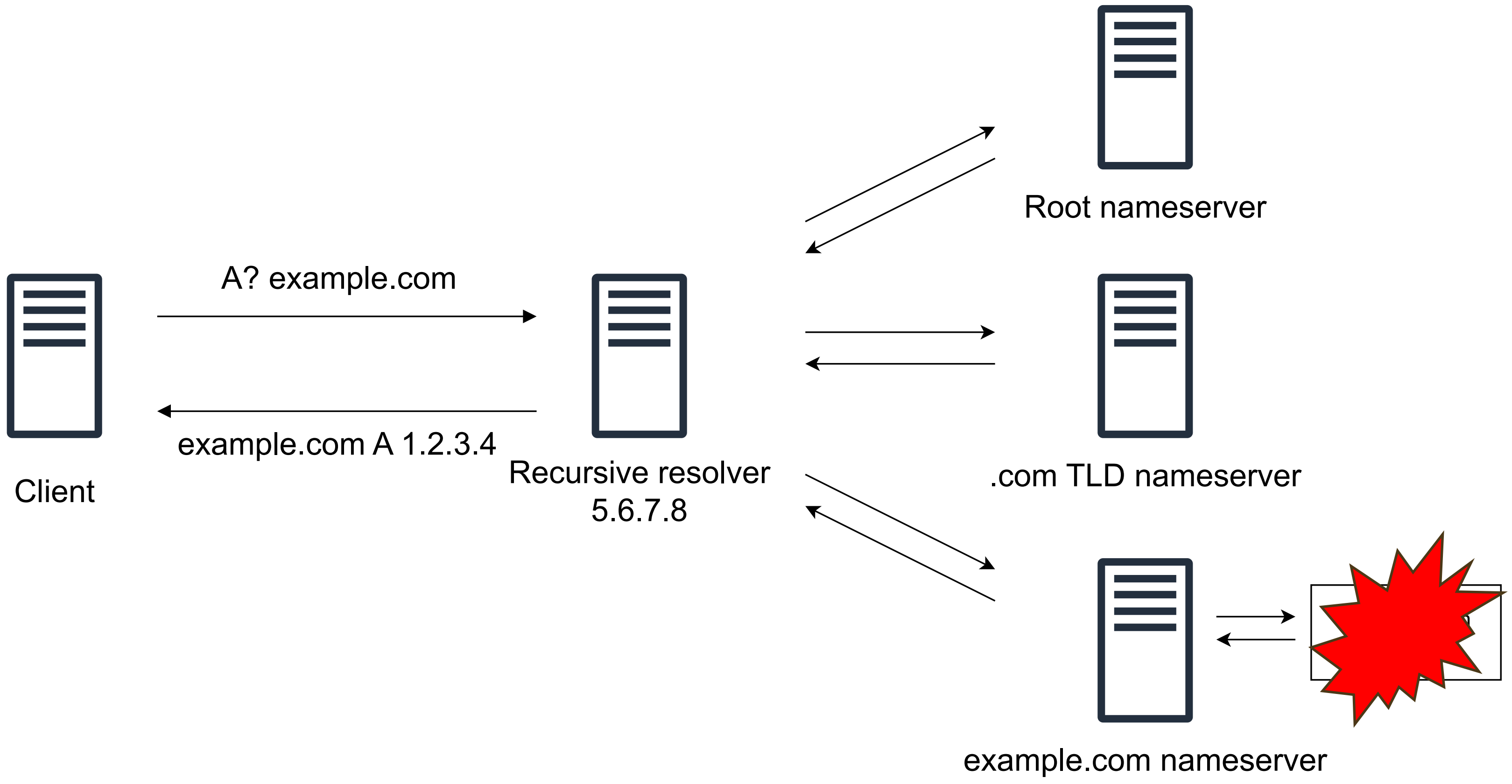
Domain Name System



What can go wrong?



