I'm currently testing Suricata with some pcaps that are known to have TLS connection (files are attached to this post). But Suricata only logs the TLS connection of a small subset of these pcaps.

I took a look at the pcap's and it seems that most of them have packets with invalid checksums. They might have been captured with checksum offloading turned on, or something else that messes up the checksums. This is quite a common problem when processing pcap files with Suricata.

Because of this, I usually use `-k none` when reading pcap files, especially when reading pcap files captured by other people. This makes Suricata disable the checksum checking.

Let me know if this solves your problem :)

yes it did solve the problem

I'm glad to hear that. Thanks for letting me know that it solved your problem :)