SURICATA - FEATURE #4967

Tasks # 4966 (New): tracking: QUIC protocol support

QUIC v1 support

01/17/2022 07:14 AM - Victor Julien

Status: In Review
Priority: Normal
Assignee: Philippe Antoine
Category: Target version: 7.0rc1
Effort: Label:

Description

QUIC v1 protocol is different from GQUIC in various ways. In the traffic I see it embeds a TLS1.3 client hello with SNI and possibly enough info for something like JA3?

Related issues:

Blocks Feature #4985: quic: support frames

Follows Feature #3440: Add GQUIC Protocol Analysis and CYU Fingerprinting

History

#1 - 01/17/2022 07:22 AM - Philippe Antoine
Should it be done after #3440?

#2 - 01/17/2022 07:28 AM - Victor Julien
- Follows Feature #3440: Add GQUIC Protocol Analysis and CYU Fingerprinting added

#3 - 01/17/2022 07:29 AM - Victor Julien
Philippe Antoine wrote in #note-1:

    Should it be done after #3440?

Yes, that work (current PR is https://github.com/OISF/suricata/pull/6796) should form the basis.

#4 - 02/22/2022 08:35 AM - Philippe Antoine
- Status changed from Assigned to In Review

https://github.com/OISF/suricata/pull/7047

#5 - 02/22/2022 01:38 PM - Philippe Antoine
- Blocks Feature #4985: quic: support frames added