C-DNS

A DNS Packet Capture Format

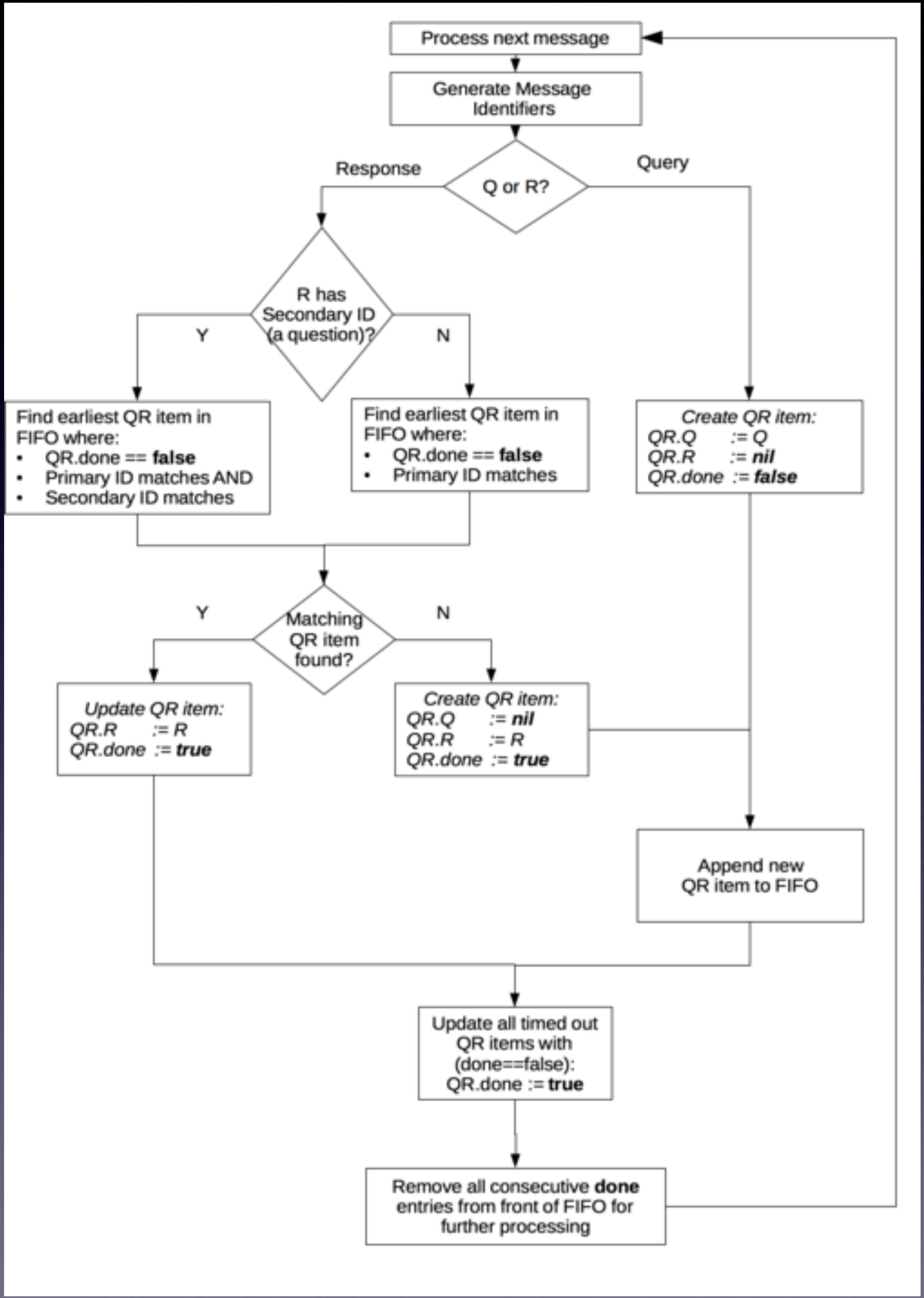
draft-dickinson-dnsop-dns-capture-format

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)



Process next message

Generate Message Identifiers

Q or R?

Response

Query

R has Secondary ID (a question)?

Y

N

Find earliest QR item in FIFO where:
- QR.done == **false**
- Primary ID matches AND
- Secondary ID matches

Find earliest QR item in FIFO where:
- QR.done == **false**
- Primary ID matches

Create QR item:
QR.Q := Q
*QR.R := **nil***
*QR.done := **false***

Matching QR item found?

