

Workgroup: DNS Operations Working Group
Internet-Draft:
draft-ietf-dnsop-structured-dns-error-00
Updates: [8914](#) (if approved)
Published: 13 February 2023
Intended Status: Standards Track
Expires: 17 August 2023
Authors: D. Wing T. Reddy N. Cook M. Boucadair
 Citrix Nokia Open-Xchange Orange

Structured Error Data for Filtered DNS

Abstract

DNS filtering is widely deployed for network security, but filtered DNS responses lack information for the end user to understand the reason for the filtering. Existing mechanisms to provide detail to end users cause harm especially if the blocked DNS response is to an HTTPS website.

This document updates RFC 8914 by structuring the EXTRA-TEXT field of the Extended DNS Error to provide details on the DNS filtering. Such details can be parsed by the client and displayed, logged, or used for other purposes. Other than that, this document does not change any thing written in RFC 8914.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at <https://ietf-wg-dnsop.github.io/draft-ietf-dnsop-structured-dns-error/draft-ietf-dnsop-structured-dns-error.html>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-ietf-dnsop-structured-dns-error/>.

Discussion of this document takes place on the dnsop Working Group mailing list (<mailto:dnsop@ietf.org>), which is archived at <https://mailarchive.ietf.org/arch/browse/dnsop/>. Subscribe at <https://www.ietf.org/mailman/listinfo/dnsop/>.

Source for this draft and an issue tracker can be found at <https://github.com/ietf-wg-dnsop/draft-ietf-dnsop-structured-dns-error>.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 17 August 2023.

Copyright Notice

Copyright (c) 2023 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

- [1. Introduction](#)
- [2. Conventions and Definitions](#)
- [3. DNS Filtering Techniques and Their Limitations](#)
- [4. I-JSON in EXTRA-TEXT field](#)
- [5. Protocol Operation](#)
 - [5.1. Client Generating Request](#)
 - [5.2. Server Generating Response](#)
 - [5.3. Client Processing Response](#)
- [6. Interoperation with RPZ Servers](#)
- [7. New Sub-Error Codes Definition](#)
 - [7.1. Reserved](#)
 - [7.2. Network Operator Policy](#)
 - [7.3. DNS Operator Policy](#)
- [8. Examples](#)
- [9. Security Considerations](#)
- [10. IANA Considerations](#)
 - [10.1. New structured-dns-error Media Type](#)
 - [10.2. New Registry for SubError Codes](#)
- [11. References](#)
 - [11.1. Normative References](#)

1. Introduction

DNS filters are deployed for a variety of reasons including endpoint security, parental filtering, and filtering required by law enforcement. Network-based security solutions such as firewalls and Intrusion Prevention Systems (IPS) rely upon network traffic inspection to implement perimeter-based security policies and operate by filtering DNS responses. In a home, DNS filtering is used for the same reasons as above and additionally for parental control. Internet Service Providers typically block access to some DNS domains due to a requirement imposed by an external entity (e.g., law enforcement agency) also performed using DNS-based content filtering.

Users of DNS services which perform filtering may wish to receive more information about such filtering to resolve problems with the filter -- for example to contact the administrator to allowlist a domain that was erroneously filtered or to understand the reason a particular domain was filtered. With that information, the user can choose another network, open a trouble ticket with the DNS administrator to resolve erroneous filtering, log the information, or other uses.

For the DNS filtering mechanisms described in [Section 3](#) the DNS server can return extended error codes Blocked, Censored, Filtered, or Forged Answer defined in Section 4 of [\[RFC8914\]](#). However, these codes only explain that filtering occurred but lack detail for the user to diagnose erroneous filtering.

No matter which type of response is generated (forged IP address(es), NXDOMAIN or empty answer, even with an extended error code), the user who triggered the DNS query has little chance to understand which entity filtered the query, how to report a mistake in the filter, or why the entity filtered it at all. This document describes a mechanism to provide such detail.

One of the other benefits of this approach is to eliminate the need to "spoof" block pages for HTTPS resources. This is achieved since clients implementing this approach would be able to display a meaningful error message, and would not need to connect to such a block page. This approach thus avoids the need to install a local root certificate authority on those IT-managed devices.

This document describes a format for computer-parsable data in the EXTRA-TEXT field of [\[RFC8914\]](#). It updates Section 2 of [\[RFC8914\]](#)

which says the information in EXTRA-TEXT field is intended for human consumption (not automated parsing).

