Suricata - Feature #1766

TLS keyword expansion

04/21/2016 07:38 AM - Mats Klepsland

Status: Assigned
Priority: Normal
Assignee: Mats Klepsland
Category: 
Target version: TBD
Effort: 
Difficulty: 

Description
Suricata should support more TLS keywords than it currently does. See TLS keyword expansion for more information of what I'm suggesting and add your comments here :) 

History
#1 - 05/11/2016 02:25 PM - Zach Rasmor
I began a prototype to add the cipher suite to the JSON output - are you already planning to do this?

#2 - 05/11/2016 02:43 PM - Mats Klepsland
Yeah, this is already planned. The plan is to add custom TLS logging (both for tls-log and json-tls), and then start logging more as more TLS stuff is decoded when more TLS keywords are added. Logging cipher-suite from server_hello is on my todo.

#3 - 09/08/2016 02:54 PM - Andreas Herz
- Target version set to TBD

#4 - 05/25/2017 02:02 PM - Zach Rasmor
Hello Mats - has there been any progress on the expanded logging, or should I resume my prototyping?

#5 - 09/27/2019 01:19 PM - Victor Julien
- Status changed from New to Assigned

Hi Mats, could you update the wiki doc to indicate what has been implemented?