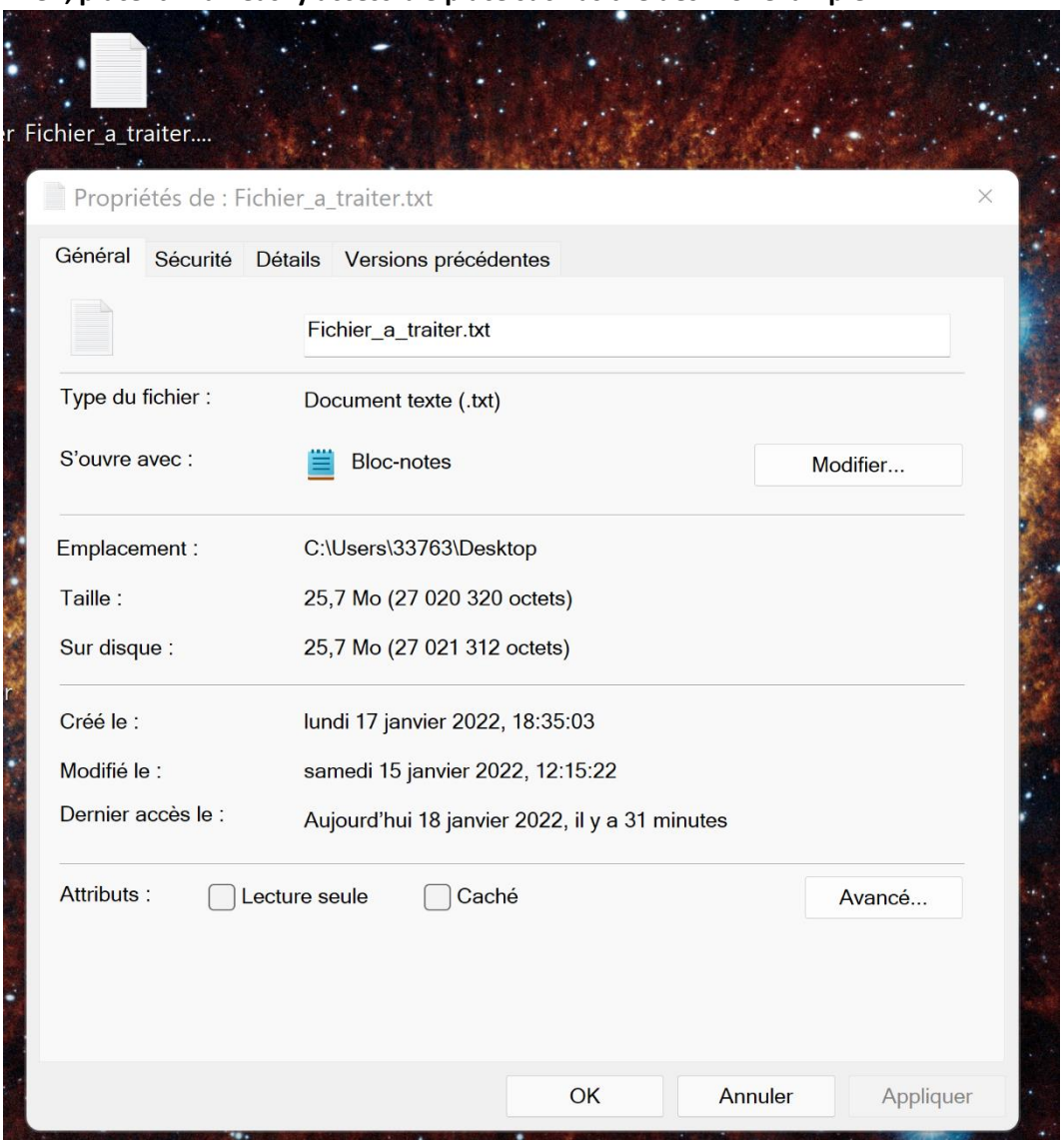
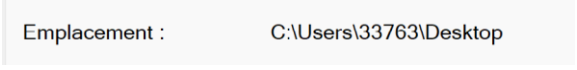
Tutorial of the use of my program

How can you use my program to sort a tcpdump file and analyze the results that interest us?