This document does not recommend DNS filtering but provides a mechanism for better transparency to explain to the users why some DNS queries are filtered.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [[RFC2119](#)] [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

This document uses terms defined in DNS Terminology [[RFC8499](#)].

"Requestor" refers to the side that sends a request. "Responder" refers to an authoritative, recursive resolver or other DNS component that responds to questions. Other terminology is used here as defined in the RFCs cited by this document.

"Encrypted DNS" refers to any encrypted scheme to convey DNS messages, for example, DNS-over-HTTPS [[RFC8484](#)], DNS-over-TLS [[RFC7858](#)], or DNS-over-QUIC [[RFC9250](#)].

The document refers to an extended DNS error using its purpose, not its INFO-CODE as per Table 3 of [[RFC8914](#)]. "Forged Answer", "Blocked", "Censored", and "Filtered" are thus used to refer to "Forged Answer (4)", "Blocked (15)", "Censored (16)", and "Filtered (17)".

3. DNS Filtering Techniques and Their Limitations

Today, DNS responses can be filtered by sending a bogus (also called "forged") A or AAAA response, NXDOMAIN error or empty answer, or an extended DNS error (EDE) code defined in [[RFC8914](#)]. Each of these methods have advantages and disadvantages that are discussed below:

1. The DNS response is forged to provide a list of IP addresses that points to an HTTP(S) server alerting the end user about the reason for blocking access to the requested domain (e.g., malware). When an HTTP(S) enabled domain name is blocked, the network security device (e.g., CPE, firewall) presents a block page instead of the HTTP response from the content provider hosting that domain. If an HTTP enabled domain name is blocked, the network security device intercepts the HTTP request and returns a block page over HTTP. If an HTTPS enabled domain is blocked, the block page is also served over HTTPS. In order to return a block page over HTTPS, man in the middle (MITM) is

enabled on endpoints by generating a local root certificate and an accompanying (local) public/private key pair. The local root certificate is installed on the endpoint while the network security device(s) stores a copy of the private key. During the TLS handshake, the network security device modifies the certificate provided by the server and (re)signs it using the private key from the local root certificate.

*However, configuring the local root certificate on endpoints is not a viable option in several deployments like home networks, schools, Small Office/Home Office (SOHO), and Small/ Medium Enterprise (SME). In these cases, the typical behavior is that the filtered DNS response points to a server that will display the block page. If the client is using HTTPS (via web browser or another application) this results in a certificate validation error which gives no information to the end-user about the reason for the DNS filtering. Browsers will display errors such as "The security certificate presented by this website was not issued by a trusted certificate authority" (Internet Explorer/Edge), "The site's security certificate is not trusted" (Chrome), "This Connection is Untrusted" (Firefox), "Safari can't verify the identity of the website ..." (Safari on MacOS). Applications might display even more cryptic error messages.

*Enterprise networks do not assume that all the connected devices are managed by the IT team or Mobile Device Management (MDM) devices, especially in the quite common Bring Your Own Device (BYOD) scenario. In addition, the local root certificate cannot be installed on IoT devices without a device management tool.

*An end user does not know why the connection was prevented and, consequently, may repeatedly try to reach the domain but with no success. Frustrated, the end user may switch to an alternate network that offers no DNS filtering against malware and phishing, potentially compromising both security and privacy. Furthermore, certificate errors train users to click through certificate errors, which is a bad security practice. To eliminate the need for an end user to click through certificate errors, an end user may manually install a local root certificate on a host device. Doing so, however, is also a bad security practice as it creates a security vulnerability that may be exploited by a MITM attack. When a manually installed local root certificate expires, the user has to (again) manually install the new local root certificate.

2. The DNS response is forged to provide a NXDOMAIN response to cause the DNS lookup to terminate in failure. In this case, an end user does not know why the domain cannot be reached and may repeatedly try to reach the domain but with no success. Frustrated, the end user may use insecure connections to reach the domain, potentially compromising both security and privacy.
3. The extended error codes Blocked, Censored, and Filtered defined in Section 4 of [RFC8914] can be returned by a DNS server to provide additional information about the cause of an DNS error. If the extended error code "Forged Answer" defined in Section 4.5 of [RFC8914] is returned by the DNS server, the client can identify the DNS response is forged together with the reason for HTTPS certificate error.
4. These extended error codes do not suffer from the limitations discussed in bullets (1) and (2), but the user still does not know the exact reason nor he/she is aware of the exact entity blocking the access to the domain. For example, a DNS server may block access to a domain based on the content category such as "Malware" to protect the endpoint from malicious software, "Phishing" to prevent the user from revealing sensitive information to the attacker, etc. A user needs to know the contact details of the IT/InfoSec team to raise a complaint.
5. When a resolver or forwarder forwards the received EDE option, the EXTRA-TEXT field only conveys the source of the error (Section 3 of [RFC8914]) and does not provide additional textual information about the cause of the error.