What can go wrong? Everything …



Root nameserver

A? example.com

Client

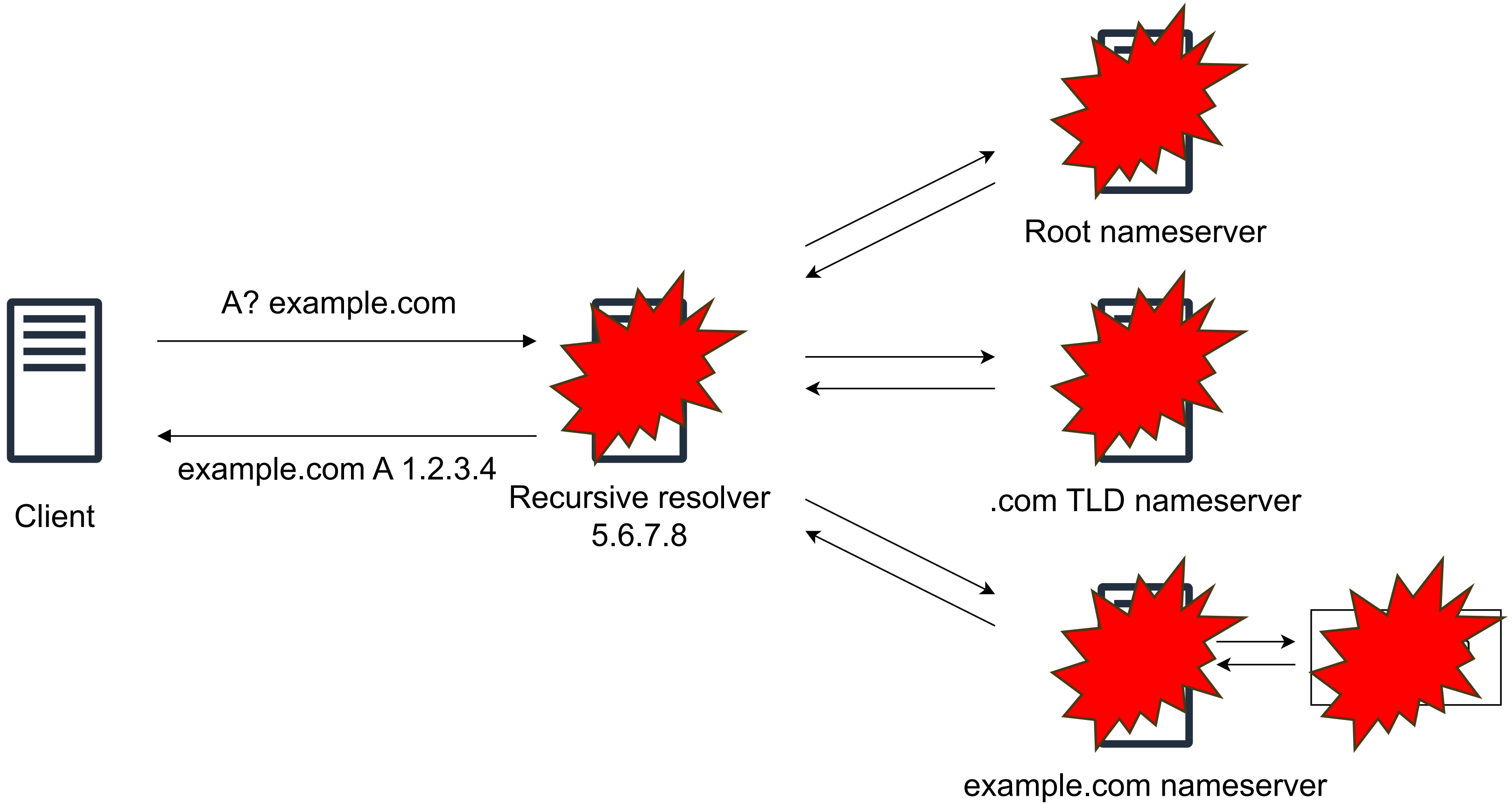
example.com A 1.2.3.4

Recursive resolver
5.6.7.8

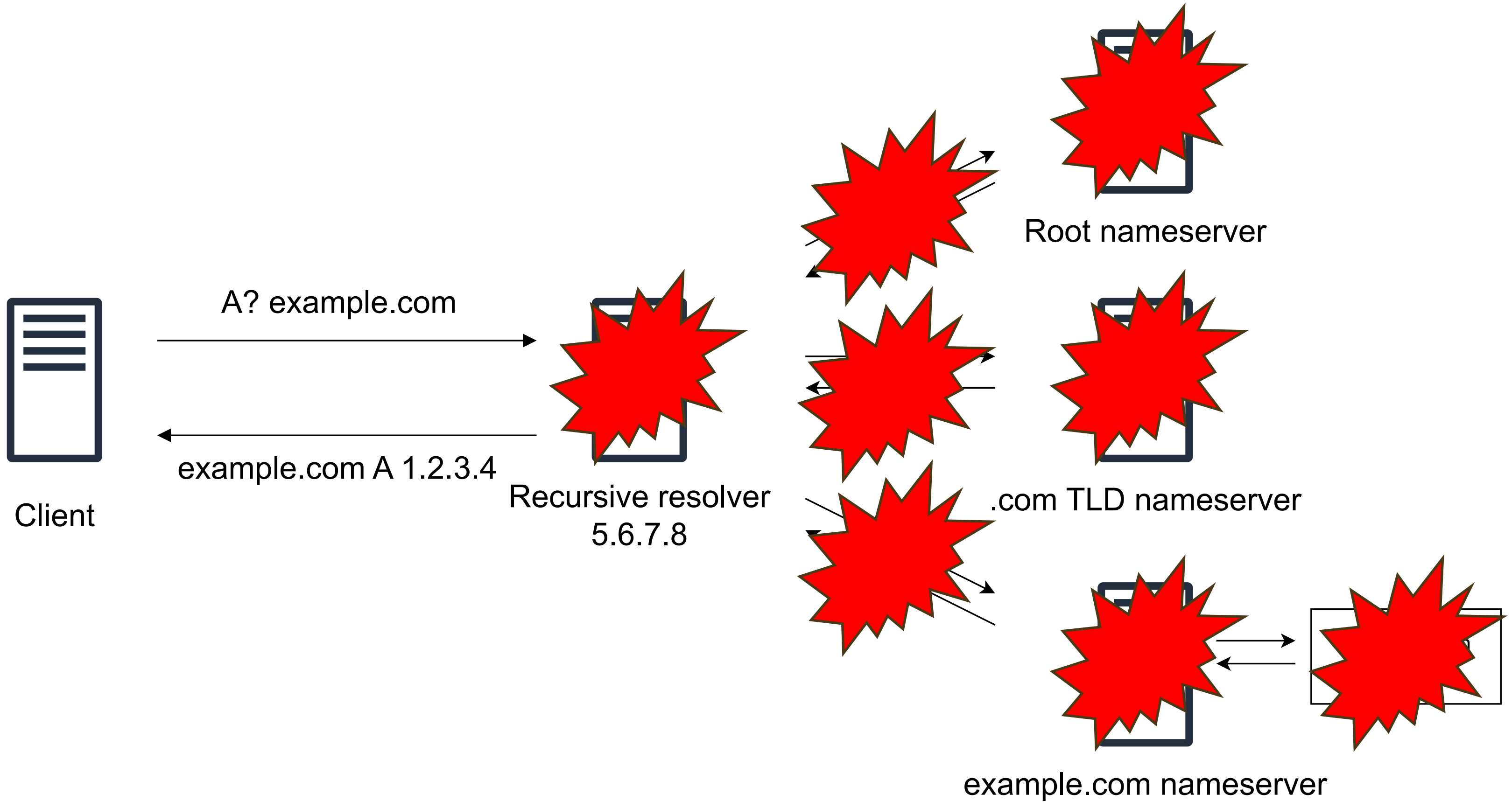
.com TLD nameserver

example.com nameserver

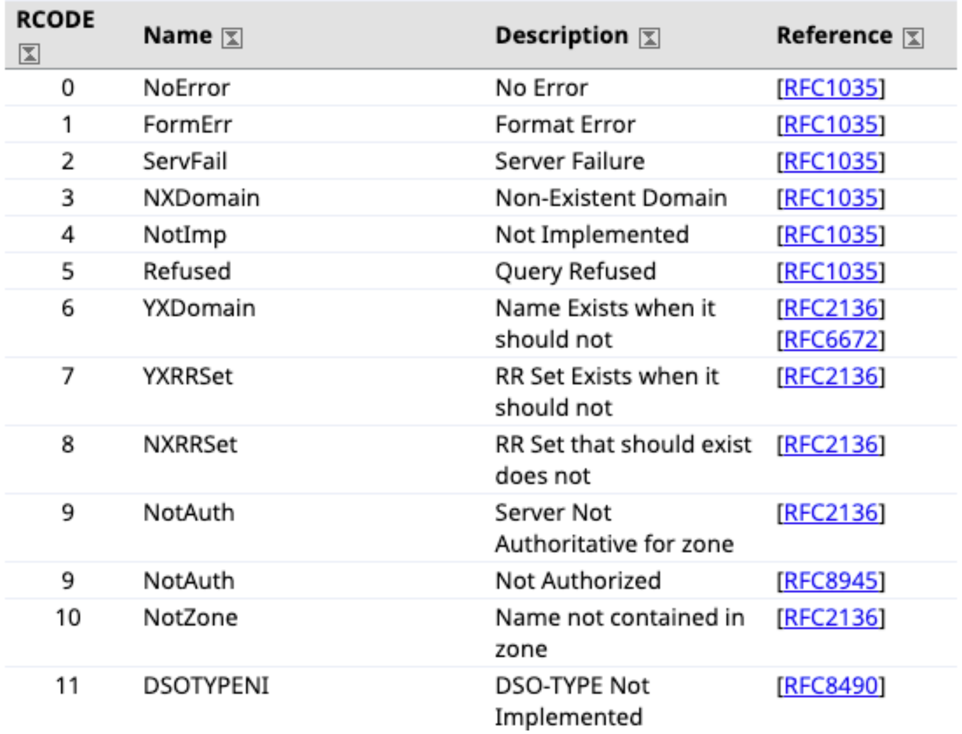
What can go wrong? Everything ...

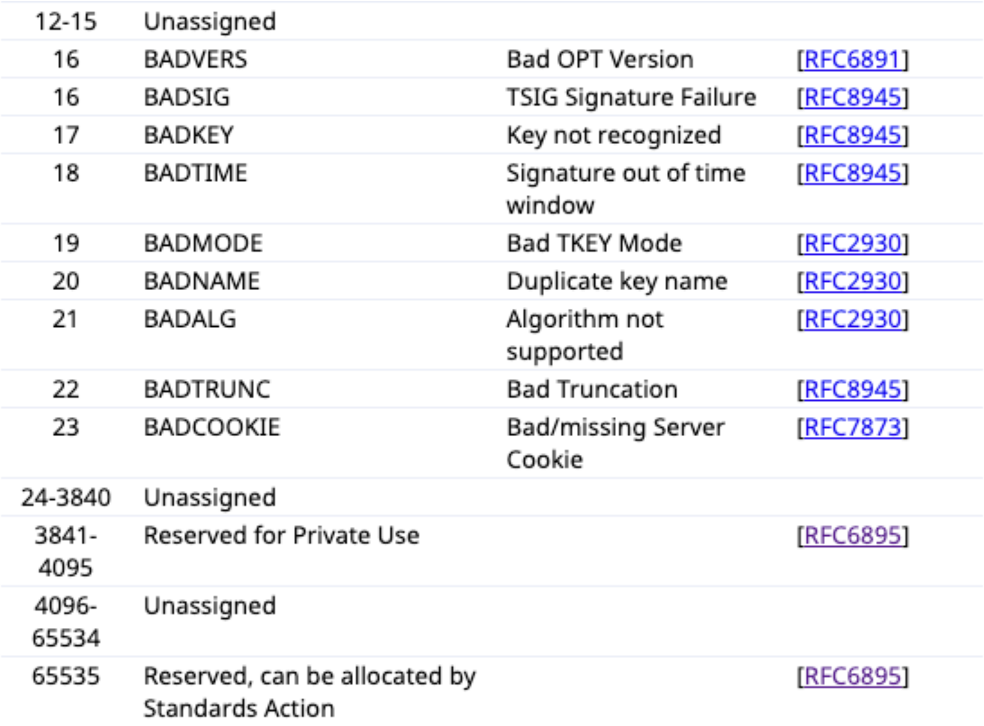


What can go wrong? Everything ...



RCODEs

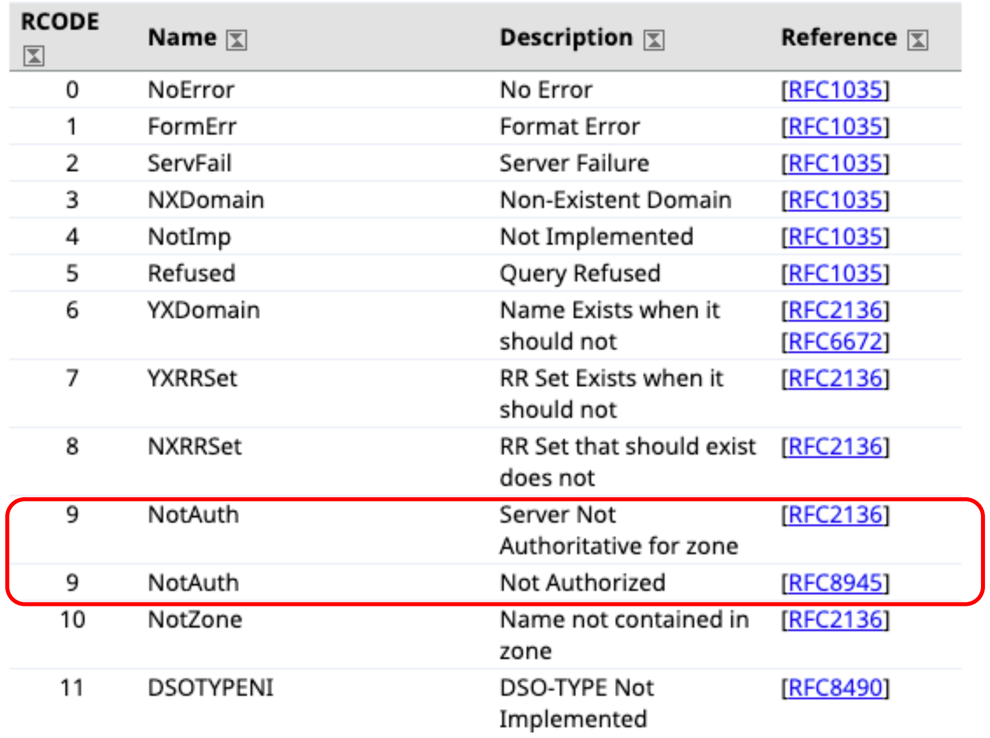


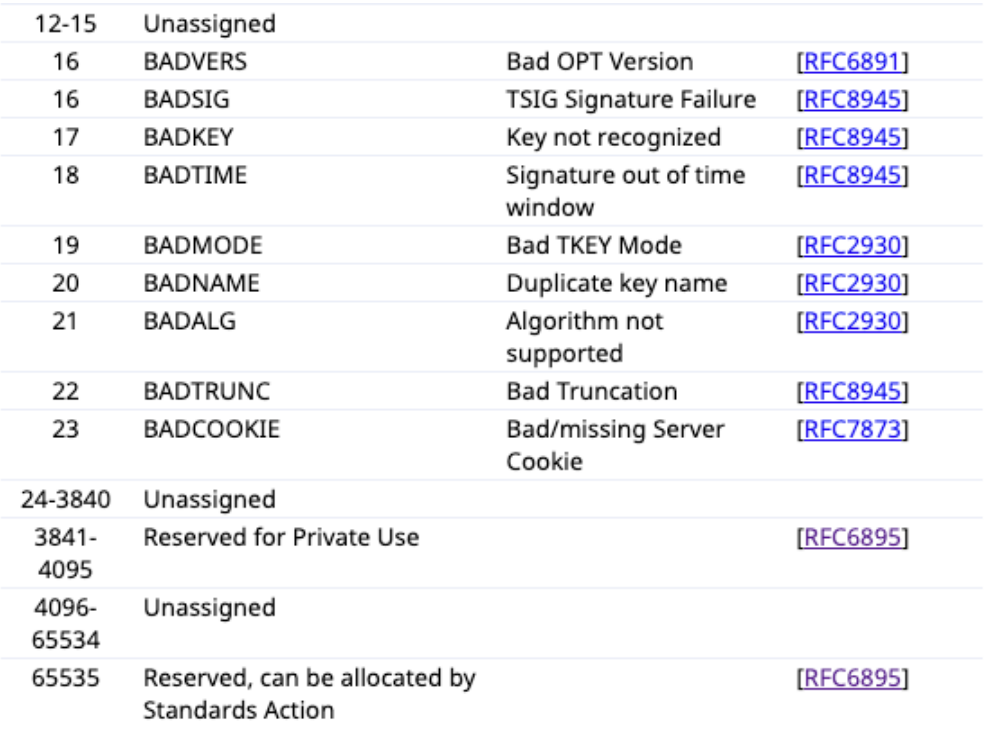


RCODE	Name	Description	Reference
0	NoError	No Error	[RFC1035]
1	FormErr	Format Error	[RFC1035]
2	ServFail	Server Failure	[RFC1035]
3	NXDomain	Non-Existent Domain	[RFC1035]
4	NotImp	Not Implemented	[RFC1035]
5	Refused	Query Refused	[RFC1035]
6	YXDomain	Name Exists when it should not	[RFC2136] [RFC6672]
7	YXRRSet	RR Set Exists when it should not	[RFC2136]
8	NXRRSet	RR Set that should exist does not	[RFC2136]
9	NotAuth	Server Not Authoritative for zone	[RFC2136]
9	NotAuth	Not Authorized	[RFC8945]
10	NotZone	Name not contained in zone	[RFC2136]
11	DSOTYPENI	DSO-TYPE Not Implemented	[RFC8490]
12-15	Unassigned		
16	BADVERS	Bad OPT Version	[RFC6891]
16	BADSIG	TSIG Signature Failure	[RFC8945]
17	BADKEY	Key not recognized	[RFC8945]
18	BADTIME	Signature out of time window	[RFC8945]
19	BADMODE	Bad TKEY Mode	[RFC2930]
20	BADNAME	Duplicate key name	[RFC2930]
21	BADALG	Algorithm not supported	[RFC2930]
22	BADTRUNC	Bad Truncation	[RFC8945]
23	BADCOOKIE	Bad/missing Server Cookie	[RFC7873]
24-3840	Unassigned		
3841-4095	Reserved for Private Use		[RFC6895]
4096-65534	Unassigned		
65535	Reserved, can be allocated by Standards Action		[RFC6895]

