Support Modbus Unit Identifier

The Modbus/TCP protocol frame format supports a field called the 'unit identifier'. When Modbus/TCP devices are directly addressable through TCP this field has recommended default values. Some Modbus/TCP devices are co-located with other devices, and occasionally some Modbus/TCP devices act as gateways to other Modbus/TCP devices (perhaps connected serially to the gateway device). When destination IP address does not suffice to uniquely identify the Modbus/TCP device, the ‘unit identifier’ field in some cases does. Support for this ‘unit identifier’ could be of utility when Suricata rules are meant to alert on device manipulation where those devices are behind a Modbus/TCP gateway or contained within a group of co-located Modbus/TCP devices.

A few references:

https://en.wikipedia.org/wiki/Modbus
https://www.snort.org/faq/readme-modbus
http://gridconnect.com/blog/tag/modbus-explained/

A few caveats:

I cannot point at a particular pcap file where I know this unit-id is used outside of device defaults (the Quickdraw Modbus/TCP pcap does use it, with what I presume is a device default (not broadcast)). I haven’t researched the devices that support it. I merely thought it would be “nice to have” without knowing exactly and precisely where (or when) it might be useful.

History

#1 - 01/01/2016 05:42 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

#2 - 04/20/2016 11:46 AM - David DIALLO
- Assignee changed from OISF Dev to David DIALLO

#3 - 02/22/2018 03:25 AM - David DIALLO
- Status changed from New to Resolved
- % Done changed from 0 to 100

#4 - 03/05/2018 03:50 PM - Andreas Herz
If it's resolved can you set the issue to closed and link further informations, like pull request if it's fixed by one?

#5 - 03/22/2018 04:46 AM - Victor Julien
- Status changed from Resolved to Closed
- Target version changed from TBD to 4.1beta1

https://github.com/OISF/suricata/pull/3279