数据结构示例

本附录包含选定的入侵事件、关联事件和发现事件的数据结构示例。每个示例均以二进制格式显示，以清楚地展示每一个位是如何设置的。

有关详细信息，请参阅以下各节：

入侵事件数据结构示例

本节包含可能由 eStreamer 传输的入侵事件的数据结构示例。提供以下示例：

管理中心 5.4+ 的入侵事件示例

下图显示了一个事件记录示例：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1	1	0
3	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0
5	0	1	0	1	0	0	1	1	1	0	1	1	0	1	0	0	0	0	1	0	1	1	1	1	0	0	1	0	1	1	1	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0
11	0	1	0	1	0	0	1	1	1	0	1	1	0	1	0	0	0	0	1	0	1	1	1	1	0	0	1	0	1	1	1	1
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	0	1	1	1	0	0	1	1	1	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	1	1	1	1	0	1	1	1	0	1	1	1	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	1	1	1	0	0	0	1	0	0	0	0	1	0	1
20	1	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	1	0	0	1	0	0	0	0
21	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	1	0	1	0	1	0	0	0	0	0	0	1	1	0	0	1	1	1	0	1	0	0	1	1	0	1	1	1	1	1	1	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	0	0
	1	0	1	0	0	1	0	0	1	0	0	0	0	1	0	1	1	1	0	1	0	0	0	0	0	1	1	1	0	0	0	1
	1	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	1	0	0	0	1	0	0	1	1	0	1	0	0	0	1	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	1	1	1
27	0	1	1	1	0	1	1	1	0	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	1	0	1	0	0	1	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	1	0	0
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
30	1	1	0	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	1	0
	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	0	0
	1	0	1	0	0	1	0	1	1	1	1	1	0	1	1	0	1	0	1	1	0	0	1	1	0	0	0	0	1	0	0	1
	0	1	0	0	0	0	0	1	1	0	0	1	0	1	1	1	1	0	0	1	1	1	1	1	0	0	0	1	0	1	0	0
31	0	1	1	0	1	0	0	1	0	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	0	0	0	1	1	0	1	0
	1	1	1	1	1	1	1	0	0	0	1	1	1	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	1	0	1	0	0	0	1	0	1	0	0	1	0	0	0	0	1	0	1	0	0	1	1	0	0	1	1	0	1
	1	0	1	0	1	0	1	1	0	0	0	1	0	1	0	0	1	1	0	0	1	1	1	1	1	0	0	1	1	1	0	0
32	0	1	1	0	1	0	0	1	0	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	0	0	0	1	1	0	1	0
	1	1	1	1	1	1	1	0	0	0	1	1	1	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	1	0	1	0	0	0	1	0	1	0	0	1	0	0	0	0	1	0	1	0	0	1	1	0	0	1	1	0	1
	1	0	1	0	1	0	1	1	0	0	0	1	0	1	0	0	1	1	0	0	1	1	1	1	1	0	0	1	1	1	0	0
33	0	0	1	0	1	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	0	0	1	1	0	0	1	1	0	0	0	0
	1	1	1	1	1	1	1	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	1
	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	0	0	1	0	0	0	1	1	0	1	0	0	1	0	0	1	1
34	0	0	1	0	1	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	0	0	1	1	0	0	1	1	0	0	0	0
	1	1	1	1	1	1	1	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	1

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	0	0	1	0	0	0	1	1	0	1	0	0	1	0	0	1	1
35	0	1	0	1	0	0	1	1	1	0	1	1	0	1	0	0	0	0	1	0	1	1	1	1	0	0	1	0	1	1	1	1
36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1	0	0	0	0	1	1	0
37	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
38	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
39	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
41	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
43	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0																

在上一个示例中，出现以下事件信息：

编号	说明
1	此行的前两个字节表示标准报头值 1。接下来的两个字节表示该消息为数据消息（也就是消息类型 4）。
2	此行表示后面的消息长度为 294 个字节。
3	这里的第一位是一个标志，表示该报头是一个含有存档时间戳的扩展报头。接下来的15位是一个可选字段，包含在其上检测到事件的域的NetmapID。该行的其余部分表示记录类型值 400，说明这是入侵事件记录。
4	此行表示后面的事件记录长度为 278 个字节。

编号	说明
5	此行是保存事件的时间戳。在本例中，事件保存时间为 2014 年 7 月 2 日，星期三，16:11:27。
6	此行留作未来使用，用 0 填充。
7	此行表示块类型为 45，这是版本 5.4+ 的入侵事件记录的块类型。
8	此行表示数据块长度为 278 个字节。
9	此行表示事件是从编号为 5 的传感器收集的。
10	此行表示事件标识号为 65580。
11	此行表示事件发生于 1404317489 秒。
12	此行表示事件发生于 46542 微秒。
13	此行表示规则 ID 号码为 4。
14	此行表示事件是由 ID 号码为 119 的生成器（也就是规则引擎）检测到的。
15	此行表示规则版本号为 1。
16	此行表示分类标识号为 1。
17	此行表示优先级标识号为 3。
18	此行表示源 IP 地址为 10.5.61.220。请注意，此字段可包含 IPv4 或 IPv6 地址。
19	此行表示目标 IP 地址为 10.5.56.133。请注意，此字段可包含 IPv4 或 IPv6 地址。
20	此行的前两个字节表示源端口号为 33018，接下来的两个字节表示目标端口号为 8080。
21	此行的第一个字节表示 TCP (6) 是事件中使用的协议。第二个字节为影响标志，由于第二位为 1，表示此事件为红色（易受攻击）事件；表示源主机或目标主机位于受系统监控的网络中，源主机或目标主机存在于网络映射中，并且在此事件中，?»机或目标主机在端口上运行服务器；因为第二和第三个标志均为 1，因此这是一个可能易受攻击的橙色事件。此行的第三个字节表示影响，该字节值为 2，表示事件为可能易受攻击的橙色事件。最后一个字节表示事件未被阻止。
22	此行包含 MPLS 标签（若有）。
23	此行的前两个字节表示 VLAN ID 为 0。最后两个字节保留，并设置为 0。
24	此行包含入侵策略的唯一 ID 号码。
25	此行包含用户的内部标识号。因为没有适用的用户，因此该行全部为 0。
26	此行包含 Web 应用的内部标识号，即 847。
27	此行包含客户端应用的内部标识号，即 2000000676。
28	此行包含应用协议的内部标识号，即 676。
29	此行包含访问控制规则的唯一标识符，即 1。
30	此行包含访问控制策略的唯一标识符。
31	此行包含入口接口的唯一标识符。
32	此行包含出口接口的唯一标识符。因为此事件已被阻止。
33	此行包含入口安全区的唯一标识符。
34	此行包含出口安全区的唯一标识符。
35	此行包含与入侵事件关联的连接事件的 Unix 时间戳。
36	此行的前两个字节表示生成连接事件的受管设备上的 Snort 示例的数字 ID。其余两个字节表示用于区别在同一秒内发生的连接事件的值。