Source: https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-6

RCODEs

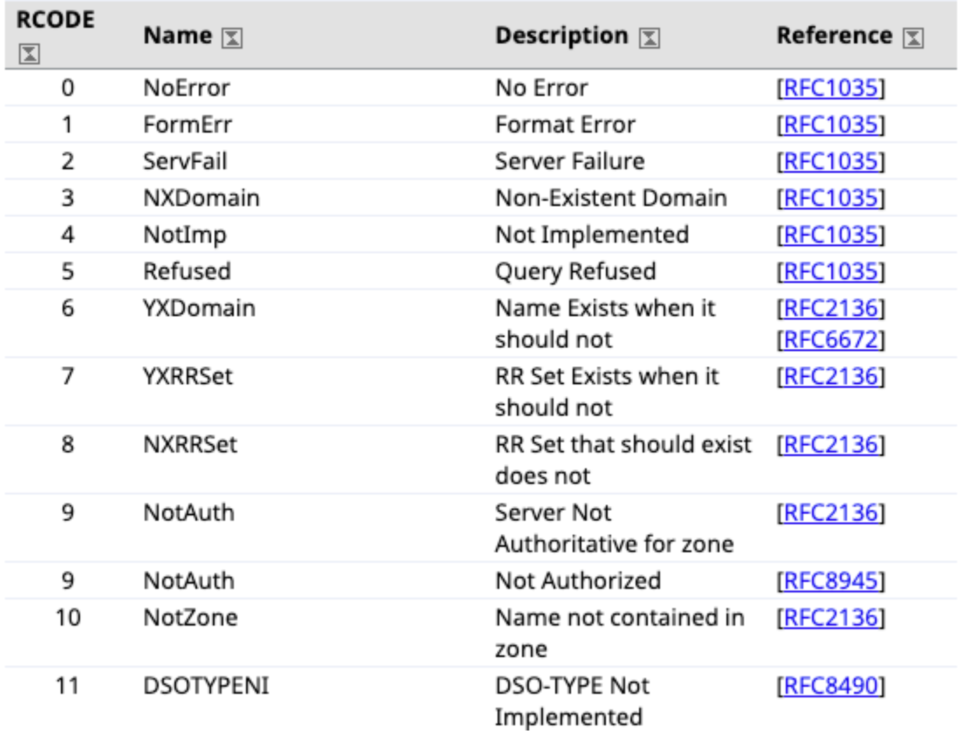




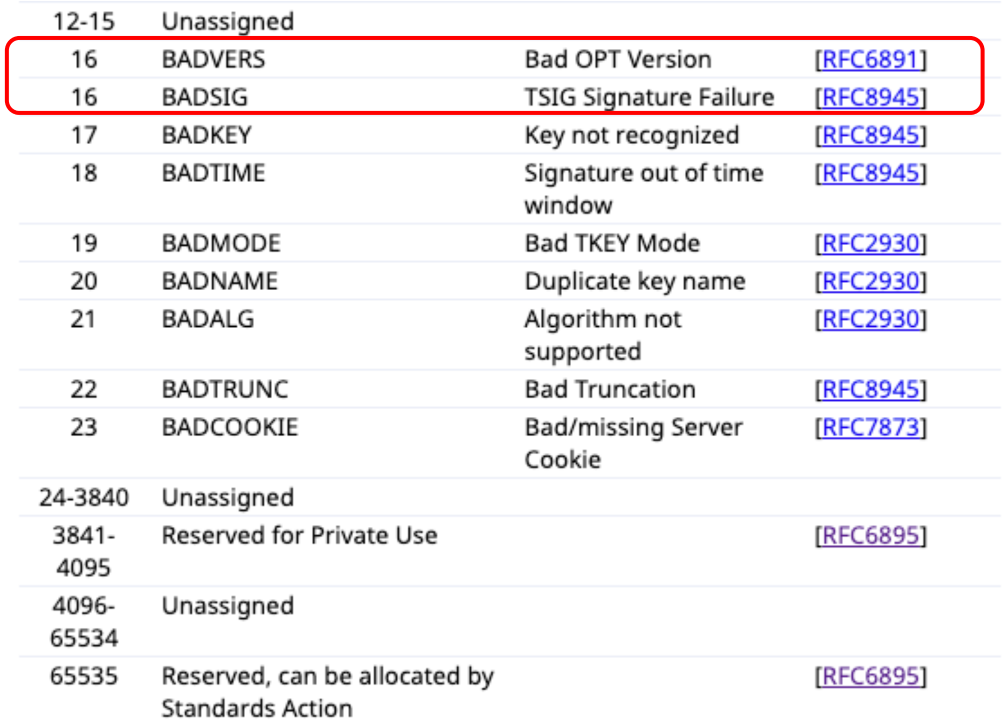
RCODE	Name	Description	Reference
0	NoError	No Error	[RFC1035]
1	FormErr	Format Error	[RFC1035]
2	ServFail	Server Failure	[RFC1035]
3	NXDomain	Non-Existent Domain	[RFC1035]
4	NotImp	Not Implemented	[RFC1035]
5	Refused	Query Refused	[RFC1035]
6	YXDomain	Name Exists when it should not	[RFC2136] [RFC6672]
7	YXRRSet	RR Set Exists when it should not	[RFC2136]
8	NXRRSet	RR Set that should exist does not	[RFC2136]
9	NotAuth	Server Not Authoritative for zone	[RFC2136]
9	NotAuth	Not Authorized	[RFC8945]
10	NotZone	Name not contained in zone	[RFC2136]
11	DSOTYPENI	DSO-TYPE Not Implemented	[RFC8490]
12-15	Unassigned		
16	BADVERS	Bad OPT Version	[RFC6891]
16	BADSIG	TSIG Signature Failure	[RFC8945]
17	BADKEY	Key not recognized	[RFC8945]
18	BADTIME	Signature out of time window	[RFC8945]
19	BADMODE	Bad TKEY Mode	[RFC2930]
20	BADNAME	Duplicate key name	[RFC2930]
21	BADALG	Algorithm not supported	[RFC2930]
22	BADTRUNC	Bad Truncation	[RFC8945]
23	BADCOOKIE	Bad/missing Server Cookie	[RFC7873]
24-3840	Unassigned		
3841-4095	Reserved for Private Use		[RFC6895]
4096-65534	Unassigned		
65535	Reserved, can be allocated by Standards Action		[RFC6895]

Source: https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-6

RCODEs



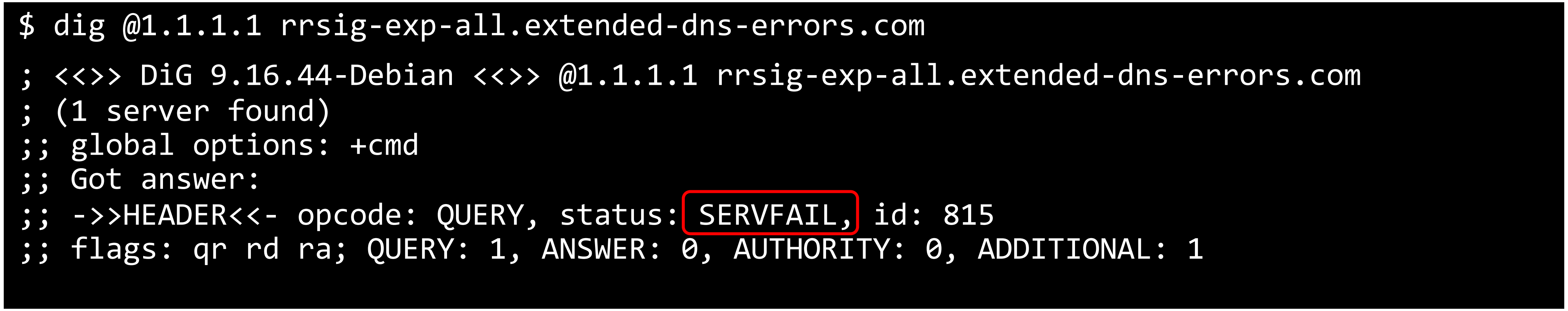
RCODE	Name	Description	Reference
0	NoError	No Error	[RFC1035]
1	FormErr	Format Error	[RFC1035]
2	ServFail	Server Failure	[RFC1035]
3	NXDomain	Non-Existent Domain	[RFC1035]
4	NotImp	Not Implemented	[RFC1035]
5	Refused	Query Refused	[RFC1035]
6	YXDomain	Name Exists when it should not	[RFC2136] [RFC6672]
7	YXRRSet	RR Set Exists when it should not	[RFC2136]
8	NXRRSet	RR Set that should exist does not	[RFC2136]
9	NotAuth	Server Not Authoritative for zone	[RFC2136]
9	NotAuth	Not Authorized	[RFC8945]
10	NotZone	Name not contained in zone	[RFC2136]
11	DSOTYPENI	DSO-TYPE Not Implemented	[RFC8490]



12-15	Unassigned		
16	BADVERS	Bad OPT Version	[RFC6891]
16	BADSIG	TSIG Signature Failure	[RFC8945]
17	BADKEY	Key not recognized	[RFC8945]
18	BADTIME	Signature out of time window	[RFC8945]
19	BADMODE	Bad TKEY Mode	[RFC2930]
20	BADNAME	Duplicate key name	[RFC2930]
21	BADALG	Algorithm not supported	[RFC2930]
22	BADTRUNC	Bad Truncation	[RFC8945]
23	BADCOOKIE	Bad/missing Server Cookie	[RFC7873]
24-3840	Unassigned		
3841-4095	Reserved for Private Use		[RFC6895]
4096-65534	Unassigned		
65535	Reserved, can be allocated by Standards Action		[RFC6895]

