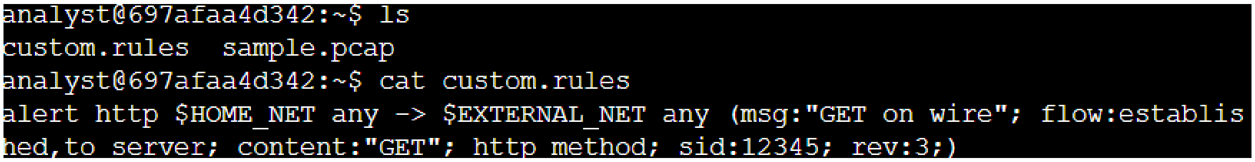
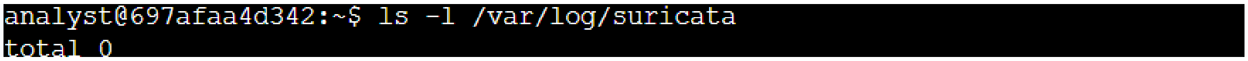
Google Cybersecurity Cert Suricata Logs Lab:

Look at the custom rules in Suricata:



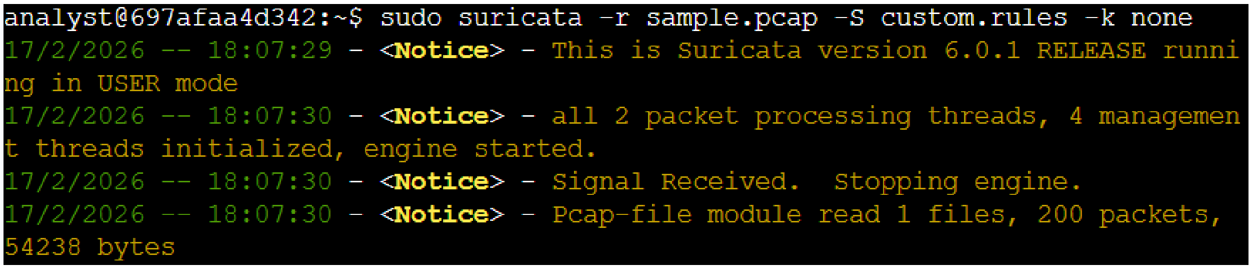
```
analyst@697afaa4d342:~$ ls
custom.rules  sample.pcap
analyst@697afaa4d342:~$ cat custom.rules
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"GET on wire"; flow:establis
hed,to_server; content:"GET"; http_method; sid:12345; rev:3;)
```

See if there are any logs in Suricata:



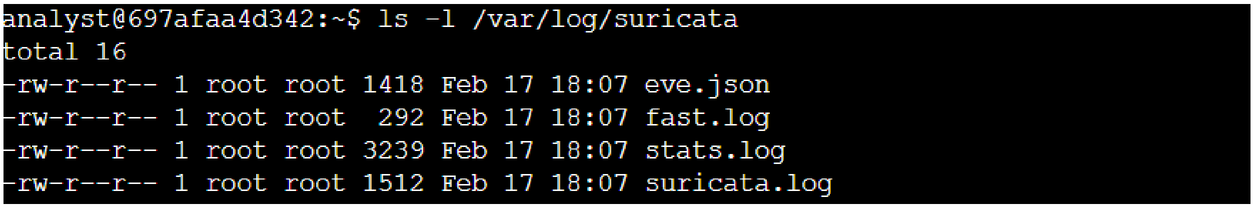
```
analyst@697afaa4d342:~$ ls -l /var/log/suricata
total 0
```

Run Suricata using the provided sample.pcap and custom.rules files:



