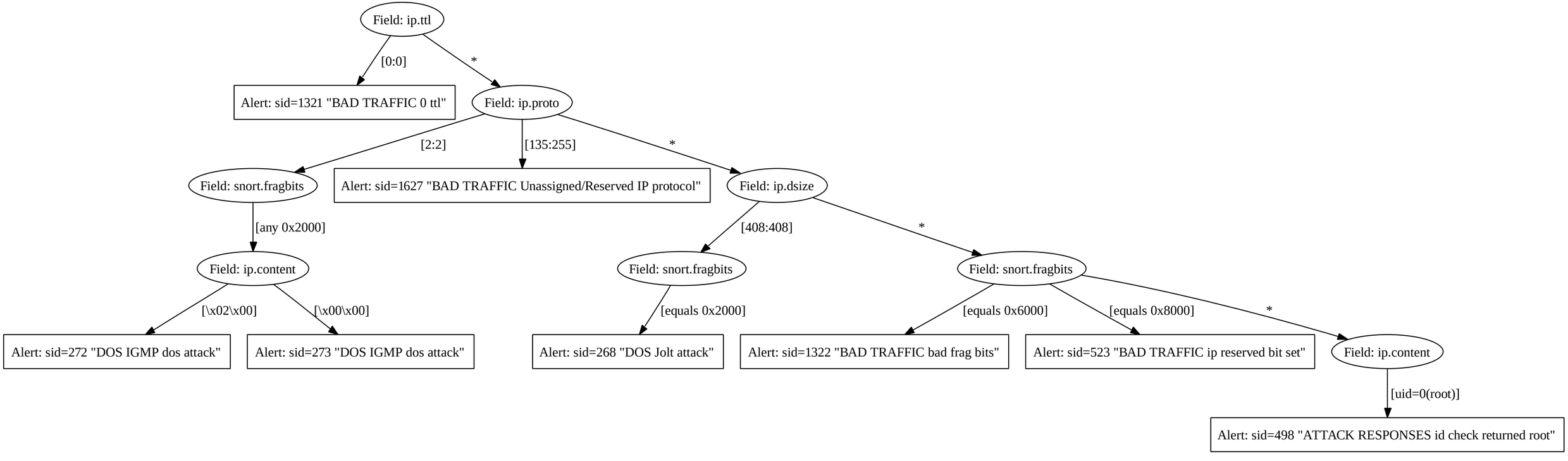
Field: ip.ttl
[0:0]
*
Alert: sid=1321 "BAD TRAFFIC 0 ttl"
Field: ip.proto
[2:2]
[135:255]
*
Field: snort.fragbits
Alert: sid=1627 "BAD TRAFFIC Unassigned/Reserved IP protocol"
Field: ip.dsize
[any 0x2000]
[408:408]
*
Field: ip.content
Field: snort.fragbits
Field: snort.fragbits
[\x02\x00]
[\x00\x00]
[equals 0x2000]
[equals 0x6000]
[equals 0x8000]
*
Alert: sid=272 "DOS IGMP dos attack"
Alert: sid=273 "DOS IGMP dos attack"
Alert: sid=268 "DOS Jolt attack"
Alert: sid=1322 "BAD TRAFFIC bad frag bits"
Alert: sid=523 "BAD TRAFFIC ip reserved bit set"
Field: ip.content
[uid=0(root)]
Alert: sid=498 "ATTACK RESPONSES id check returned root"