C-DNS

A DNS Packet Capture Format

draft-dickinson-dnsop-dns-capture-format
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 CBOR

• Combine DNS Query and the associated Response

• Optional sections

• Collected into blocks of (a few thousand) Q/R items

• Common data in a block is abstracted and referenced from individual Q/R items

• Compress the data making use of knowledge of the DNS packet structure (~ 30% size of PCAPs)
Interesting Factoids

• libpcap doesn’t guarantee to return packets in time order

• Different name server implementations use different DNS name compression algorithms
Comments so far/TODOs

• Complicated but achieves goals

• Minor updates to improve format

• TODO: Include representation of malformed packets/non DNS packets

• TODO: Better data on file sizes, etc

• Candidate for adoption - WG thoughts?
An IPR disclosure exists

WO2014128463A1: (Pending - filed Feb 2014)

ABSTRACT

For monitoring traffic in a communications network, network protocol requests sent over the network are obtained. The resulting network protocol responses sent over said network are also obtained. It is then determined which request corresponds to which response and each request and corresponding response pair is stored as a single request-response record. Preferably, the time of capture of the request in each record is stored. Moreover, a request lookup key may be created from specific attributes of the request. The requests and responses preferably adhere to the domain name system (DNS) protocol.