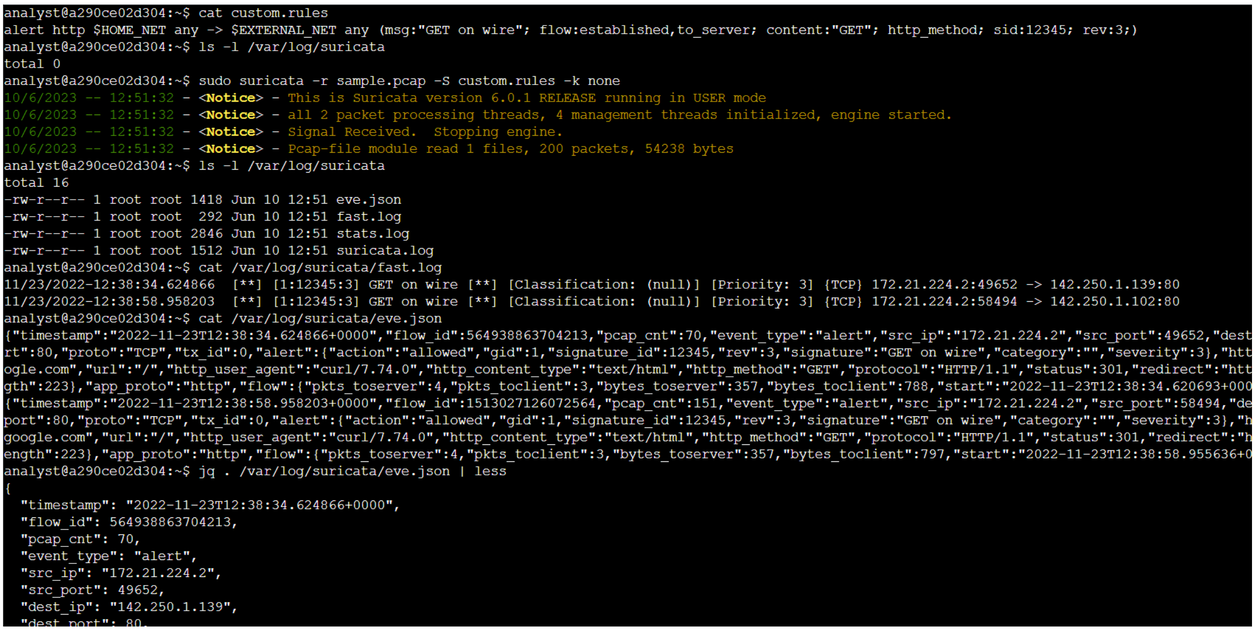
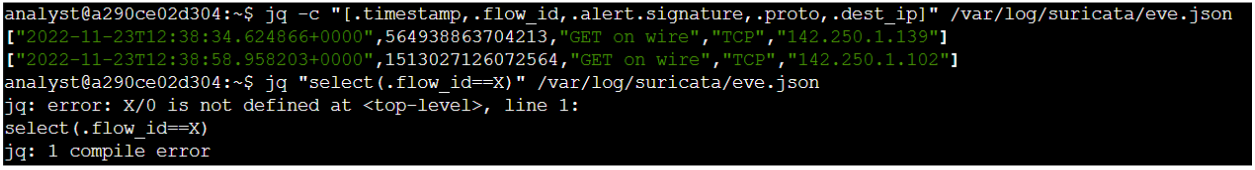
This lab involved examining a custom rule in Suricata, triggering the rule, and examining the alert logs generated by Suricata. I also explored the output in the eve.json file.



```
analyst@a290ce02d304:~$ cat custom.rules
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"GET on wire"; flow:established,to_server; content:"GET"; http_method; sid:12345; rev:3;)
analyst@a290ce02d304:~$ ls -l /var/log/suricata
total 0
analyst@a290ce02d304:~$ sudo suricata -r sample.pcap -S custom.rules -k none
10/6/2023 -- 12:51:32 - <Notice> - This is Suricata version 6.0.1 RELEASE running in USER mode
10/6/2023 -- 12:51:32 - <Notice> - all 2 packet processing threads, 4 management threads initialized, engine started.
10/6/2023 -- 12:51:32 - <Notice> - Signal Received.  Stopping engine.
10/6/2023 -- 12:51:32 - <Notice> - Pcap-file module read 1 files, 200 packets, 54238 bytes
analyst@a290ce02d304:~$ ls -l /var/log/suricata
total 16
-rw-r--r-- 1 root root 1418 Jun 10 12:51 eve.json
-rw-r--r-- 1 root root  292 Jun 10 12:51 fast.log
-rw-r--r-- 1 root root 2846 Jun 10 12:51 stats.log
-rw-r--r-- 1 root root 1512 Jun 10 12:51 suricata.log
analyst@a290ce02d304:~$ 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
analyst@a290ce02d304:~$ cat /var/log/suricata/eve.json
{"timestamp":"2022-11-23T12:38:34.624866+0000","flow_id":564938863704213,"pcap_cnt":70,"event_type":"alert","src_ip":"172.21.224.2","src_port":49652,"dest
rt":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":12345,"rev":3,"signature":"GET on wire","category":"","severity":3},"htt
ogle.com","url":"/","http_user_agent":"curl/7.74.0","http_content_type":"text/html","http_method":"GET","protocol":"HTTP/1.1","status":301,"redirect":"htt
gth":223},"app_proto":"http","flow":{"pkts_toserver":4,"pkts_toclient":3,"bytes_toserver":357,"bytes_toclient":788,"start":"2022-11-23T12:38:34.620693+000
{"timestamp":"2022-11-23T12:38:58.958203+0000","flow_id":1513027126072564,"pcap_cnt":151,"event_type":"alert","src_ip":"172.21.224.2","src_port":58494,"de
port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":12345,"rev":3,"signature":"GET on wire","category":"","severity":3},"h
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":"h
ength":223},"app_proto":"http","flow":{"pkts_toserver":4,"pkts_toclient":3,"bytes_toserver":357,"bytes_toclient":797,"start":"2022-11-23T12:38:58.955636+0