4. I-JSON in EXTRA-TEXT field

Servers that are compliant with this specification send I-JSON data in the EXTRA-TEXT field [RFC8914] using the Internet JSON (I-JSON) message format [RFC7493].

Note that [RFC7493] was based on [RFC7159], but [RFC7159] was replaced by [RFC8259].

This document defines the following JSON names:

- c: (contact)** The contact details of the IT/InfoSec team to report mis-classified DNS filtering. This field is structured as an array of contact URIs (e.g., tel, sips, https). At least one contact URI **MUST** be included. This field is mandatory.
- j: (justification)** UTF-8-encoded [RFC5198] textual justification for this particular DNS filtering. The field should be treated only as diagnostic information for IT staff. This field is mandatory.

s: (suberror)

the suberror code for this particular DNS filtering.
This field is optional.

o: (organization) UTF-8-encoded human-friendly name of the organization that filtered this particular DNS query. This field is optional.

New JSON names can be defined in the IANA "application/json+structured-dns-error" registry ([Section 10](#)). Such names **MUST** consist only of lower-case ASCII characters, digits, and hyphens (that is, Unicode characters U+0061 through 007A, U+0030 through U+0039, and U+002D). Also, these names **MUST** be 63 characters or shorter and it is **RECOMMENDED** they be as short as possible.

The text in the "j" and "o" names can include international characters. If the text is displayed in a language not known to the end user, browser extensions to translate to user's native language can be used. For example, "Google Translate" extension [[Chrome-Translate](#)] provided by Google on Chrome can be used to translate the text.

To reduce packet overhead the generated JSON **SHOULD** be as short as possible: short domain names, concise text in the values for the "j" and "o" names, and minified JSON (that is, without spaces or line breaks between JSON elements).

The JSON data can be parsed to display to the user, logged, or otherwise used to assist the end-user or IT staff with troubleshooting and diagnosing the cause of the DNS filtering.

5. Protocol Operation

5.1. Client Generating Request

When generating a DNS query, the client includes the Extended DNS Error option Section 2 of [[RFC8914](#)] in the OPT pseudo-RR [[RFC6891](#)] to elicit the Extended DNS Error option in the DNS response.

5.2. Server Generating Response

When the DNS server filters its DNS response to an A or AAAA record query, the DNS response **MAY** contain an empty answer, NXDOMAIN, or (less ideally) forged A or AAAA response, as desired by the DNS server. In addition, if the query contained the OPT pseudo-RR the DNS server **MAY** return more detail in the EXTRA-TEXT field as described in [Section 5.3](#).

Servers may decide to return small TTL values in filtered DNS responses (e.g., 2 seconds) to handle domain category and reputation updates.

Because the DNS client signals its EDE support ([Section 5.1](#)) and because EDE support is signaled via a non-cached OPT resource record (Section 6.2.1 of [[RFC6891](#)]) the EDE-aware DNS server can tailor its filtered response to be most appropriate to that client's EDE support. If EDE support is signaled in the query the server **MUST NOT** return the "Forged Answer" extended error code because the client can take advantage of EDE's more sophisticated error reporting (e.g., "Censored", "Filtered", "Blocked"). Continuing to send "Forged Answer" even to an EDE-supporting client will cause the persistence of the drawbacks described in [Section 3](#).

5.3. Client Processing Response

On receipt of a DNS response with an Extended DNS Error option, the following actions are performed if the EXTRA-TEXT field contains valid JSON:

- *The response **MUST** be received over an encrypted DNS channel. If not, the requestor **MUST** discard data in the EXTRA-TEXT field.
- *The response **MUST** be received from a DNS server which advertised EDE support via a trusted channel, e.g., RESINFO [[I-D.reddy-add-resolver-info](#)].
- *Servers which don't support this specification might use plain text in the EXTRA-TEXT field so that requestors **SHOULD** properly handle both plaintext and JSON text in the EXTRA-TEXT field.
- *The DNS response **MUST** also contain an extended error code of "Censored", "Blocked", "Filtered" or "Forged Answer" [[RFC8914](#)], otherwise the EXTRA-TEXT field is discarded.
- *If either of the mandatory JSON names "c" and "j" are missing or have empty values in the EXTRA-TEXT field, the entire JSON is discarded.
- *The JSON name "s" **MUST NOT** be present with the extended error code "Censored".
- *If a DNS client has enabled opportunistic privacy profile (Section 5 of [[RFC8310](#)]) for DoT, the DNS client will either fallback to an encrypted connection without authenticating the DNS server provided by the local network or fallback to clear text DNS, and cannot exchange encrypted DNS messages. Both of these fallback mechanisms adversely impacts security and privacy. If the DNS client has enabled opportunistic privacy profile for

