Suricata Examples from Google Cert

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"GET on wire"; flow:established,to_server; content:"GET"; http_method; sid:12345; rev:3;)
```

This rule consists of three components: an action, a header, and rule options. 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.

```
sudo suricata -r sample.pcap -S custom.rules -k none
```

This command starts the Suricata application and processes the sample.pcap file using the rules in the custom.rules file. It returns an output stating how many packets were processed by Suricata. The -r sample.pcap option specifies an input file to mimic network traffic. In this case, the sample.pcap file. The -S custom.rules option instructs Suricata to use the rules defined in the custom.rules file. The -k none option instructs Suricata to disable all checksum checks

Use the jq command to display the entries in an improved format

~~cat /var/log/suricata/eve.json~~ `jq . /var/log/suricata/eve.json | less`

Press Q to exit the less command and to return to the command-line prompt.

```
jq -c "[.timestamp,.flow_id,.alert.signature,.proto,.dest_ip]" /var/log/suricata/eve.json
```

The jq command above extracts the fields specified in the list in the square brackets from the JSON payload. The fields selected are the timestamp (.timestamp), the flow id (.flow_id), the alert signature or msg (.alert.signature), the protocol (.proto), and the destination IP address (.dest_ip).

```
jq "select(.flow_id==X)" /var/log/suricata/eve.json
```

Use the jq command to display all event logs related to a specific flow_id