编号	说明
37	此行的前两个字节表示源主机的国家/地区代码。其余两个字节表示目标主机的国家/地区代码。
38	此行的前两个字节包含与此事件关联的威胁的 ID 号码。其余两个字节包含流量通过的安全情景（虚拟防火墙）的 ID 号码的开头。
39	此行包含流量通过的安全情景（虚拟防火墙）的 ID 号码的其余部分。
40	此行的前两个字节包含流量通过的安全情景（虚拟防火墙）的最后两个字节。接下来的两个字节包含 SSL 服务器证书的 SHA1 散列的开头（若使用 SSL）。
41	此行包含 SSL 服务器证书的 SHA1 散列的其余部分（若使用 SSL）。
42	此行的前两个字节包含SSL服务器证书的SHA1散列的最后两个字节。接下来的两个字节包含实际采取的 SSL 操作。由于此连接未使用 SSL，所以其值为 0。
43	此行的前两个字节包含 SSL 流状态。由于此连接未使用SSL，所以其值为0。接下来的两个字节包含与此事件关联的网络分析策略的 UUID 的前两个字节。
44	此行包含与此事件关联的网络分析策略的 UUID 的其余部分。

入侵影响警报示例

下图显示了一个入侵影响警报记录示例：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	1	0	0	0	1	0	1	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
9	0	1	0	0	0	0	0	1	1	0	0	1	1	0	1	1	0	1	1	0	1	1	1	1	0	0	1	0	1	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
11	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0
15	0	1	0	1	0	1	1	0	0	1	1	1	0	1	0	1	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1	0
	0	1	1	0	0	1	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	0	0	1	0
	0	1	1	0	1	1	0	0	0	1	1	0	0	1	0	1																

在上一个实例中，出现以下信息：

编号	说明
1	此行的前两个字节表示标准报头值 1。接下来的两个字节表示该消息为数据消息（消息类型 4）。
2	此行表示后面的消息长度为 58 个字节。
3	这里的第一位是一个标志，表示该报头不是一个含有存档时间戳的扩展报头。接下来的15位是一个可选字段，包含在其上检测到事件的域的NetmapID。该行的其余部分表示记录类型值 9，说明这是入侵影响警报记录。
4	此行表示后面的数据长度为 50 个字节。
5	此行包含值 20，表示后面跟着一个入侵影响警报数据块。
6	此行表示影响警报块的长度（包括影响警报块报头）为 50 个字节。
7	此行表示事件标识号为 201256。
8	此行表示事件是从编号为 2 的设备收集的。
9	此行表示事件发生于 1087223700 秒。
10	此行表示与事件相关联的影响级别是 1（红色，易受攻击）。
11	此行表示与违规事件关联的 IP 地址为 172.16.1.22。
12	此行表示不存在与违规关联的目标 IP 地址（值设置为 0）。
13	此行表示后面跟着一个字符串块，包含字符串块长度和文本字符串（在本例中，该文本字符串包含影响名称）。有关字符串块的详细信息，请参阅字符串数据块，第 3-59 页。
14	此行表示字符串块的总长度（包括字符串块指示符和长度）为 18 个字节。其中，影响描述占 10 个字节，字符串报头占 8 个字节。
15	此行表示影响的描述为“Vulnerable”（易受攻击）。

数据包记录示例

下图显示了一个数据包记录示例：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	1	1	0	1
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	0	1	0	1
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1	0	1	1	0	1	1	0	0	1	1	0
7	0	0	1	1	1	1	1	1	0	0	0	0	0	1	0	0	0	1	1	1	1	1	1	1	0	1	1	1	0	0	1	0
8	0	0	1	1	1	1	1	1	0	0	0	0	0	1	0	0	0	1	1	1	1	1	1	1	0	1	1	1	0	1	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	1	1	0	0	1	1	1	0	1
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	0	1
12	0	0	1	1	0	0	0	0	0	1	1	1	1	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	0
	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	0	1	0	0	0	1	0	0	0	0	0

在上一个示例中，出现以下数据包信息：

编号	说明
1	此行的前两个字节表示标准报头值 1。接下来的两个字节表示该消息为数据消息（消息类型 4）。
2	此行表示后面的消息长度为 989 个字节。
3	这里的第一位是一个标志，表示该报头不是一个含有存档时间戳的扩展报头。接下来的 15 位是一个可选字段，包含在其上检测到事件的域的 NetmapID。该行的其余部分表示记录类型值 2，说明这是数据包记录。
4	此行表示后面的数据包记录长度为 981 个字节。
5	此行表示事件是从编号为 3 的设备收集的。
6	此行表示事件标识号为 195430。
7	此行表示事件发生于 10572378 秒。
8	此行表示数据包采集于 10572380 秒。
9	此行表示数据包采集于 254365 微秒。

编号	说明
10	此行表示链路类型为 1（以太网层）。
11	此行表示后面的数据包数据长度为 953 个字节。
12	此行及后面一行显示实际负载数据。请注意，实际数据为 953 个字节，此示例中将其截断，以便展示。

