Data Structure Examples

This appendix contains data structure examples for selected intrusion, correlation, and discovery events. Each example is displayed in binary format to clearly display how each bit is set.

See the following sections for more information:

- Intrusion Event Data Structure Examples
- Discovery Data Structure Examples, page A-17

Intrusion Event Data Structure Examples

This section contains examples of data structures that may be transmitted by eStreamer for intrusion events. The following examples are provided:

- Example of an Intrusion Event for the Management Center 5.4+, page A-1
- Example of an Intrusion Impact Alert, page A-6
- Example of a Packet Record, page A-8
- Example of a Classification Record, page A-9
- Example of a Priority Record, page A-11
- Example of a Rule Message Record, page A-12
- Example of a Version 5.1+ User Event, page A-14

Example of an Intrusion Event for the Management Center 5.4+

The following diagram shows an example event record:

Byte	0								1								2								3							
Bit	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

Byte	0								1								2								3							
Bit	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	0	1	0	1
10	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	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	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	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

Byte	0								1								2								3							
Bit	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
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
	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

Byte	0								1								2								3							
Bit	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	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
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																

In the preceding example, the following event information appears:

Number	Description
1	The first two bytes of this line indicate the standard header value of `1`. The second two bytes indicate that the message is a data message (that is, message type four).
2	This line indicates that the message that follows is `294` bytes long.

Number	Description
3	The first bit of this is a flag indicating that the header is an extended header containing an archive timestamp. The next 15 bits are an optional field containing the Netmap ID for the domain on which the event was detected. The remainder of the line indicates a record type value of `400`, which represents an intrusion event record.
4	This line indicates that the event record that follows is `278` bytes long.
5	This line is the timestamp when the event was saved. In this case, it was saved on Wednesday, July 2, 2014 at 16:11:27.
6	This line is reserved for future use and is populated with zeros.
7	This line indicates that the block type is `45`, which is the block type for Intrusion Event records for version 5.4+.
8	This line indicates that the data block is `278` bytes long.
9	This line indicates that the event is collected from sensor number `5`.
10	This line indicates that the event identification number is `65580`.
11	This line indicates that the event occurred at second `1404317489`.
12	This line indicates that the event occurred at microsecond `46542`.
13	This line indicates that the rule ID number is `4`.
14	This line indicates that the event was detected by generator ID number `119`, the rules engine.
15	This line indicates that the rule revision number is `1`.
16	This line indicates that the classification identification number is `1`.
17	This line indicates that the priority identification number is `3`.
18	This line indicates that the source IP address is `10.5.61.220`. Note that this field can contain either IPv4 or IPv6 addresses.
19	This line indicates that the destination IP address is `10.5.56.133`. Note that this field can contain either IPv4 or IPv6 addresses.
20	The first two bytes in this line indicate that the source port number is `33018`, and the second two bytes indicate that the destination port number is `8080`.
21	This first byte in this line indicates that TCP (`6`) is the protocol used in the event. The second byte is the impact flag, which indicates that the event is red (vulnerable) since the second bit is `1`; that the source or destination host is in a network monitored by the system, the source or destination host exists in the network map, and that the source or destination host is running a server on the port in the event; because the second and third flags are one, this is an orange event which is potentially vulnerable. The third byte in this line is the impact, which is 2 indicating that the event is orange and potentially vulnerable. The last byte indicates that the event was not blocked.
22	This line contains the MPLS label, if present.
23	The first two bytes in this line indicate that the VLAN ID is `0`. The last two bytes are reserved and set to `0`.
24	This line contains the unique ID number for the intrusion policy.
25	This line contains the internal identification number for the user. Since there is no applicable user, it is all zeros.
26	This line contains the internal identification number for the web application, which is `847`.

