TCPDUMP Analyser User guide

# Prerequisites

TCPDUMP analyser needs different softwares to work:

* **Python:**

You can download python on the python site:

<https://www.python.org/downloads/>

* **Openpyxl:**

If you want to have results formatted in excel from your tcpdump file, you’ll need to install the openpyxl library. Once you have installed python, you’ll need to open a terminal and write:

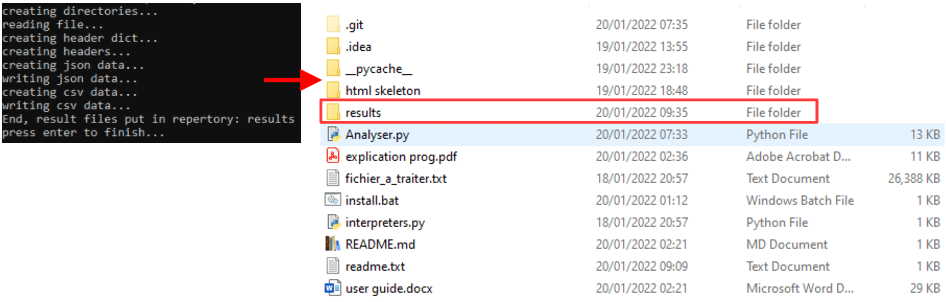


# Usage

To start using tcpdump analyser, you need to run the “analyser.py” program. A new command prompt will appear:



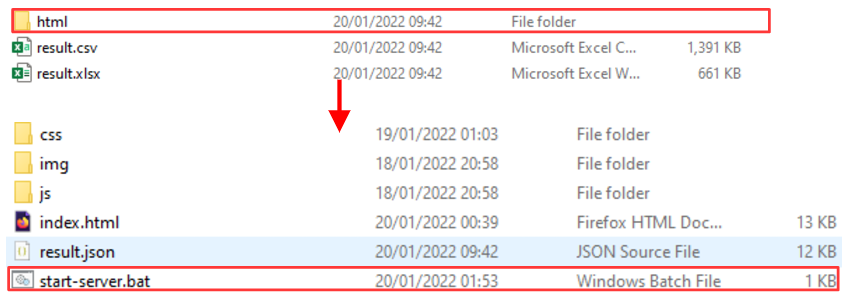
You will have to provide the file name you want to analyse (if nothing is entered, the default value will be “fichier\_a\_traiter.txt”) and then the repertory to store the results (if nothing is entered, the default value will be “results”). Once you have provided the two information the program will create the different result files in the repertory you have provided.



