
SAE 15 PROJECT

Analysis of a dump file

Created by Theo Dufour

HOW TO USE

MY SAE 15 PROJECT

1. WHAT IS A TCPDUMP FILE

2. THE PYTHON CODE

3. THE EXCEL

4. CONCLUSION

What is a Tcpdump file :

1. HOW DOES THE COMMAND WORK ?

Tcpdump command is a popular network packet analysis tool which is used to view TCP/IP and other network packets transmitted over the network attached to the system on which tcpdump has been installed . Tcpdump uses the libcap library to capture network packets and is available on almost all Linux/Unix flavors.

2. WHAT IS TCPDUMP AND HOW DOES IT WORK

Tcpdump is a command line packet analyzer . It provides details of the traffic visible from a network interface .

3. IS TCPDUMP OPEN SOURCE ?

Tcpdump and libcap are open source software and anyone can contribute .

THE PYTHON CODE :

```
import csv
import pandas as pd
import sys
import webbrowser
import time
import typing
import os
from pathlib import Path
```

I started by importing these libraries

```
path = Path("ipsource")
path.mkdir(parents=True, exist_ok=True)

path = Path("flag")
path.mkdir(parents=True, exist_ok=True)

path = Path("ipdestination")
path.mkdir(parents=True, exist_ok=True)
```

After the program will create 3 directories that will serve us for the rest.

```

caractere=["IP"]#texte à rechercher

print("Démmarage du programme")

with open("Fichier_a_traiter.txt", 'r') as fichier: #ouverture du fichier
    with open("Fichier_a_traiter2.txt", "w") as file: #ouverture du 2nd fichier
        lignes = fichier.readlines()

        for ligne in lignes:
            for caracteres in caractere:
                if caracteres in ligne:
                    #print(ligne) Affiche les lignes
                    file.write(ligne) #Creer un nouveau fichier et insere variables lign
file.close() #Fermer le fichier creer

```

The program copies the lines which interest us and ignores those which do not interest us.


```

f=open('Fichier_a_traiter2.txt','r')
chaine=f.read().replace('IP',';')
f.close()
f=open('Fichier_a_traiter2.txt','w')
f.write(chaine)
f.close()
f=open('Fichier_a_traiter2.txt','r')
chaine=f.read().replace('>',';')

```

replaces the desired characters with the separator “;”

And finally to finish it create a Fichier_a_traiter2.txt but it does not stop there .

 Fichier_a_traiter.txt	07/01/2022 20:50	Document texte	26 388 Ko
 Fichier_a_traiter2.txt	18/01/2022 16:25	Document texte	1 771 Ko
 Fichier_a_traiter3.txt	18/01/2022 16:25	Document texte	1 771 Ko

In all the python code it generates 3 text files that we will retire thanks to another file that you will see later in the instruction.

```
with open("Fichier_a_traiter2.txt", 'r') as fichier: #ouverture du fichier
    with open("Fichier_a_traiter3.txt", "w") as file: #ouverture du 2nd fichier
        for ligne in lignes:
            for caracteres in caractere:
                if caracteres in ligne:
                    #print(ligne) Affiche les lignes
                    file.write(ligne)
with open("Fichier_a_traiter3.txt", 'r') as data: #réouvre le fichier creer sous un au
    ligne= data.readlines()
f=open('Fichier_a_traiter3.txt','r')
chaine=f.read().replace('IP',';')
f.close()
f=open('Fichier_a_traiter3.txt','w')
f.write(chaine)
f.close()
f=open('Fichier_a_traiter3.txt','r')
chaine=f.read().replace('>',';')
f.close()
f=open('Fichier_a_traiter3.txt','w')
f.write(chaine)
f.close()
f=open('Fichier_a_traiter3.txt','r')
chaine=f.read().replace(',',',';')
f.close()
f=open('Fichier_a_traiter3.txt','w')
f.write(chaine)
f.close()
f=open('Fichier_a_traiter3.txt','r')
chaine=f.read().replace('http',';')
f.close()
f=open('Fichier_a_traiter3.txt','w')
```

Finally it regenerates a complete file 3.