Number	Description
27	This line contains the internal identification number for the client application, which is `2000000676`.
28	This line contains the internal identification number for the application protocol, which is `676`.
29	This line contains the unique identifier for the access control rule, which is `1`.
30	This line contains the unique identifier for the access control policy.
31	This line contains the unique identifier for the ingress interface.
32	This line contains unique identifier for the egress interface. Since this event was blocked.
33	This line contains the unique identifier for the ingress security zone.
34	This line contains the unique identifier for the egress security zone.
35	This line contains the Unix timestamp of the connection event associated with the intrusion event.
36	The first two bytes in this line indicate the numerical ID of the Snort instance on the managed device that generated the connection event. The remaining two bytes indicate the value used to distinguish between connection events that happen during the same second.
37	The first two bytes in this line indicate the code for the country of the source host. The remaining two bytes indicate the code for the country of the destination host.
38	The first two bytes of this line contain the ID number of the compromise associated with this event. The remaining two bytes contain the beginning of the ID number for the security context (virtual firewall) that the traffic passed through.
39	This line contains the rest of the ID number for the security context (virtual firewall) that the traffic passed through.
40	The first two bytes of this line contain the last two bytes of the security context (virtual firewall) that the traffic passed through. The second two bytes contain the beginning of the SHA1 Hash of the SSL Server certificate if SSL was used.
41	This line contains the rest of the SHA1 Hash of the SSL Server certificate if SSL was used.
42	The first two bytes of this line contain the last two bytes of the SHA1 Hash of the SSL Server certificate. The second two bytes contain the SSL Action which was actually taken. Since SSL was not used in this connection, this is `0`.
43	The first two bytes of this line contain the SSL Flow Status. Since SSL was not used in this connection, this is `0`. The second two bytes contain the first two bytes of the UUID of the Network Analysis Policy associated with this event.
44	This line contains the rest of the UUID of the Network Analysis Policy associated with this event.

Example of an Intrusion Impact Alert

The following diagram shows an example intrusion impact alert record:

Byte	0								1								2								3							
Bit	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	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
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
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																

In the preceding example, the following information appears:

Number	Description
1	The first two bytes of this line indicate the standard header value of `1`. The second two bytes indicate that the message is a data message (message type four).
2	This line indicates that the message that follows is `58` bytes long.
3	The first bit of this is a flag indicating that the header is not an extended header containing an archive timestamp. The next 15 bits are an optional field containing the Netmap ID for the domain on which the event was detected. The remainder of the line indicates a record type value of `9`, which represents an intrusion impact alert record.
4	This line indicates that the data that follows is `50` bytes long.
5	This line contains a value of `20`, indicating that an intrusion impact alert data block follows.

Number	Description
6	This line indicates that the length of the impact alert block, including the impact alert block header, is `50` bytes.
7	This line indicates that the event identification number is `201256`.
8	This line indicates that the event is collected from device number `2`.
9	This line indicates that the event occurred at second `1087223700`.
10	This line indicates that `1` (red, vulnerable) is the impact level associated with the event.
11	This line indicates that the IP address associated with the violation event is `172.16.1.22`.
12	This line indicates that there is no destination IP address associated with the violation (values are set to `0`).
13	This line indicates that a string block follows, containing a string block length and a text string which, in this case, contains the impact name. For more information about string blocks, see String Data Block, page 3-58.
14	This line indicates that the total length of the string block, including the string block indicator and length is `18` bytes. This includes 10 bytes for the impact description and 8 bytes for the string header.
15	This line indicates that the description of the impact is “Vulnerable.”