Y

N

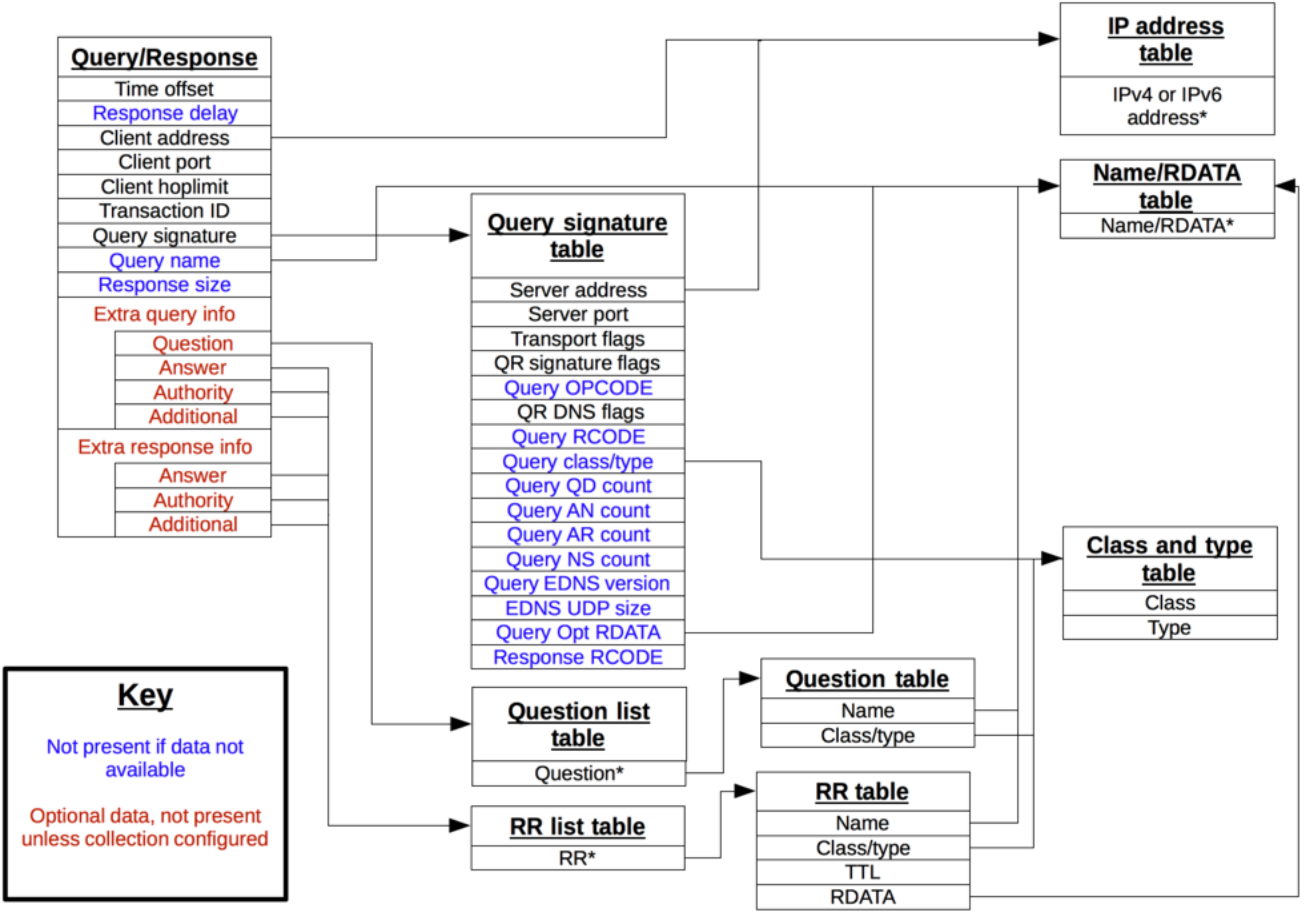
Update QR item:
QR.R := R
*QR.done := **true***

Create QR item:
*QR.Q := **nil***
QR.R := R
*QR.done := **true***

Append new QR item to FIFO

Update all timed out QR items with (done==false): QR.done := **true**

Remove all consecutive **done** entries from front of FIFO for further processing



Query/Response

- Time offset
- Response delay
- Client address
- Client port
- Client hoplimit
- Transaction ID
- Query signature
- Query name
- Response size
- Extra query info
  - Question
  - Answer
  - Authority
  - Additional
- Extra response info
  - Answer
  - Authority
  - Additional

Query signature table

- Server address
- Server port
- Transport flags
- QR signature flags
- Query OPCODE
- QR DNS flags
- Query RCODE
- Query class/type
- Query QD count
- Query AN count
- Query AR count
- Query NS count
- Query EDNS version
- EDNS UDP size
- Query Opt RDATA
- Response RCODE

IP address table

- IPv4 or IPv6 address*

Name/RDATA table

- Name/RDATA*

Class and type table

- Class
- Type

Question list table

- Question*

Question table

- Name
- Class/type

RR list table

- RR*

RR table

- Name
- Class/type
- TTL
- RDATA

Key

Not present if data not available

Optional data, not present unless collection configured

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.