C-DNS

Opportunities to Hack

jabley@nsrc.org

What is the DNS?

- For the purposes of this weekend, DNS a wire format representation of requests and responses
  - pulled off the wire, or out of PCAPs, or something
- Format per the venerable RFC 1035

All communications inside of the domain protocol are carried in a single format called a message. The top level format of message is divided into 5 sections (some of which are empty in certain cases) shown below:

```
    +---------------------+
    |        Header       |
    +---------------------+
    |       Question      | the question for the name server
    +---------------------+
    |        Answer       | RRs answering the question
    +---------------------+
    |      Authority      | RRs pointing toward an authority
    +---------------------+
    |      Additional     | RRs holding additional information
    +---------------------+
```

The header section is always present. The header includes fields that specify which of the remaining sections are present, and also specify whether the message is a query or a response, a standard query or some other opcode, etc.

What is CBOR?

- CBOR is a standard representation of structured data
  - like JSON, but for binary data
- Defined in RFC 7049

What is C-DNS?

- A lossless representation of DNS (request, response) pairs in CBOR
    - within blocks, repeated structures can be replaced by pointers to give some degree of compression
    - ability to count but not record non-DNS traffic (e.g. other junk that lands on a nameserver)
    - draft-dickinson-dnsop-dns-capture-format-00

Things We Could Do

- Review the draft
    - suggest text for missing sections, review, write code to test the specification
- Write code based on the draft
    - identify (request, response) pairs in a stream of packet captures (e.g. BPF, PCAP files)
    - encode or decode (request, response) pairs into a block of CBOR
    - test or measure reference implementations
    - reproduce the test results included in the draft appendicies
    - something else!
- Write up our findings in internet-draft format?