### Suricata - Feature #2311

**math on extracted values**

12/01/2017 03:48 AM - Victor Julien

<table>
<thead>
<tr>
<th>Status</th>
<th>In Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee</td>
<td>Jeff Lucovsky</td>
</tr>
<tr>
<td>Category</td>
<td></td>
</tr>
<tr>
<td>Target version</td>
<td>6.0.0rc1</td>
</tr>
<tr>
<td>Effort</td>
<td>low</td>
</tr>
<tr>
<td>Difficulty</td>
<td>medium</td>
</tr>
</tbody>
</table>

**Description**

**Related issues:**

- Related to Task #2309: SuriCon 2017 brainstorm

**History**

**#1 - 12/01/2017 03:48 AM - Victor Julien**
- Related to Task #2309: SuriCon 2017 brainstorm added

**#2 - 04/13/2018 03:55 PM - Victor Julien**
We need feedback on what usecases would need to be added/supported.

**#3 - 07/13/2018 06:27 PM - Victor Julien**
- Effort set to low
- Difficulty set to medium

**#4 - 09/12/2018 02:46 PM - David Wharton**
While Suricata has matured to the point where it should be defining IDS rule capabilities instead of reacting to other vendors, I think in this case it makes sense to try to make this compatible with the existing Snort `byte_math` keyword.

**Format:**

```
byte_math:bytes <bytes_to_extract>, offset <offset_value>, oper <operator>,
value <r_value>, result <result_variable> [, relative]
[, endian <endian>][], string <number type>][, dce]
[, bitmask <bitmask_value>];
```

**Ref:** Snort 2.9.9.0 manual, section 3.5.34

This keyword is functionally different but structurally similar (not exact) to other 'byte_**"**' keywords such as 'byte_test', 'byte_extract' and 'byte_jump'.

Cross-variable buffer usage should be allowed, however this may be a challenge (or secondary goal) since currently cross-buffer byte extraction and usage isn't currently supported.

**#5 - 03/11/2019 02:51 PM - Victor Julien**
- Assignee set to Community Ticket
- Priority changed from Low to Normal

**#6 - 09/27/2019 08:24 AM - Victor Julien**
- Status changed from New to Assigned
- Assignee changed from Community Ticket to Jeff Lucovsky
- Target version changed from TBD to 6.0.0rc1

**#7 - 02/18/2020 11:14 AM - Victor Julien**
#8 - 04/11/2020 12:22 PM - Jeff Lucovsky
https://github.com/OISF/suricata/pull/4502