分类记录示例

下图显示了一个分类记录示例：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	1	0	1	0	0	0	1	1	1	0	0	1	0
	0	1	1	0	1	1	1	1	0	1	1	0	1	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
	0	0	1	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	0	0	1	1	0	1	1	1	0	1	0	0
	0	1	1	0	1	0	0	1	0	1	1	1	0	1	1	0	0	1	1	0	1	0	0	1	0	1	1	1	0	1	0	0
7	0	1	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	1	0	0	0	0	0	1
	0	0	1	0	0	0	0	0	0	1	0	0	1	1	1	0	0	1	1	0	0	1	0	1	0	1	1	1	0	1	0	0
	0	1	1	1	0	1	1	1	0	1	1	0	1	1	1	1	0	1	1	1	0	0	1	0	0	1	1	0	1	0	1	1
	0	0	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	1	0	0	1	0	0	1	1	0	1	1	1	1
	0	1	1	0	1	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0	0	0	1	0	0	0	0	0
	0	1	1	1	0	1	1	1	0	1	1	0	0	0	0	1	0	1	1	1	0	0	1	1	0	0	1	0	0	0	0	0
	0	1	0	0	0	1	0	0	0	1	1	0	0	1	0	1	0	1	1	1	0	1	0	0	0	1	1	0	0	1	0	1
	0	1	1	0	0	0	1	1	0	1	1	1	0	1	0	0	0	1	1	0	0	1	0	1	0	1	1	0	0	1	0	0
8	1	0	0	1	1	1	0	1	1	1	0	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	1	0	1	0	0	0
	1	1	0	0	1	0	1	1	1	0	1	0	0	0	1	0	0	0	0	1	0	0	0	1	1	1	0	1	1	0	0	1
	1	0	0	0	1	0	0	1	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0	1	0	1	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

在上一个示例中，出现以下事件信息：

编号	说明
1	此行的前两个字节表示标准报头值 `1`。接下来的两个字节表示该消息为数据消息（消息类型 4）。
2	此行表示后面的消息长度为 `92` 个字节。
3	这里的第一位是一个标志，表示该报头不是一个含有存档时间戳的扩展报头。接下来的 15 位是一个可选字段，包含在其上检测到事件的域的 Netmap ID。该行的其余部分表示记录类型值 `67`，说明这是分类记录。
4	此行表示后面的分类记录长度为 `84` 个字节。
5	此行表示分类 ID 为 `35`。
6	此行的前两个字节表示其后的分类名称长度为 `15` 个字节。接下来的两个字节开始显示分类名称自身，（在本例中为"trojan-activity"（特洛伊木马事件）。
7	此行的第一个字节是第 6 行描述的分类名称的继续。此行中接下来的两个字节表示其后的分类描述长度为 `29` 个字节。其余字节开始分类描述（在本例中为 `A Network Trojan was Detected`（检测到网络特洛伊木马））。
8	此行表示充当分类的唯一标识符的分类 ID 号码。
9	此行表示充当分类修订的唯一标识符的分类修订版本 ID 号码（空值，因为该分类没有修订）。

优先级记录示例

以下示例显示了一个优先级记录示例：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	0	0	0	0	1	1	0	1	0	0	1
	0	1	1	0	0	1	1	1	0	1	1	0	1	0	0	0																

在上一个示例中，出现以下事件信息：

编号	说明
1	此行的前两个字节表示标准报头值 1。接下来的两个字节表示该消息为数据消息（消息类型 4）。
2	此行表示后面的消息长度为 16 个字节。
3	此行表示记录类型值 4，说明这是优先级记录。
4	此行表示后面的优先级记录长度为 8 个字节。
5	此行表示优先级 ID 为 1。
6	此行的前两个字节表示优先级名称中包含四个字节。接下来的两个字节以及后面一行的两个字节显示优先级名称自身（“高”）。

规则消息记录示例

以下示例显示了一个规则记录示例：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	1
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	1	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	1	0
9	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1	1	0	1	1	0	0	0	1	1	0	1	1	1	1

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0	0	1	0	0	1	1	1	0	0	1	1	1	0	0	1	0	0	1	0	0	1	1	0	0	0	0	1	1	1	1	1
	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	1
	1	0	0	0	0	1	0	0	1	0	0	0	1	1	1	1	0	1	1	0	1	0	0	1	1	1	1	0	0	0	1	1
10	0	1	1	0	1	1	0	1	1	1	0	1	0	0	1	0	1	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1
	0	0	1	0	1	0	1	0	1	0	1	0	0	1	0	1	0	0	1	0	0	1	1	0	0	0	0	1	1	1	1	1
	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	1
	1	0	0	0	0	1	0	0	1	0	0	0	1	1	1	1	0	1	1	0	1	0	0	1	1	1	1	0	0	0	1	1
11	0	1	1	0	1	1	0	1	1	1	0	1	0	0	1	0	0	1	0	0	0	0	0	1	0	1	0	1	0	0	0	0
	0	1	0	1	0	0	0	0	0	0	1	0	1	1	0	1	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	1
	0	1	0	1	0	1	0	0	0	1	0	0	0	1	0	1	0	1	0	0	0	0	1	1	0	1	0	1	0	1	0	0
	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	1	1	1	0	0	1	0	1	0	0	1	1
	0	0	1	0	0	0	0	0	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	1	1	1	0	0	0	1
	0	1	1	1	0	1	0	1	0	1	1	0	0	1	0	1	0	1	1	1	0	0	1	1	0	1	1	1	0	1	0	0
	0	0	1	0	0	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	1	1	1	1	0	1	1	1	0	0	1	0
	0	0	1	0	0	0	0	0	0	1	1	1	0	0	0	0	0	1	1	0	1	1	1	1	0	1	1	1	0	1	0	0
	0	1	1	0	0	1	0	1	0	1	1	0	1	1	1	0	0	1	1	1	0	1	0	0	0	1	1	0	1	0	0	1
	0	1	1	0	0	0	0	0	1	0	1	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	1	1	0	1	1	0	1
	0	1	1	0	0	0	0	1	0	1	1	0	1	1	0	0	0	1	1	1	0	1	1	1	0	1	1	0	0	0	0	1
	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	1	0	1	0	0	1	1
	0	1	1	0	0	0	0	1	0	1	1	0	0	1	1	0	0	1	1	0	0	1	0	1	0	1	0	0	0	1	1	1
	0	1	1	1	0	1	0	1	0	1	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	0
	0	0	1	0	0	0	0	0	0	1	1	1	0	1	0	0	0	1	1	0	0	1	1	1	0	0	1	0	0	0	0	0
	0	1	1	0	0	1	0	0	0	1	1	0	1	1	1	1	0	1	1	0	1	1	0	1	0	1	1	0	0	0	0	1
	0	1	1	0	1	0	0	1	0	1	1	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	1
	0	0	1	1	0	1	1	0	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	0	0	1	1	0	0	0	1	1
	0	1	1	0	1	1	1	0																								

