Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 8 February 2026

M. Nottingham
Cloudflare
D. Adrian
Google

7 August 2025

# DNS Filtering Details for Applications
# draft-nottingham-public-resolver-errors-02

## Abstract

[I-D.ietf-dnsop-structured-dns-error] introduces structured error data for DNS responses that have been filtered. This specification allows more specific details of filtering incidents to be conveyed.

## Discussion Venues

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

Source for this draft and an issue tracker can be found at https://github.com/mnot/public-resolver-errors.

## 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 8 February 2026.

## Copyright Notice

Table of Contents



## 1. Introduction

Internet DNS resolvers are increasingly subject to legal orders that require blocking or filtering of specific names. Because such filtering happens during DNS resolution, there is not an effective way to communicate what is happening to end users, often resulting in misattribution of the issue as a technical problem, rather than a policy intervention.

Some organizations, such as Lumen [lumen], monitor legally-mandated filtering as a public service, tracking specific filtering incidents in publicly accessible databases. Public resolvers themselves may also choose to track filtering requests over time and make them available.

This draft defines a mechanism for DNS resolvers to convey identifiers for entries in such databases, based upon the structured error data for DNS responses introduced by [I-D.ietf-dnsop-structured-dns-error].

A consuming party (e.g., a Web browser) can use this information to construct a link to the specific entry in the provider's database of filtering incidents. This enables user agents to direct users to additional context about the filtering incident they encountered.

The information conveyed is a DNS Filtering Database Entry, specified in Section 2.1. This abstraction is necessary because allowing DNS resolvers to inject links or user-visible messages would bring unique challenges. DNS resolvers are often automatically configured by unknown networks and DNS responses are unauthenticated, so these messages can come from untrusted parties -- including attackers (e.g., the so-called "coffee shop" attack) that leverage many users' lack of a nuanced model of the trust relationships between all of the parties that are involved in the service they are using.

This draft attempts to mitigate these risks by minimising the information carried in the DNS response to abstract, publicly registered identifiers associated with databases of filtering incidents -- the DNS Filtering Database Entry -- rather than arbitrary URLs. A consuming party can choose which database identifiers they support are are willing to direct their users to, without enabling every DNS server to surface arbitrary links and text, and without requiring every consuming party to independently track which URLs are in use.

## 1.1. Example

In typical use, a DNS query that is filtered might contain an Extended DNS Error Code 17 (see [RFC8914]) and an EXTRA-TEXT field "fdb", which is an array of references to filtering database entries:

```
{
  "fdbs": [
    {"db": "example",
    "id": "abc123"},
    {"db": "lumen",
    "id": "def456"}
  ]
}
```

This indicates that the filtering incident can be accessed in two different databases, and the ID associated with each database. In this example, the data is available in the "example" database at identifier "abc123", and in the "lumen" database at identifier "def456".

An application that evaluates the DNS server and decides to present links to "example" to its users would look up "example" in a local copy of the DNS Filtering Incident Database Registry (see Section 4.2) and obtain the corresponding template (see Section 3). For purposes of this example, assume that the registry entry for that value contains:

https://resolver.example.com/filtering-incidents/{id}

That template can be expanded using the value of "id" to:

https://resolver.example.com/filtering-incidents/abc123

The application could (but might not) then decide to convey some or all of this information to its user; for example, with a statement that conveys:

> The webpage at www.example.net was blocked due to a legal request. Your DNS resolver may have more information about the legal request here:
>
> https://resolver.example.com/filtering-incidents/abc123

Note that there is no requirement for the resolver to construct links to any database, nor for results from any DNS server. The resolver both chooses which database providers it supports, and can evaluate whatever mechanisms it chooses to determine if and when to provide a link to the database entry.

### 1.2. Notational Conventions

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.

## 2. Data Types

This section defines the data types used to look up the details of a filtering incident from a DNS error response. Note that these identifiers are not for presentation to end users.

### 2.1. DNS Filtering Database Entry

A Filtering Database Operator ID is a string identifier for the operator of a database of filtering incidents. It uses the key "db".

A Filtering Incident ID is a string identifier for a particular filtering incident. It might be specific to a particular request, but need not be. It uses the key "id".