Example of a Packet Record

The following diagram shows an example packet record:

Byte	0								1								2								3							
Bit	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

Byte	0								1								2								3							
Bit	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
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

In the preceding example, the following packet information appears:

Number	Description
1	The first two bytes of this line indicate the standard header value of `1`. The second two bytes indicate that the message is a data message (message type four).
2	This line indicates that the message that follows is `989` bytes long.
3	The first bit of this is a flag indicating that the header is not an extended header containing an archive timestamp. The next 15 bits are an optional field containing the Netmap ID for the domain on which the event was detected. The remainder of the line indicates a record type value of `2`, which represents a packet record.
4	This line indicates that the packet record that follows is `981` bytes long.
5	This line indicates that the event is collected from device number `3`.
6	This line indicates that the event identification number is `195430`.
7	This line indicates that the event occurred at second `10572378`.
8	This line indicates that the packet was collected at second `10572380`.
9	This line indicates that the packet was collected at microsecond `254365`.
10	This line indicates that the link type is `1` (Ethernet layer).
11	This line indicates that the packet data that follows is `953` bytes long.
12	This line and the following line show the actual payload data. Note that the actual data is `953` bytes and has been truncated for the sake of this example.

Example of a Classification Record

The following diagram shows an example classification record:

Byte	0								1								2								3							
Bit	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

Byte	0								1								2								3							
Bit	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	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	1	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
	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

In the preceding example, the following event information appears:

Number	Description
1	The first two bytes of the line indicate the standard header value of `1`. The second two bytes indicate that the message is a data message (message type four).
2	This line indicates that the message that follows is `92` bytes long.
3	The first bit of this is a flag indicating that the header is not an extended header containing an archive timestamp. The next 15 bits are an optional field containing the Netmap ID for the domain on which the event was detected. The remainder of the line indicates a record type value of `67`, which represents a classification record.
4	This line indicates that the classification record that follows is `84` bytes long.
5	This line indicates that the Classification ID is `35`.
6	The first two bytes of this line indicate that the classification name that follows it is `15` bytes long. The second two bytes begin the classification name itself, which, in this case, is “trojan-activity”.
7	The first byte in this line is a continuation of the classification name described in line 6. The next two bytes in this line indicate that the classification description that follows it is `29` bytes long. The remaining byte begins the classification description, which, in this case, is `“A Network Trojan was Detected.”`
8	This line indicates the classification ID number that acts as a unique identifier for the classification.
9	This line indicates the classification revision ID number that acts as a unique identifier for the classification revision, which is null because there are no revisions to the classification.

Example of a Priority Record

The following example shows a sample priority record:

Byte	0								1								2								3							
Bit	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	0	1	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
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
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	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																

In the preceding example, the following event information appears:

Number	Description
1	The first two bytes in this line indicate the standard header value of `1`. The second two bytes indicate that the message is a data message (message type four).
2	This line indicates that the message that follows is `16` bytes.
3	This line indicates a record type value of `4`, which represents a priority record.
4	This line indicates that the priority record that follows is `8` bytes long.
5	This line indicates that the priority ID is one.
6	The first two bytes of this line indicate that there are four bytes included in the priority name. The second two bytes plus the two bytes on the following line show the priority name itself (“high”).

Example of a Rule Message Record

The following example shows a sample rule record:

Byte	0								1								2								3							
Bit	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	1	1	0	1	1	0	1	1	0	1	0	0	1	0	1
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	1	1	0	1	1	0	1	1	0	1	0	0	1	0	1
9	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1	1	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1
	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	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

Byte	0								1								2								3							
Bit	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	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	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	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																								

In the preceding example, the following event information appears:

Number	Description
1	The first two bytes of this line indicate the standard header value of `1`. The second two bytes indicate that the message is a data message (that is, message type four).
2	This line indicates that the message that follows is `129` bytes.

Number	Description
3	The first bit of this is a flag indicating that the header is not an extended header containing an archive timestamp. The next 15 bits are an optional field containing the Netmap ID for the domain on which the event was detected. The remainder of the line indicates a record type value of `66`, which represents a rule message record.
4	This line indicates that the rule message record that follows is `121` bytes long.
5	This line indicates that the generator identification number is `1`, the rules engine.
6	This line indicates that the rule identification number is `28069`.
7	This line indicates that the rule revision number is `1`.
8	This line indicates that the rule identification number rendered to the Firepower System is `28069`.
9	The first two bytes of this line indicate that there are `71` bytes included in the rule text name. The second two bytes begin the unique identifier number for the rule.
10	The first two bytes of this line finish the unique identifier number of the rule. The next two bytes begin the unique identifier number for the revision of the rule.
11	The first two bytes of this line finish the unique identifier number for the revision of the rule. The second two bytes begin the text of the rule message itself. The full text of the transmitted rule message is: `APP-DETECT DNS request for potential malware SafeGuard to domain 360.cn`.