DoT, the DNS client **MUST** ignore the EXTRA-TEXT field of the EDE responses, but **SHOULD** process other parts of the response.

*If a DNS client has enabled strict privacy profile (Section 5 of [\[RFC8310\]](#)) for DoT, the DNS client requires an encrypted connection and successful authentication of the DNS server; this mitigates both passive eavesdropping and client redirection (at the expense of providing no DNS service if an encrypted, authenticated connection is not available). If the DNS client has enabled strict privacy profile for DoT, the client **MAY** process the EXTRA-TEXT field of the DNS response. Note that the strict and opportunistic privacy profiles as defined in [\[RFC8310\]](#) only apply to DoT; there has been no such distinction made for DoH.

*If the DNS client determines that the encrypted DNS server does not offer DNS filtering service, it **MUST** discard the EXTRA-TEXT field of the EDE response. For example, the DNS client can learn whether the encrypted DNS resolver performs DNS-based content filtering or not by retrieving resolver information using the method defined in [\[I-D.reddy-add-resolver-info\]](#).

*When a forwarder receives an EDE option, whether or not (and how) to pass along JSON information in the EXTRA-TEXT on to their client is implementation dependent [\[RFC5625\]](#). Implementations **MAY** choose to not forward the JSON information, or they **MAY** choose to create a new EDE option that conveys the information in the "c", "s" and "j" fields encoded in the JSON object.

6. Interoperation with RPZ Servers

This section discusses operation with an RPZ server [\[RPZ\]](#) that indicates filtering with a NXDOMAIN response with the Recursion Available bit cleared (RA=0).

When the DNS client supports this specification but the server does not, the server will continue replying when a query is RPZ filtered with NXDOMAIN and RA=0. An DNS client upgraded to support this specification can continue to accept responses with NXDOMAIN and RA=0 from the RPZ server that does not support this specification.

When the DNS client supports this specification and the server supports this specification, the client learns of the server's support via [\[I-D.reddy-add-resolver-info\]](#) and the client includes the EDE OPT pseudo-RR in the query. This allows the server to differentiate EDE-aware clients from EDE-unaware clients and respond appropriately.

7. New Sub-Error Codes Definition

The document defines the following new IANA-registered Sub-Error codes.

7.1. Reserved

*Number: 0

*Meaning: Reserved. This sub-error code value **MUST NOT** be sent. If received, it has no meaning.

*Applicability: This code should never be used

*Reference: This-Document

*Change Controller: IETF

7.2. Network Operator Policy

*Number: 5

*Meaning: Network Operator Policy. The code indicates that the request was filtered according to policy determined by the operator of the local network.

*Applicability: Blocked, Forged

*Reference: This-Document

*Change Controller: IETF

7.3. DNS Operator Policy

*Number: 6

*Meaning: DNS Operator Policy. The code indicates that the request was filtered according to policy determined by the operator of the DNS server.

*Applicability: Blocked, Forged

*Reference: This-Document

*Change Controller: IETF

8. Examples

An example showing the nameserver at 'ns.example.net' that filtered a DNS "A" record query for 'example.org' is shown in [Figure 1](#).

```
{
  "c": [
    "tel:+358-555-1234567",
    "sips:bob@bobphone.example.com",
    "https://ticket.example.com?d=example.org&t=1650560748"
  ],
  "j": "malware present for 23 days",
  "s": 1,
  "o": "example.net Filtering Service"
}
```

Figure 1: JSON returned in EXTRA-TEXT field of Extended DNS Error response

In [Figure 2](#) the same content is shown with minified JSON (no whitespace, no blank lines) with '\\' line wrapping per [\[RFC8792\]](#).

===== NOTE: '\\' line wrapping per RFC 8792 =====

```
{"c":["tel:+358-555-1234567","sips:bob@bobphone.example.com", \
"https://ticket.example.com?d=example.org&t=1650560748"],"s":1, \
"j":"malware present for 23 days","o":"example.net Filtering \
Service"}
```

Figure 2: Minified response

9. Security Considerations

Security considerations in Section 6 of [\[RFC8914\]](#) apply to this document.

