Attributes in Alert dataset

Attribute Name	Description	Barnyard2 Table Name
timestamp	time of when the event was logged	event
signature	Signature ID /alert ID	event
sig_name	Signature Name /Alert Name	signature
sig_class_name	Classification name / Alert Class Name	sig_class
sid	Sensor ID	iphdr
cid	Event ID	iphdr
ip_src	Source IP address (32-bit unsigned int)	iphdr
ip_dst	Destination IP address (32-bit unsigned int)	iphdr
ip_ver	IP version	iphdr
ip_hlen	IP Header length	iphdr
ip_tos	IP type-of-service	iphdr
ip_len	IP datagram length	iphdr
ip_id	IP ID	iphdr
ip_flags	IP flags	iphdr
ip_off	IP fragment offset	iphdr
ip_ttl	IP time-to-live	iphdr
ip_proto	IP protocol	iphdr
ip_csum	IP checksum	iphdr
sport	TCP & UDP soure port	tcphdr + uphdr
dport	TCP & UDP destination port	tcphdr + uphdr
seq	TCP sequence number	tcphdr
ack	TCP ACK number	tcphdr
offload	TCP offset	tcphdr
res	TCP reserved	tcphdr
csum	TCP checksum	tcphdr
win	TCP window	tcphdr

urp	TCP urgent pointer	tcphdr
udp_len	UDP length	udphdr
icmp_type	ICMP type	icmp
icmp_code	ICMP code	icmp
protocol_type	Type of Protocol	tcp/udp/icmp