Source: https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-6

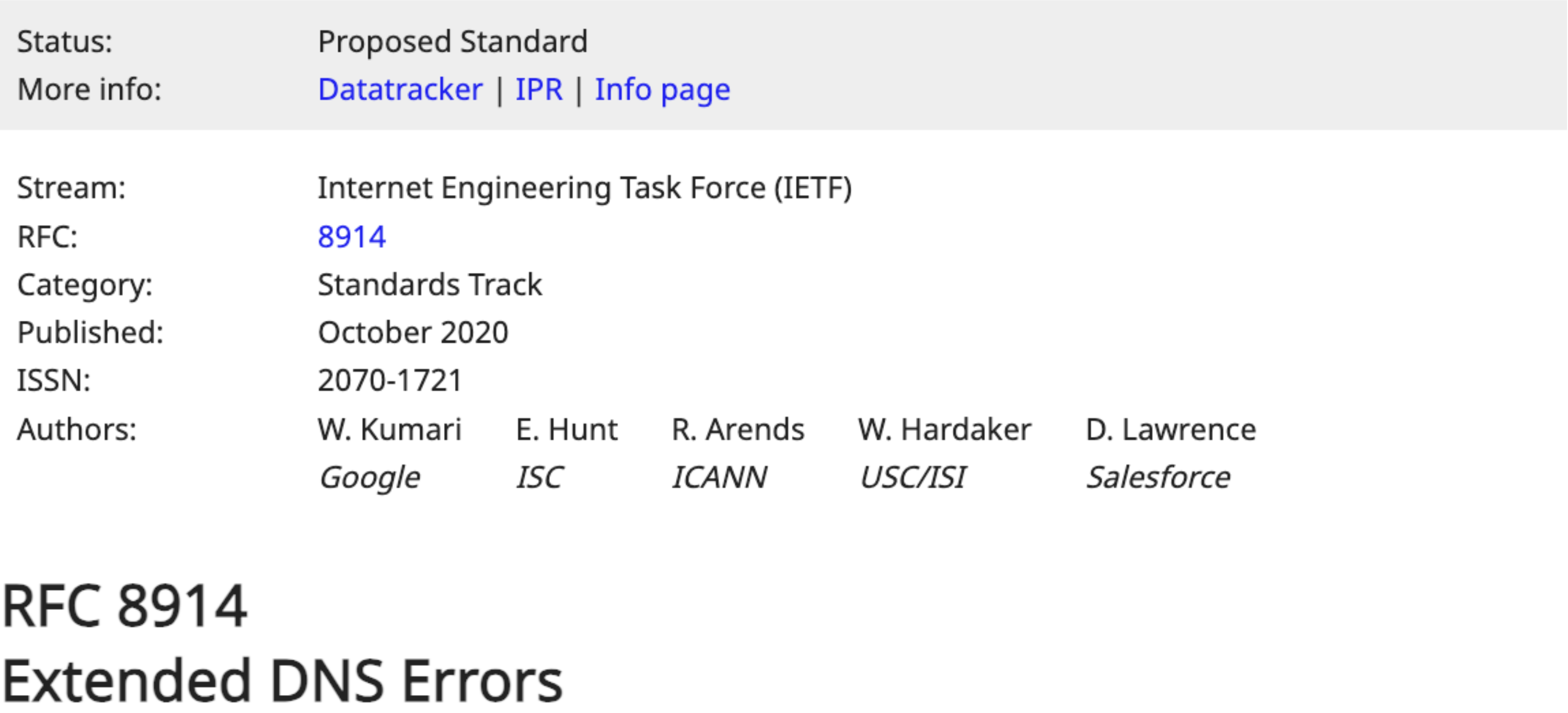
Prevalence of SERVFAILs



```
$ dig @1.1.1.1 rrsig-exp-all.extended-dns-errors.com

; <<>> DiG 9.16.44-Debian <<>> @1.1.1.1 rrsig-exp-all.extended-dns-errors.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 815
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
```

Solution:
Extended DNS Errors

RFC 8914



Status:	Proposed Standard
More info:	Datatracker | IPR | Info page

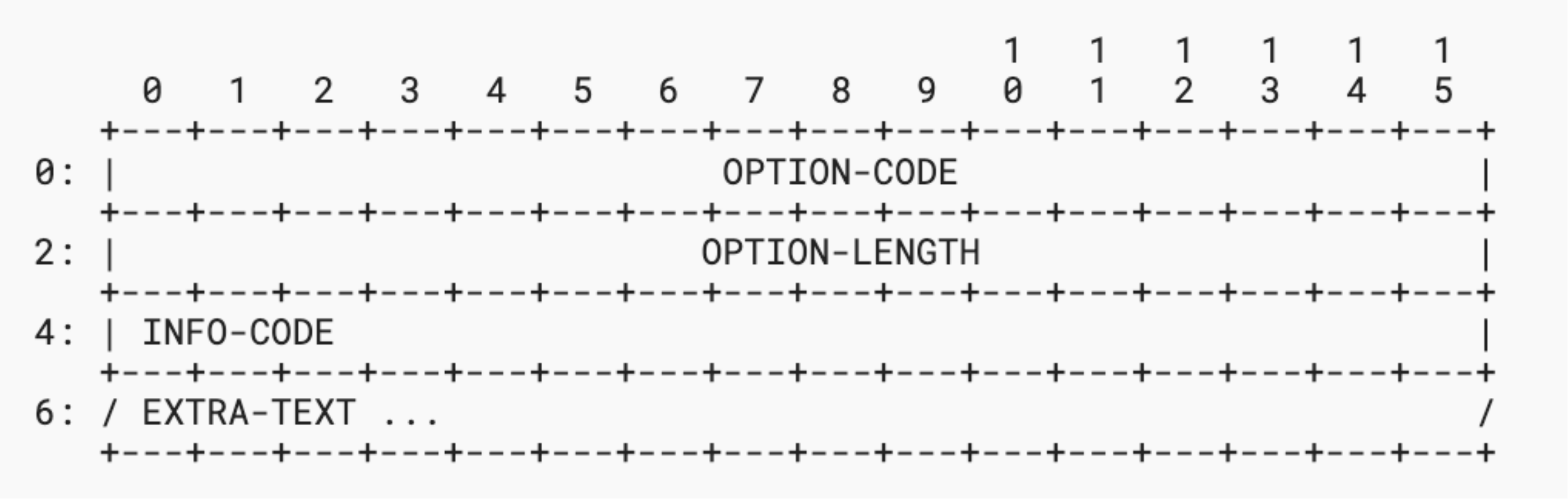
Stream:	Internet Engineering Task Force (IETF)
RFC:	8914
Category:	Standards Track
Published:	October 2020
ISSN:	2070-1721

Authors:	W. Kumari	E. Hunt	R. Arends	W. Hardaker	D. Lawrence
	Google	*ISC*	*ICANN*	*USC/ISI*	*Salesforce*

RFC 8914
Extended DNS Errors

Source: https://www.rfc-editor.org/rfc/rfc8914.html

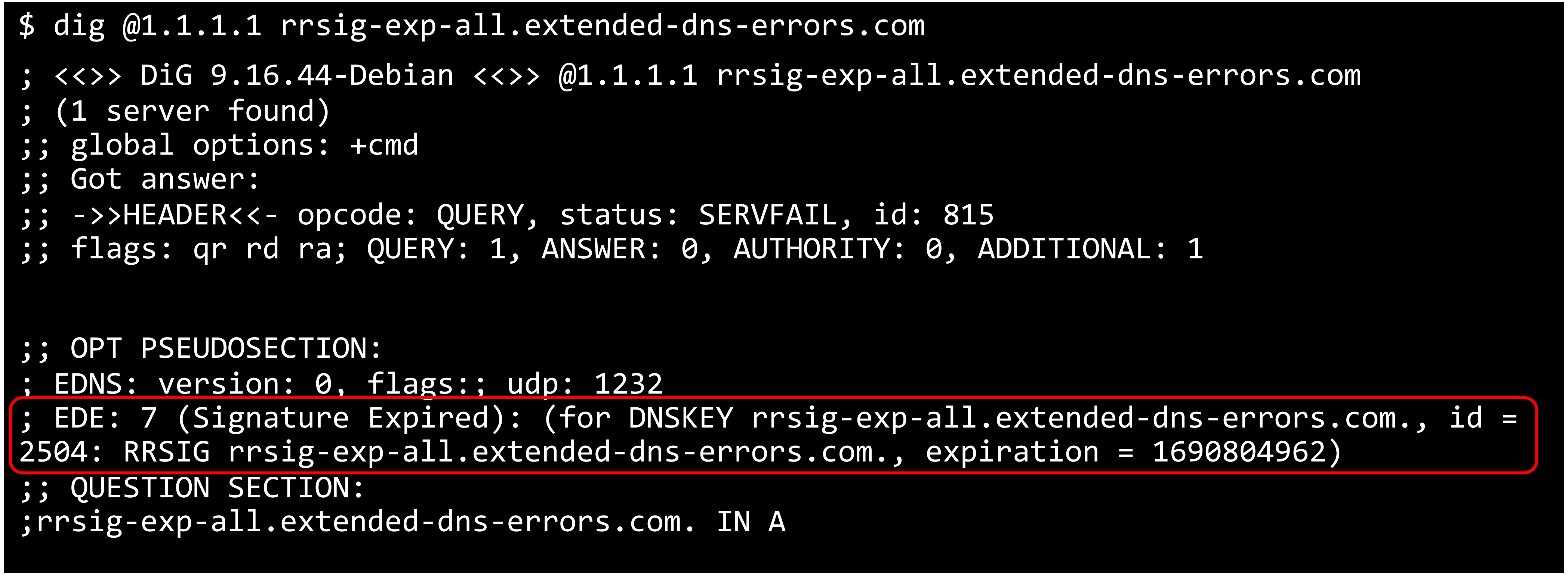
RFC 8914: Format



```
                                             1   1   1   1   1   1
     0   1   2   3   4   5   6   7   8   9   0   1   2   3   4   5
   +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
0: |                            OPTION-CODE                        |
   +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
2: |                           OPTION-LENGTH                       |
   +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
4: | INFO-CODE                                                     |
   +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
6: / EXTRA-TEXT ...                                                /
   +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

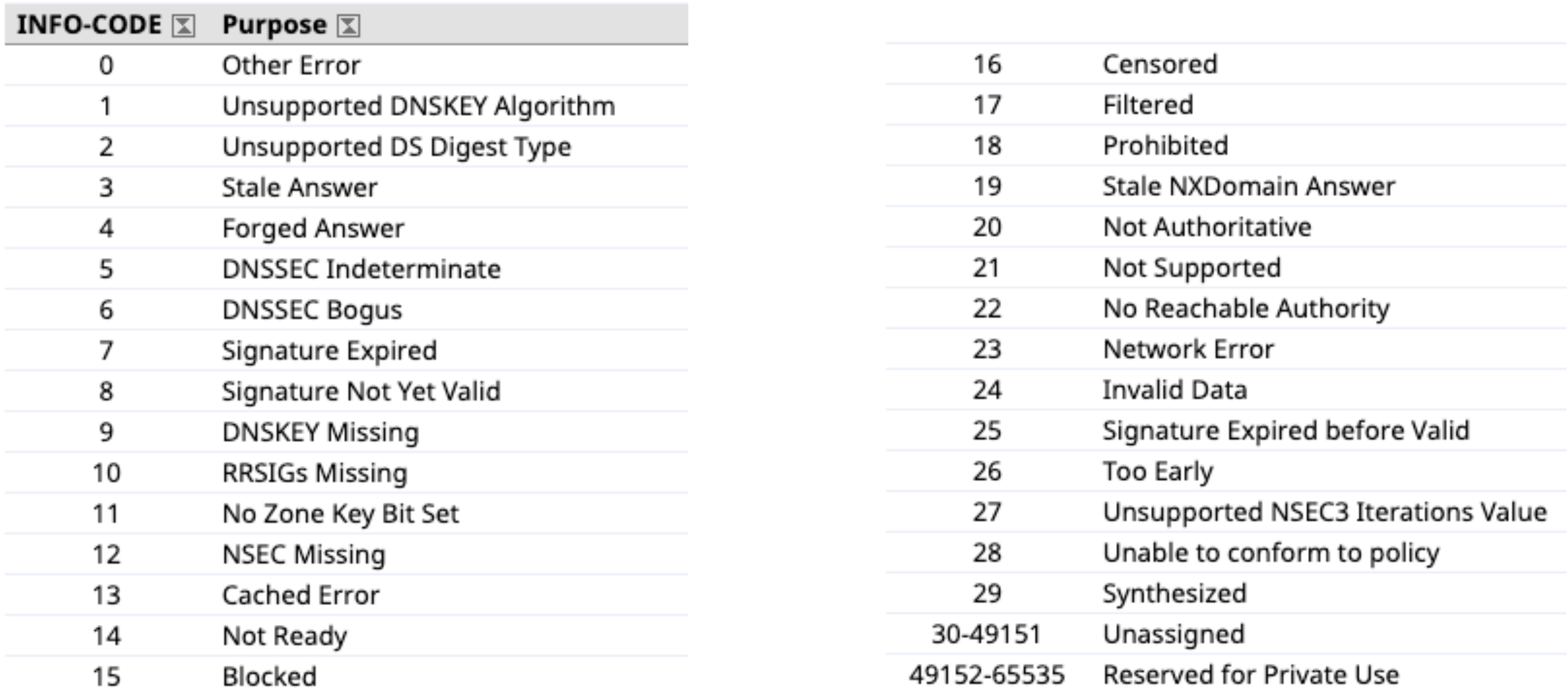
Source: https://www.rfc-editor.org/rfc/rfc8914.html

EDE 7 (Signature Expired)



