Suricata - Feature #3086
app_proto for Torrent traffic?

07/12/2019 05:25 PM - Kenneth Kolano

<table>
<thead>
<tr>
<th>Status:</th>
<th>Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Aaron Bungay</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>7.0rc1</td>
</tr>
<tr>
<td>Effort:</td>
<td>medium</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>medium</td>
</tr>
</tbody>
</table>

### Description
Currently the app_proto registered for Torrent traffic is "failed". Can the detection be revised to detect Torrent traffic?

It should be identifiable by the payload pre-fix: "d1:ad2:id20:"

### Related issues:
Related to Task #4151: Research: New protocol support

### History

**#1 - 07/19/2019 09:40 PM - Andreas Herz**
- Assignee set to Community Ticket
- Target version set to TBD
- Effort set to medium
- Difficulty set to medium

**#2 - 11/19/2020 04:26 PM - Aaron Bungay**
Working on this.

**#3 - 11/19/2020 05:45 PM - Victor Julien**
- Status changed from New to Assigned
- Assignee changed from Community Ticket to Aaron Bungay

**#4 - 11/19/2020 05:45 PM - Victor Julien**
Are you doing protocol detection only or a full parser?

**#5 - 11/19/2020 05:46 PM - Victor Julien**
- Related to Task #4151: Research: New protocol support added

**#6 - 11/20/2020 06:36 AM - Aaron Bungay**
Victor Julien wrote in #note-4:

> Are you doing protocol detection only or a full parser?

Doing a full parser in rust for the BitTorrent DHT protocol :)

**#7 - 11/20/2020 06:42 AM - Victor Julien**
- Target version changed from TBD to 7.0rc1
- Label Protocol added

Great!

**#8 - 01/31/2021 10:39 PM - Aaron Bungay**
Victor Julien wrote in #note-7:
Great!

PR created - [https://github.com/OISF/suricata/pull/5809](https://github.com/OISF/suricata/pull/5809) ;)

07/16/2022