eve.json

```
tiago-paquete@Linux:~$ sudo cat /var/log/suricata/eve.json
```


```
{
  // === Top-level metadata ===
  "timestamp": "2025-05-06T09:57:44.249318+0200", // When this stats snapshot was taken
  "event_type": "stats",                          // Type of log entry ("stats" = performance metrics)

  "stats": {
    // === General ===
    "uptime": 31, // Uptime in seconds since Suricata started

    // === Capture statistics ===
    "capture": {
      "kernel_packets": 730, // Total packets received from kernel
      "kernel_drops": 0,     // Packets dropped before Suricata processed them
      "errors": 0,           // General errors in packet capture
      "afpacket": {
        "busy_loop_avg": 0,
        "polls": 1370,       // Number of polling attempts to read packets
        "poll_signal": 0,
        "poll_timeout": 629,  // Times poll timed out waiting for packets
        "poll_data": 741,     // Times data was successfully received
        "poll_errors": 0,
        "send_errors": 0
      }
    },

    // === Decoder statistics (packet parsing) ===
    "decoder": {
      "pkts": 755,         // Total packets decoded
      "bytes": 67938,      // Total bytes processed
      "invalid": 0,        // Invalid packets
      "ipv4": 755,         // IPv4 packets
      "ipv6": 0,           // IPv6 packets
      "ethernet": 755,     // Ethernet-level packets
      "arp": 0,
      "unknown_ethertype": 0,
      "chdlc": 0,
      "raw": 0,
      "null": 0,
      "sll": 0,
      "tcp": 755,          // TCP packets
      "udp": 0,            // UDP packets
      "sctp": 0,
      "esp": 0,
      "icmpv4": 0,
      "icmpv6": 0,
      "ppp": 0,
      "pppoe": 0,
      "geneve": 0,
      "gre": 0,
      "vlan": 0,
      "vlan_qinq": 0,
      "vlan_qinqinq": 0,
      "vxlan": 0,
```

```
"vntag": 0,
"ieee8021ah": 0,
"teredo": 0,
"ipv4_in_ipv6": 0,
"ipv6_in_ipv6": 0,
"mpls": 0,
"avg_pkt_size": 89,     // Average packet size
"max_pkt_size": 102,    // Largest packet seen
"max_mac_addrs_src": 0,
"max_mac_addrs_dst": 0,
"erspan": 0,
"nsh": 0,

// === Decoder Errors (by protocol) ===
"event": {
 // -- IPv4 decoding errors --
 "ipv4": {
  "pkt_too_small": 0,
  "hlen_too_small": 0,
  "iplen_smaller_than_hlen": 0,
  "trunc_pkt": 0,
  "opt_invalid": 0,
  "opt_invalid_len": 0,
  "opt_malformed": 0,
  "opt_pad_required": 0,
  "opt_eol_required": 0,
  "opt_duplicate": 0,
  "opt_unknown": 0,
  "wrong_ip_version": 0,
  "icmpv6": 0,
  "frag_pkt_too_large": 0,
  "frag_overlap": 0,
  "frag_ignored": 0
 },

 // -- ICMPv4 decoding errors --
 "icmpv4": {
  "pkt_too_small": 0,
  "unknown_type": 0,
  "unknown_code": 0,
  "ipv4_trunc_pkt": 0,
  "ipv4_unknown_ver": 0
 },

 // -- ICMPv6 decoding errors --
 "icmpv6": {
  "unknown_type": 0,
  "unknown_code": 0,
  "pkt_too_small": 0,
  "ipv6_unknown_version": 0,
  "ipv6_trunc_pkt": 0,
  "mld_message_with_invalid_hl": 0,
  "unassigned_type": 0,
  "experimentation_type": 0
 },

 // -- IPv6 decoding errors --
 "ipv6": {