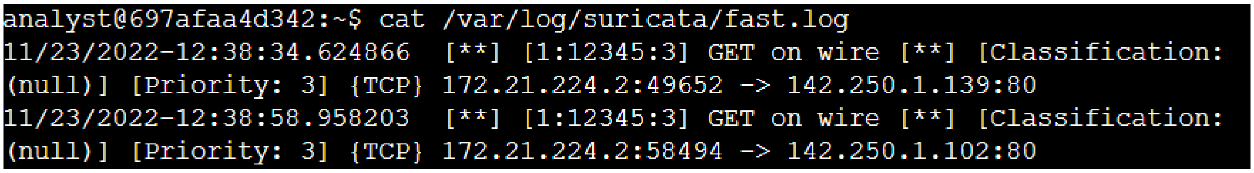
```
analyst@697afaa4d342:~$ sudo suricata -r sample.pcap -S custom.rules -k none
17/2/2026 -- 18:07:29 - <Notice> - This is Suricata version 6.0.1 RELEASE runni
ng in USER mode
17/2/2026 -- 18:07:30 - <Notice> - all 2 packet processing threads, 4 managemen
t threads initialized, engine started.
17/2/2026 -- 18:07:30 - <Notice> - Signal Received.  Stopping engine.
17/2/2026 -- 18:07:30 - <Notice> - Pcap-file module read 1 files, 200 packets,
54238 bytes
```

See what logs are in Suricata:



```
analyst@697afaa4d342:~$ ls -l /var/log/suricata
total 16
-rw-r--r-- 1 root root 1418 Feb 17 18:07 eve.json
-rw-r--r-- 1 root root  292 Feb 17 18:07 fast.log
-rw-r--r-- 1 root root 3239 Feb 17 18:07 stats.log
-rw-r--r-- 1 root root 1512 Feb 17 18:07 suricata.log
```

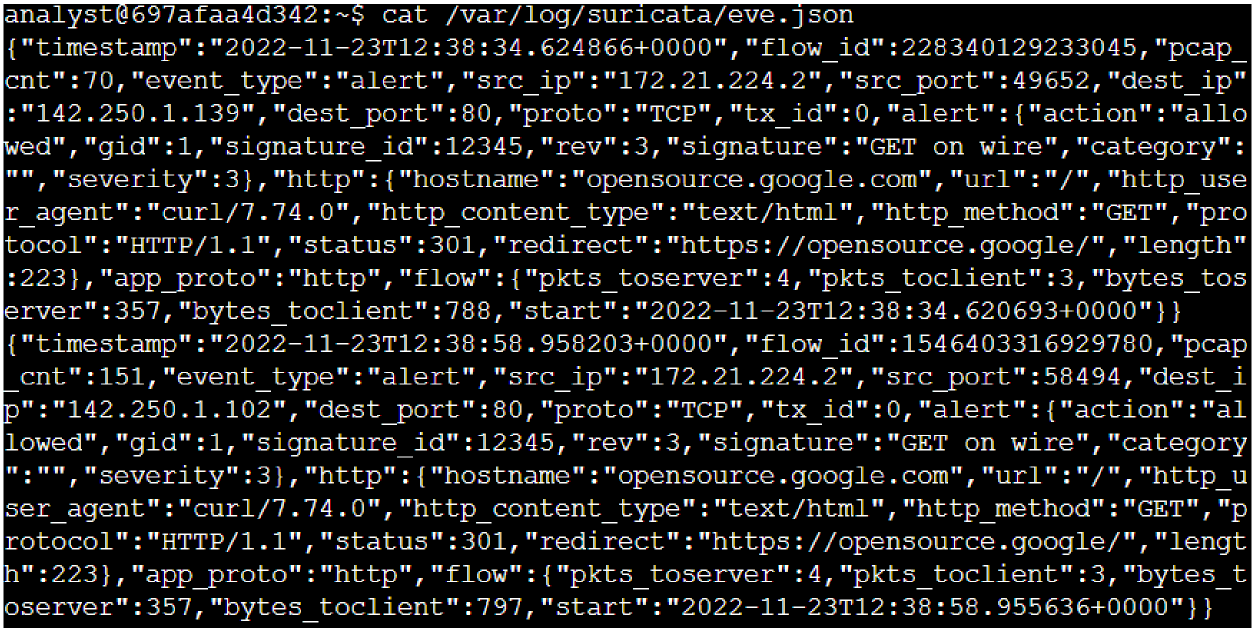
Look at the fast.log file:



```
analyst@697afaa4d342:~$ cat /var/log/suricata/fast.log
11/23/2022-12:38:34.624866  [**] [1:12345:3] GET on wire [**] [Classification:
(null)] [Priority: 3] {TCP} 172.21.224.2:49652 -> 142.250.1.139:80
11/23/2022-12:38:58.958203  [**] [1:12345:3] GET on wire [**] [Classification:
(null)] [Priority: 3] {TCP} 172.21.224.2:58494 -> 142.250.1.102:80
```

- Corresponds to alerts generated by Suricata, includes the message, source, destination, and direction.