在上一个示例中，出现以下事件信息：

编号	说明
1	此行的前两个字节表示标准报头值 1。接下来的两个字节表示该消息为数据消息（也就是消息类型 4）。
2	此行表示后面的消息长度为 129 个字节。
3	这里的第一位是一个标志，表示该报头不是一个含有存档时间戳的扩展报头。接下来的 15 位是一个可选字段，包含在其上检测到事件的域的 NetmapID。该行的其余部分表示记录类型值 66，说明这是规则消息记录。
4	此行表示后面的规则消息记录长度为 121 个字节。
5	此行表示生成器标识号为 1，表示规则引擎。
6	此行表示规则标识号为 28069。
7	此行表示规则版本号为 1。
8	此行表示向 Cisco Secure Firewall 系统呈现的规则标识号为 28069。
9	此行的前两个字节表示规则文本名称中包含 71 个字节。接下来的两个字节开始显示规则的唯一标识符号码。
10	此行的前两个字节完成规则的唯一标识符号码。接下来的两个字节开始显示规则修订版的唯一标识符号码。
11	此行的前两个字节完成规则修订版的唯一标识符号码。接下来的两个字节开始显示规则消息自身的文本。传输的规则消息的完整文本为：APP-DETECT DNS request for potential malware SafeGuard to domain 360.cn（潜在恶意软件 SafeGuard 向域 360.cn 发出的 APP-DETECT DNS 请求）。

6.1.x 的连接统计数据块示例

下图显示了一个连接统计记录示例：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	1	1	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	1	1	1	0	0
5	0	1	0	1	0	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	0	1	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	1	1
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
15	1	1	0	1	0	0	0	1	1	0	0	0	0	1	0	0	1	1	1	1	1	0	1	1	0	1	0	1	0	1	1	1
16	0	0	0	0	1	0	0	0	1	0	1	1	1	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	1	1
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
21	0	1	0	1	1	0	0	1	1	1	1	0	0	1	0	0	0	1	0	1	0	0	0	0	0	1	0	1	1	1	0	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	1	0	0	1	1	0	0	0	1	0	1	1	0	1	1	1	1	1	0	0	0	1	1	1	0	1	1	1	0	1
	1	1	1	1	0	1	1	1	0	0	1	1	0	0	0	1	1	0	1	0	1	0	0	0	0	1	0	1	1	1	1	0
22	0	1	1	0	0	0	0	0	1	1	0	1	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	0	1	1	0	0	0	0	1	0	0	0	0	1	1	1	0	0	0	0	1	0	0	1	1	0	1	1	0	0	0
	1	1	0	1	0	1	1	0	1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0
23	0	1	0	1	1	0	0	1	1	0	0	1	0	0	0	1	0	0	1	0	0	1	1	0	1	1	0	1	1	1	1	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	1	0	0	1	1	0	0	0	1	0	1	1	0	1	1	1	1	1	0	0	0	1	1	1	0	1	1	1	1	1
	1	1	1	1	0	1	1	1	0	0	1	1	0	0	0	1	1	0	1	0	1	0	0	0	0	1	0	1	1	1	1	0
24	0	1	1	0	0	0	0	0	1	0	0	0	1	1	0	1	0	1	1	0	1	1	0	0	1	1	1	1	0	1	0	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	0	1	1	0	0	0	0	1	0	0	0	0	1	1	1	0	0	0	0	1	0	0	1	1	0	1	1	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	1	1	0	1	0	1	1	0	1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	1
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	1	0	0	1	0	0	0	0	0	1	1	0	0	0	0	1	0	0	1	0	1	0	1	1	1	1	1	0	1	0	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	1	0	1	0	1	1	1	1	1	1	0	1	0	0	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	0	1
29	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	1	1
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
32	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	0	1	0	1	1	0	0	0	0	1	0	1	0
33	0	0	0	0	0	0	0	1	1	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	1	1	1	0	0
36	0	1	1	1	0	0	1	1	0	1	0	1	0	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	1	0
37	0	0	1	1	0	0	1	1	0	1	0	1	0	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	1	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
38	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
39	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0
41	1	1	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
43	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
45	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
46	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
47	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
48 个	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
49	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
50	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
51	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
52	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
53	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
54	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
55	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
56	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
57	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
58	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
59	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
60	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
61	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
62	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
63	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
65	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
66	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
67	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
68	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
69	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
70	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
71	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
72	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
73	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
74	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
76	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
77	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
78	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
79	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
80	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
81	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
82	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
83	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
84	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
85	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
86	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
87	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
88	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
89	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
90	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
91	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
92	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
93	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
94	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
95	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
96	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	1	0	0	1	1	1	0	0	1	1	1	1	0	0	0	1	1	0	0	1	0	1	1	0	1	1	1	0	0	0	0
	0	1	1	1	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	1	0	1	0	0	1	1	0	0	1	1	0	1	1	1	1	0	0	1	1	0	1	1	0	1	1	0	0	0	1
97	1	0	0	1	1	1	0	0	1	0	1	1	0	1	0	1	0	1	0	1	0	0	1	1	1	1	1	1	1	1	0	1
98	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
99	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
101	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
102	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
103	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
104	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
105	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
106	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
107	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0								