```
$ dig @1.1.1.1 rrsig-exp-all.extended-dns-errors.com
; <<>> DiG 9.16.44-Debian <<>> @1.1.1.1 rrsig-exp-all.extended-dns-errors.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 815
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1


;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; EDE: 7 (Signature Expired): (for DNSKEY rrsig-exp-all.extended-dns-errors.com., id =
2504: RRSIG rrsig-exp-all.extended-dns-errors.com., expiration = 1690804962)
;; QUESTION SECTION:
;rrsig-exp-all.extended-dns-errors.com. IN A
```

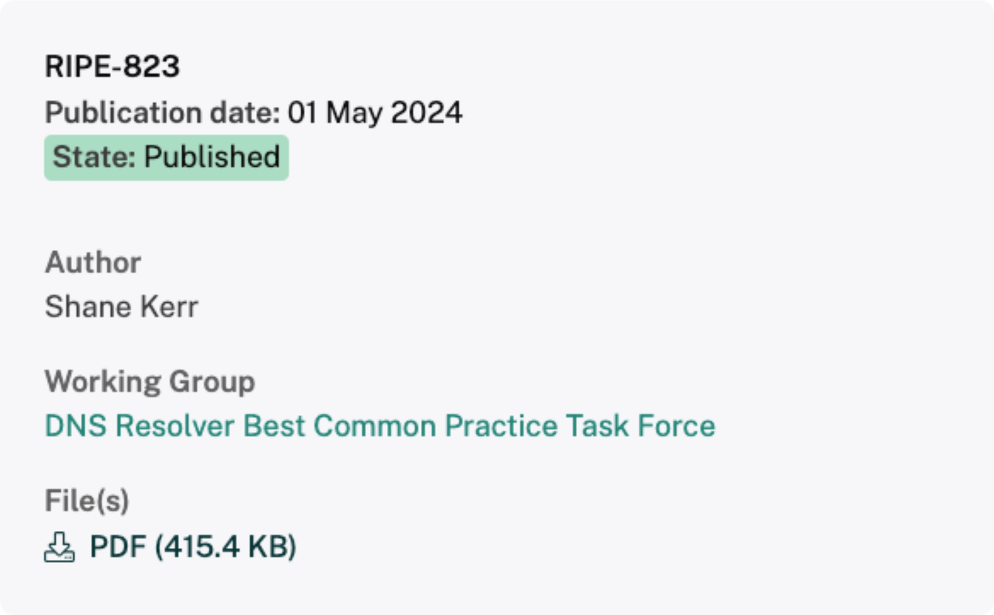
Extended DNS Error Codes



INFO-CODE	Purpose
0	Other Error
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
25	Signature Expired before Valid
26	Too Early
27	Unsupported NSEC3 Iterations Value
28	Unable to conform to policy
29	Synthesized
30-49151	Unassigned
49152-65535	Reserved for Private Use

Source: https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#extended-dns-error-codes

DNS Resolver Recommendations



RIPE-823

Publication date: 01 May 2024

State: Published

Author

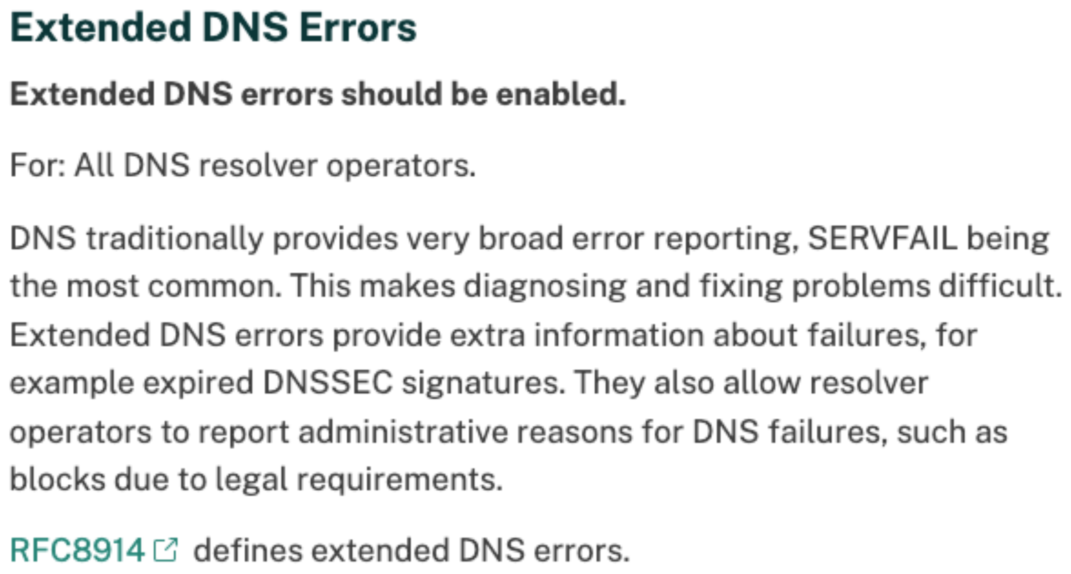
Shane Kerr

Working Group

DNS Resolver Best Common Practice Task Force

File(s)

PDF (415.4 KB)



Extended DNS Errors

Extended DNS errors should be enabled.

For: All DNS resolver operators.

DNS traditionally provides very broad error reporting, SERVFAIL being the most common. This makes diagnosing and fixing problems difficult. Extended DNS errors provide extra information about failures, for example expired DNSSEC signatures. They also allow resolver operators to report administrative reasons for DNS failures, such as blocks due to legal requirements.

RFC8914 defines extended DNS errors.

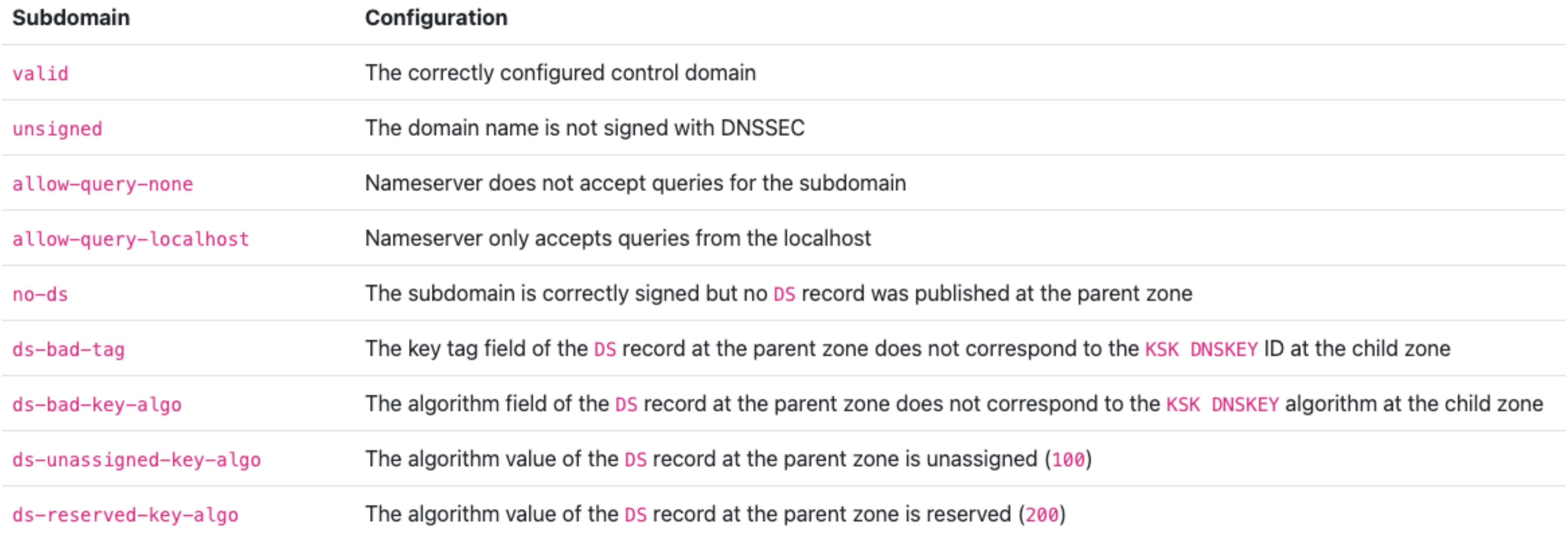
Source: https://www.ripe.net/publications/docs/ripe-823/

How is the RFC-8914 implemented by software vendors and public resolver providers?

Tested Systems

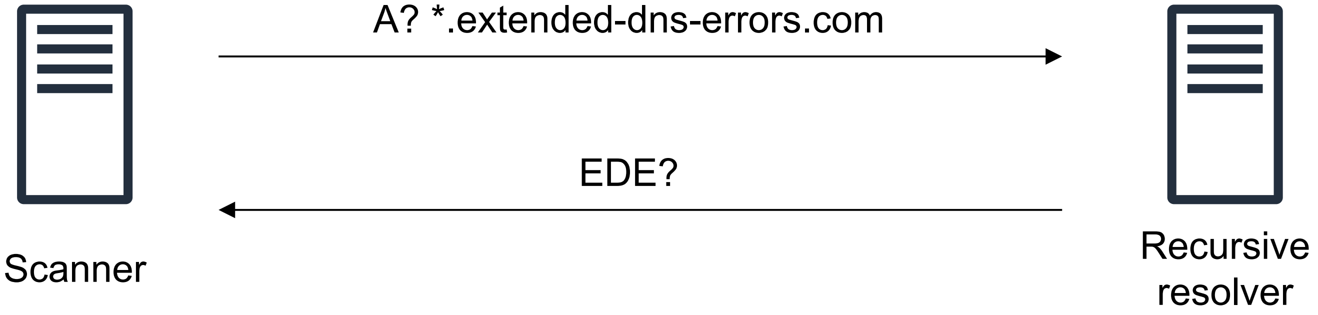
- BIND 9.19.23
- Unbound 1.20.0
- PowerDNS Recursor 5.0.4
- Knot Resolver 5.7.3
- Cloudflare (1.1.1.1)
- Google (8.8.8.8)
- Quad9 (9.9.9.9)
- DNS4ALL (194.0.5.3)
- OpenDNS (208.67.222.222)

extended-dns-errors.com



Subdomain	Configuration
`valid`	The correctly configured control domain
`unsigned`	The domain name is not signed with DNSSEC
`allow-query-none`	Nameserver does not accept queries for the subdomain