First, upload your tcpdump file and give it a name. For my part, its name is "Fichier_a_traiter.txt". Then, place it in an easily accessible place such as the desk for example.





For me the location is « C:\Users\33763\Desktop ».

Then open the sae15.py program with software such as Spyder to make sure the program works with the modules I used.

Go to line 5 of the file and specify the path you copied previously, while not forgetting to add "/nameofyourfile" at the end of the location. Second step: replace all the "\" in your path with "/" because python does not understand the "\" of Windows.

In my case it gives that:

```
file = open('C:/Users/33763/Desktop/Fichier_a_traiter.txt', "r")
```

Then go to line 302, you will put the path you want here, the program will create an html page at the place you specify, I advise you to do it in the same place as the one mentioned above : on the desktop.

For me the path is this:

```
c = open('C:/Users/33763/Desktop/page.html', 'w')
```

My file will be named "page.html" (html being the extension, you should not touch it) however you can name your file as you wish, it can for example be named "mypage.html"

Then go to line 460, here you will put the path for the automatic creation of the first csv file usable by excel which will contain the sorted data of the tcpdump file.

Again, in order not to get lostI advise you to put it on the desk.

This is the path for me :

```
with open('C:/Users/33763/Desktop/donnees.csv', 'w',
```

Which is « C:/Users/33763/Desktop/donnees.csv ».

Here you can change the name of the file again (therefore replace "donnees" with something else) but do not touch the extension (.csv) otherwise the file will not be the one expected.

Then go to line 467, you will do the same thing as before but to create a second csv file usable by excel which will be statistics concerning the tcpdump file.

Here is the link for me:

```
with open('C:/Users/33763/Desktop/statistiques.csv', 'w',
```

You can change the "statistiques" which corresponds to the name of the file but do not touch the extension, as before.

If you put the same link each time (the link that points to your desktop) you are sure not to get lost and then find all your files created by the python program.

Then go to line 174 and 184, here you have 2 paths to modify. I advise you to put the same path that points to your desktop.

If you want you can change the names of the 2 graphs by replacing "graphique" and "graphique2" by the name of your choice.

(These are the link to modify):

```
("C:/Users/33763/Desktop/graphique.png")
```

```
"C:/Users/33763/Desktop/graphique2.png")
```

2 last steps:

Go to lines 206 and 231, you will copy the paths entered lines 174 and 184 to line 206 and 231 respectively.

My paths are as follows:

```
"C:/Users/33763/Desktop/graphique.png"
```

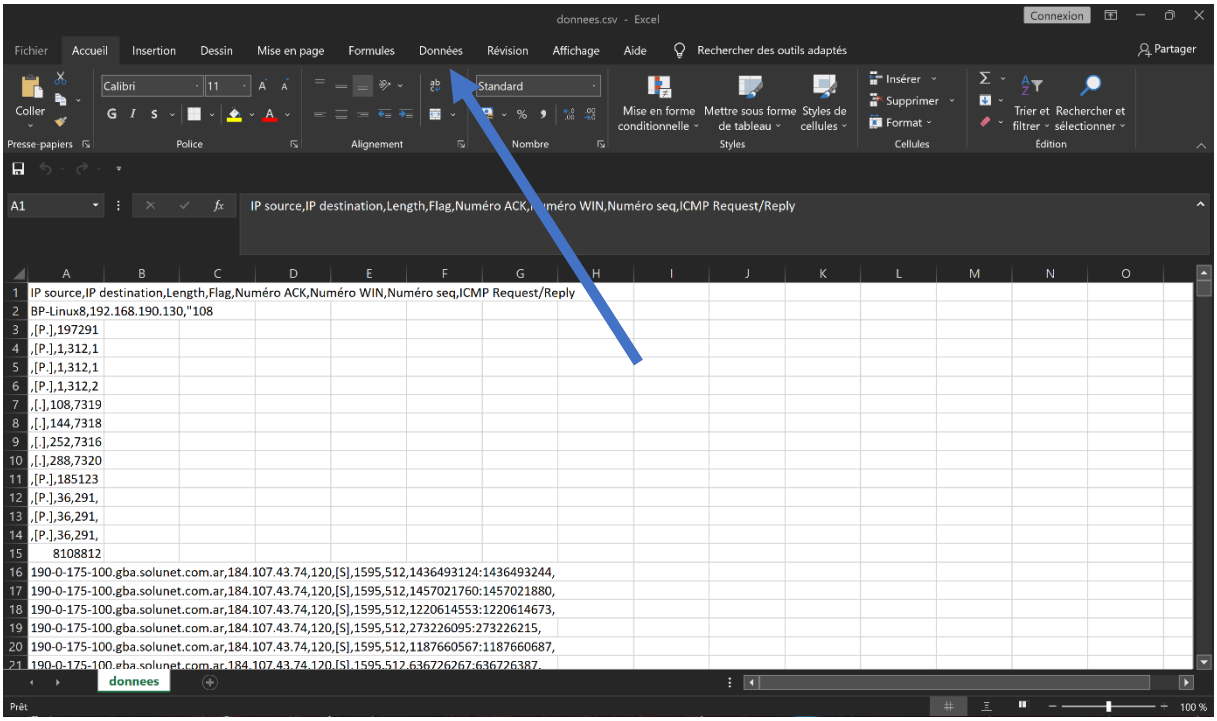
```
"C:/Users/33763/Desktop/graphique2.png"
```

