***NOTICE FOR THE SAE15 CODE***

1. **Objective of the script**

The file **monprojetsae15.py** is a Python script designed to process a network capture file to extract relevant information, such as source and destination IP addresses, TCP flags, sequence numbers, packet lengths, etc. It then generates statistics, graphs, and a web page to present the analysis results.

This Python script was created to detect network anomalies.

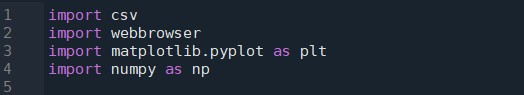
.

1. **Structure of the code**

The code is divided into several main sections:

* Importing libraries
* Opening the capture file
* Initializing lists and counters
* Processing file lines
* Calculating statistics
* Creating graphs
* Generating a web page
* Writing data to CSV files
* Closing files

1. **Detailed explanations of each code section :**
2. **Importing libraries**



* **csv** : Used to write data to CSV files.
* **webbrowser** : Although imported, it is not used in the script. It could be used to open the generated web page.
* **matplotlib.pyplot** : Used to create graphs..
* **numpy** : Imported but not used in the script. It could be removed if unnecessary.

1. **Opening the Capture File**



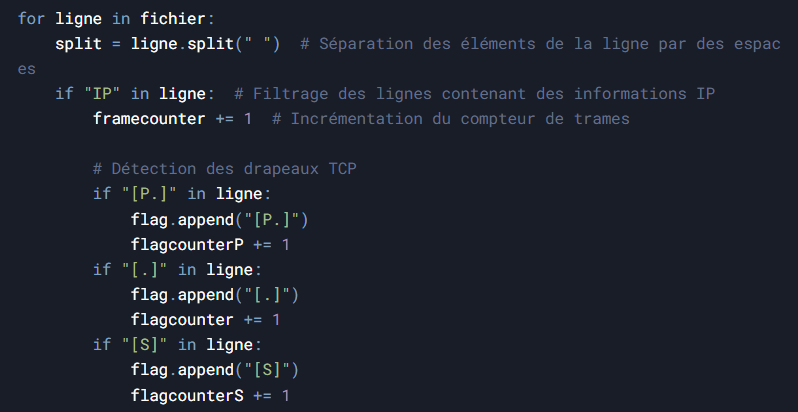
The file **Dumphile.txt** is opened in read mode. This file contains the network capture data to be analyzed.

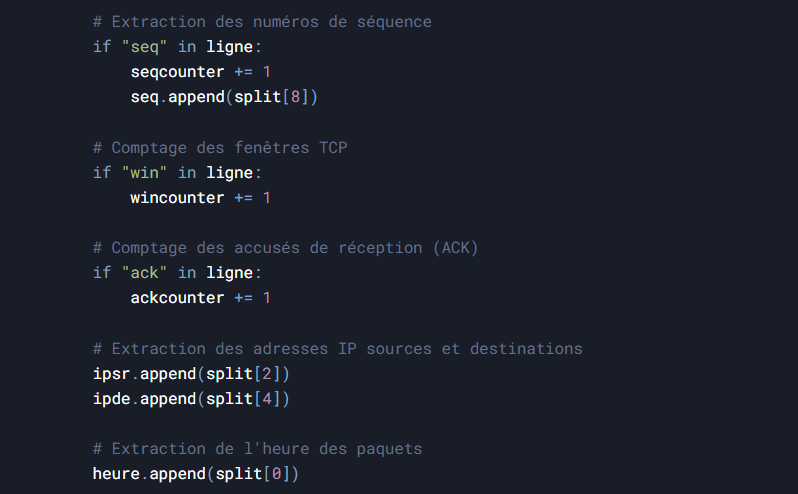
1. **Initializing lists and counters**

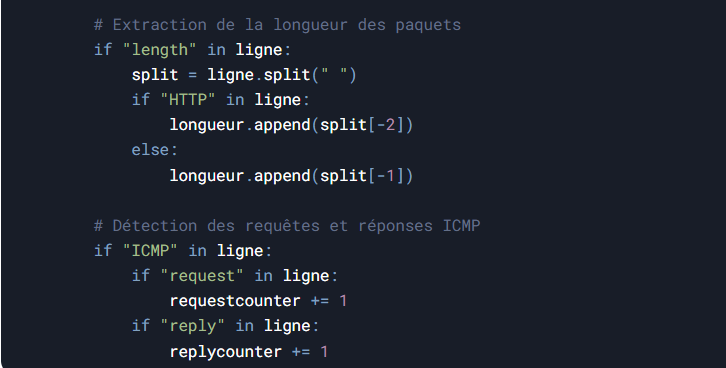


Several lists and counters are initialized to store the information extracted from the capture file.

1. **Processing file lines**

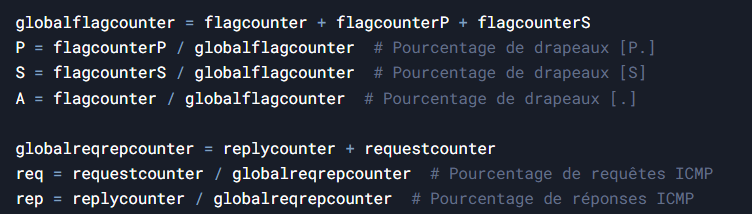






* The script processes each line of the capture file.
* it  uses the **split** method to separate line elements based on spaces.
* Relevant information is extracted and stored in the corresponding lists.

1. **Calculating statistics**



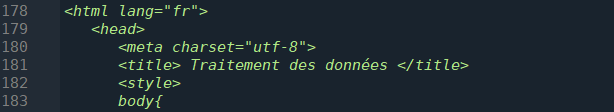
Percentages for different TCP flags and ICMP requests/replies are calculated.

1. **Creating graphs**



* Two pie charts are created to visualize the percentages of TCP flags and ICMP requests/replies.
* The graphs are saved as images (graphe1.png and graphe2.png).

1. **Generating the web page :**



* A web page is generated to display the analysis results.
* The page contains information about frames, TCP flags, ICMP requests/replies, and graphs.
* The page is saved as **clément.html**.

1. **Writing data to CSV files**



The extracted data is written to two CSV files:

* **nguimby.csv**: Contains detailed data (timestamp, source IP, destination IP, flag, sequence number, length).
* **benie.csv**: Contains global statistics.

1. **Closing files** :



The capture file is closed after processing.

1. **Usage :**

Place the capture file in the same directory as the script. Then, execute the script using a text editor. The results will be saved in files located in the same directory as the script and the capture file.

1. **Annexe :**

* **TCP flags** are control indicators used for communication between TCP clients and servers. The ACK, SEQ, and PSH flags are commonly used TCP flags.
* The **SEQ flag** is used to indicate the sequence of bytes sent by the client or server.
* The **ACK flag** is used to inform the client of the last sequence of bytes received by the server.
* The **PSH flag** is used to indicate that incoming data should be passed directly to the application rather than being buffered.