Example of a Version 5.1+ User Event

The following diagram shows an example user event record:

Byte	0								1								2								3							
Bit	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	0	1	0	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
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

Byte	0								1								2								3							
Bit	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
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	0	1	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	1	1	1	1	0	1	1	1	1	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	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	0	1	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	0	1	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

Byte	0								1								2								3							
Bit	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	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
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																								

In the preceding example, the following information appears:

Number	Description
1	The first two bytes of this line indicate the standard header value of `1`. The second two bytes indicate that the message is a data message (that is, message type four).
2	This line indicates that the message that follows is `153` bytes long.
3	The first bit of this is a flag indicating that the header is an extended header containing an archive timestamp. The next 15 bits are an optional field containing the Netmap ID for the domain on which the event was detected. The remainder of the line indicates a record type value of `95`, which represents a user information update message block.
4	This line indicates that the data that follows is `137` bytes long.
5	This line contains the archive timestamp. It is included since bit 23 was set. The timestamp is a Unix timestamp, stored as seconds since 1/1/1970. This time stamp is `1,391,789,354`, which is Mon Feb 3 19:43:49 2014.
6	This line contains zeros and is reserved for future use.
7	This line indicates that the detection engine ID is `3`.
8	This line is for the legacy (IPv4) IP address. It contains all zeros as it is not populated and the IPv4 address is stored in the IPv6 field.
9	This line contains the MAC address associated with the event. As there is no MAC address, it contains zeros.
10	The first half of this line is the remainder of the MAC address, which is zeros. The next byte indicates the presence of an IPv6 address. The last byte in this line is reserved for future use and contains zeros.
11	This line contains the UNIX timestamp (seconds since 01/01/1970) that the system generated the event.
12	This line contains the microsecond (one millionth of a second) increment that the system generated the event.
13	This line contains the event type. This has a value of `1004`, which indicates a user modification message.
14	This line contains the event subtype. This has a value of `2`, which indicates a user login event.

Number	Description
15	This line contains the serial file number. This field is for internal use and can be disregarded.
16	This line contains the event's position in the serial file. This field is for internal use and can be disregarded.
17	This line contains the IPv6 address. This field is present and used if the Has IPv6 flag is set. In this case, however, it contains the IPv4 address `10.4.15.120`.
18	This line initiates a User Login Information data block, indicated by block type `127`.
19	This line indicates that the block that follows is `81` bytes long.
20	This line indicates that the user login timestamp is `1,391,456,7`, which means it was generated at Mon, 03 Oct 2014 19:43:47 GMT.
21	This line is for the legacy (IPv4) IP address. It contains all zeros as it is not populated and the IPv4 address is stored in the IPv6 field.
22	This line indicates that a string block follows, containing a string block length and a text string which, in this case, contains the user name. For more information about string blocks, see String Data Block, page 3-58.
23	This line indicates that the length of the data in the string block is `16` bytes.
24	This line indicates that the name of the user is "`301@10.4.11.175`."
25	The line indicates the ID number of the user.
26	This line indicates the application ID for the application protocol used in the connection that the login information was derived from.
27	This line indicates that a string block follows, containing a string block length and a text string which, in this case, contains the email address. For more information about string blocks, see String Data Block, page 3-58.
28	This line indicates that the length of the data in the string block is `0` bytes. This is because there is no email address associated with this user.
29	This line contains IP address from the host where the user was detected logging in.
30	The first bye contains the login type. The remainder of this line indicates that a string block follows, containing a string block length and a text string which, in this case, contains the name of the Active Directory server reporting a login. For more information about string blocks, see String Data Block, page 3-58.
31	The first byte of this line completes the initiation of the string data block.This remainder of this line indicates that the length of the data in the string block is `0` bytes. This is because there is no Active Directory server associated with this login.