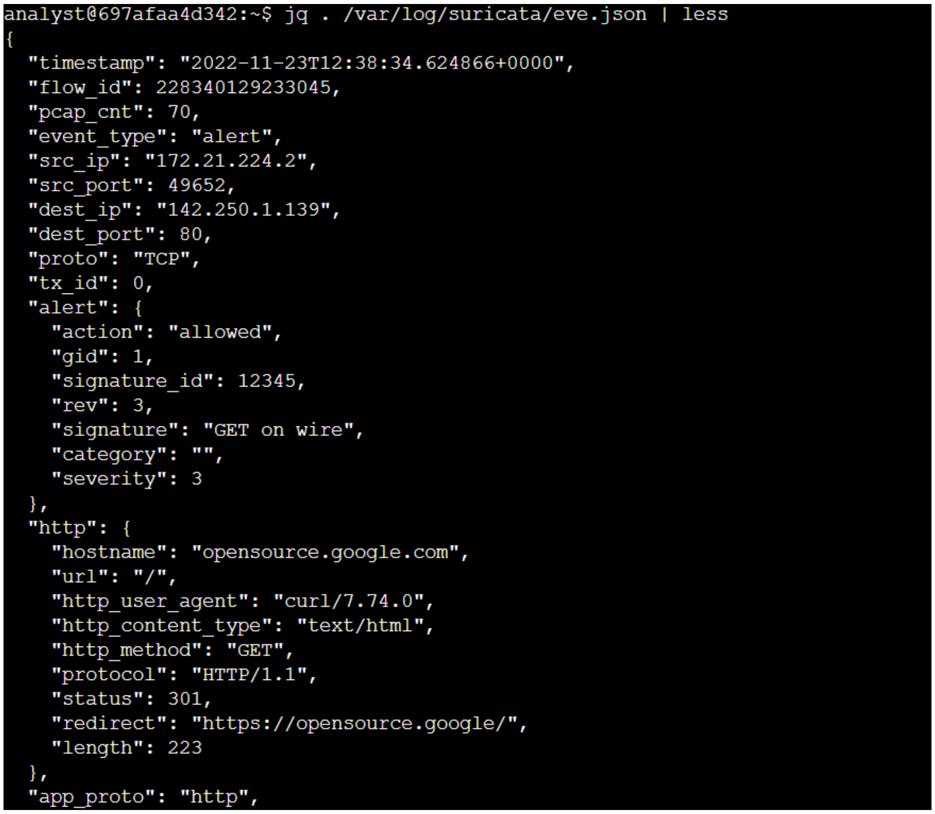
Look at the eve.json file:



```
analyst@697afaa4d342:~$ cat /var/log/suricata/eve.json
{"timestamp":"2022-11-23T12:38:34.624866+0000","flow_id":228340129233045,"pcap_
cnt":70,"event_type":"alert","src_ip":"172.21.224.2","src_port":49652,"dest_ip"
:"142.250.1.139","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allo
wed","gid":1,"signature_id":12345,"rev":3,"signature":"GET on wire","category":
"","severity":3},"http":{"hostname":"opensource.google.com","url":"/","http_use
r_agent":"curl/7.74.0","http_content_type":"text/html","http_method":"GET","pro
tocol":"HTTP/1.1","status":301,"redirect":"https://opensource.google/","length"
:223},"app_proto":"http","flow":{"pkts_toserver":4,"pkts_toclient":3,"bytes_tos
erver":357,"bytes_toclient":788,"start":"2022-11-23T12:38:34.620693+0000"}}
{"timestamp":"2022-11-23T12:38:58.958203+0000","flow_id":1546403316929780,"pcap
_cnt":151,"event_type":"alert","src_ip":"172.21.224.2","src_port":58494,"dest_i
p":"142.250.1.102","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"al
lowed","gid":1,"signature_id":12345,"rev":3,"signature":"GET on wire","category
":"","severity":3},"http":{"hostname":"opensource.google.com","url":"/","http_u
ser_agent":"curl/7.74.0","http_content_type":"text/html","http_method":"GET","p
rotocol":"HTTP/1.1","status":301,"redirect":"https://opensource.google/","lengt
h":223},"app_proto":"http","flow":{"pkts_toserver":4,"pkts_toclient":3,"bytes_t
oserver":357,"bytes_toclient":797,"start":"2022-11-23T12:38:58.955636+0000"}}
```

