**HOW TO INTEGRATE SURICATA WITH WAZUH**

**Installation Guide For Suricata On Windows Machine :-**

**Step 1:- Install wincap and NPCAP for windows.**

[**WinPcap · Download**](https://www.winpcap.org/install/)

**Step 2:- Install winPcap and NPCAP for windows.**

[**Npcap: Windows Packet Capture Library & Driver**](https://npcap.com/)

**Step 3:- Visit the download page of Suricata and download the latest version of Suricata.**

[**Download - Suricata**](https://suricata.io/download/)

A screenshot of a computer

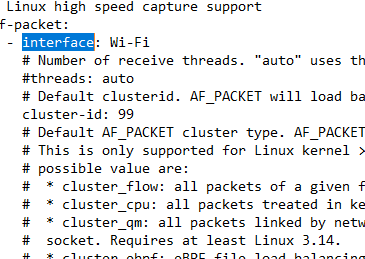
AI-generated content may be incorrect.

**Step 4:-**  Finish the Installation by clicking on the msi installer. Do same with the Npcap and WinPcap.

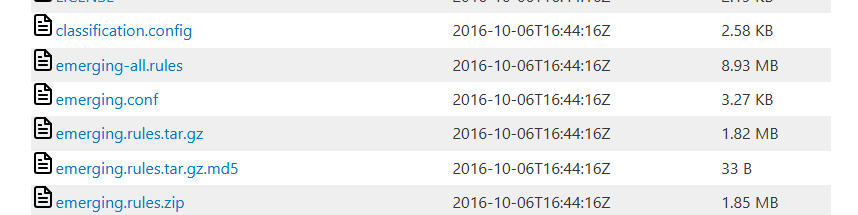
**Step 5:-** Open the directory where you installed Suricata and search for suricata.yaml . And open the file using any text editor.

Search for the interface keyword and edit the interface name according to yours .

You can check your interface by typing **ipconfig** in cmd.

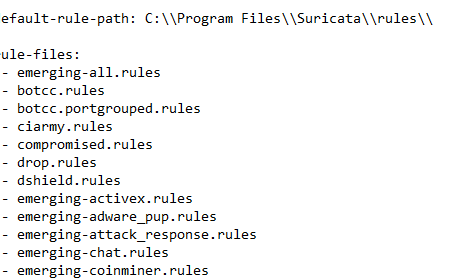


**Step 6:-** Update the rule file by downloading this file from [Proofpoint Emerging Threats Rules](https://rules.emergingthreats.net/open/old/suricata-1.0/)



Please note that download the rules in default **Rules** directory of suricata .

Or if you change something please edit the suricata.yaml.



**Step 6:-** Open cmd and as administrator and go into the Suricata directory.

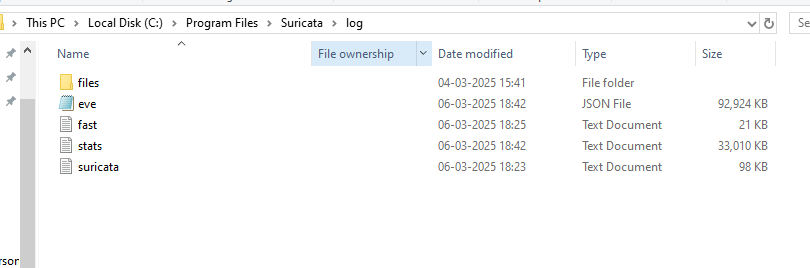
Run Suricata by using following command.

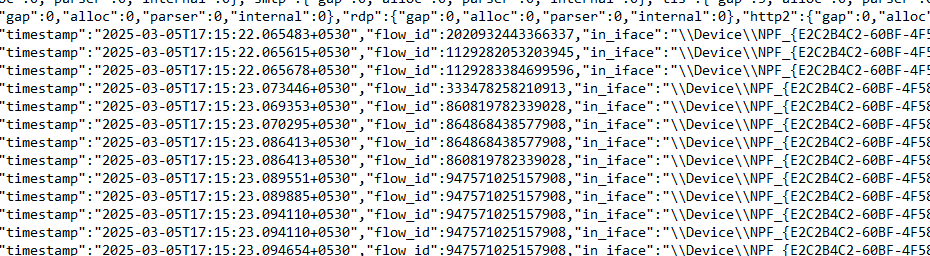
**“suricata.exe -c suricata.yaml -I <Your IP >”**

A screenshot of a computer program

AI-generated content may be incorrect.

**Step 7:-** Check the Suricata log directory and check **eve**.**Json** and if you see logs like this your Suricata is running successfully.





**Now we have Suricata running so lets integrate it with wauh agent so wazuh can read the logs.**

**Step 8:-** Run cmd as administrator and open the **ossec.config** fileby going into ossec directory.

A screenshot of a computer program

AI-generated content may be incorrect.

**Step 9:-** Add the following code in the ossec.config file and restart the wazuh agent.

**<localfile>**

**<log\_format>json</log\_format>**

**<location>C:\Program Files\Suricata\log\eve.json</location>**

**</localfile>**

A computer code with black text

AI-generated content may be incorrect.

Please note that this code must be in between <ossec config >tag .

**Step 10:-** Restart the wazuh agent to synch with the changes.