In the python program it also generates a csv file but it is not important for the rest, as well as a variable which exactly counts the number of lines in our case there are **11017** but the program displays two more.

```

with open('Fichier_a_traiter.csv','w') as fichiercsv:
    with open("Fichier_a_traiter2.txt", 'r') as data:
        writer=csv.writer(fichiercsv)
        writer.writerow(['HEURES ;IP SOURCE ;IP DESTINATION;FLAG;SEQUENCE;ACK/WIN
        writer.writerow(data)
        print("Creation du cvs + trie")

compteurligne = 0
for row in open("Fichier_a_traiter.csv"):
    compteurligne+=1
    print("Nombres de ligne dans le fichier csv: - ", compteurligne)

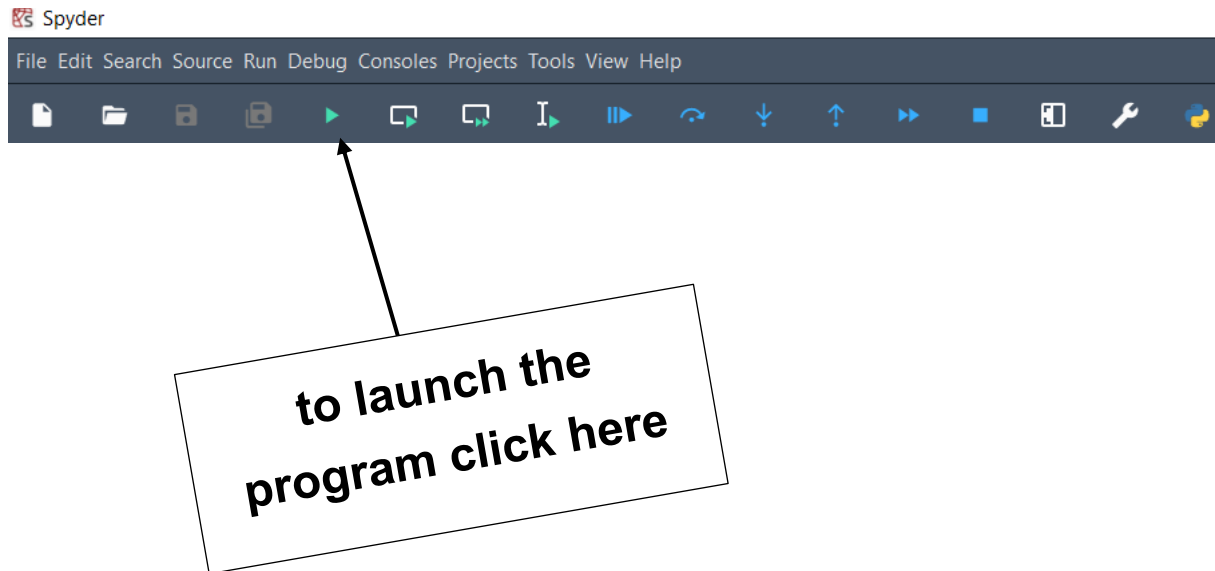
```

```

Nombres de ligne dans le fichier csv: - 11001
Nombres de ligne dans le fichier csv: - 11002
Nombres de ligne dans le fichier csv: - 11003
Nombres de ligne dans le fichier csv: - 11004
Nombres de ligne dans le fichier csv: - 11005
Nombres de ligne dans le fichier csv: - 11006
Nombres de ligne dans le fichier csv: - 11007
Nombres de ligne dans le fichier csv: - 11008
Nombres de ligne dans le fichier csv: - 11009
Nombres de ligne dans le fichier csv: - 11010
Nombres de ligne dans le fichier csv: - 11011
Nombres de ligne dans le fichier csv: - 11012
Nombres de ligne dans le fichier csv: - 11013
Nombres de ligne dans le fichier csv: - 11014
Nombres de ligne dans le fichier csv: - 11015
Nombres de ligne dans le fichier csv: - 11016
Nombres de ligne dans le fichier csv: - 11017
Nombres de ligne dans le fichier csv: - 11018
Nombres de ligne dans le fichier csv: - 11019
Nombres de ligne dans le fichier csv: - 11020

```

To launch the program you just click above on the play button in the spyder interface



And normally y should execute.
We are done with the python code.

