When a flow is long duration and is not yet dead, we can know it exists (via application layer logging) but we can't know anything about the volume of data exchanged. This is not helping to characterize the nature of the flow. For example, we can not differentiate a scp session and a ssh session (same example work on TLS tunnel).

A way to get information is to be able to query the unix socket to get the volumetry information from the flow.

History

#1 - 03/29/2021 08:14 AM - Victor Julien
It's unclear to me what your idea is here? Can you expand more?

#2 - 06/03/2022 09:28 AM - Victor Julien
- Subject changed from Get flow information by flow_id to unix socket: Get flow information by flow_id
- Status changed from New to In Review

https://github.com/OISF/suricata/pull/6077