Suricata - Feature #4515
Add DNS logging of Z flag
06/05/2021 01:52 PM - Odin Jenseg

Status: Closed
Priority: Normal
Assignee: Odin Jenseg
Category: 
Target version: 7.0rc1
Effort: 
Difficulty: 
Label: Protocol, Rust

Description
The this Z field is logged by Zeek: https://docs.zeek.org/en/master/logs/dns.html
And has shown good value to have in investigations, and there has been created a sigma rule that is based on this flag:

I think this should be pretty strightforward, so I will great a PR

Related issues:
Related to Bug #4924: dns: transaction not created when z-bit set
Closed

History
#1 - 06/05/2021 03:02 PM - Odin Jenseg
https://github.com/OISF/suricata/pull/6181

#2 - 12/21/2021 08:36 PM - Jason Ish
- Related to Bug #4924: dns: transaction not created when z-bit set added

#3 - 12/22/2021 08:47 PM - Jason Ish
- Status changed from New to In Review

PR: https://github.com/OISF/suricata/pull/6731

#4 - 01/04/2022 04:22 PM - Jason Ish
- Status changed from In Review to Closed
- Target version set to 7.0rc1

PR merged.