



- 0: proto=udp
- 1: proto=tcp
- 2: proto=icmp
- 6: conn\_state=S0
- 7: conn\_state=SF
- 8: conn\_state=other
- 10: history=D
- 11: history=Dd
- 12: history=S
- 13: history=other
- 14: orig\_pkts
- 15: orig\_ip\_bytes
- 16: resp\_pkts
- 17: resp\_ip\_bytes