在上一个示例中，出现以下事件信息：

编号	说明
1	此行的前两个字节表示标准报头值 1。接下来的两个字节表示该消息为数据消息（也就是消息类型 4）。
2	此行表示后面的消息长度为 716 个字节。
3	这里的第一位是一个标志，表示该报头是一个含有存档时间戳的扩展报头。接下来的15位是一个可选字段，包含在其上检测到事件的域的NetmapID。该行的其余部分表示记录类型值 71，说明这是连接统计记录。
4	此行表示后面的事件记录长度为 700 个字节。
5	此行是保存事件的时间戳。在本例中，其保存时间为 2016 年 10 月 10 日（星期一）08:48:52（上午）。
6	此行留作未来使用，用 0 填充。
7	此行提供生成发现事件的设备的 ID 号码。设备 ID 为 1?
8	此行用作旧版 (IPv4) IP 地址。此行的值全部为 0，因为尚未填充，而 IPv4 地址存储在 IPv6 字段中。
9	此行包含事件所涉及主机的 MAC 地址。MAC 地址为 00:00:00:00:00:00。
10	此行的前 16 位包含 MAC 地址的其余部分。接下来的 8 位是一个标志，用于指示主机是否具有 IPv6 地址。最后 8 位为空，保留以供将来使用。
11	此行包含事件发生时的 Unix 时间戳。
12	此行包含事件微秒。在本例中，此值为 0。
13	此行包含事件类型。此处的类型为 1003。
14	此行包含事件子类型。在本例中，事件子类型为 1，与事件类型 1003一致，这意味着它是连接统计事件。
15	此行用于文件编号。仅供内部使用。
16	此行用于文件位置。仅供内部使用。
17	此行包含 IPv6 地址。若设置了 Has IPv6 标志，则此字段存在且可使用。在本例中，它包含 IPv6 地址 0:3eb:0:1:d184:fb57:8ba:c00。
18	此行包含块类型。值为 163，表示连接统计数据块类型。
19	此行包含数据块的长度，表示它包含 644 字节的数据。
20	此行提供生成发现事件的设备的 ID 号码。设备 ID 为 1?
21	这包含入口安全区域。此区域为 59e4505c-4493-11e6-a62d-f1dff731a85。
22	这包含出口安全区域。区域为 60d50c80-4493-11e6-9843-84d8d6a3e008。
23	这包含入口接口。此接口为 599126de-4493-11e6-a62d-f1dff731a85e。
24	这包含出口接口。此接口为 608d6cf4-4493-11e6-9843-84d8d6a3e008。
25	此行包含发起连接事件中描述的会话的主机的 IP 地址。此 IP 地址为 172.16.3.5。
26	此行包含对发起主机作出响应的主机的 IP 地址。此 IP 地址为 72.48.149.244。
27	位于发起请求的代理后面的主机的 IP 地址。此地址在本例中为空。
28	此行包含与触发的关联事件相关的规则版本号。此版本号为 00000000-0000-0000-0000-000057e9c39d。
29	这包含触发事件的规则的内部标识符。此规则为 268439603。

编号	说明
30	此行包含触发事件的隧道规则的内部标识符。由于此事件并非由隧道规则触发，因此该值为 0。
31	此行的前两个字节包含规则指定的操作。在本例中，此值为 4，表示该操作为阻止。最后两个字节包含规则原因，在本例中为 64，表示入侵阻止。
32	前两个字节包含规则原因的其余部分。后两个字节包含发起方主机使用的端口 43786。
33	此行的前两个字节包含响应方端口 443。其余两个字节包含 TCP 标志。
34	此行的第一个字节包含协议 6，这表示此事件通过 TCP 发生。其余 24 位包含 Netflow 源 IP 地址的第一部分，即 00000000-0000-0000-0000-000000000000
35	此行的第一个字节包含 Netflow 源的最后 8 位。接下来的两个字节包含生成事件的 Snort 实例的标识符 7。剩余字节包含连接计数器。
36	此行的第一个字节包含连接计数器的剩余部分。最后 24 位包含会话中交换的第一个数据包的 Unix 时间戳开头。此时间戳为 1476103731，表示时间为 2016 年 10 月 10 日星期一上午 8:48:51。
37	第一个字节包含第一个数据包时间戳的其余部分。剩余的三个字节包含会话中要交换的最后一个数据包的时间戳，此时间戳给出的时间为 2016 年 10 月 10 日星期一上午 8:48:51，表示会话持续时间不到一秒。
38	此行的第一个字节包含最后一个数据包时间戳的最后 8 位。剩余的 24 位包含发起主机传输的数据包数量，本例中为 13。
39	此行中的第一个字节是发起方传输的数据包的其余部分。接下来的 24 位包含响应方传输的数据包数量 0。
40	此行中的第一个字节是响应方传输的数据包的其余部分。接下来的 24 位包含发起方传输的字节数 1743。
41	第一个字节是发起方传输字节的末尾，其余 24 位是响应方传输字节 0 的开头。
42	第一个字节是响应方传输字节的末尾，其余 24 位是发起方丢弃的数据包 0 的开头。
43	第一个字节是发起方丢弃的数据包的末尾，其余 24 位是响应方丢弃的数据包 0 的开头。
44	第一个字节是响应方丢弃的数据包的末尾，其余 24 位是发起方丢弃的字节 0 的开头。
45	第一个字节是发起方丢弃的字节的末尾，其余 24 位是响应方丢弃的字节 0 的开头。
46	第一个字节是响应方丢弃的字节的末尾，其余 24 位是应用了速率限制的接口名称 00000000-0000-0000-0000-000000000000 的开头。
47	此行的第一个字节是 QOS 应用接口的其余部分。其余部分是应用于连接的 QOS 规则；因为没有应用于此接口的 QoS 规则，所以 ID 为 0。
48	此行的第一个字节是 QoS 规则 ID 的其余部分。其余部分为登录生成流量的主机的最后一个用户的 ID 编号 16466。
49	此行的第一个字节是用户 ID 的其余部分。其余部分是连接中使用的应用协议的 ID 1122，此值表示连接是 HTTPS 连接。
50	此行的第一个字节是应用协议 ID 的其余部分。其余部分为 URL 类别。
51	此行的第一个字节是 URL 类别的其余部分。其余部分为 URL 信誉，即 0，表示“未知风险”。
52	此行的第一个字节是 URL 信誉的其余部分。其余部分为客户端应用 ID，即 1296，表示“SSL客户端”。

