Project Setup Instructions — Honeypot AI

This project demonstrates a real-time intrusion detection and alert classification system using simulated Suricata alerts and a pre-trained machine learning model. It includes an auto-updating Flask-based dashboard for visualizing threat activity within a monitored network.

💼 Required Files and Structure

Ensure all the following files are placed in a single directory (e.g., `D:\AI_Honeypot`):

File Name	Purpose
suricata.py	Simulates dynamic Suricata alerts in eve.json
realtime.py	Classifies alerts using a trained ML model
dashboard.py	Web-based UI showing latest classified alerts
start.py	Master script to launch all modules
classifier.pkl	Pre-trained scikit-learn model for classification
dataset.csv	Used for fitting label encoders
output.csv	Final output of classified alerts *(auto-generated)*
eve.json	Simulated Suricata alert file *(auto-generated)*
cred.txt	Contains credentials or API keys used by modules *(if applicable)*

⚙ Environment Setup

1. Install Python 3.7 or above.
2. Install the required Python libraries using:

```
pip3 install flask pandas scikit-learn joblib
```

▶ Running the System

To start the entire honeypot detection pipeline:

1. Open Command Prompt or terminal.
2. Navigate to the project directory:

```
cd D:\AI_Honeypot
```

3. Launch the full system using:

```
python3 start.py
```

This will automatically:

- Start simulated Suricata alerts (`suricata.py`)
- Begin real-time classification (`realtime.py`)
- Launch the local web dashboard (`dashboard.py`)

🌐 Accessing the Dashboard

Once running, open your browser and visit:
http://127.0.0.1:5000

- The dashboard auto-refreshes every 5 seconds.
- It displays the 5 most recent classified alerts from `output.csv`.

🛑 Stopping the System

To stop all services, press:
Ctrl + C
in the terminal window.

✓ Output Format

Each alert row in `output.csv` has the following structure:

```
src_ip,dest_ip,protocol,signature,status
192.168.1.10,192.168.1.100,TCP,ET MALWARE Possible Malicious Traffic,Malicious
```

Where `status` is predicted as **Malicious** or **Benign** by the trained model.