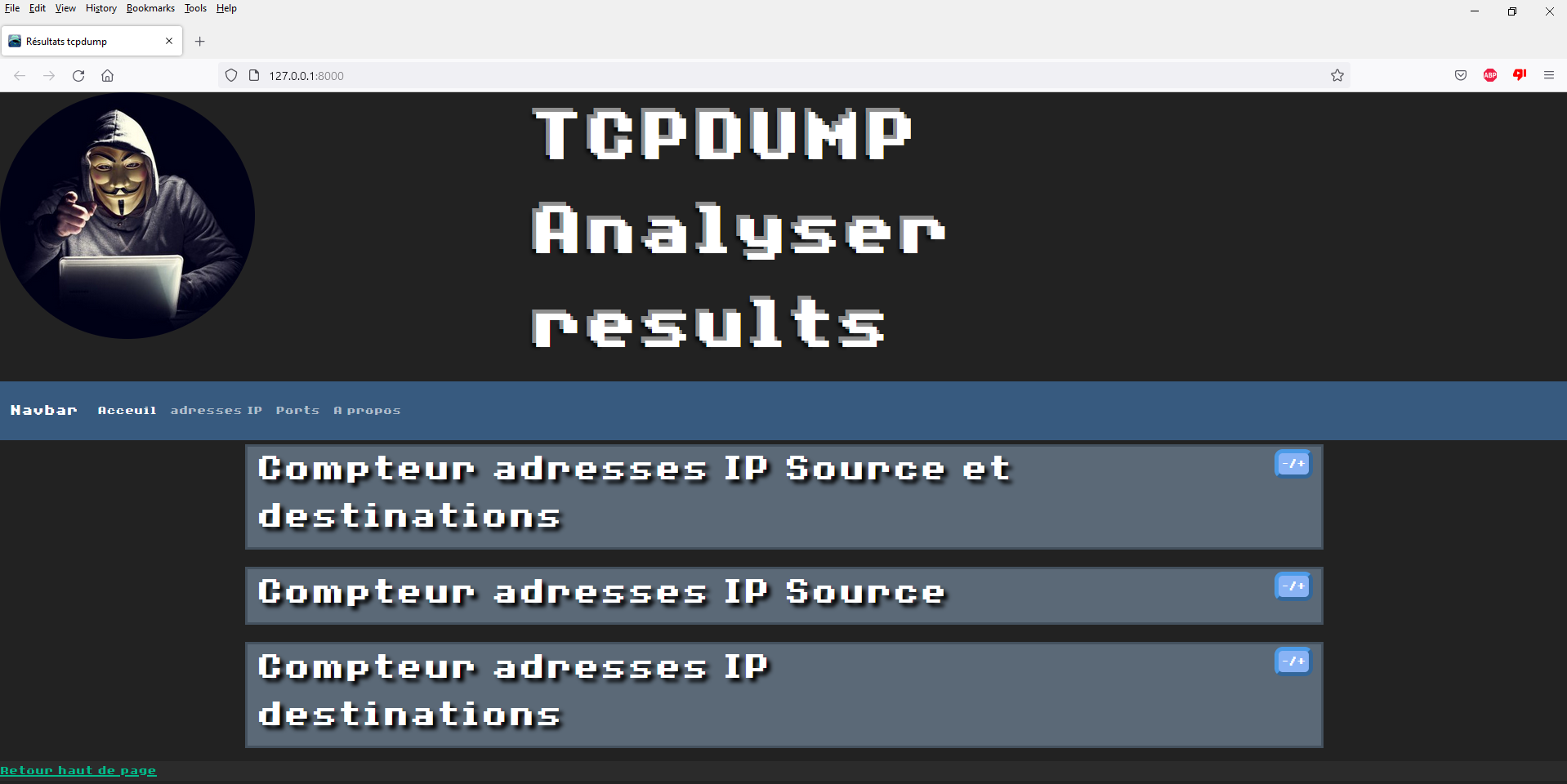
# Results

Once the program is finished, you can open the result file and check the results in different formats:

* **HTML results:**

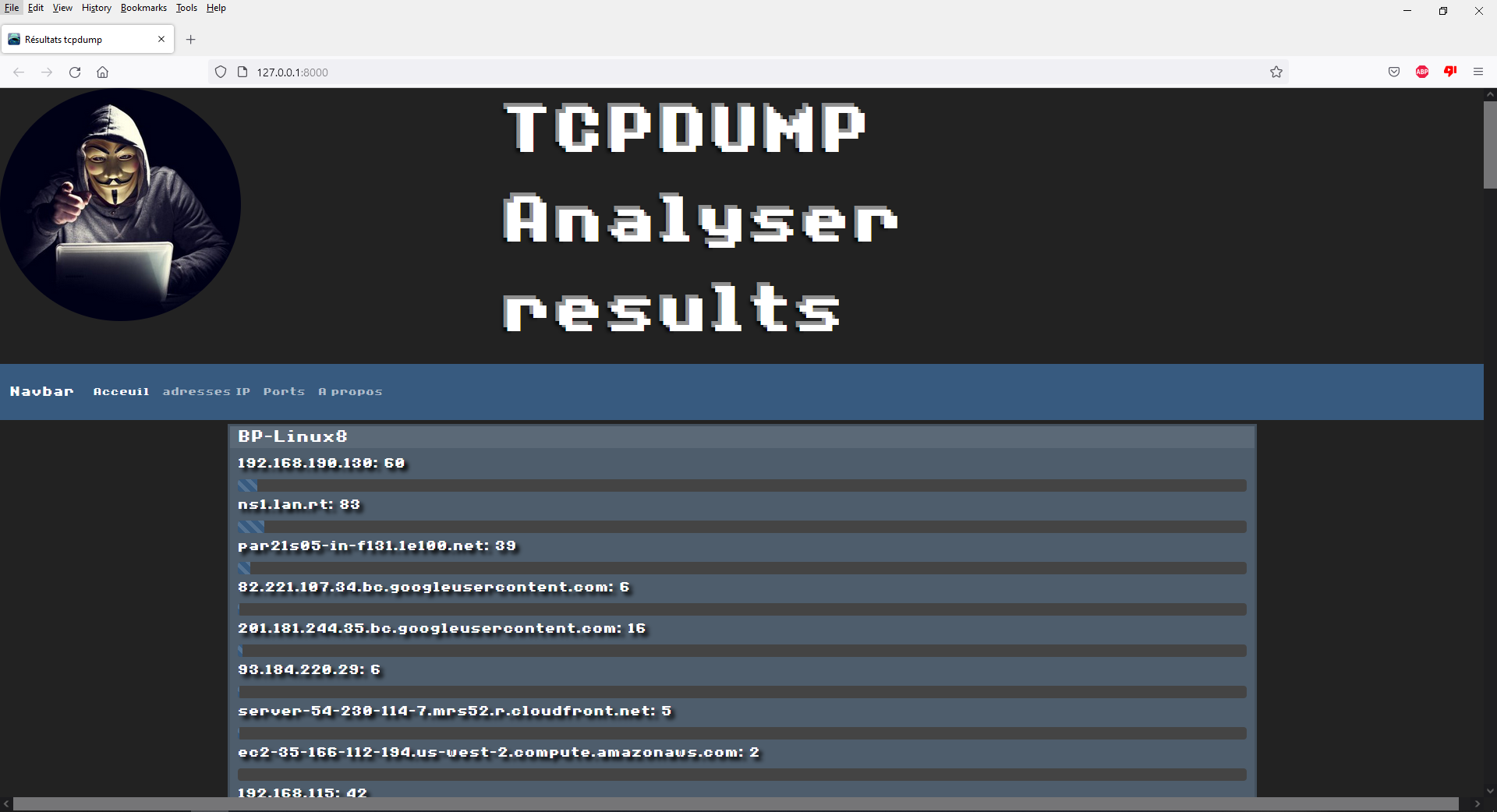


To see the results in a web browser, you’ll have to go in the html directory in the result directory and start the “start-server.bat” script. A new web browser page will open:



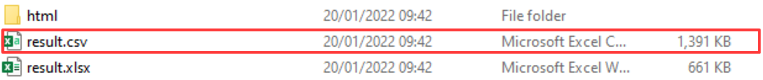
On the first page, you will find the different results:

* + The different ip addresses with the number of times they appear as destination address and source address
  + The different ip addresses with the number of times they appear as source address
  + The different ip addresses with the number of times they appear as destination address



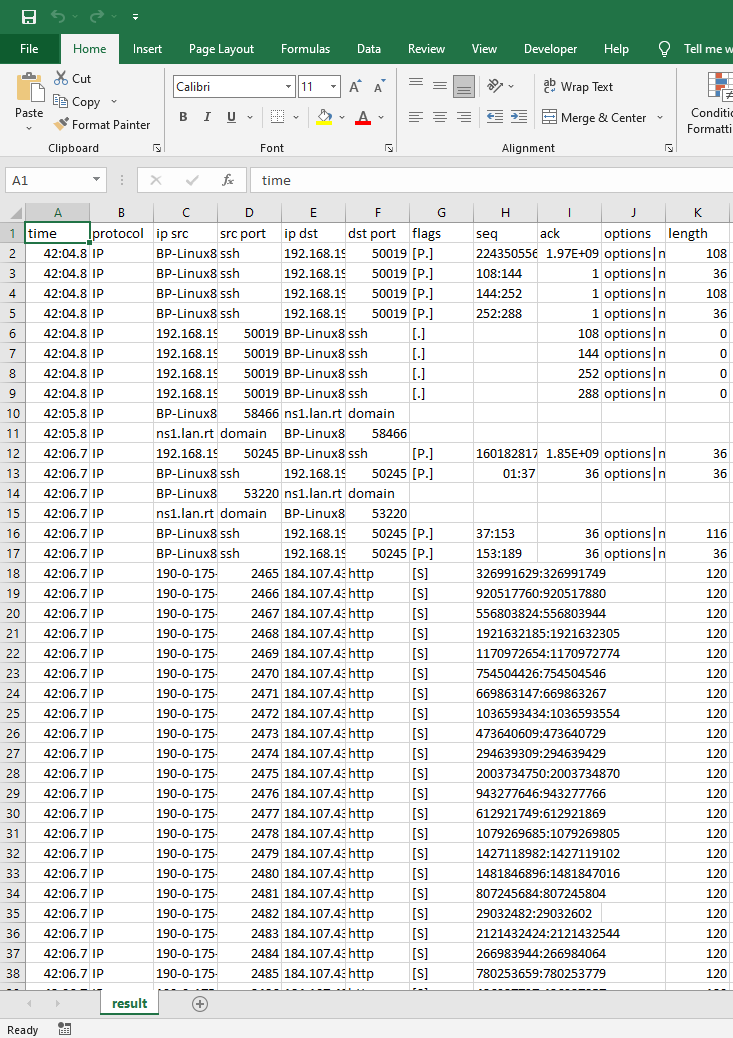
On the second page, you will find the different source addresses with the different addresses they tried to reach and the number of times they tried to reach this address.

* **CSV file:**

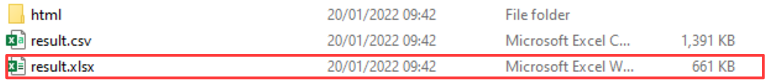


In the csv file you will only find the different packet informations separated in this order:

Time, protocol, source ip, source port, destination ip, destination port, TCP flags, sequence, ack, options, length



* **Excel file**



Finally in the excel file, you will find different sheets:

* + “Header” sheet: the same sheet as in the csv file
  + “Ip\_count” sheet: contains the different ip addresses with the number of times they appear as destination address and source address
  + IP sheets: containshe different ip addresses with the number of times they appear as source address