Once these steps are completed, you can launch the program. If it doesn't work, make sure you have changed the "\" to "/" and that you have the right path. To check the correct path, just right click on a file on the desktop, for example, to see the file path (its location), as explained at the beginning.

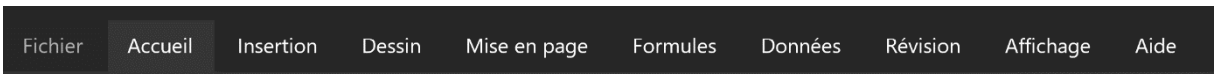
The files should appear on your desktop if you took the same paths than me.

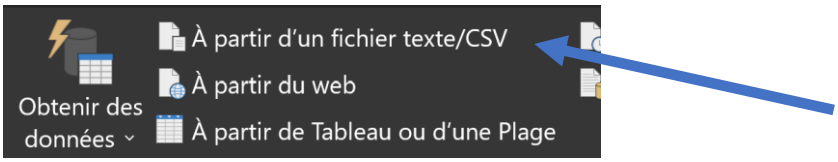
Then open the first csv file with excel.

This should appear :

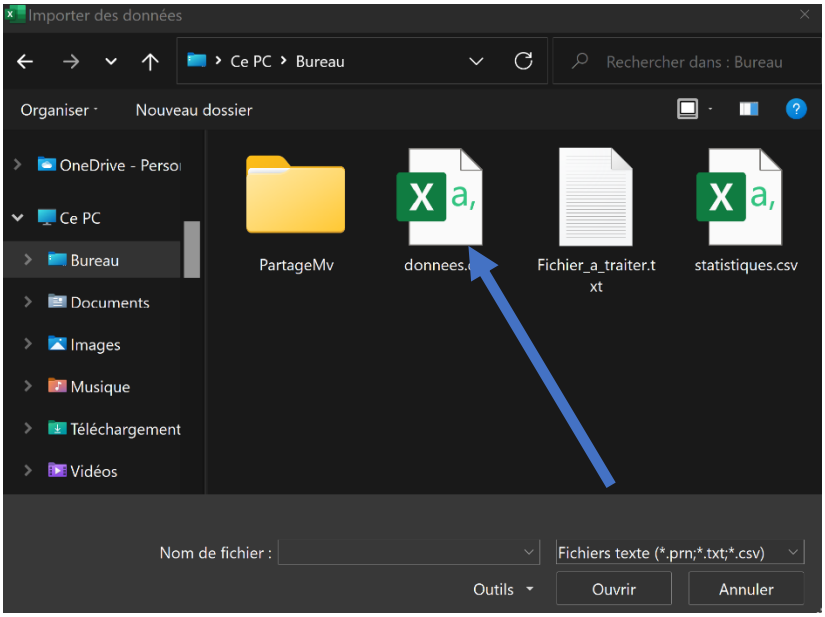


Then click on data (here in french it's données).