To minimize impact of active on-path attacks on the DNS channel, the client validates the response as described in [Section 5.3](#).

A client might choose to display the information in the "c", "j" and "o" fields if and only if the encrypted resolver has sufficient reputation, according to some local policy (e.g. user configuration, administrative configuration, or a built-in list of respectable resolvers). This limits the ability of a malicious encrypted resolver to cause harm. If the client decides not to display the all of the information in the EXTRA-TEXT field, it can be logged for diagnostics purpose and the client can only display the resolver hostname that blocked the domain, error description for the EDE code and the suberror description for the "s" field to the end-user.

When displaying the free-form text of "c" and "o", the browser **SHOULD NOT** make any of those elements into actionable (clickable) links.

An attacker might inject (or modify) the EDE EXTRA-TEXT field with an DNS proxy or DNS forwarder that is unaware of EDE. Such a DNS proxy or DNS forwarder will forward that attacker-controlled EDE option. To prevent such an attack, clients supporting this document **MUST** discard the EDE option if their DNS server does not signal EDE support via RESINFO [[I-D.reddy-add-resolver-info](#)]. As recommended in [[I-D.reddy-add-resolver-info](#)], RESINFO should be retrieved over an encrypted DNS channel or integrity protected with DNSSEC.

10. IANA Considerations

This document requests two IANA actions as described in the following subsections.

10.1. New structured-dns-error Media Type

This document requests IANA to register the "application/json+structured-dns-error" media type in the "Media Types" registry [[IANA-MediaTypes](#)]. This registration follows the procedures specified in [[RFC6838](#)]:

Type name: application

Subtype name: json+structured-dns-error

Required parameters: N/A

Optional parameters: N/A

Encoding considerations: as defined in Section NN of [RFCXXXX].

Security considerations: See Section NNN of [RFCXXXX].

Interoperability considerations: N/A

Published specification: [RFCXXXX]

Applications that use this media type: Section NNNN of [RFCXXXX].

Fragment identifier considerations: N/A

Additional information: N/A

Person & email address to contact for further information: IETF,
iesg@ietf.org

Intended usage: COMMON

Restrictions on usage: none

Author: See Authors' Addresses section.

Change controller: IESG

Provisional registration? No

10.2. New Registry for SubError Codes

This document requests IANA to create a new registry, entitled "SubError Codes" under "Domain Name System (DNS) Parameters, Extended DNS Error Codes" registry [[IANA-DNS](#)]. The registration request for a new suberror codes **MUST** include the following fields:

*Number: Wire format suberror code (range 0-255)

*Meaning: A short description of the sub-error

*Applicability: Indicates which RFC8914 error codes apply to this sub-error code

*Reference: A pointer to IETF-approved specification that registered the code and/or an authoritative specification that describes the meaning of this code

*Change Controller: Person or entity, with contact information if appropriate.

The SubError Code registry shall initially be populated with the following suberror codes:

Number	Meaning	RFC8914 error code applicability	Reference	Change Controller
0	Reserved	Not used	Section 7.1 of this document	IETF
1	Malware	"Forged Answer", "Blocked", "Censored", "Filtered"	Section 5.5 of [RFC5901]	IETF
2	Phishing	"Forged Answer", "Blocked", "Censored", "Filtered"	Section 5.5 of [RFC5901]	IETF
3	Spam	"Forged Answer", "Blocked", "Censored", "Filtered"	Page 289 of [RFC4949]	IETF
4	Spyware	"Forged Answer", "Blocked", "Censored", "Filtered"	Page 291 of [RFC4949]	IETF
5	Network operator policy	"Forged Answer", "Blocked"	Section 7.2 of this document	IETF
6	DNS operator policy	"Forged Answer", "Blocked"	Section 7.3 of this document	IETF

Table 1: Initial SubError Code Registry

New entries in this registry are subject to an Expert Review registration policy [\[RFC8126\]](#). The designated expert **MUST** ensure that the Reference is stable and publicly available, and that it specifies the suberror code and a short description. The reference may be an individual Internet-Draft, or a document from any other source with similar assurances of stability and availability.

Review requests are evaluated on the advice of one or more designated experts. Criteria that should be applied by the

designated experts include determining whether the proposed registration duplicates existing entries and whether the registration description is sufficiently detailed and fits the purpose of this registry. The designated experts will either approve or deny the registration request, communicating this decision to IANA. Denials should include an explanation and, if applicable, suggestions as to how to make the request successful.

