C-DNS

A DNS Packet Capture Format

draft-ietf-dnsop-dns-capture-format

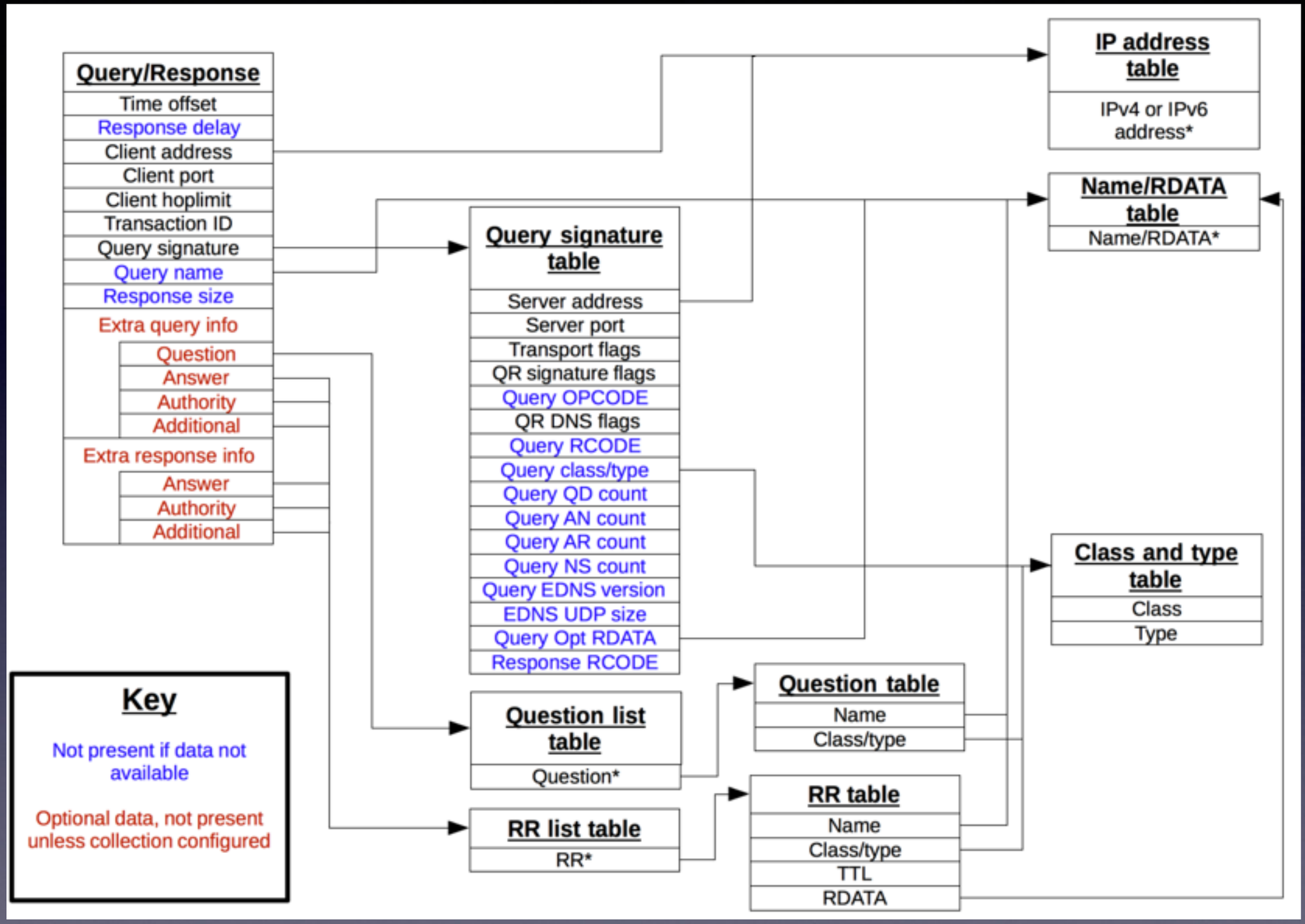
Jim Hague jim@sinodun.com

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


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
IP address table
IPv4 or IPv6 address*
Name/RDATA table
Name/RDATA*
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
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

Draft Status

- -02 April 2017
    - Editorial improvements, image correction
- -03 Jul 2017 (latest version)
    - Added Implementation Status:
        - Compactor (Open source)
          https://github.com/dns-stats/compactor
    - Multiple implementations would be nice…
- We use SVG files…. tools?

Open Questions

- STILL!: Partially malformed packet handling
  - What is a malformed packet?
  - How to compress?
- (Minor) Undefined configuration values

Comments on -03

- Standard mechanism for implementation-specific data items (extensions)
- New use cases where traffic reconstruction not required:
    - Allow more fields to be optional
    - Minimum timestamp resolution

Other

- Hallway discussions on another new use case: Capture inside the nameserver e.g., use with *dnstap*?
    - Capture additional Q/R data such as did the answer come from the cache, balliwick
    - Need everything to be optional?
    - Work at the Hackathon on this….
- Next steps?