Suricata - Bug #1602

eve-log prefix field feature broken

11/25/2015 02:45 PM - Zach Rasmor

Status: Closed
Priority: Normal
Assignee: Eric Leblond
Category: 
Target version: 3.0RC2
Affected Versions: 
Effort: 
Difficulty: 
Label: 

Description
The eve-log prefix field is ignored. This was added as a feature in this release, but was undone by a later PR.

History:
Bug 1204 ([https://redmine.openinfosecfoundation.org/issues/1454](https://redmine.openinfosecfoundation.org/issues/1454)) added the prefix field and was fixed in PR 1532 (Merged through PR 1540)

In this commit, the prefix logic is not moved to the the newly created function: util-logopenfile.c:LogFileWrite
[https://github.com/inliniac/suricata/commit/a13be67b5e6c26c53149b88f9565c58f7fde3381](https://github.com/inliniac/suricata/commit/a13be67b5e6c26c53149b88f9565c58f7fde3381) (Merged through 1712)

Related issues:
Related to Feature #1454: Proposal to add Lumberjack/CEE formatting option to... Closed 04/20/2015

History
#1 - 11/25/2015 02:47 PM - Zach Rasmor
Correction: it was Feature 1454 that added the prefix field (link is correct, text is incorrect)

#2 - 11/25/2015 02:47 PM - Zach Rasmor
- Related to Feature #1454: Proposal to add Lumberjack/CEE formatting option to EVE JSON syslog output for compatibility with rsyslog parsing added

#3 - 11/26/2015 12:09 PM - Victor Julien
This should be restored through Eric's [https://github.com/inliniac/suricata/pull/1757](https://github.com/inliniac/suricata/pull/1757) (now also in master), can you confirm?

#4 - 11/26/2015 01:34 PM - Zach Rasmor
Confirmed. Thanks a lot!

#5 - 11/27/2015 02:25 AM - Victor Julien
- Subject changed from eve-log prefix field feature ignored (undone by PR 1712) to eve-log prefix field feature broken
- Status changed from New to Closed
- Assignee set to Eric Leblond
- Target version set to 3.0RC2