`allow-query-localhost`	Nameserver only accepts queries from the localhost
`no-ds`	The subdomain is correctly signed but no `DS` record was published at the parent zone
`ds-bad-tag`	The key tag field of the `DS` record at the parent zone does not correspond to the `KSK DNSKEY` ID at the child zone
`ds-bad-key-algo`	The algorithm field of the `DS` record at the parent zone does not correspond to the `KSK DNSKEY` algorithm at the child zone
`ds-unassigned-key-algo`	The algorithm value of the `DS` record at the parent zone is unassigned (`100`)
`ds-reserved-key-algo`	The algorithm value of the `DS` record at the parent zone is reserved (`200`)

Methodology



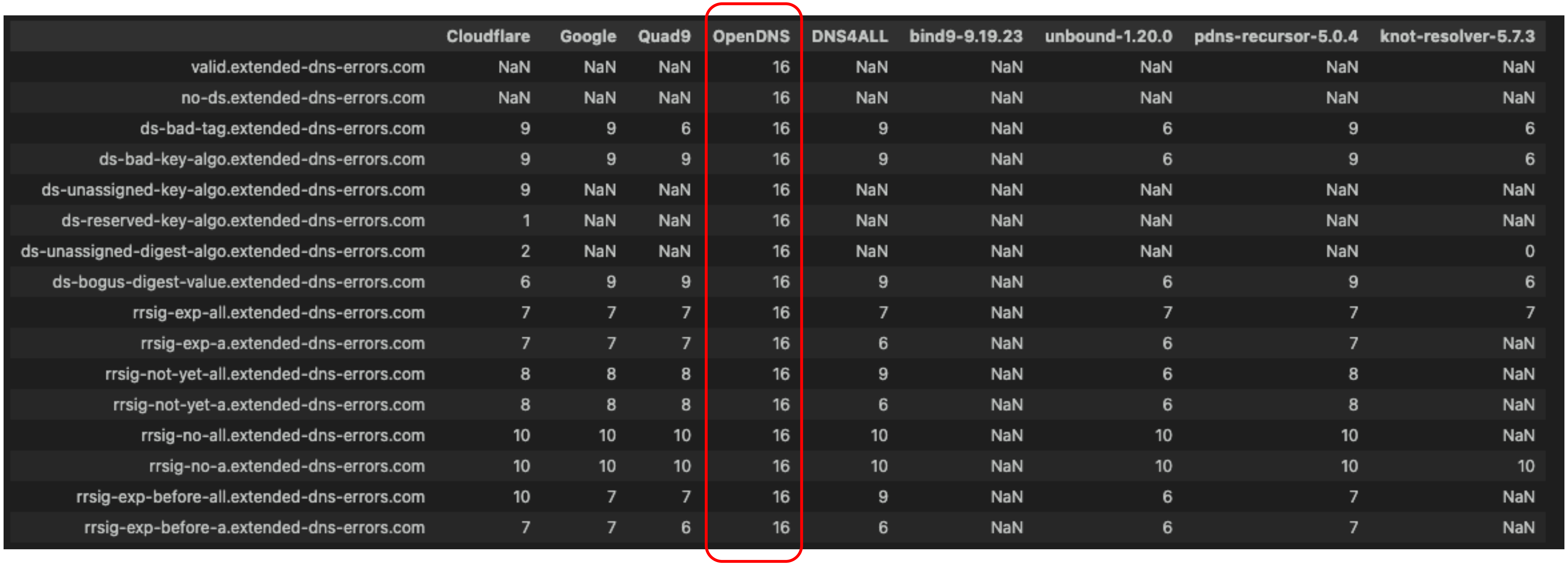
A? *.extended-dns-errors.com

EDE?

Scanner

Recursive resolver

OpenDNS Censored?

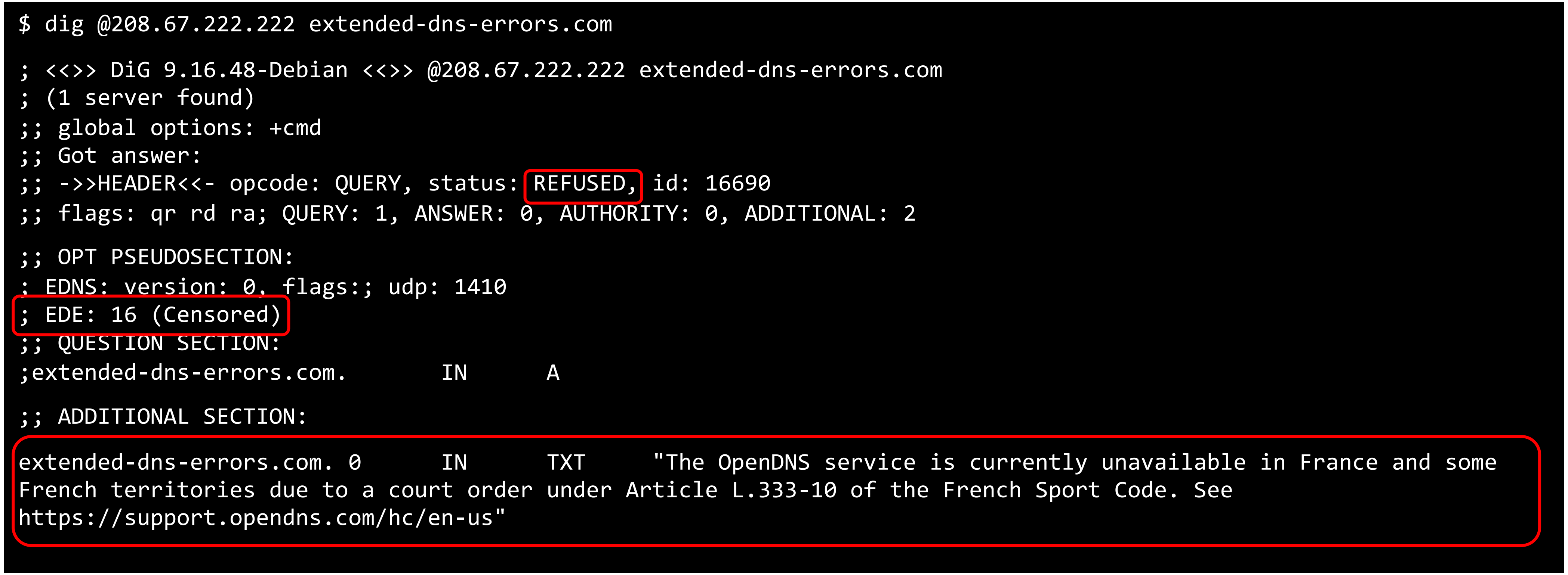


	Cloudflare	Google	Quad9	OpenDNS	DNS4ALL	bind9-9.19.23	unbound-1.20.0	pdns-recursor-5.0.4	knot-resolver-5.7.3
valid.extended-dns-errors.com	NaN	NaN	NaN	16	NaN	NaN	NaN	NaN	NaN
no-ds.extended-dns-errors.com	NaN	NaN	NaN	16	NaN	NaN	NaN	NaN	NaN
ds-bad-tag.extended-dns-errors.com	9	9	6	16	9	NaN	6	9	6
ds-bad-key-algo.extended-dns-errors.com	9	9	9	16	9	NaN	6	9	6
ds-unassigned-key-algo.extended-dns-errors.com	9	NaN	NaN	16	NaN	NaN	NaN	NaN	NaN
ds-reserved-key-algo.extended-dns-errors.com	1	NaN	NaN	16	NaN	NaN	NaN	NaN	NaN
ds-unassigned-digest-algo.extended-dns-errors.com	2	NaN	NaN	16	NaN	NaN	NaN	NaN	0
ds-bogus-digest-value.extended-dns-errors.com	6	9	9	16	9	NaN	6	9	6
rrsig-exp-all.extended-dns-errors.com	7	7	7	16	7	NaN	7	7	7
rrsig-exp-a.extended-dns-errors.com	7	7	7	16	6	NaN	6	7	NaN
rrsig-not-yet-all.extended-dns-errors.com	8	8	8	16	9	NaN	6	8	NaN
rrsig-not-yet-a.extended-dns-errors.com	8	8	8	16	6	NaN	6	8	NaN
rrsig-no-all.extended-dns-errors.com	10	10	10	16	10	NaN	10	10	NaN
rrsig-no-a.extended-dns-errors.com	10	10	10	16	10	NaN	10	10	10
rrsig-exp-before-all.extended-dns-errors.com	10	7	7	16	9	NaN	6	7	NaN
rrsig-exp-before-a.extended-dns-errors.com	7	7	6	16	6	NaN	6	7	NaN

OpenDNS Censored?

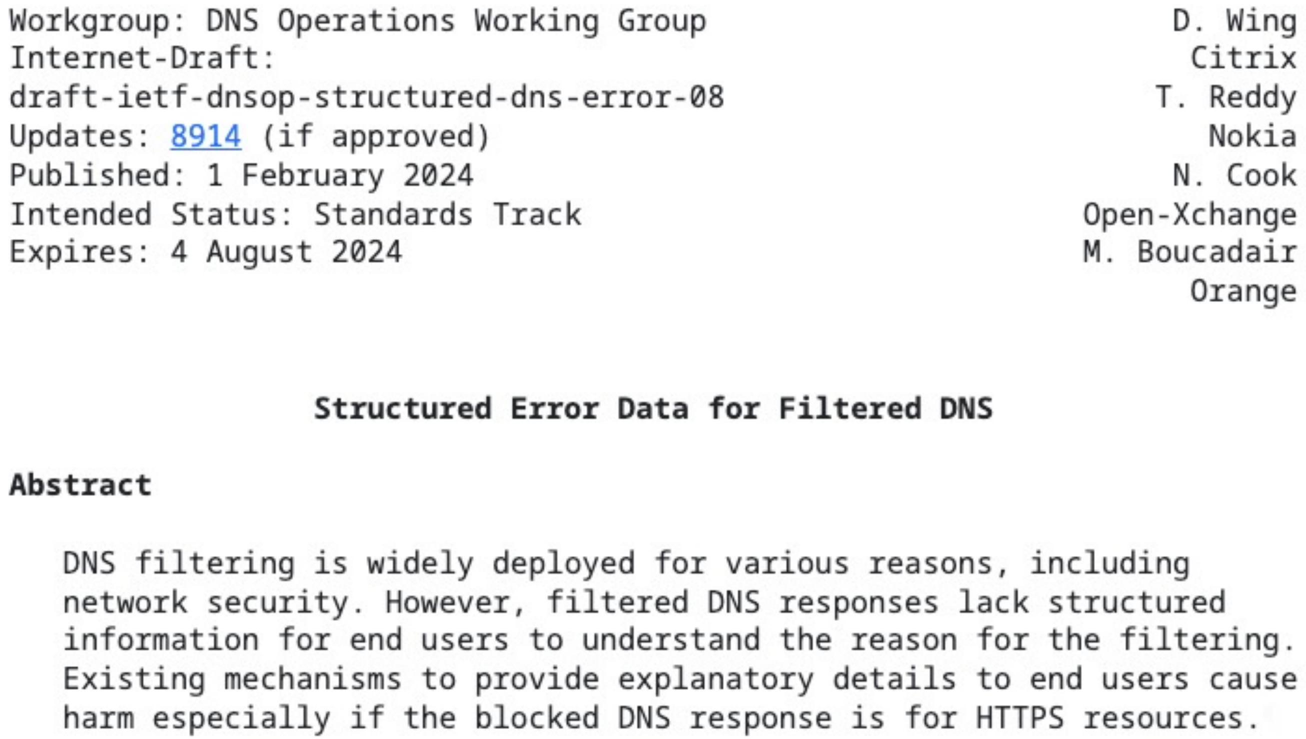
The server is unable to respond to the request because the domain is on a blocklist due to an external requirement imposed by an entity other than the operator of the server resolving or forwarding the query. Note that how the imposed policy is applied is irrelevant (in-band DNS filtering, court order, etc.)

OpenDNS Censored