If you want to see the result click on this link to see a short video : [LINK VIDEO](#)

THE EXCEL CODE :

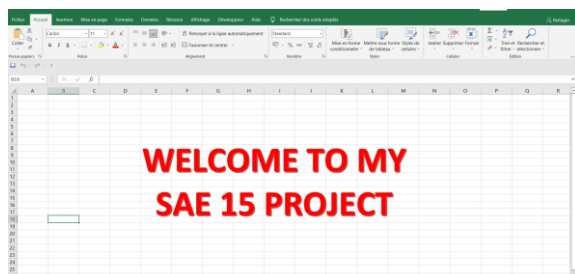
Now that you have generated the 2 new text files and folders we will reuse them thanks to MS Excel.

flag	18/01/2022 17:15	Dossier de fichiers	
ipdestination	18/01/2022 16:28	Dossier de fichiers	
ipsource	18/01/2022 13:58	Dossier de fichiers	
Fichier_a_traiter.csv	18/01/2022 18:58	Fichier CSV Micros...	1 804 Ko
Fichier_a_traiter.txt	07/01/2022 20:50	Document texte	26 388 Ko
Fichier_a_traiter2.txt	18/01/2022 18:58	Document texte	1 771 Ko
Fichier_a_traiter3.txt	18/01/2022 18:58	Document texte	1 771 Ko

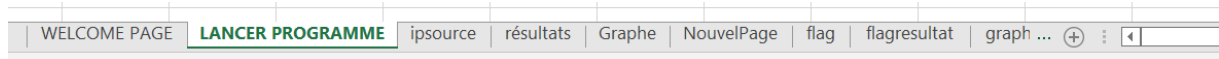
Normally you should have this

triefinal.xlsm	18/01/2022 17:29	Feuille de calcul M...	215 Ko
----------------	------------------	------------------------	--------

After this click on the second file named triefinal.xlsm



This is the home page of the project



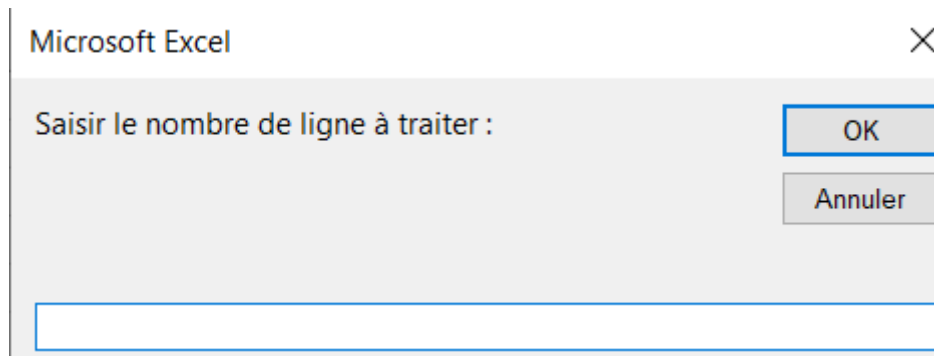
click just below on
launch a program



You will see a page with a write button launch the program.

Click on the button

Select Fichier_a_traiter2.txt



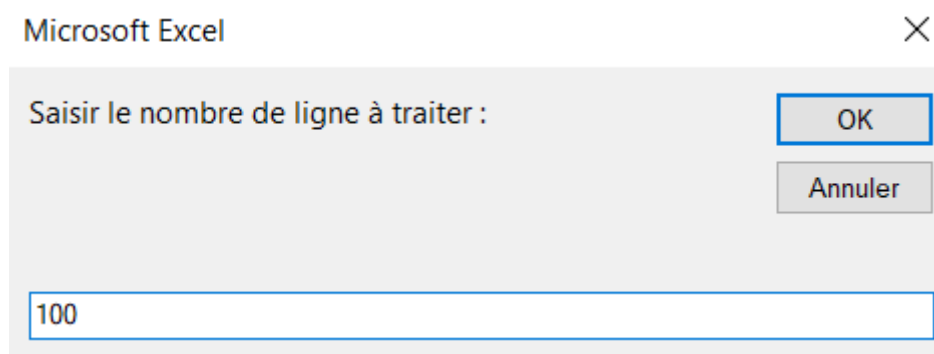
Microsoft Excel

Saisir le nombre de ligne à traiter :