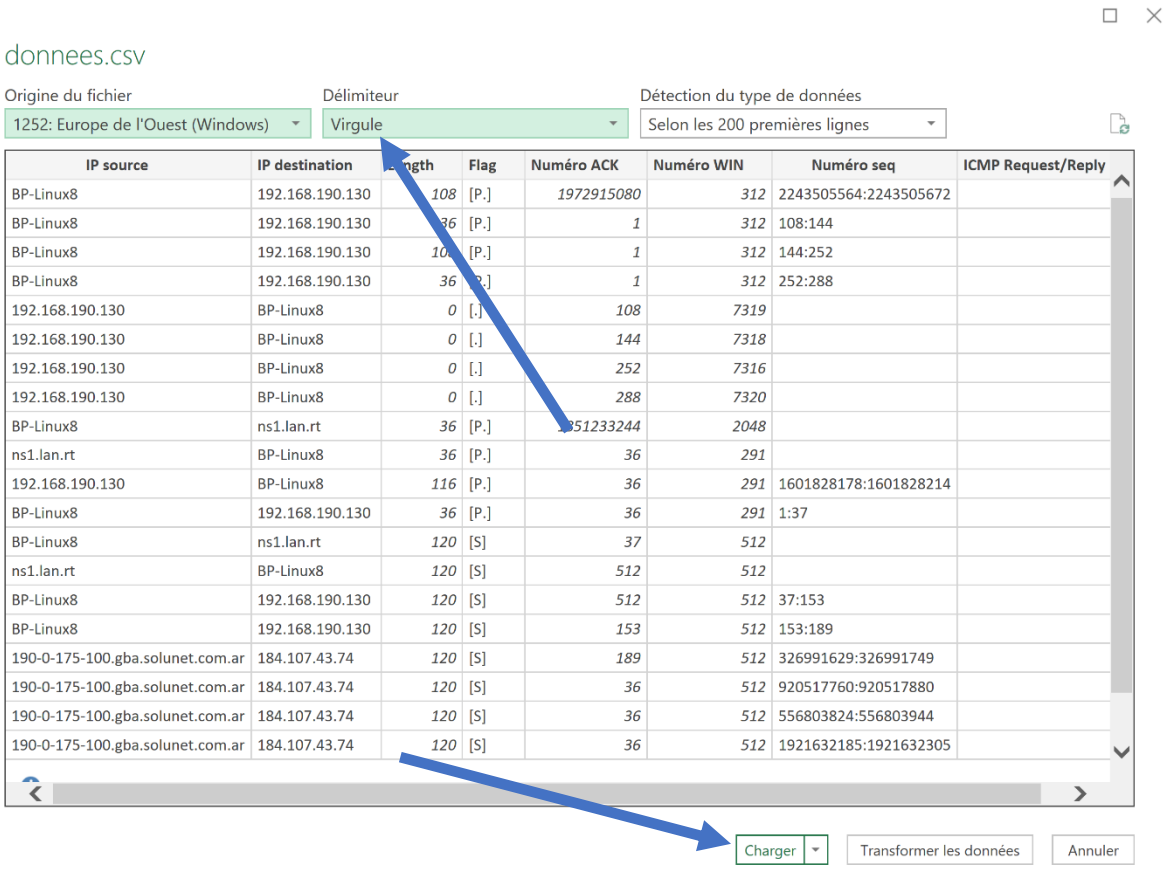




Then click to "From text/CSV file" (in french it's "A partir d'un fichier texte/CSV")