```
$ dig @208.67.222.222 extended-dns-errors.com

; <<>> DiG 9.16.48-Debian <<>> @208.67.222.222 extended-dns-errors.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 16690
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1410
; EDE: 16 (Censored)
;; QUESTION SECTION:
;extended-dns-errors.com.       IN      A

;; ADDITIONAL SECTION:

extended-dns-errors.com. 0      IN      TXT     "The OpenDNS service is currently unavailable in France and some
French territories due to a court order under Article L.333-10 of the French Sport Code. See
https://support.opendns.com/hc/en-us"
```

Structured Error Data for Filtered DNS



Workgroup: DNS Operations Working Group
Internet-Draft:
draft-ietf-dnsop-structured-dns-error-08
Updates: 8914 (if approved)
Published: 1 February 2024
Intended Status: Standards Track
Expires: 4 August 2024

D. Wing
Citrix
T. Reddy
Nokia
N. Cook
Open-Xchange
M. Boucadair
Orange

Structured Error Data for Filtered DNS

Abstract

DNS filtering is widely deployed for various reasons, including network security. However, filtered DNS responses lack structured information for end users to understand the reason for the filtering. Existing mechanisms to provide explanatory details to end users cause harm especially if the blocked DNS response is for HTTPS resources.

Source: https://www.ietf.org/archive/id/draft-ietf-dnsop-structured-dns-error-08.html

Results

- 63 testcases, 9 tested systems, 18 unique EDEs:

Results

- 63 testcases, 9 tested systems, 18 unique EDEs:
  - 3 testcases with the same result (no EDE for valid, no-ds, and unsigned subdomains)

Results

- 63 testcases, 9 tested systems, 18 unique EDEs:
  - 3 testcases with the same result (no EDE for valid, no-ds, and unsigned subdomains)
  - 14 testcases with the same EDEs

Why inconsistent?

1. EDE not implemented:
    - BIND9 did not return any EDE when resolving our domains

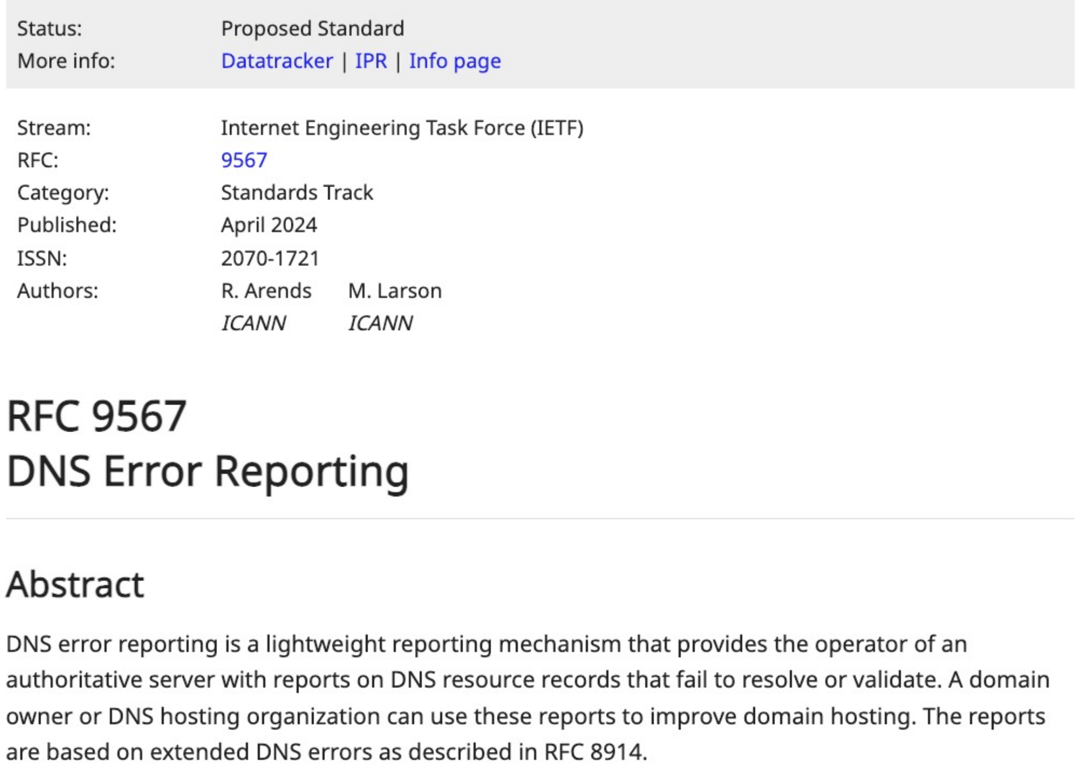
Why inconsistent?

1. EDE not implemented:
   - BIND9 did not return any EDE when resolving our domains
2. EDE specificity:
   - EDE 6 (DNSSEC Bogus) in 34/38 DNSSEC-misconfigured domains

Why inconsistent?

1. EDE not implemented:
    - BIND9 did not return any EDE when resolving our domains
2. EDE specificity:
    - EDE 6 (DNSSEC Bogus) in 34/38 DNSSEC-misconfigured domains
3. Resolver capabilities:
    - EDE 1 (Unsupported DNSKEY Algorithm) returned by Cloudflare for domains signed with ED448, RSAMD5, DSA

Why important?



Status:	Proposed Standard	
More info:	Datatracker | IPR | Info page	
Stream:	Internet Engineering Task Force (IETF)	
RFC:	9567	
Category:	Standards Track	
Published:	April 2024	
ISSN:	2070-1721	
Authors:	R. Arends	M. Larson
	ICANN	*ICANN*

RFC 9567
DNS Error Reporting

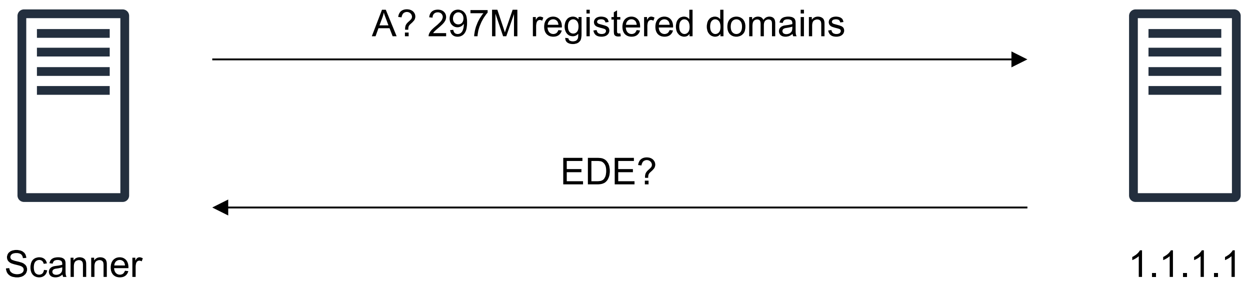
Abstract

DNS error reporting is a lightweight reporting mechanism that provides the operator of an authoritative server with reports on DNS resource records that fail to resolve or validate. A domain owner or DNS hosting organization can use these reports to improve domain hosting. The reports are based on extended DNS errors as described in RFC 8914.

Source: https://www.rfc-editor.org/rfc/rfc9567.html

Can we rely on EDEs to find the most common misconfigurations in the wild?

Methodology



Results

- 19.4M domains trigger EDEs
- 19 unique EDE codes
- 215 combinations of up to 5 individual EDEs

EDE 22 (No Reachable Authority)

- “The resolver could not reach any of the authoritative name servers (or they potentially refused to reply).”
- 13.5 million domains flagged

```
$ dig @1.1.1.1 example.com

…

;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 32496

…

; EDE: 22 (No Reachable Authority): (at delegation example.com.)
```

EDE 23 (Network Error)

- “An unrecoverable error occurred while communicating with another server.”
- 9.9 million domains flagged

