Cara Menjalankan Program

1) Install Suricata (latest version) from PPA repository.
   a. Add Suricata resource on default Ubuntu 18.04 repository:

```
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt update
```

Once the PPA repo is set:

```
apt-cache policy suricata
suricata:
  Installed: 4.1.2-0ubuntu6
  Candidate: 4.1.2-0ubuntu6
  Version table:
 *** 4.1.2-0ubuntu6 500
        500 http://ppa.launchpad.net/oisf/suricata-stable/ubuntu
bionic/main amd64 Packages
        100 /var/lib/dpkg/status
     3.2-2ubuntu3 500
        500 http://ke.archive.ubuntu.com/ubuntu bionic/universe
amd64 Packages
```

   b. Install Lib apps Suricata for supported machine:

```
sudo apt-get -y installlibpcre3 libpcre3-dbg libpcre3-dev
\build-essential autoconf automake libtool libpcap-dev libnet1-
dev \libyaml-0-2 libyaml-dev zlib1g zlib1g-dev libcap-ng-dev
libcap-ng0\make libmagic-dev libjansson-dev libjansson4 pkg-
config
```

   c. Install Suricata:

```
sudo apt install suricata
```

   d. Add IPS mode on Suricata:

```
sudo apt-get -y install libnetfilter-queue-dev libnetfilter-
queue1 libnfnetlink-dev libnfnetlink0
```

   e. List the Suricata rules:

```
ls -C /etc/suricata/rules/
app-layer-events.rules   emerging-attack_response.rules
emerging-malware.rules         emerging-telnet.rules
LICENSE
botcc.portgrouped.rules  emerging-chat.rules
emerging-misc.rules            emerging-tftp.rules
modbus-events.rules
botcc.rules              emerging-current_events.rules
emerging-mobile_malware.rules  emerging-trojan.rules
nfs-events.rules
BSD-License.txt          emerging-deleted.rules
emerging-netbios.rules         emerging-user_agents.rules
ntp-events.rules
ciarmy.rules             emerging-dns.rules
emerging-p2p.rules             emerging-voip.rules
sid-msg.map
```

```
classification.config    emerging-dos.rules
emerging-policy.rules          emerging-web_client.rules
smb-events.rules
compromised-ips.txt      emerging-exploit.rules
emerging-pop3.rules            emerging-web_server.rules
smtp-events.rules
compromised.rules        emerging-ftp.rules
emerging-rpc.rules             emerging-web_specific_apps.rules
stream-events.rules
decoder-events.rules     emerging-games.rules
emerging-scada.rules           emerging-worm.rules
suricata-4.0-enhanced-open.txt
dnp3-events.rules        emerging-icmp_info.rules
emerging-scan.rules            files.rules
tls-events.rules
dns-events.rules         emerging-icmp.rules
emerging-shellcode.rules       gpl-2.0.txt
tor.rules
drop.rules               emerging-imap.rules
emerging-smtp.rules            http-events.rules
dshield.rules            emerging-inappropriate.rules
emerging-snmp.rules            ipsec-events.rules
emerging-activex.rules   emerging-info.rules
```

2) Configure Suricata on Ubuntu 18.04.
   a. Nano /etc/suricata/suricata.yaml

```
    HOME_NET: "[192.168.100.0/24]" //listening on network
...
    EXTERNAL_NET: "!$HOME_NET"
...
```

   b. Suricata rules configure:

Default-rule-path: /etc/suricata/rules
Rule-files:
- Emerging-clabs_dos.rules
- Emerging-clabs-metasploit.rules
- Emerging-clabs_nmap.rules

   c. Rules of suricata, please see on BAB IV IMPLEMENTASI DAN PENGUJIAN or 9_175410194_LISTING_PROGRAM.

3) Running Suricata *Intrusion Detection Prevention System*.
   a. Suricata machine started. Follow the comment:

idps@suricata:~$ **sudo suricata -c /etc/suricata.yaml –af-packet**

   b. To see Logs by suricata:

idps@suricata:~$ **sudo tail -f /var/log/suricata/fast.log**

4) For testing, please see BAB IV IMPLEMENTASI DAN PENGUJIAN.