Suricata - Feature #2166
output: log only triggering buffers
06/28/2017 09:17 AM - Eric Leblond

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>OISF Dev</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
</tbody>
</table>

**Label:**

**Description**
When adding to the alert events the protocol buffer, we provide valuable information but logging all of them will cause a serious increase in event size. So we should only log the triggering buffers.

Jason Ish is proposing the following (https://github.com/inliniac/suricata/pull/2663#issuecomment-293952371)

```
{
    "timestamp": ...
    "alert": ...
    "buffers": [
        {
            "name": "http_response_body",
            "data": "....",
            "data-printable": "...",
        },
        {
            ...
        }
    ]
}
```

**History**

#1 - 06/29/2017 08:34 AM - Victor Julien
- Subject changed from Log only triggering buffers to output: log only triggering buffers

#2 - 07/04/2017 03:32 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD