Suricata - Feature #2713
protocol detection w/o protocol parsing
11/24/2018 10:20 AM - Victor Julien

<table>
<thead>
<tr>
<th>Status</th>
<th>Feedback</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee</td>
<td>Pierre Chifflier</td>
</tr>
<tr>
<td>Category</td>
<td></td>
</tr>
<tr>
<td>Target version</td>
<td>TBD</td>
</tr>
</tbody>
</table>

Description
At the Suricon2018 it was requested to add better support for detection of protocols w/o implementing full parsers.
Pierre, could you fill in more details of what you have in mind?

Related issues:
- Related to Task #2685: SuriCon 2018 brainstorm
- Related to Feature #2757: improve protocol detection

History
#1 - 11/24/2018 10:20 AM - Victor Julien
- Related to Task #2685: SuriCon 2018 brainstorm added

#2 - 11/01/2019 03:08 PM - Philippe Antoine
Are there specific protocols in mind?
What is the use case?
We have to watch for evasions to use this in a rules context...

#3 - 11/01/2019 03:08 PM - Philippe Antoine
- Related to Feature #2757: improve protocol detection added