An object containing both a Filtering Database Operator ID and a Filtering Incident ID is a Filtering Database Entry.

```
{
  "db": "example",
  "id": "abc123"
}
```

### 2.2. DNS Filtering Database Entry List

A DNS Filtering Database Entries list is an array of Filtering Database Entry objects. Each entry MUST be related to the same underlying incident.

It is carried in the EXTRA-TEXT field of the Extended DNS Error with the JSON field name "fdbs". For example:

```
{
  "fdbs": [ { ... }, { ... }, ... ]
}
```

Different clients will implement support for a varying set of database operators. Resolvers provide a list of entries (rather than a single entry) so that they can support as many clients with diverse database sets as possible.

## 3. Database Entry Resolution Templates

An Incident Resolution Template is a URI Template [RFC6570] contained in the DNS Filtering Database Registry (Section 4.2) that, upon expansion, provides a URI that can be dereferenced to obtain details about the filtering incident.

It MUST be a Level 1 or Level 2 template (see Section 1.2 of [RFC6570]). It has the following variables from the Filtering Database Entry (see Section 2.1) available to it:

db: the Filtering Database Operator ID

id: the Filtering Incident ID

For example:

https://resolver.example.com/filtering-incidents/{inc}

Applications MUST store a local copy of the DNS Filtering Database Registry (Section 4.2) for purposes of template lookup; they MUST NOT query the IANA registry upon each use. The registry is keyed by the Filtering Database Operator ID.

## 4. IANA Considerations

### 4.1. EXTRA-TEXT JSON Names

IANA will register the following fields in the "EXTRA-TEXT JSON Names" sub-registry established by [I-D.ietf-dnsop-structured-dns-error]:

JSON Name: "fdbs"
Short Description: a array of filtering database entries
Mandatory: no
Specification: this document

### 4.2. The DNS Filtering Database Registry

IANA will establish a new registry, the "DNS Filtering Database Registry." Its registration policy is first-come, first-served (FCFS), although IANA may refuse registrations that it deems to be deceptive or spurious.

It contains the following fields:

Name: The name of the DNS Filtering Database

Contact: an e-mail address or other appropriate contact mechanism

Filtering Database Operator ID: see Section 2.1

Incident Resolution Template: see Section 3

The Incident Resolution Template can be updated by the contact at any time. However, operators SHOULD accommodate potentially long lag times for applications to update their copies of the registry.

## 5. Security Considerations

This specification does not provide a way to authenticate that a particular filtering incident as experienced by an application was actually associated with the information presented. This means that an attacker (for example, one controlling a DNS resolver) can claim that a particular filtering incident is occurring when in fact it is not. However, a successful attack would need to reuse an existing DNS Filtering Database Operator ID and Filtering Incident ID that

combine to expand to a URL that can be successfully dereferenced. Doing so is not currently thought to be particularly advantageous to an attacker to do so. Future iterations of this specification may introduce more robust protections.

The details of DNS responses are not available to all applications, depending on how they are architected and the information made available to them by their host. As a result, this mechanism is not reliable; some applications will not be able to display this error information.

Because the registry is first-come, first-served, Applications (such as Web browsers) will need to exercise judgement regarding which database operators' error messages they display to users. This decision might be influenced by the identity of the resolver producing the error message, the database operator, or local configuration.

# 6. References

## 6.1. Normative References

[I-D.ietf-dnsop-structured-dns-error]
Wing, D., Reddy.K, T., Cook, N., and M. Boucadair, "Structured Error Data for Filtered DNS", Work in Progress, Internet-Draft, draft-ietf-dnsop-structured-dns-error-15, 5 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-structured-dns-error-15>.

[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>.

[RFC6570] Gregorio, J., Fielding, R., Hadley, M., Nottingham, M., and D. Orchard, "URI Template", RFC 6570, DOI 10.17487/RFC6570, March 2012, <https://www.rfc-editor.org/rfc/rfc6570>.

[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>.

[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>.

### 6.2. Informative References

[lumen] "Lumen", n.d., <https://lumendatabase.org/>.

## Appendix A. Acknowledgements

Thanks to Lars Eggert, Tommy Pauly, Emily Stark, and Martin Thomson for their input to this specification.

## Authors' Addresses

Mark Nottingham
Cloudflare
Melbourne
Australia
Email: mnot@mnot.net
URI: https://www.mnot.net/

David Adrian
Google
United States of America
Email: davidcadrian@gmail.com