11. References

11.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/rfc/rfc2119>>.
- [RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <<https://www.rfc-editor.org/rfc/rfc4949>>.
- [RFC5198] Klensin, J. and M. Padlipsky, "Unicode Format for Network Interchange", RFC 5198, DOI 10.17487/RFC5198, March 2008, <<https://www.rfc-editor.org/rfc/rfc5198>>.
- [RFC5901] Cain, P. and D. Jevans, "Extensions to the IODEF-Documents Class for Reporting Phishing", RFC 5901, DOI 10.17487/RFC5901, July 2010, <<https://www.rfc-editor.org/rfc/rfc5901>>.
- [RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, DOI 10.17487/RFC6838, January 2013, <<https://www.rfc-editor.org/rfc/rfc6838>>.
- [RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <<https://www.rfc-editor.org/rfc/rfc6891>>.
- [RFC7159] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014, <<https://www.rfc-editor.org/rfc/rfc7159>>.
- [RFC7493] Bray, T., Ed., "The I-JSON Message Format", RFC 7493, DOI 10.17487/RFC7493, March 2015, <<https://www.rfc-editor.org/rfc/rfc7493>>.
- [RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26,

RFC 8126, DOI 10.17487/RFC8126, June 2017, <<https://www.rfc-editor.org/rfc/rfc8126>>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/rfc/rfc8174>>.

[RFC8310] Dickinson, S., Gillmor, D., and T. Reddy, "Usage Profiles for DNS over TLS and DNS over DTLS", RFC 8310, DOI 10.17487/RFC8310, March 2018, <<https://www.rfc-editor.org/rfc/rfc8310>>.

[RFC8914] Kumari, W., Hunt, E., Arends, R., Hardaker, W., and D. Lawrence, "Extended DNS Errors", RFC 8914, DOI 10.17487/RFC8914, October 2020, <<https://www.rfc-editor.org/rfc/rfc8914>>.

11.2. Informative References

[Chrome-Translate] "Change Chrome languages & translate webpages", <<https://support.google.com/chrome/answer/173424>>.

[I-D.reddy-add-resolver-info] Reddy, K. T. and M. Boucadair, "DNS Resolver Information", Work in Progress, Internet-Draft, draft-reddy-add-resolver-info-06, 31 August 2022, <<https://datatracker.ietf.org/doc/html/draft-reddy-add-resolver-info-06>>.

[IANA-DNS] IANA, "Domain Name System (DNS) Parameters, Extended DNS Error Codes", <<https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#extended-dns-error-codes>>.

[IANA-MediaTypes] IANA, "Media Types", <<https://www.iana.org/assignments/media-types>>.

[RFC5625] Bellis, R., "DNS Proxy Implementation Guidelines", BCP 152, RFC 5625, DOI 10.17487/RFC5625, August 2009, <<https://www.rfc-editor.org/rfc/rfc5625>>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <<https://www.rfc-editor.org/rfc/rfc7858>>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <<https://www.rfc-editor.org/rfc/rfc8259>>.

[RFC8484]

Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <<https://www.rfc-editor.org/rfc/rfc8484>>.

[RFC8499]

Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <<https://www.rfc-editor.org/rfc/rfc8499>>.

[RFC8792]

Watsen, K., Auerswald, E., Farrel, A., and Q. Wu, "Handling Long Lines in Content of Internet-Drafts and RFCs", RFC 8792, DOI 10.17487/RFC8792, June 2020, <<https://www.rfc-editor.org/rfc/rfc8792>>.

[RFC9250]

Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <<https://www.rfc-editor.org/rfc/rfc9250>>.

[RPZ]

"Response Policy Zone", <<https://dnssrpz.info>>.

Acknowledgements

Thanks to Vittorio Bertola, Wes Hardaker, Ben Schwartz, Erid Orth, Viktor Dukhovni, Warren Kumari, Paul Wouters, John Levine, and Bob Harold for the comments.

Authors' Addresses

Dan Wing
Citrix Systems, Inc.
United States of America

Email: dwing-ietf@fuggles.com

Tirumaleswar Reddy
Nokia
Bangalore
Karnataka
India

Email: kondtir@gmail.com

Neil Cook
Open-Xchange
United Kingdom

Email: neil.cook@noware.co.uk

Mohamed Boucadair

Orange
Rennes
35000
France

Email: mohamed.boucadair@orange.com