- Has all wanted information but is hard for a human to read.

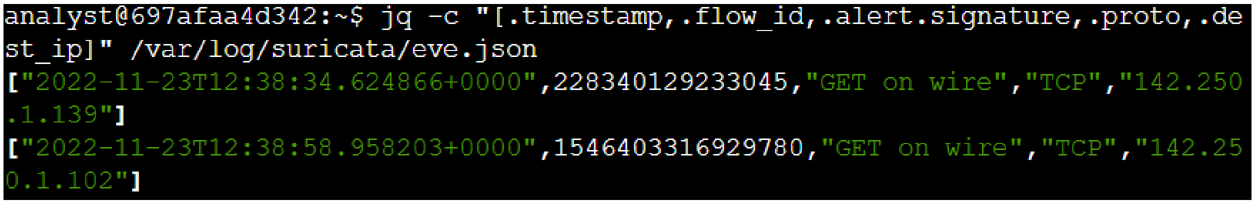
Improve the format:



```
analyst@697afaa4d342:~$ jq . /var/log/suricata/eve.json | less
{
  "timestamp": "2022-11-23T12:38:34.624866+0000",
  "flow_id": 228340129233045,
  "pcap_cnt": 70,
  "event_type": "alert",
  "src_ip": "172.21.224.2",
  "src_port": 49652,
  "dest_ip": "142.250.1.139",
  "dest_port": 80,
  "proto": "TCP",
  "tx_id": 0,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 12345,
    "rev": 3,
    "signature": "GET on wire",
    "category": "",
    "severity": 3
  },
  "http": {
    "hostname": "opensource.google.com",
    "url": "/",
    "http_user_agent": "curl/7.74.0",
    "http_content_type": "text/html",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "status": 301,
    "redirect": "https://opensource.google/",
    "length": 223
  },
  "app_proto": "http",
```

