Event Analysis: Blocked Website Access Attempt

These analysed events occurred when a website specified by a Suricata rule was accessed, in this case Facebook.

Information captured by Suricata is fairly similar to the firewall event information with a few differences. The Destination Port field in Suricata shows 53 instead of 443, which is used for DNS requests. The Suricata rule monitors both DNS and TLS requests for Facebook rather than HTTP/HTTPS. It also includes the additional field "data.flow.bytes" for the server and the client, describing the movement of data in bytes, which the firewall events lack. There are also various DNS-specific flags, describing the version and the name of the requested domain.

Figure 1: Some Important Suricata Fields