**Purpose of the Script**

The script is designed to analyze a TCP dump log file, extract network traffic data, detect anomalies, and generate a detailed HTML report that includes traffic statistics and protocol distribution charts.

**Code Breakdown**

**1. Importing Required Libraries**

The script begins by importing several Python libraries:

* **pandas, re, and datetime**: For data manipulation, regular expressions, and timestamp parsing.
* **matplotlib.pyplot and base64**: For creating and encoding charts.
* **webbrowser and os**: To open the generated report in a browser.
* **collections.Counter**: For counting occurrences of protocols and IPs.

**2. Analyzing the TCP Dump File (analyze\_tcpdump)**

This function performs the main analysis:

* **File Parsing**: Reads the log line-by-line.
* **Data Extraction**:
  + Extracts timestamps, source and destination IPs, and packet details using regular expressions.
  + Counts protocol occurrences and identifies IPs involved.
* **Anomaly Detection**:
  + Detects anomalies based on suspicious flag patterns (e.g., TCP "SYN" flags).
  + Identifies IPs with high traffic bursts.
* **Outputs**:
  + A structured dictionary containing network statistics, protocol distribution, and detected anomalies.

**3. Generating a Protocol Distribution Chart (generate\_protocol\_chart)**

This function:

* Creates a pie chart of the protocol distribution.
* Converts the chart to a Base64-encoded image string for embedding in the HTML report.

**4. Generating the HTML Report (generate\_html\_report)**

This function:

* Constructs an HTML report with:
  + **Summary Statistics**: Total packets, anomalies detected, suspicious IPs, and service counts.
  + **Charts**: A pie chart showing protocol distribution.
  + **Anomalies Table**: A detailed list of detected anomalies with timestamps and severity levels.
* Writes the HTML content to a file and opens it in the default web browser.

**5. Main Function**

The script's entry point:

* Specifies the file path to the TCP dump log (fichier182.txt).
* Calls the analysis and report generation functions.

**Key Features**

1. **Data Parsing**:
   * Extracts meaningful insights from raw TCP dump logs.
   * Identifies suspicious network activities.
2. **Visualization**:
   * Generates charts to simplify understanding of network traffic.
3. **User-Friendly Report**:
   * Outputs a visually appealing and organized HTML report.

**Usage Instructions**

1. Place the script in the same directory as the TCP dump log file.
2. Update the file\_path variable in the main function with the log file's name.
3. Run the script to generate and view the HTML report.