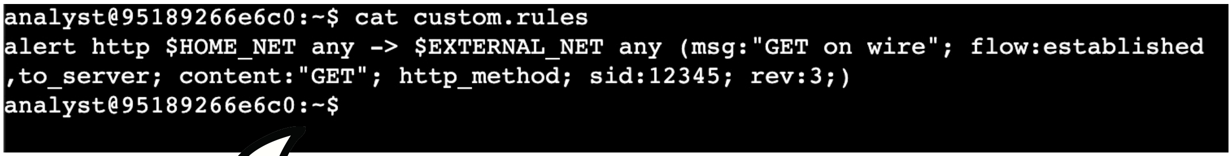
# Project

I've been tasked with configuring Suricata to monitor our corporate network for security threats. My goals include creating custom detection rules and setting up an effective alert mechanism. I will focus on real-time packet inspection, minimizing false positives. Ultimately, I aim to enhance our network security by quickly identifying and responding to potential intrusions.

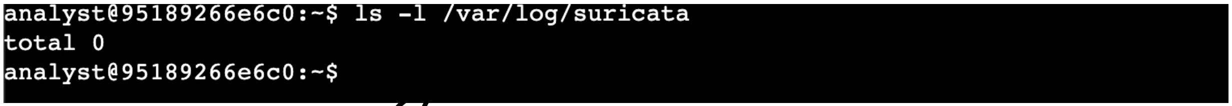
I used the cat command to display the rule in the custom.rules file.



```
analyst@95189266e6c0:~$ cat custom.rules
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"GET on wire"; flow:established
,to_server; content:"GET"; http_method; sid:12345; rev:3;)
analyst@95189266e6c0:~$
```

This signature triggers an alert whenever Suricata observes the text GET as the HTTP method in an HTTP packet from the home network going to the external network.

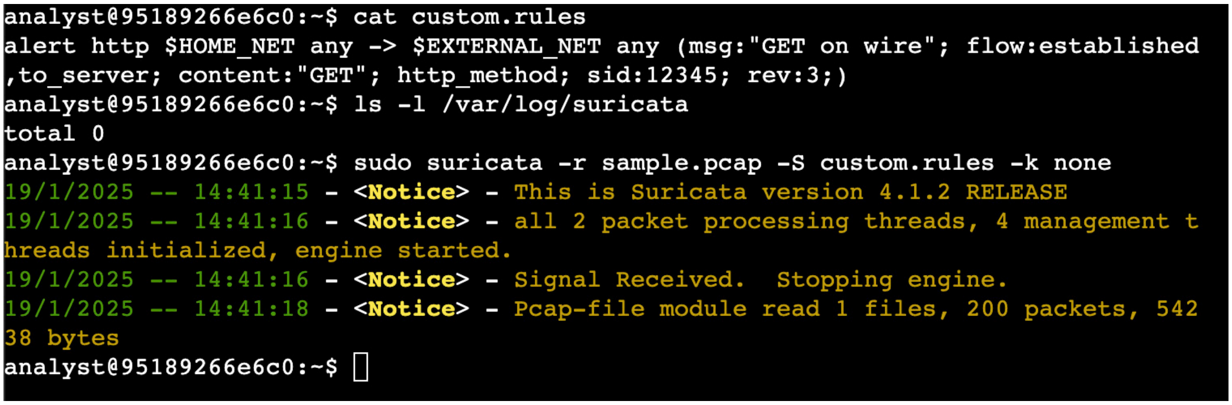
I listed the files in the /var/log/suricata folder



```
analyst@95189266e6c0:~$ ls -l /var/log/suricata
total 0
analyst@95189266e6c0:~$
```

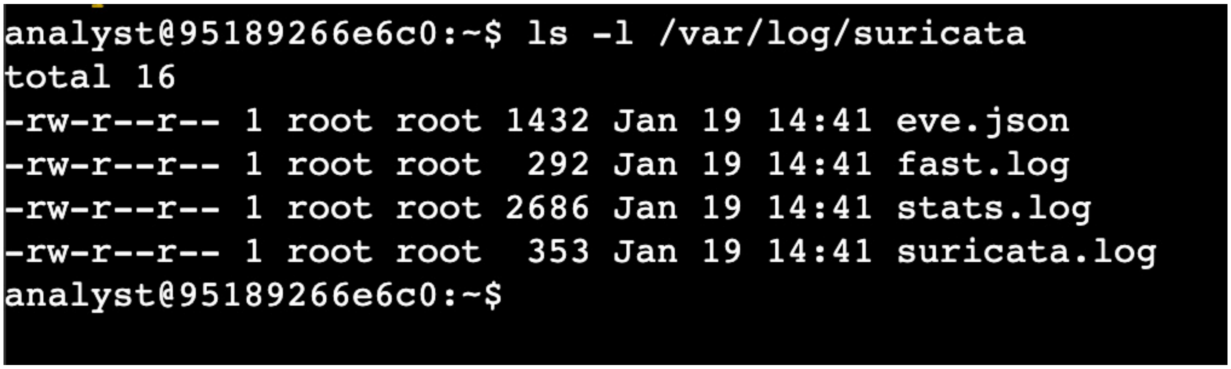
before running Suricata, there are no files in the /var/log/suricata directory.