编号	说明
53	此行的第一个字节是客户端应用 ID 的其余部分。其余部分为 Web 应用 ID，即 0，表示“未知”。
54	此行的第一个字节是 Web 应用 ID 的其余部分。此行的其余部分是块类型 0 的开头，表示字符串块类型的开头。
55	此行的第一个字节是字符串块类型的其余部分。其余部分为块长度，表明客户端应用 URL 包含 8 个字节（包括报头和长度），这意味着客户端应用 URL 中没有数据。
56	此行的第一个字节是字符串块长度的其余部分。由于客户端应用 URL 中没有数据，因此，此行的其余部分为块类型 0 的开头，表示 NetBIOS 名称字符串块类型的开头。
57	此行的第一个字节是字符串块类型的其余部分。其余部分为块长度，表明 NetBIOS 名称包含 8 个字节（包括报头和长度），这意味着 NetBIOS 名称中没有数据。
58	此行的第一个字节是字符串块长度的其余部分。由于NetBIOS名称中没有数据，因此，此行的其余部分为块类型 0 的开头，表示客户端应用版本的字符串块类型的开头。
59	此行的第一个字节是字符串块类型的其余部分。其余部分为块长度，表明客户端应用版本包含 8 个字节（包括信头和长度），这意味着客户端应用版本中没有数据。
60	此行包含客户端应用版本块长度的剩余字节。最后三个字节是与连接事件关联的第一个监控规则的 ID 268439553。
61	此行包含第一个监控规则的 ID 的最后一个字节。其余三个字节是第二个监控规则的 ID，即 0。
62	此行包含第二个监控规则的 ID 的最后一个字节。其余三个字节是第三个监控规则的 ID，即 0。
63	此行包含第三个监控规则的 ID 的最后一个字节。其余三个字节是第四个监控规则的 ID，即 0。
64	此行包含第四个监控规则的 ID 的最后一个字节。其余三个字节是第五个监控规则的 ID，即 0。
65	此行包含第六个监控规则的 ID 的最后一个字节。其余三个字节是第七个监控规则的0。
66	此行包含第七个监控规则的 ID 的最后一个字节。其余三个字节是第八个监控规则的 ID，即 0。
67	此行包含第八个监控规则的 ID 的最后一个字节。此行中的第二个字节指明源或目标 IP 地址是否与 IP 阻止列表匹配。此行中的第三个字节是与 IP 阻止列表匹配的 IP 层。最后一个字节为文件事件计数 0 的开头。
68	此行的第一个字节是剩余文件事件计数。接下来的两个字节包含入侵事件计数。最后一个字节包含发起方所在国家/地区，在本例中为 0，表示“未知”。
69	此行的第一个字节是发起方所在国家/地区的第二个字节。接下来的两个字节是响应方所在国家/地区 840。最后一个字节是原始客户端所在国家/地区的开头，在本例中为 0，表示“未知”。
70	此行的第一个字节是原始客户端所在国家/地区的结尾。接下来的两个字节是 IOC 编号 0。最后一个字节是源自治系统的第一个字节，即 0。
71	此行的前三个字节是源自治系统。最后一个字节是目标自治系统的第一个字节，即 0。
72	此行的前三个字节是目标自治系统。最后一个字节是输入接口的 SNMP 索引，即 0。
73	此行的第一个字节是输入接口的 SNMP索引。接下来的两个字节是输出接口的 SNMP索引，即 0。此行中的最后一个字节是传入接口的服务类型设置 0。

编号	说明
74	此行的第一个字节是传出接口的服务类型设置 0。第二个字节是源掩码 0。第三个字节是目标掩码 0。最后一个字节是流量通过的安全背景的 ID 号码的开头。在本例中，安全背景为 00000000-0000-0000-0000-000000000000。
75	此行的前三个字节是安全背景的其余部分。最后一个字节是 VLAN ID，即 0。
76	第一个字节是 VLAN ID。最后三个字节以 0 值作为一个字符串块的开头。此字符串块包含引用的主机的名称。
77	第一个字节是字符串块类型的其余部分。最后三个字节提供字符串块的总长度，包括块类型和长度，此总长度为 8 个字节，这意味着字符串块中没有数据，因为没有引用的主机。
78	第一个字节是字符串块长度的其余部分。最后三个字节以 0 值作为一个字符串块的开头。此字符串块包含用户代理。
79	第一个字节是字符串块类型的其余部分。最后三个字节提供字符串块的总长度，包括块类型和长度，此总长度为 8 个字节，这意味着字符串块中没有数据，因为没有用户代理。
80	第一个字节是字符串块长度的其余部分。最后三个字节以 0 值作为一个字符串块的开头。此字符串块包含 HTTP 引用站点。
81	第一个字节是字符串块类型的其余部分。最后三个字节提供字符串块的总长度，包括块类型和长度，此总长度为 8 个字节，这意味着字符串块中没有数据，因为没有 HTTP 引用站点。
82	此行的第一个字节包含字符串块长度的最后部分。最后三个字节包含SSL证书指纹，即 0000000000000000000。
83	此行的第一个字节包含 SSL 证书指纹 ID 的最后部分。此行的其余部分包含 SSL 策略 ID，即 00000000-0000-0000-0000-000000000000。
84	此行的第一个字节是 SSL 策略 ID 的结尾。其余三个字节是 SSL 规则 ID，即 0。
85	此行的第一个字节是 SSL 规则 ID 的其余部分。接下来的两个字节是 SSL 密码套件，即 0，表示 TLS_NULL_WITH_NUL_NULL。最后一个字节是 SSL 版本，即 0。
86	此行包含 SSL 服务器证书状态，即 0，表示未检查。
87	此行的前两个字节是 SSL 实际操作，即 0，表示未知。接下来的两个字节是 SSL 预期操作，即 0，表示未知。
88	此行的前两个字节是 SSL 流状态，即 0，表示未知。接下来的两个字节是 SSL 流错误，即 0，表示未知。
89	此行的前两个字节是SSL流错误的其余部分。接下来的两个字节是为0的SSL流消息。
90	此行的前两个字节是 SSL 流消息。接下来的两个字节是 SSL 流标志，即 0。
91	此行的前两个字节是SSL流标志的其余部分。接下来的两个字节是SSL服务器名称的类型为 0 的字符串块开头。
92	此行的前两个字节 结束字符串块类型，接下来的两个字节包含字符串块长度。块长度为 8，这包括块类型和长度，表示字符串块不包含数据。
93	前两个字节包含字符串块长度的其余部分。接下来的两个字节包含SSLURL类别，即 0，表示未知。
94	此行的前两个字节包含 SSL URL 类别的其余部分。接下来的两个字节是 SSL 会话 ID 00000000000000000000000000000000 的开头。
95	此行的第一个字节包含 SSL 会话 ID 的结尾。下一个字节包含 SSL 会话 ID 0 的长度。接下来的两个字节是 SSL 票证0000000000000000000 的开头。

