Suricata - Bug #1379

EVE json missing CNAME rdata

02/09/2015 07:49 AM - jason jones

<table>
<thead>
<tr>
<th>Status</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee</td>
<td>David Cannings</td>
</tr>
<tr>
<td>Category</td>
<td></td>
</tr>
<tr>
<td>Target version</td>
<td>2.1beta4</td>
</tr>
<tr>
<td>Affected Versions</td>
<td></td>
</tr>
<tr>
<td>Difficulty</td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

Using suricata 2.0.6, dns output for CNAME entries appear to be missing rdata in the EVE json log. I have verified that this is in the raw dns.log.

Example below of CNAME responses for the same hostname with the missing data:

DNS Log:

```
<Redacted> [**] Response TX <redacted> [**] init-p01st.push.apple.com [**] CNAME [**] TTL 32 [**]
init-p01st.push.apple.com.edgesuite.net [**] <redacted>
```

EVE Json:

```
{"timestamp":"<redacted>","event_type":"dns","src_ip":"<redacted>","src_port":53,"dest_ip":","dest_port":","proto":"UDP","dns":{"type":"answer","id":","rrname":"init-p01st.push.apple.com","rrtype":"CNAME","ttl":13}}
```

**History**

**#1 - 05/21/2015 04:46 AM - David Cannings**
- Status changed from New to Resolved
- Assignee set to David Cannings
- Target version set to 3.0RC1
- % Done changed from 0 to 100

This should have been fixed in PR #1425 ([https://github.com/inliniac/suricata/pull/1425](https://github.com/inliniac/suricata/pull/1425)). Changes are in 2.1beta4.

**#2 - 05/21/2015 04:53 AM - Victor Julien**
- Status changed from Resolved to Closed
- Target version changed from 3.0RC1 to 2.1beta4