

# Structured Data for Filtered DNS

draft-ietf-dnsop-structured-dns-error-01

**IETF116, March 2023**

D. Wing (Citrix)

**T. Reddy** (Nokia)

N. Cook (Open-Xchange)

M. Boucadair (Orange)

# Agenda

- An update of how the comments received in the WG adoption call were addressed
- Some discussion points

# Sub-Error Codes

- Added citations, meaning and registry for the sub-error codes
  - Malware, Phishing [RFC5901]
  - Spam, Spyware [RFC4949]
  - Network Operator Policy
  - DNS Operator Policy

# RFC8914 Error Codes Applicability

Structured Sub-Error Code	RFC8914 Error Code			
	Forged Answer	Blocked	Censored	Filtered
Malware		X	X	X
Phishing		X	X	X
Spam		X	X	X
Spyware		X	X	X
Network Operator Policy		X		
DNS Operator Policy		X		

# Backward Support

- DNS server returns "Forged Answer" to non-EDE-supporting clients, and forges the answer
  - return RFC8914 EDE ("Blocked", "Censored" and "Filtered") that better explains the filtering

# Other Changes

- Added text to better explain changes vs. RFC8914
- Display the information in the "c", "j" and "o" fields only if the resolver has sufficient reputation
- Allow "j" and "o" fields to contain UTF-8
- User's preferred language: Not addressed
  - May harm client privacy
  - Same issue as RFC8914's EXTRA-TEXT

## Discussion Point #1: JSON Names

- We consider the document as a base to set the structure with a limited set of JSON names
- How additional JSON names are added:
  - Designated Experts?
  - Or adopt a more restrictive policy by requiring IETF Review?
- Any preference?

## Discussion Point #2: Sub-Errors

- The current version requires Expert Review for registering new sub-errors
  - Review criteria are included in the spec
- Are there additional items that we need to record the in the guidelines?



# Next Steps

- Please review and share comments