```
$ dig @1.1.1.1 example.com

…

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32496

…

; EDE: 23 (Network Error): (X.X.X.X:53 rcode=REFUSED for example.com A)
```

EDE 23 (Network Error)

- “An unrecoverable error occurred while communicating with another server.”
- 9.9 million domains flagged

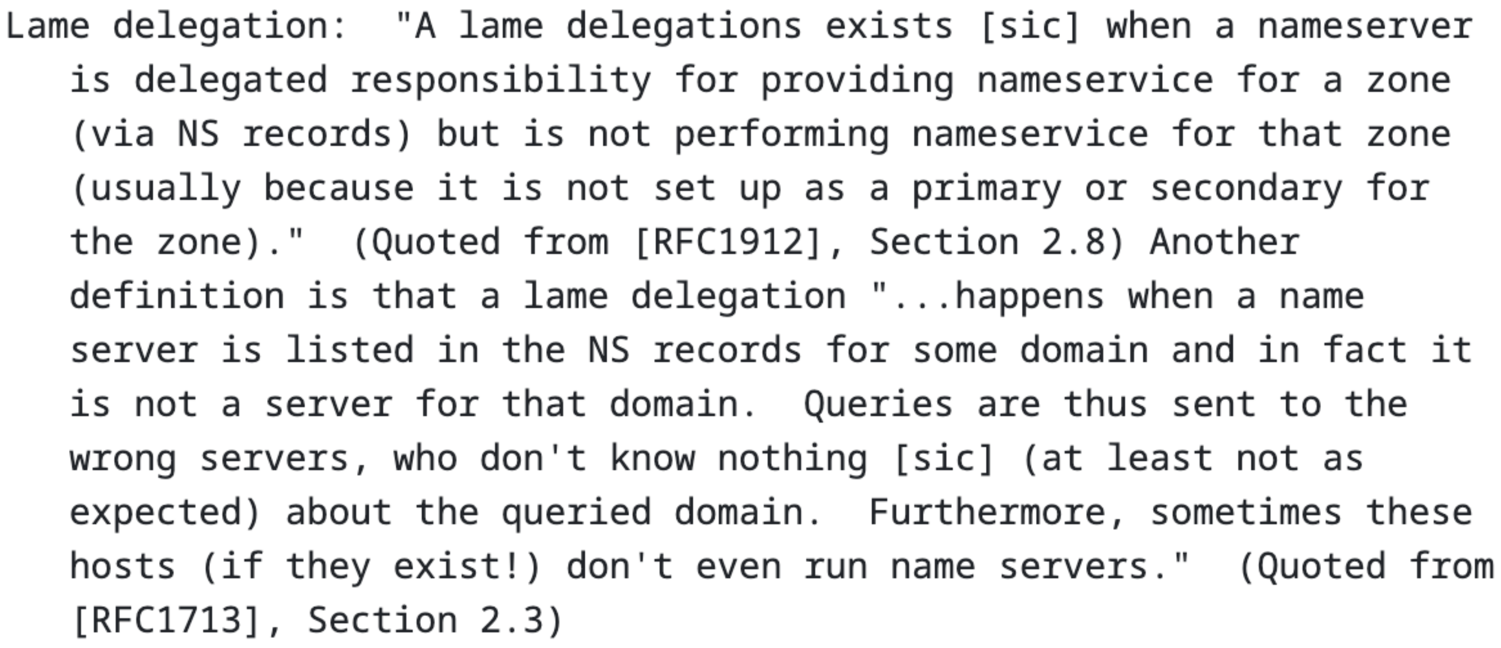
```
$ dig @1.1.1.1 example.com

…

;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 32496

…

; EDE: 22 (No Reachable Authority): (at delegation example.com.)
; EDE: 23 (Network Error): (X.X.X.X:53 timed out for example.com A)
```

EDE 20 (Not Authoritative)

- “An authoritative server that receives a query with the Recursion Desired (RD) bit clear, or when it is not configured for recursion for a domain for which it is not authoritative, SHOULD include this EDE code in the REFUSED response. A resolver that receives a query with the RD bit clear SHOULD include this EDE code in the REFUSED response.”
- 2 million domains flagged

```
$ dig @1.1.1.1 example.com

…

;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 17365

…

; EDE: 20 (Not Authoritative): (zone not managed by server)
; EDE: 22 (No Reachable Authority): (at delegation example.com.)
```

Lame delegations (RFC 8499)



Lame delegation: "A lame delegations exists [sic] when a nameserver is delegated responsibility for providing nameservice for a zone (via NS records) but is not performing nameservice for that zone (usually because it is not set up as a primary or secondary for the zone)." (Quoted from [RFC1912], Section 2.8) Another definition is that a lame delegation "...happens when a name server is listed in the NS records for some domain and in fact it is not a server for that domain. Queries are thus sent to the wrong servers, who don't know nothing [sic] (at least not as expected) about the queried domain. Furthermore, sometimes these hosts (if they exist!) don't even run name servers." (Quoted from [RFC1713], Section 2.3)

Source: https://datatracker.ietf.org/doc/html/rfc8499

(One of the) longest EDE combos

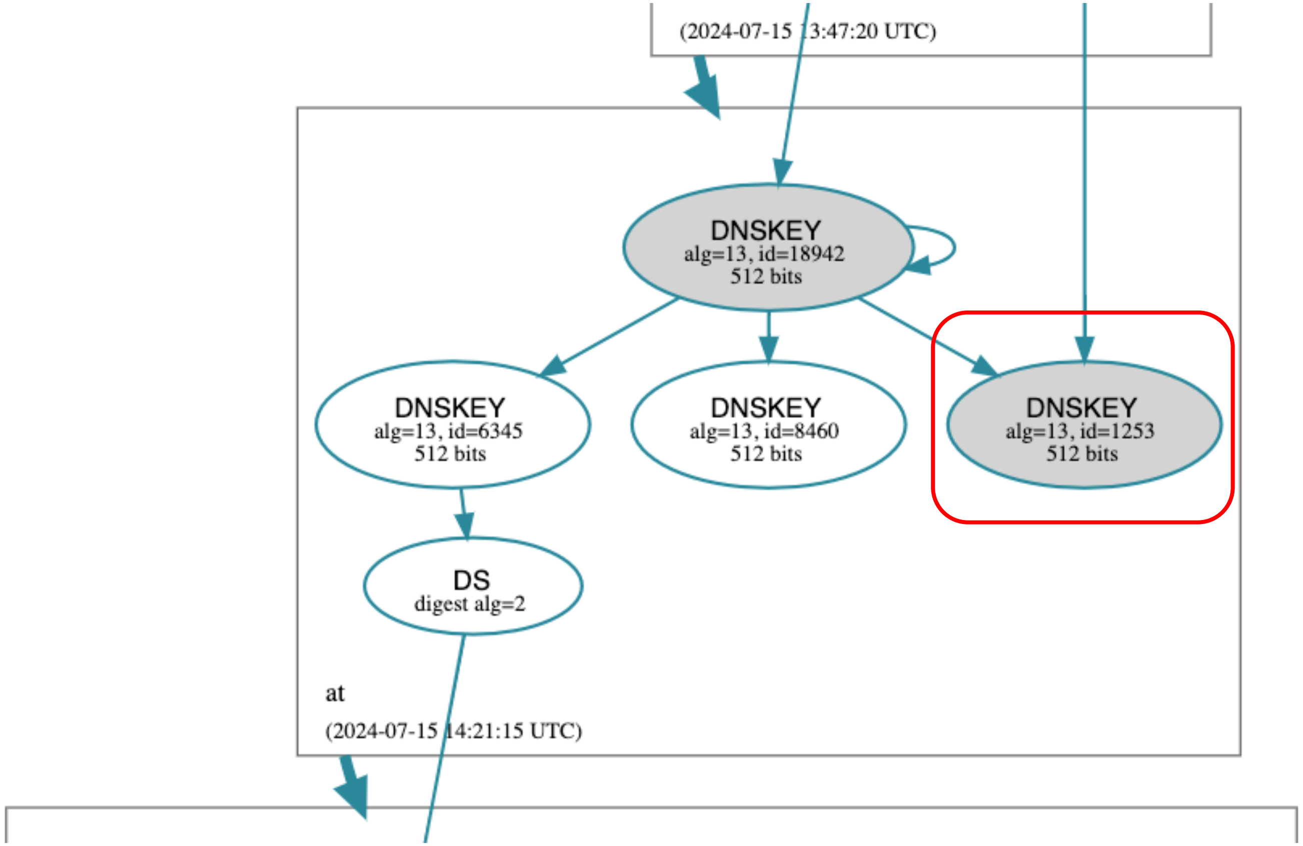
```
$ dig @1.1.1.1 example.com

…

;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 17365

…

; EDE: 9 (DNSKEY Missing): (no SEP matching the DS found for example.com.)
; EDE: 18 (Prohibited)
; EDE: 20 (Not Authoritative)
; EDE: 22 (No Reachable Authority): (at delegation example.com.)
; EDE: 23 (Network Error): (X.X.X.X:53 rcode=REFUSED for example.com A)
```

EDE 10 (RRSIGs Missing)

- “The resolver attempted to perform DNSSEC validation, but no RRSIGs could be found for at least one RRset where RRSIGs were expected.”
- 4 million domains flagged

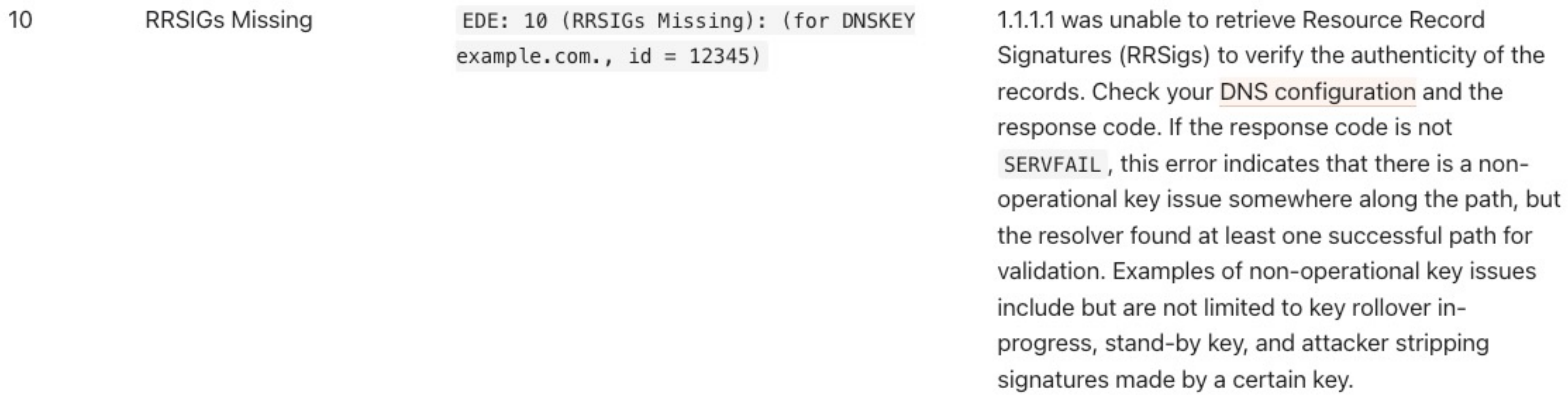
```
$ dig @1.1.1.1 nic.at

…

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17365

…

; EDE: 10 (RRSIGs Missing): (for DNSKEY at., id = 1253)
```

EDE 10 (RRSIGs Missing)



Source: https://dnsviz.net/d/nic.at/dnssec/

EDE 10 (RRSIGs Missing)



10	RRSIGs Missing	`EDE: 10 (RRSIGs Missing): (for DNSKEY example.com., id = 12345)`	1.1.1.1 was unable to retrieve Resource Record Signatures (RRSigs) to verify the authenticity of the records. Check your DNS configuration and the response code. If the response code is not `SERVFAIL`, this error indicates that there is a non-operational key issue somewhere along the path, but the resolver found at least one successful path for validation. Examples of non-operational key issues include but are not limited to key rollover in-progress, stand-by key, and attacker stripping signatures made by a certain key.

Source: https://developers.cloudflare.com/1.1.1.1/infrastructure/extended-dns-error-codes/

Many more interesting cases to dig into …

Conclusions

- Supported by major DNS systems
- Identifies the root cause of problems
- Different specificity
- Efficient at scale

Thanks!

yevheniya.nosyk@univ-grenoble-alpes.fr