**Suricata - Feature #2448**

**Add additional buffers for DNS Responses**

02/16/2018 11:59 AM - Jack Mott

<table>
<thead>
<tr>
<th>Status: New</th>
<th>Priority: Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignee: OISF Dev</td>
<td>Category:</td>
</tr>
<tr>
<td>Target version: 8.0beta1</td>
<td>Effort:</td>
</tr>
<tr>
<td>Label: Beginner, Protocol</td>
<td>Difficulty:</td>
</tr>
</tbody>
</table>

**Description**

Hi,

It would be nice to be able to include additional buffers for the DNS protocol responses to help write more efficient and effective signatures.

I think buffers for sections like rdata and rrtype should be included to cover things like data in TXT Records, but it could be expanded to cover the other sections of the response.

```json
{
    "timestamp": "2018-02-14T19:12:58.760866-0700",
    "flow_id": 345727363089610,
    "pcap_cnt": 4,
    "event_type": "dns",
    "src_ip": "8.8.8.8",
    "src_port": 53,
    "dest_ip": "192.168.0.105",
    "dest_port": 49153,
    "proto": "UDP",
    "dns": {
        "type": "answer",
        "id": 2,
        "rcode": "NOERROR",
        "rrname": "shinobotps1[.]com",
        "rrtype": "TXT",
        "ttl": 3600,
    }
}
```

Thanks!

**Related issues:**

- Related to Feature #2498: Extend the DNS parser to accept dns_response keyword in signatures added
- Related to Task #4097: Suricon 2020 brainstorm

**History**

**#1 - 02/16/2018 09:36 AM**

- Related to Feature #2198: Extend the DNS parser to accept dns_response keyword in signatures added

**#2 - 02/16/2018 03:45 PM**

- Assignee set to OISF Dev
- Target version set to TBD

**#3 - 09/26/2019 03:24 PM**

- Target version changed from TBD to 6.0.0beta1
As discussed today in the 2020 brainstorm this is still a desired feature. It should be more or less trivial, but could serve as an example of unifying eve logged buffers, and buffers available for detection. At the very least, the rdata buffer should be exposed a sticky for content matches.