  "pkt_too_small": 0,
  "trunc_pkt": 0,
```

```
  "trunc_exthdr": 0,
  "exthdr_dupl_fh": 0,
  "exthdr_useless_fh": 0,
  "exthdr_dupl_rh": 0,
  "exthdr_dupl_hh": 0,
  "exthdr_dupl_dh": 0,
  "exthdr_dupl_ah": 0,
  "exthdr_dupl_eh": 0,
  "exthdr_invalid_optlen": 0,
  "wrong_ip_version": 0,
  "exthdr_ah_res_not_null": 0,
  "hopopts_unknown_opt": 0,
  "hopopts_only_padding": 0,
  "dstopts_unknown_opt": 0,
  "dstopts_only_padding": 0,
  "rh_type_0": 0,
  "zero_len_padn": 0,
  "fh_non_zero_reserved_field": 0,
  "data_after_none_header": 0,
  "unknown_next_header": 0,
  "icmpv4": 0,
  "frag_pkt_too_large": 0,
  "frag_overlap": 0,
  "frag_invalid_length": 0,
  "frag_ignored": 0,
  "ipv4_in_ipv6_too_small": 0,
  "ipv4_in_ipv6_wrong_version": 0,
  "ipv6_in_ipv6_too_small": 0,
  "ipv6_in_ipv6_wrong_version": 0
},

// -- TCP decoding errors --
"tcp": {
  "pkt_too_small": 0,
  "hlen_too_small": 0,
  "invalid_optlen": 0,
  "opt_invalid_len": 0,
  "opt_duplicate": 0
},

// -- UDP decoding errors --
"udp": {
  "pkt_too_small": 0,
  "hlen_too_small": 0,
  "hlen_invalid": 0,
  "len_invalid": 0
},

// -- Other link-layer and tunnel errors --
"sll": { "pkt_too_small": 0 },
"ethernet": { "pkt_too_small": 0 },
"ppp": {
  "pkt_too_small": 0,
  "vju_pkt_too_small": 0,
  "ip4_pkt_too_small": 0,
  "ip6_pkt_too_small": 0,
  "wrong_type": 0,
  "unsup_proto": 0
},
"pppoe": {
```

```
  "pkt_too_small": 0,
  "wrong_code": 0,
  "malformed_tags": 0
},
"gre": {
  "pkt_too_small": 0,
  "wrong_version": 0,
  "version0_recur": 0,
  "version0_flags": 0,
  "version0_hdr_too_big": 0,
  "version0_malformed_sre_hdr": 0,
  "version1_chksum": 0,
  "version1_route": 0,
  "version1_ssr": 0,
  "version1_recur": 0,
  "version1_flags": 0,
  "version1_no_key": 0,
  "version1_wrong_protocol": 0,
  "version1_malformed_sre_hdr": 0,
  "version1_hdr_too_big": 0
},
"vlan": {
  "header_too_small": 0,
  "unknown_type": 0,
  "too_many_layers": 0
},
"ieee8021ah": { "header_too_small": 0 },
"vntag": {
  "header_too_small": 0,
  "unknown_type": 0
},
"ipraw": { "invalid_ip_version": 0 },
"ltnull": {
  "pkt_too_small": 0,
  "unsupported_type": 0
},
"sctp": { "pkt_too_small": 0 },
"esp": { "pkt_too_small": 0 },
"mpls": {
  "header_too_small": 0,
  "pkt_too_small": 0,
  "bad_label_router_alert": 0,
  "bad_label_implicit_null": 0,
  "bad_label_reserved": 0,
  "unknown_payload_type": 0
},
"vxlan": { "unknown_payload_type": 0 },
"geneve": { "unknown_payload_type": 0 },
"erspan": {
  "header_too_small": 0,
  "unsupported_version": 0,
  "too_many_vlan_layers": 0
},
"dce": { "pkt_too_small": 0 },
"chdlc": { "pkt_too_small": 0 },
"nsh": {
  "header_too_small": 0,
  "unsupported_version": 0,
  "bad_header_length": 0,
  "reserved_type": 0,
```

```
        "unsupported_type": 0,
        "unknown_payload": 0
      }
    },

    // === General decoding state ===
    "too_many_layers": 0 // Indicates if packets had too many nested protocol layers
  }

  // (continued: TCP, Flow, Detect, etc.)
 }
}
```