I ran Suricata using the custom.rules and sample.pcap files. I used the command sudo suricata -r sample.pcap -S custom.rules -k none. This allowed me to analyze the packet data in the sample.pcap file while applying the rules defined in custom.rules.



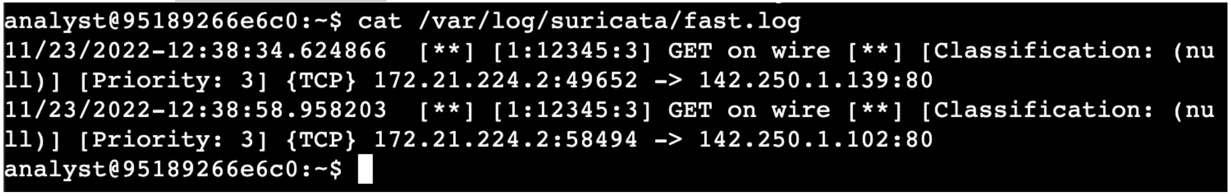
```
analyst@95189266e6c0:~$ cat custom.rules
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"GET on wire"; flow:established
,to_server; content:"GET"; http_method; sid:12345; rev:3;)
analyst@95189266e6c0:~$ ls -l /var/log/suricata
total 0
analyst@95189266e6c0:~$ sudo suricata -r sample.pcap -S custom.rules -k none
19/1/2025 -- 14:41:15 - <Notice> - This is Suricata version 4.1.2 RELEASE
19/1/2025 -- 14:41:16 - <Notice> - all 2 packet processing threads, 4 management t
hreads initialized, engine started.
19/1/2025 -- 14:41:16 - <Notice> - Signal Received.  Stopping engine.
19/1/2025 -- 14:41:18 - <Notice> - Pcap-file module read 1 files, 200 packets, 542
38 bytes
analyst@95189266e6c0:~$ 
```

Then I listed the files in the /var/log/suricata folder again with the command ls -l /var/log/suricata



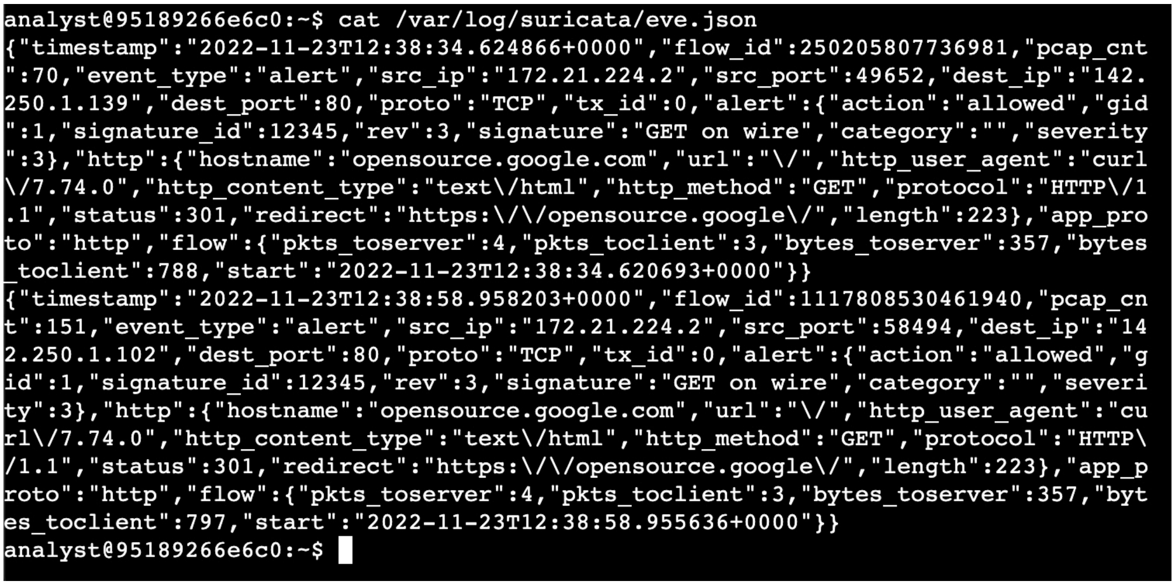
```
analyst@95189266e6c0:~$ ls -l /var/log/suricata
total 16
-rw-r--r-- 1 root root 1432 Jan 19 14:41 eve.json
-rw-r--r-- 1 root root  292 Jan 19 14:41 fast.log
-rw-r--r-- 1 root root 2686 Jan 19 14:41 stats.log
-rw-r--r-- 1 root root  353 Jan 19 14:41 suricata.log
analyst@95189266e6c0:~$
```