编号	说明
96	此行的第两个字节包含SSL票证ID的结尾。第三个字节包含为0的SSL票证ID长度。最后一个字节为网络分析策略修订（即 4e78cb70-7842-11e6-a99b-cdb19cb553fd）的开头。
97	此行的前三个字节包含网络分析策略修订的结尾。最后一个字节为终端配置文件ID 0的开头。
98	此行的前三个字节是终端配置文件 ID。其余字节是安全组 ID 0 的开头。
99	此行的前三个字节是安全组 ID。其余字节为位置 IPv6（即与 ISE 进行的接口通信的 IP 地址，该地址为空）的开头。
100	此行的前三个字节结束位置IPv6。其余字节为HTTP响应（即0，表示没有HTTP响应）的开头。
101	此行的前三个字节结束 HTTP 响应。其余字节为字符串块（类型为 0，表示 DNS 查询）的开头。
102	前三个字节完成字符串块类型。其余字节包含字符串块长度，此长度为 8 个字节，包括块类型和长度，这意味着 DNS 查询中没有数据。
103	前三个字节结束字符串块长度。此行中的其余字节为DNS记录类型（即 71）的开头。
104	此行中的第一个字节结束DNS记录类型。接下来的两个字节是DNS响应类型，即0。最后一个字节为 DNS TTL 的开头。
105	此行的前三个字节是DNSTTL。最后一个字节是SinkholeUUID（即 00000000-0000-0000-0000-000000000000）的开头。
106	此行的前三个字节为 Sinkhole UUID 的结尾。最后一个字节为第一个安全情报列表（即 0）的开头。
107	此行中的前三个字节为第一个安全情报列表的结尾。最后一个字节为第二个安全情报列表（即 0）的开头。

版本 5.1+ 用户事件示例

下图显示了一个用户事件记录示例：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	1
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	1
5	0	1	0	1	0	0	1	1	0	0	1	1	0	0	0	0	0	1	1	1	1	1	0	0	0	0	1	0	1	0	0	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
11	0	1	0	1	0	0	1	0	1	1	1	0	1	1	1	1	1	1	1	1	0	0	0	1	0	1	1	1	0	0	1	1
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	0	0	1	0	0	1	1	1	1
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	1	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
15	0	1	1	1	0	0	1	1	1	1	1	1	0	0	0	1	1	1	1	0	1	1	1	1	0	1	0	1	0	0	1	0
16	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	1	0	1	1	1	1	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	1
20	0	1	0	1	0	0	1	0	1	1	1	0	1	1	1	1	1	1	1	1	0	0	0	1	0	1	1	1	0	0	1	1
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
24	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	1
	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	0
	0	0	1	1	0	1	0	0	0	0	1	0	1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	1	0	0	0	1
	0	0	1	0	1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	1	0	1	1	1	0	0	1	1	0	1	0	1
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	1	0	1	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	1	0	1	1	1	1	0	0	0
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0																								

在上一个实例中，出现以下信息：

编号	说明
1	此行的前两个字节表示标准报头值 1。接下来的两个字节表示该消息为数据消息（也就是消息类型 4）。
2	此行表示后面的消息长度为 153 个字节。
3	这里的第一位是一个标志，表示该报头是一个含有存档时间戳的扩展报头。接下来的15位是一个可选字段，包含在其上检测到事件的域的NetmapID。该行的其余部分表示记录类型值95，说明这是用户信息更新消息块。
4	此行表示后面的数据长度为 137 个字节。
5	此行包含存档时间戳。因为设置了位 23，所以包含该时间戳。该时间戳为Unix 时间戳，存储为自 1/1/1970 起经过的秒数。此时间戳为 1,391,789,354，表示 2014 年 2 月 3 日，星期一，19:43:49。
6	此行全部为 0，留作未来使用。
7	此行表示检测引擎 ID 为 3。
8	此行用作旧版 (IPv4) IP 地址。此行的值全部为 0，因为尚未填充，而 IPv4 地址存储在 IPv6 字段中。
9	此行包含与事件关联的 MAC 地址。因为没有 MAC 地址，此行的值全部为 0。
10	此行的前半部分为MAC地址的剩余部分，全部为0。接下来的一个字节表示存在IPv6地址。此行的最后一个字节留作未来使用，全部为 0。
11	此行包含系统生成事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
12	此行包含系统生成事件的微秒（一秒的一百万分之一）增量。
13	此行包含事件类型。事件类型值为 1004，表示用户修改消息。
14	此行包含事件子类型。事件子类型值为 2，表示用户登录消息。
15	此行包含串行文件编号。此字段供内部使用，可以忽略。
16	此行包含串行文件中的事件位置。此字段供内部使用，可以忽略。
17	此行包含 IPv6 地址。若设置了 Has IPv6 标志，则此字段存在且可使用。但是在本例中，它包含 IPv4 地址 10.4.15.120。
18	此行可启动用户登录信息数据块，以块类型 127 表示。
19	此行表示后面的块长度为 81 个字节。
20	此行表示用户登录时间戳为 1,391,456,7，说明其生成时间为 2014 年 10 月 3 日，星期一，19:43:47 GMT（格林威治标准时间）。

编号	说明
21	此行用作旧版 (IPv4) IP 地址。此行的值全部为 0，因为尚未填充，而 IPv4 地址存储在 IPv6 字段中。
22	此行表示后面跟着一个字符串块，包含字符串块长度和文本字符串（在本例中，该文本字符串包含用户名称）。有关字符串块的详细信息，请参阅字符串数据块，第 3-59 页。
23	此行表示字符串块中数据的长度为 16 个字节。
24	此行表示用户的名称为“301@10.4.11.175”。
25	此行表示用户的 ID 号码。
26	此行表示在连接（登录信息源自此连接）中使用的应用协议的应用 ID。
27	此行表示后面跟着一个字符串块，包含字符串块长度和文本字符串（在本例中，该文本字符串包含电子邮件地址）。有关字符串块的详细信息，请参阅字符串数据块，第 3-59 页。
28	此行表示字符串块中数据的长度为 0 个字节。这是因为没有电子邮件地址与此用户关联。
29	此行包含检测到用户登录的主机的 IP 地址。
30	第一个字节包含登录类型。此行的其余部分表示后面跟着一个字符串块，包含字符串块长度和文本字符串（在本例中，该文本字符串包含报告登录的 Active Directory 的名称）。有关字符串块的详细信息，请参阅字符串数据块，第 3-59 页。
31	此行的第一个字节完成字符串数据块的启动。此行的其余部分表示字符串块中数据的长度为 0 个字节。这是因为没有 Active Directory 服务器与此登录关联。