OK

Annuler

Select the number of rows you want to process



Microsoft Excel

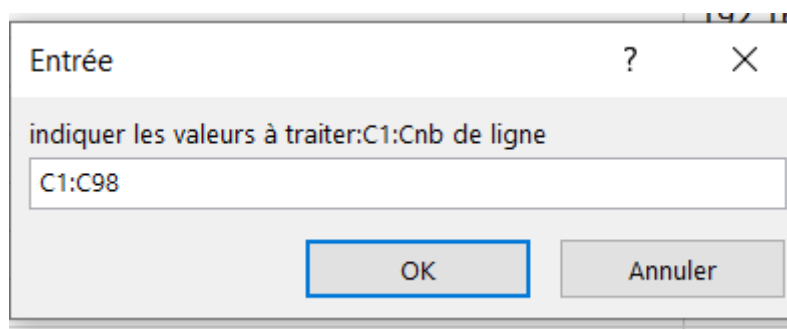
Saisir le nombre de ligne à traiter :

OK

Annuler

100

For exemple : 100



Entrée

indiquer les valeurs à traiter:C1:Cnb de ligne

C1:C98

OK

Annuler

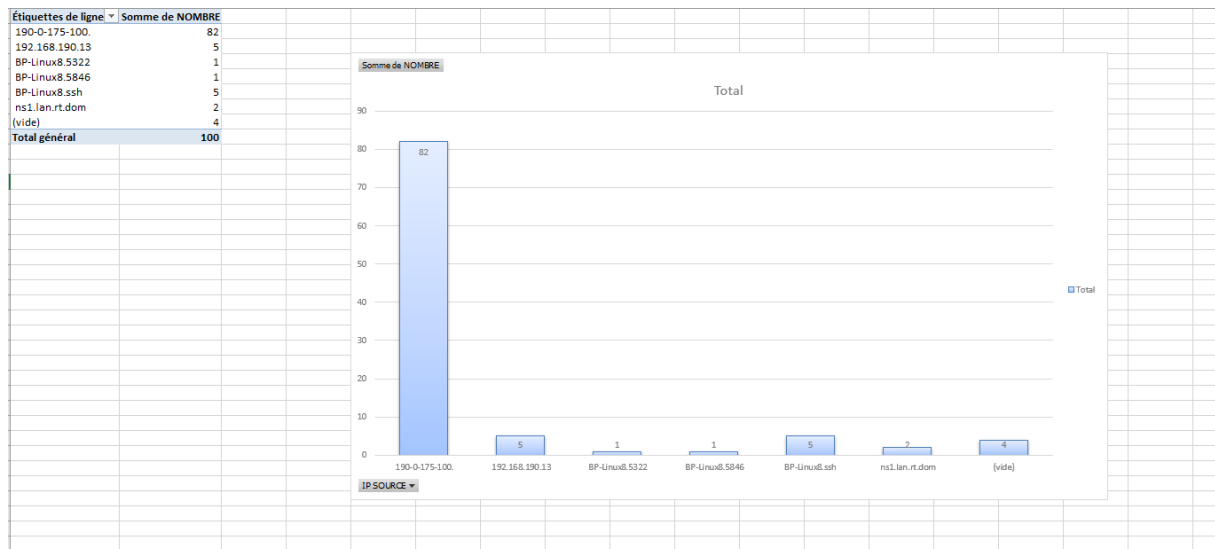
Indicate the values to be processed by putting
C1:Clinenumber



If you want to analyze 100 lines you have to put 98 because the program count +2

Étiquettes de lignes ▼	Somme de NOMBRE
190-0-175-100.	82
192.168.190.13	5
BP-Linux8.5322	1
BP-Linux8.5846	1
BP-Linux8.ssh	5
ns1.lan.rt.dom	2
(vide)	4
Total général	100

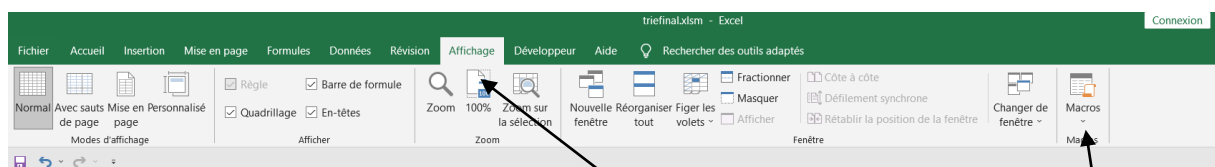
We therefore treated our 100 values well

