C-DNS
A DNS Packet Capture Format

draft-ietf-dnsop-dns-capture-format

Sara Dickinson  sara@sinodun.com
A DNS Packet Capture Format

• **GOALS:**

  • **Efficient storage** of large packet captures of DNS traffic (CBOR [RFC7049])
  
  • Works in restricted environments

  • Relatively low overhead to produce and minimizes the requirement for further compression

  • WBN if reversible (it almost is)
C-DNS Format

- **Combine** DNS Query and the associated Response
- **Collected** Q/R items into blocks of (a few thousand)
- **Common data** in a block is abstracted and referenced from individual Q/R items
- **Optional** collection for Sections/RRs
Draft Status

• Adopted by working group in Nov 2016
• Latest version is -01 Feb 2017
  • Comprehensive editorial review
  • Added option to store malformed packets
  • Timestamp resolution, few new fields
Comments on -01

• Clarify configuration settings
• Terminology clean up
• OPEN QUESTION: Partially malformed packet handling
• NOTED: Images are not up to date - will fix asap