发现数据结构示例

本节包含可能由 eStreamer 传输的发现事件的数据结构示例。提供以下示例：

新网络协议消息示例

下图说明 3.0+ 的新网络协议消息的示例：

字节	0								1								2								3								
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
报头版本	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	以事件消息 (4) 开始标准消息报头
消息长度 (49B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	
新网络协议消息 (13)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	
消息长度 (41B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	0	0	
检测引擎	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	
IP (192.168.1.10)	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	0
MAC 地址（无）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	保留的字节 (0)
Unix 秒 (1047242787)	0	0	1	1	1	1	1	0	0	1	1	0	1	0	1	1	1	0	1	0	1	0	0	0	0	0	1	0	0	0	1	1	
Unix 微秒 (973208)	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0	0	
保留的字节 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	0	事件类型 1000—新
事件子类型 4 - 新传输协议	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
文件编号	0	1	0	0	0	0	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	0	0	1	1	1	0	1	0	0	0	1	
文件位置	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	结束标准消息报头
协议 (6—TCP)	0	0	0	0	0	1	1	0																									

新 TCP 服务器消息示例

下图说明 3.0 的新 TCP 服务器消息的示例：

字节	0								1								2								3								
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
报头版本	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	以事件消息 (4) 开始标准消息报头
消息长度 (256B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	
新TCP服务消息 (11)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	
消息长度 (248B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	
检测引擎	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	
IP (192.168.1.10)	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	0	
MAC 地址（无）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	保留的字节 (0)
Unix 秒 (1047242787)	0	0	1	1	1	1	1	0	0	1	1	0	1	0	1	1	1	0	1	0	1	0	0	0	0	0	1	0	0	0	1	1	
Unix 微秒 (973208)	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0	
保留的字节 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	0	0	事件类型 1000—新
事件子类型 2 - 新主机	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	
文件编号	0	1	0	0	0	0	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	0	0	1	1	1	0	1	0	0	0	1	
文件位置	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	结束标准消息报头
服务器块报头 (12)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	开始服务器数据块
服务器长度 (208B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	
服务器端口 (80)	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	命中数 (Hits)	
命中数 (1)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块报头	
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块长度	
字符串块长度 (13B)	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	1	1	0	1	0	0	0	1	1	1	0	1	0	0		

字节	0								1								2								3								
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
服务器名称 (https)	0	1	1	1	0	1	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块报头
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块长度
字符串块长度 (15B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	0	0	0	0	0	1	
服务器供应商 (Apache + 空字节)	0	1	1	1	0	0	0	0	0	1	1	0	0	0	0	1	0	1	1	0	0	0	1	1	0	1	1	0	1	0	0	0	
	0	1	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块报头
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块长度
字符串长度（8 - 无产品）	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块报头
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块长度
字符串块长度 (22B)	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	1	1	0	0	0	1	0	0	1	0	1	1	1	0	
版本 - 1.3.26 (Unix)	0	0	1	1	0	0	1	1	0	0	1	0	1	1	1	0	0	0	1	1	0	0	1	0	0	0	1	1	0	1	1	0	
	0	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	1	0	1	0	1	0	1	1	0	1	1	1	0	
	0	1	1	0	1	0	0	1	0	1	1	1	1	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	
列表块报头 (11)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	开始子服务器列表
列表块大小 (94B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	0	
子服务器报头 (1)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	开始子服务器块
子服务器长度 (46B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	0	
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
字符串长度 (16B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		
子服务器名称 - mod_ssl	0	1	1	0	1	1	0	1	0	1	1	0	1	1	1	1	0	1	1	0	0	1	0	0	0	1	0	1	1	1	1	1		
	0	1	1	1	0	0	1	1	0	1	1	1	0	0	1	1	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0		
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
字符串块长度 (8B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	（无子类型供应商）	

字节	0								1								2								3								
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
字符串块长度 (14B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	
子服务器版本 - 2.8.9 + 空字符	0	0	1	1	0	0	1	0	0	0	1	0	1	1	1	0	0	0	1	1	1	0	0	0	0	0	1	0	1	1	1	0	结束子服务器块
	0	0	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	开始子服务器块
子服务器报头 (1)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	子服务器长度
子服务器长度 (48B)	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块报头
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块大小
字符串块大小 (16B)	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	1	1	1	1	0	1	1	1	0	0	0	0	
子服务器名称 - OpenSSL	0	1	1	0	0	1	0	1	0	1	1	0	1	1	1	0	0	1	0	1	0	0	1	1	0	1	0	1	0	0	1	1	
	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块报头
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串数据长度
字符串长度（8 - 无供应商）	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块报头
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块长度
字符串块长度 (16B)	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	0	
子服务器版本 - 0.9.6.d + 空字节	0	0	1	1	1	0	0	1	0	0	1	0	1	1	1	0	0	0	1	1	0	1	1	0	0	0	1	0	1	1	1	0	结束子服务器块
	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	置信度 %
置信度 % (100)	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	1	1	上次使用时间
首次使用时间 (1047242787)	1	0	1	0	1	0	0	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Blob 数据块
Blob 数据块 (10)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Blob 数据长度
Blob 数据长度 (22B)	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	1	0	0	1	0	0	0	0	1	0	1	0	1	0	0	

字节	0								1								2								3								
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
服务器横幅（HTTP/1.1 414 请求）- 服务器横幅缩短以便用于示例，通常为 256B。	0	1	0	1	0	1	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	1	1	1	0	0	1	1	0	0	0	1	
	0	0	1	0	1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	1	1	0	1	0	0
	0	0	1	1	0	0	0	1	0	0	1	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	0	0	1	0
	0	1	1	0	0	1	0	1	0	1	1	1	0	0	0	1	0	1	1	1	0	1	0	1	0	1	1	0	0	1	0	1	结束服务器数据块

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。