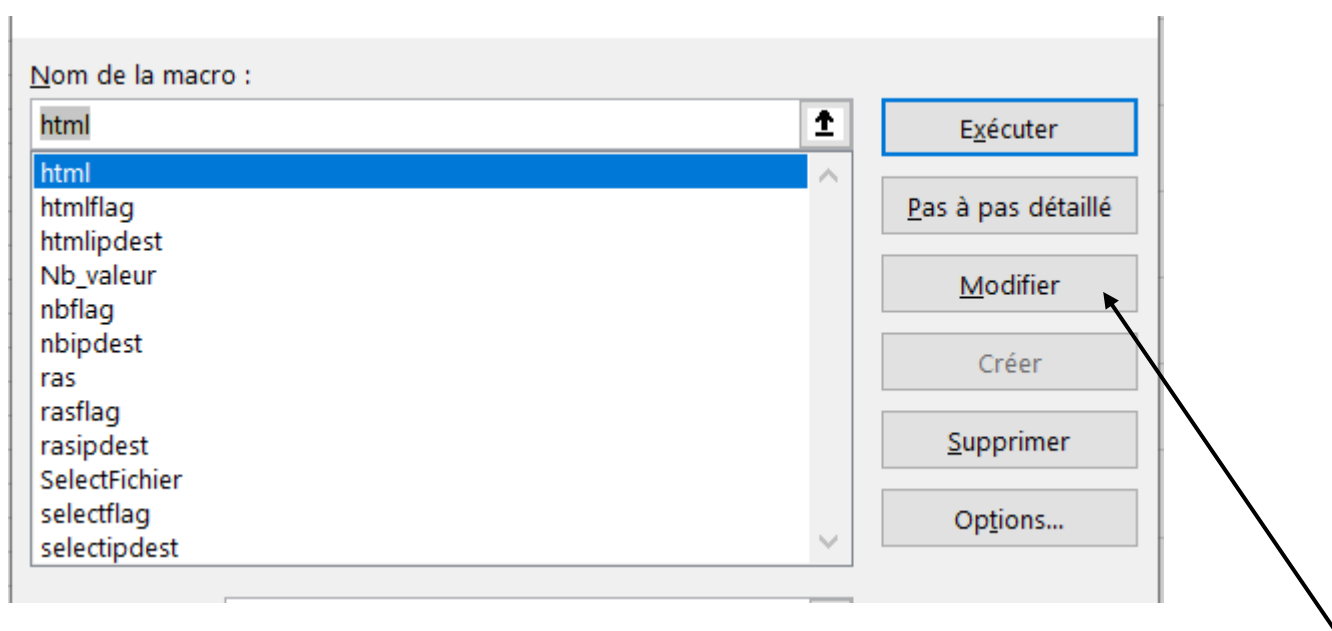
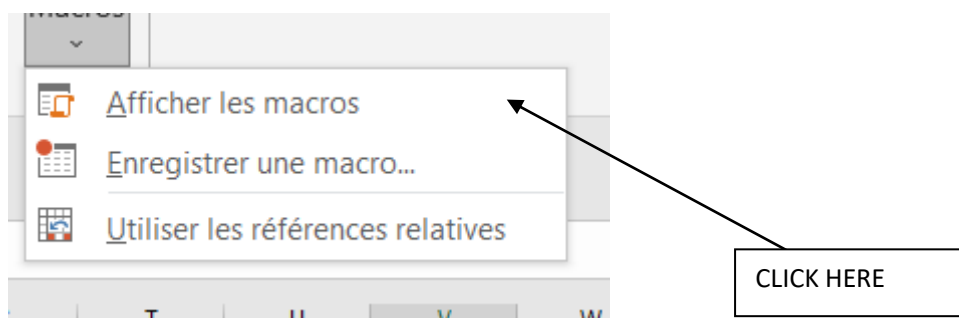


And thanks to a dynamic table it shows us the stick diagram of the ipsource .

In my program we can choose to trill the source / destination ip as well as the flags.

Now to generate the html page there is a button just below the group named html click on it, but be careful to check and replace the destination folder of the web page in the macro named html.





CONCLUSION

If you have followed these steps, step by step, you are in a position to carry out an analysis.

Made By Theo Dufour

