C-DNS

A DNS Packet Capture Format

draft-ietf-dnsop-dns-capture-format

Jim Hague jim@sinodun.com

A DNS Packet Capture Format

- **Efficient storage** of large packet captures of DNS traffic
- Uses CBOR (RFC7049) => ~40% size of PCAP
- Combine Q/R records, abstract common data, use block structure (few thousand)
- -06 is latest version (will discuss changes since -03)

Latest big changes: Make it much more generic

- Now **no** mandatory items in top level tables
    - ‘hints’ provided for consumers instead
- Re-worked file pre-amble: split into
    - ‘storage’ - hints, flags for sample/anon/norm
    - ‘configuration’ - wire capture parameters
- Support per block storage parameters (merging)
- IP address flexibility (full address or prefix)

Other changes

- Added mechanism to store malformed messages
- Change timing storage: now using variable sub-second timing (storage multiplier and values)
- Added response bailiwick and response type (for capture inside nameservers)
- Clarified extension mechanism

Last big questions before WGLC?

- (Implicit) Assumption that any stored message could be **fully parsed,** including all RRs, even if not all data is stored
  - There is discussion of storing **partially parsed** messages but no feedback, planning to remove
  - Should this assumption be made clearer/stronger?

- Outstanding requests for format changes:
  - Make RDATA optional in RR storage
  - Request for variable IP address storage