analyst@a290ce02d304:~$ jq . /var/log/suricata/eve.json | less
{
  "timestamp": "2022-11-23T12:38:34.624866+0000",
  "flow_id": 564938863704213,
  "pcap_cnt": 70,
  "event_type": "alert",
  "src_ip": "172.21.224.2",
  "src_port": 49652,
  "dest_ip": "142.250.1.139",
  "dest_port": 80,
```



```
analyst@a290ce02d304:~$ jq -c "[.timestamp,.flow_id,.alert.signature,.proto,.dest_ip]" /var/log/suricata/eve.json
["2022-11-23T12:38:34.624866+0000",564938863704213,"GET on wire","TCP","142.250.1.139"]
["2022-11-23T12:38:58.958203+0000",1513027126072564,"GET on wire","TCP","142.250.1.102"]
analyst@a290ce02d304:~$ jq "select(.flow_id==X)" /var/log/suricata/eve.json
jq: error: X/0 is not defined at <top-level>, line 1:
select(.flow_id==X)
jq: 1 compile error
```

I examined a custom rule in Suricata. I used the **cat** command to display the rule in the **custom.rules** file. The rule had an action, a header, and rule options.

The action of the rule determined the action to take if all conditions were met. In this case, the action was an alert, which instructed Suricata to alert on selected network traffic.

The header of the rule defined the signature's network traffic, including protocols, source and destination IP addresses, source and destination ports, and traffic direction.

The rule options allowed for customization of the signature with additional parameters. These options narrowed down the network traffic to be analyzed. In the example rule, options such as **msg**, **flow**, **content**, **sid**, and **rev** were used to specify the conditions for generating an alert.

I then proceeded to trigger the custom rule in Suricata by running the Suricata application with the **custom.rules** and **sample.pcap** files. This simulated the monitoring of network traffic and generated alert logs.

After running Suricata, I examined the alert logs generated by Suricata in the **fast.log** file. Each entry in the **fast.log** corresponded to an alert triggered by Suricata when it processed a packet that met the conditions of the rule.

Finally, I examined the additional output generated by Suricata in the **eve.json** file. Using the **jq** command, I was able to extract and view specific event data in an improved format.

In conclusion, I successfully examined a custom rule, triggered it in Suricata, and analyzed the resulting alert logs and additional output in Suricata's log files.