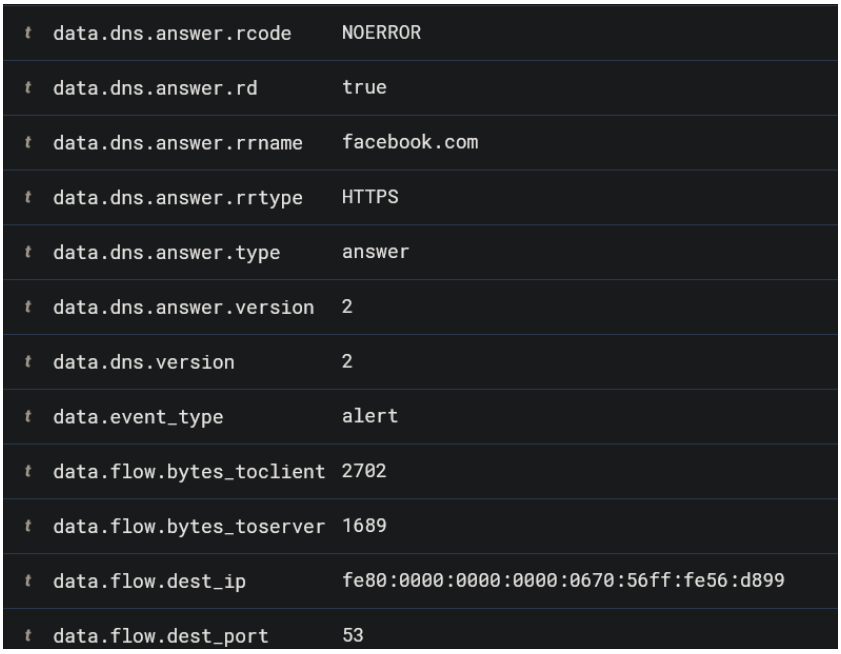
These analysed events occurred when a website specified by a Suricata rule was accessed, in this case Facebook.

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.



t	data.dns.answer.rcode	NOERROR
t	data.dns.answer.rd	true
t	data.dns.answer.rrname	facebook.com
t	data.dns.answer.rrtype	HTTPS
t	data.dns.answer.type	answer
t	data.dns.answer.version	2
t	data.dns.version	2
t	data.event_type	alert
t	data.flow.bytes_toclient	2702
t	data.flow.bytes_toserver	1689
t	data.flow.dest_ip	fe80:0000:0000:0000:0670:56ff:fe56:d899
t	data.flow.dest_port	53

Figure 1: Some Important Suricata Fields