I used the cat command to display the contents of the fast.log file generated by Suricata located in the /var/log/suricata directory.



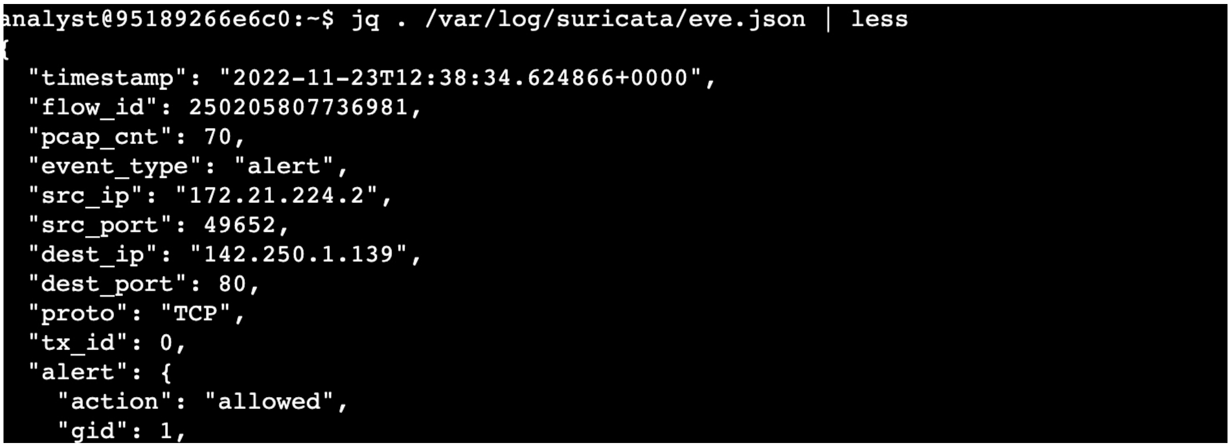
```
analyst@95189266e6c0:~$ cat /var/log/suricata/fast.log
11/23/2022-12:38:34.624866  [**] [1:12345:3] GET on wire [**] [Classification: (nu
ll)] [Priority: 3] {TCP} 172.21.224.2:49652 -> 142.250.1.139:80
11/23/2022-12:38:58.958203  [**] [1:12345:3] GET on wire [**] [Classification: (nu
ll)] [Priority: 3] {TCP} 172.21.224.2:58494 -> 142.250.1.102:80
analyst@95189266e6c0:~$ 
```

I used the cat command to display the entries in the eve.json file generated by Suricata, specifically by accessing it in the /var/log/suricata directory.

