# **User Guide for TCPDump Analysis Tool**

## **Introduction**

This guide provides clear, step-by-step instructions to help you use the TCPDump Analysis Tool effectively. Follow these instructions to install dependencies, launch the application, and interpret the analysis results.

## **Installation and Setup**

1. **Install Dependencies:**
   * Locate the file dep.bat in the root directory.
   * Double-click dep.bat to install the necessary dependencies for the program.
2. **Open the Project Folder:**
   * Navigate to the folder named SAE-105-REAL.
3. **Launch the Application:**
   * Run the file app.py with Python.
   * If it does not work:
     1. Open Visual Studio Code (VSCode).
     2. Use the shortcut Ctrl + K, then Ctrl + O to open the folder SAE-105-REAL.
     3. Locate app.py open a terminal and type python app.py
4. **Access the Web Interface:**
   * When the application is running, http://127.0.0.1:5000 will be displayed.
   * Press Ctrl + Click on the link, or copy and paste it into a web browser to open the HTML page.

## **Using the Application**

1. **Upload a TCPDump File:**
   * On the HTML page, click the button labeled "Choisir un fichier" (Choose a file).
   * Select your TCPDump capture file from your computer.
2. **Start the Analysis:**
   * After selecting a file, click the button labeled "Démarrer l'analyse" (Start Analysis).
   * The Python program will process the capture file and generate analysis results.

## **Understanding the Analysis Results**

### **Summary Section**

* **Total Packets:** Displays the total number of packets in the capture.
* **Unique Sizes:** Shows the distinct packet sizes identified.
* **Average Size:** Indicates the average packet size.

### **Visualizations**

1. **TCP Flags Distribution:**
   * A pie chart representing the distribution of TCP flags in the capture.
2. **Packet Size Distribution:**
   * A chart displaying the distribution of packet sizes, including the number of packets and their respective sizes

### **Attackers Profile**

* **Potential Attackers:**
  + Names or IP addresses of suspected attackers.
  + Total packets sent by each attacker.
  + Average packet size.
  + Number of targeted ports.

### **Detected Anomalies**

Below the attackers' profile, you’ll see:

* **Anomalies Details:**
  + Types of anomalies detected (e.g., "Syn Flood," "Traffic Burst").
  + Risk levels for each anomaly ("HIGH," "MEDIUM," "LOW").
  + Options to sort anomalies by type or risk level.

## **Analyzing a New File**

* To analyze another TCPDump file:
  1. Click "Choisir un fichier" (Choose a file).
  2. Select the new file.
  3. Click "Démarrer l'analyse" (Start Analysis).

The results for the new file will replace the previous analysis on the HTML page.