Suricata - Feature #2673
Split out DNS parser to be reusable
11/12/2018 08:00 PM - Ed Page

Status: New
Priority: Normal
Assignee: Community Ticket
Category: TBD
Target version: TBD
Effort:
Difficulty:
Label:

Description
Suricata has a built-in DHCP parser written in Rust, https://github.com/OISF/suricata/tree/master/rust/src/dns

Splitting this out into a dedicated crate can allow leverage/collaboration between Suricata and other projects.

History
#1 - 11/12/2018 08:01 PM - Ed Page
Looks like there are a couple of existing DNS parsers that I've not evaluated

- https://crates.io/crates/dns

#2 - 05/23/2019 09:51 PM - Andreas Herz
- Assignee set to Community Ticket
- Target version set to TBD

#3 - 04/22/2020 07:07 PM - Jason Ish
I'm not sure I would want to break out the DNS parser into its own repo, as that as extra overhead to the development process. But something possibly worth considering is breaking out some stuff, within the repo to their own crates. A while back I did this with the DHCP parser. It breaks out just the parsing, as the other parts of the DHCP module are pretty Suricata specific. The commit is now stale, but it still gets the idea across:
https://github.com/OISF/suricata/pull/4129/commits/fda42f73257e8a9f2703a2db24d5894731ece19f

API stability also needs to be considered, as now we are free to refactor as needed. Publishing it as a reusable component may imply some level of stability, and we don't exactly follow semver. However, Cargo does make it easy to specify specific versions.