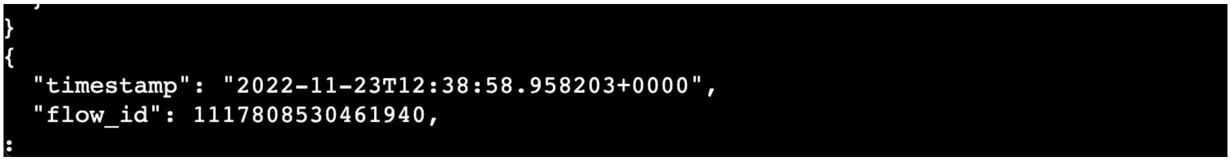


```
analyst@95189266e6c0:~$ cat /var/log/suricata/eve.json
{"timestamp":"2022-11-23T12:38:34.624866+0000","flow_id":250205807736981,"pcap_cnt
":70,"event_type":"alert","src_ip":"172.21.224.2","src_port":49652,"dest_ip":"142.
250.1.139","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid
":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_pro
to":"http","flow":{"pkts_toserver":4,"pkts_toclient":3,"bytes_toserver":357,"bytes
_toclient":788,"start":"2022-11-23T12:38:34.620693+0000"}}
{"timestamp":"2022-11-23T12:38:58.958203+0000","flow_id":1117808530461940,"pcap_cn
t":151,"event_type":"alert","src_ip":"172.21.224.2","src_port":58494,"dest_ip":"14
2.250.1.102","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","g
id":1,"signature_id":12345,"rev":3,"signature":"GET on wire","category":"","severi
ty":3},"http":{"hostname":"opensource.google.com","url":"\/","http_user_agent":"cu
rl\/7.74.0","http_content_type":"text\/html","http_method":"GET","protocol":"HTTP\
/1.1","status":301,"redirect":"https:\/\/opensource.google\/","length":223},"app_p
roto":"http","flow":{"pkts_toserver":4,"pkts_toclient":3,"bytes_toserver":357,"byt
es_toclient":797,"start":"2022-11-23T12:38:58.955636+0000"}}
analyst@95189266e6c0:~$ 
```

I used the jq command to display the entries in the eve.json file generated by Suricata in an improved format, specifically by accessing it in the /var/log/suricata directory and piping the output to less for easier viewing.

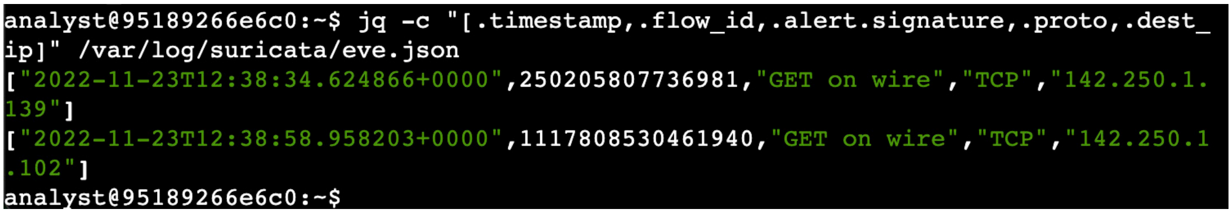


```
analyst@95189266e6c0:~$ jq . /var/log/suricata/eve.json | less
{
  "timestamp": "2022-11-23T12:38:34.624866+0000",
  "flow_id": 250205807736981,
  "pcap_cnt": 70,
  "event_type": "alert",
  "src_ip": "172.21.224.2",
  "src_port": 49652,
  "dest_ip": "142.250.1.139",
  "dest_port": 80,
  "proto": "TCP",
  "tx_id": 0,
  "alert": {
    "action": "allowed",
    "gid": 1,
```



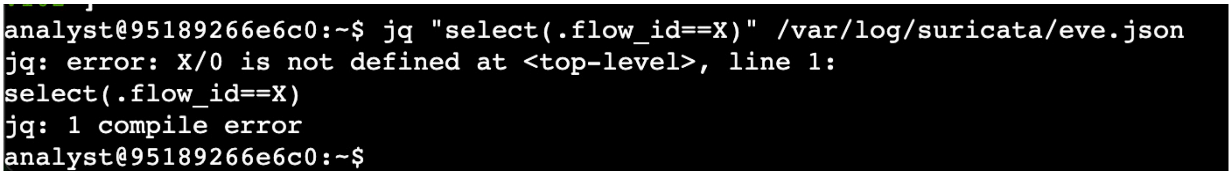
```
}
{
  "timestamp": "2022-11-23T12:38:58.958203+0000",
  "flow_id": 1117808530461940,
:
```

I used the jq command to extract specific event data from the eve.json file generated by Suricata.



```
analyst@95189266e6c0:~$ jq -c "[.timestamp,.flow_id,.alert.signature,.proto,.dest_
ip]" /var/log/suricata/eve.json
["2022-11-23T12:38:34.624866+0000",250205807736981,"GET on wire","TCP","142.250.1.
139"]
["2022-11-23T12:38:58.958203+0000",1117808530461940,"GET on wire","TCP","142.250.1
.102"]
analyst@95189266e6c0:~$
```

I used the jq command to display all event logs related to a specific flow_id from the eve.json file. The flow_id value is a 16-digit number that varies for each log entry, and I replaced X with one of the flow_id values returned by the previous query.



```
analyst@95189266e6c0:~$ 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
analyst@95189266e6c0:~$
```