Suricata - Optimization #1044
TLS buffers evaluated by fast_pattern matcher.
11/23/2013 07:40 AM - Will Metcalf

Status: Closed
Priority: Normal
Assignee: Mats Klepsland
Category:
Target version: 3.2beta1
Effort:
Difficulty:

Label:

Description
As far as I can tell tls.* buffers are not evaluated by the fast_pattern matcher. If this is correct is there a reason why this is the case? If no reason can we add them?

History
#1 - 11/25/2013 02:41 AM - Victor Julien
  - Assignee deleted (Anoop Saldanha)
  - Target version set to 3.0RC2

#2 - 05/20/2015 09:03 AM - Victor Julien
  - Target version changed from 3.0RC2 to TBD

#3 - 01/01/2016 06:20 PM - Andreas Herz
  - Assignee set to OISF Dev

#4 - 06/15/2016 05:44 AM - Victor Julien
  - Status changed from New to Assigned
  - Assignee changed from OISF Dev to Mats Klepsland

#5 - 09/22/2016 02:34 AM - Victor Julien
  - Status changed from Assigned to Closed
  - Target version changed from TBD to 3.2beta1

https://github.com/inliniac/suricata/pull/2249 adds: tls_cert_issuer and tls_cert_subject, which replace tls.issuerdn and tls.subject. They are 'sticky buffers' like file_data, so all your regular matching (content/pcre/isdataat/etc) applies.