Discovery Data Structure Examples

This section contains examples of data structures that may be transmitted by eStreamer for discovery events. The following examples are provided:

- Example of a New Network Protocol Message, page A-18
- Example of a New TCP Server Message, page A-19

Example of a New Network Protocol Message

The following diagram illustrates a sample new network protocol message for 3.0+:

Byte	0								1								2								3								
Bit	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	
Header Version 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	Start Standard Message Header with Event Msg (4)
Message Length (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	
New NW Protocol Msg (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	
Msg Length 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	
Detection Engine ID (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	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 Address (none)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Reserved Bytes (0)
Unix Sec (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 MSec (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	
Reserved Bytes (0)	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	Event Type 1000—New
EventSub 4-New Trans Prot	0	0	0	0	0	0	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	
File Number	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	
File Position	0	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	End Standard Message Header
Protocol (6—TCP)	0	0	0	0	0	1	1	0																									

Example of a New TCP Server Message

The following diagram illustrates a sample new TCP server message for 3.0:

Byte	0								1								2								3								
Bit	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	
Header Version 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	Start Standard Message Header with Event Msg (4)
Message Length (256B)	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	
New TCP Svc Msg (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	
Msg Length (248B)	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		
Detection Engine ID (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	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	1	0	0	0	0	1	0	1	0	
MAC Address (none)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Reserved Bytes (0)
Unix Sec (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 MSec (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	
Reserved Bytes (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	Event Type 1000—New
Event Subtype 2 -New Host	0	0	0	0	0	0	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	
File Number	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	
File Position	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	0	End Standard Message Header
Server Block Header (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	Start Server Data Block

Byte	0								1								2								3								
Bit	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	
Server Length (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	1	1	0	1	0	0	0	0	
Server Port (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	Hits
Hits (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	String Block Header
String Block Header (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	String Block Length
String Block Length (13B)	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	1	1	0	1	0	0	0	0	1	1	1	0	1	0	0	
Server Name (`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	String Block Header
String Block Header (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	String Block Length
String Block Length (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	
Server Vendor (`Apache` + null byte)	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	String Block Header
String Block Header (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	String Block Length
String Length (8-no product)	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	String Block Header
String Block Header (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	String Block Length
String Block Length (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	
Version - 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	
List Block Header (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	Start Sub-server List
List Block Size (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	1	0	1	1	1	1	0	

Byte	0								1								2								3								
Bit	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	
Sub-server Hdr (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	1	Start Sub-server Block
Sub-server Len (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	1	0	1	1	1	0	
String Block Header (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
String Length (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	1	0	0	0	0	
Sub-server Name - 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	0	1	1	0	0	0	0	0	0	0	0	0	0	
String Block Header (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
String Block Len (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	(No subtype vendor)
String Block Header (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
String Block Length (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	
Sub-server Version - 2.8.9 + null character	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	End Sub-server Block
	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	Start Sub-server Block
Sub-server Hdr (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	Sub-server Length
Sub-server Length (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	String Block Header
String Block Header (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	String Block Size
String Block Size (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	
Sub-server Name - 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	String Block Header

Byte	0								1								2								3								
Bit	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	
String Block Header (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	String Data Length
String Length (8-no vendor)	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	String Block Header
String Block Hdr (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	String Block Length
String Block Len (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	
Sub-server Version - 0.9.6.d + null byte	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	End Sub-server Block
	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	Confidence %
Confidence % (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	Last used
Last Used (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 Data Block
Blob Data Block (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 Data Length
Blob Data Length (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	
Server Banner (HTTP/1.1 414 Reque) -Server banner shortened for example, typically 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	End Server Data Block