Top-Level Fields

timestamp
- **Description:** When this stats snapshot was taken.
- **Use Case:** Correlate with other logs or alert events for timeline analysis.

event_type: "stats"
- **Description:** Indicates this log is a performance statistics report.
- **Use Case:** Filters stats logs in dashboards or scripts; distinguishes from alert or flow events.

General Engine Status

uptime
- **Description:** Number of seconds Suricata has been running since the last restart.
- **Use Case:** Detect restarts or service interruptions; useful for uptime monitoring and forensic timelines.

Capture Section

kernel_packets
- **Description:** Number of packets received from the kernel.
- **Use Case:** Measures Suricata's workload. Helps assess whether the traffic load is growing or stable.

kernel_drops
- **Description:** Packets dropped before Suricata could inspect them.
- **Use Case:** Critical performance indicator. Persistent drops may require tuning buffer sizes, offloading settings, or upgrading hardware.

errors
- **Description:** General packet capture errors.
- **Use Case:** Non-zero values could indicate interface misconfiguration or driver issues.

afpacket.polls / poll_data / poll_timeout
- Description:
  - `polls`: Number of times Suricata asked for packets.
  - `poll_data`: How often that polling returned actual packets.
  - `poll_timeout`: Polling returned no data (idle traffic or inefficient polling).
- **Use Case:** Helps diagnose polling inefficiencies or underutilized sensors. High timeouts with low data may mean a misconfigured capture interface.

Decoder Section

`pkts` and `bytes`
- **Description:** Total packets and bytes successfully decoded.
- **Use Case:** Useful for calculating throughput, bandwidth trends, or diagnosing sensor overload.

invalid
- **Description:** Number of packets that failed to decode.
- **Use Case:** Should generally be zero. A non-zero count may indicate malformed traffic, interface errors, or attack traffic.

Protocol Fields (`ipv4`, `ipv6`, `tcp`, `udp`)
- **Description:** Count of packets by protocol.

- **Use Case:** Identifies dominant traffic types. Sudden changes may indicate anomalies (e.g., UDP floods, IPv6 tunnels).

avg_pkt_size, max_pkt_size
- **Description:** Average and maximum size of observed packets.
- **Use Case:** Large packet sizes may indicate file transfers. Small sizes with high packet count can suggest scanning activity or denial-of-service behavior.

Decoder Event Errors

These are protocol-specific decoding error counters under `“event"`.

IPv4 Error Fields (e.g., `pkt_too_small`, `opt_invalid`)
- **Description:** Errors encountered when parsing IPv4 packets.
- **Use Case:** High counts can signal malformed or intentionally evasive traffic.

ICMPv4 / ICMPv6 Error Fields
- **Description:** Decoding errors related to ping and control message types.
- **Use Case:** May reveal network mapping, tunneling activity, or malformed packets used in reconnaissance.

IPv6 Error Fields
- **Description:** Extension header and fragmentation errors.
- **Use Case:** Crucial in IPv6-enabled environments. Can help detect evasion techniques using deeply nested extension headers or fragmented payloads.

TCP / UDP Error Fields
- **Description:** Errors in parsing TCP/UDP headers and options.
- **Use Case:** Important for detecting malformed scans, corrupted streams, or fuzzing tools.

Tunnel and Link-Layer Error Fields (e.g., `gre`, `mpls`, `pppoe`)
- **Description:** Indicates issues in parsing encapsulated or virtual network traffic.
- **Use Case:** Relevant in cloud environments and VPN traffic. Errors may point to configuration problems or tunneling-based evasion attempts.

General Parsing Indicator

too_many_layers
- **Description:** Suricata encountered packets with more protocol layers than it is configured to handle.

- **Use Case:** May indicate tunneling, VPN misuse, or layered evasion tactics. Can also mean packet inspection depth needs to be increased.

Summary: When to Monitor Specific Fields

Field / Group	Monitor For	Reason or Action
`kernel_drops`	Non-zero values	Packet loss; investigate buffer tuning or performance bottlenecks
`invalid`, `event.*`	Anything above zero	Malformed packets, possible evasion or scanning
`tcp`, `udp`, `ipv6`	Unexpected spikes	Change in service usage or attack traffic
`avg_pkt_size`drops	Low average with many TCP packets	Potential scan or SYN flood
`too_many_layers`	Repeated high values	Deep tunneling, evasion, or configuration limits