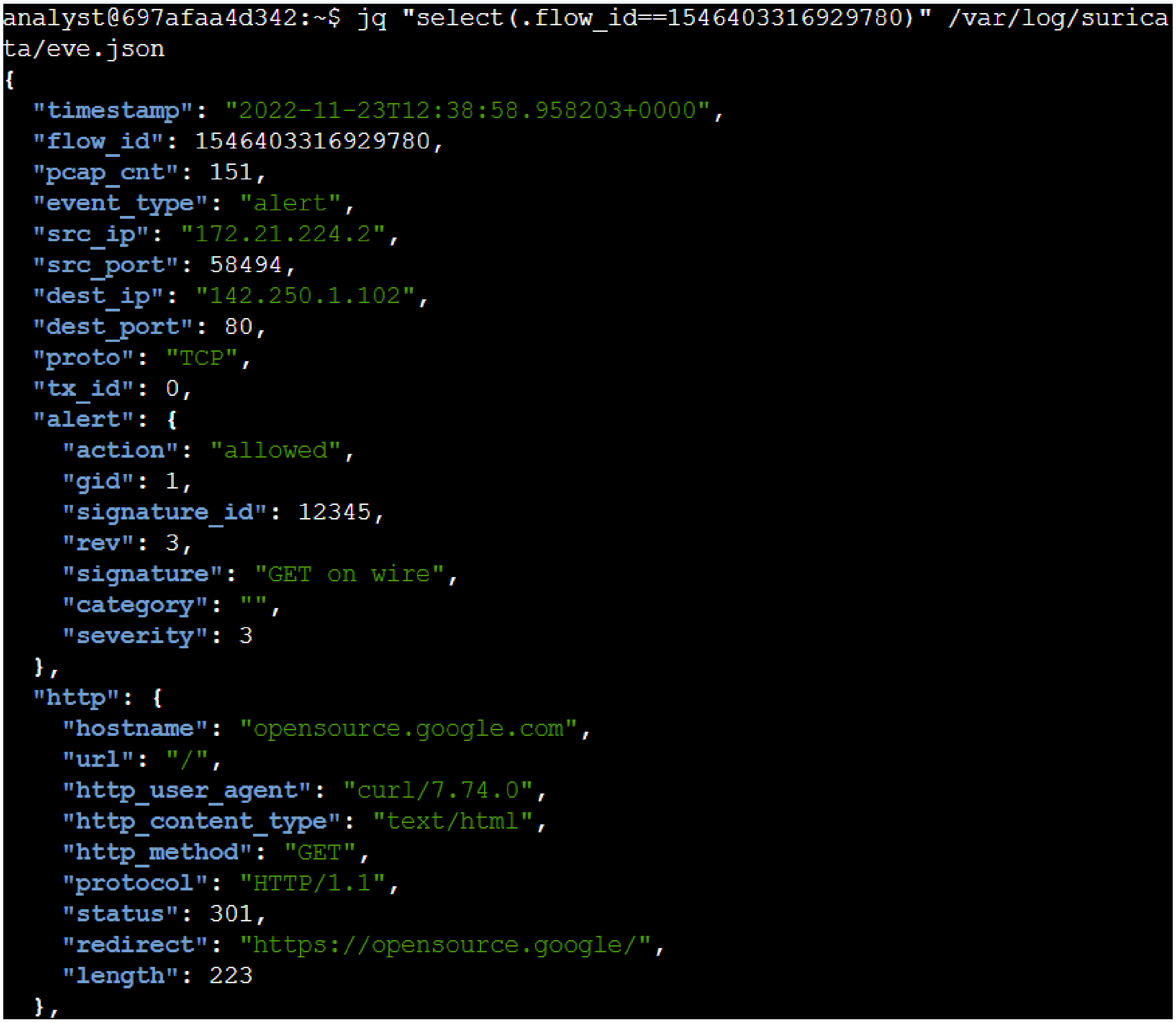
- Jp tool is useful for processing JSON data, has more complex uses.

Get the timestamp, flow id, alert signature, protocol, and destination IP event data from eve.json:



```
analyst@697afaa4d342:~$ jq -c "[.timestamp,.flow_id,.alert.signature,.proto,.de
st_ip]" /var/log/suricata/eve.json
["2022-11-23T12:38:34.624866+0000",228340129233045,"GET on wire","TCP","142.250
.1.139"]
["2022-11-23T12:38:58.958203+0000",1546403316929780,"GET on wire","TCP","142.25
0.1.102"]
```

Show event logs that have flow ID of 1546403316929780:



```
analyst@697afaa4d342:~$ jq "select(.flow_id==1546403316929780)" /var/log/surica
ta/eve.json
{
  "timestamp": "2022-11-23T12:38:58.958203+0000",
  "flow_id": 1546403316929780,
  "pcap_cnt": 151,
  "event_type": "alert",
  "src_ip": "172.21.224.2",
  "src_port": 58494,
  "dest_ip": "142.250.1.102",
  "dest_port": 80,
  "proto": "TCP",
  "tx_id": 0,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 12345,
    "rev": 3,
    "signature": "GET on wire",
    "category": "",
    "severity": 3
  },
  "http": {
    "hostname": "opensource.google.com",
    "url": "/",
    "http_user_agent": "curl/7.74.0",
    "http_content_type": "text/html",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "status": 301,
    "redirect": "https://opensource.google/",
    "length": 223
  },
```