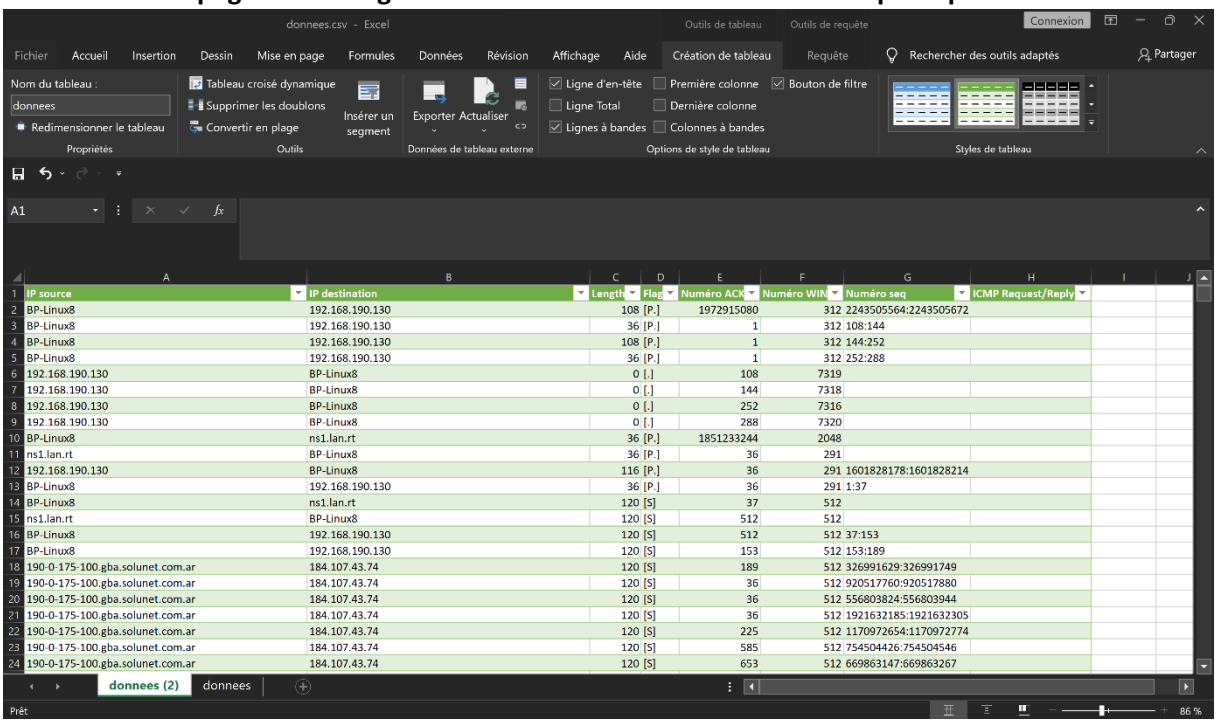
Then select the file you just launched, so mine was donnees.csv.



IP source	IP destination	Length	Flag	Numéro ACK	Numéro WIN	Numéro seq	ICMP Request/Reply
BP-Linux8	192.168.190.130	108	[P.]	1972915080	312	2243505564:2243505672	
BP-Linux8	192.168.190.130	36	[P.]	1	312	108:144	
BP-Linux8	192.168.190.130	10	[P.]	1	312	144:252	
BP-Linux8	192.168.190.130	36	[P.]	1	312	252:288	
192.168.190.130	BP-Linux8	0	[.]	108	7319		
192.168.190.130	BP-Linux8	0	[.]	144	7318		
192.168.190.130	BP-Linux8	0	[.]	252	7316		
192.168.190.130	BP-Linux8	0	[.]	288	7320		
BP-Linux8	ns1.lan.rt	36	[P.]	1951233244	2048		
ns1.lan.rt	BP-Linux8	36	[P.]	36	291		
192.168.190.130	BP-Linux8	116	[P.]	36	291	1601828178:1601828214	
BP-Linux8	192.168.190.130	36	[P.]	36	291	1:37	
BP-Linux8	ns1.lan.rt	120	[S]	37	512		
ns1.lan.rt	BP-Linux8	120	[S]	512	512		
BP-Linux8	192.168.190.130	120	[S]	512	512	37:153	
BP-Linux8	192.168.190.130	120	[S]	153	512	153:189	
190-0-175-100.gba.solunet.com.ar	184.107.43.74	120	[S]	189	512	326991629:326991749	
190-0-175-100.gba.solunet.com.ar	184.107.43.74	120	[S]	36	512	920517760:920517880	
190-0-175-100.gba.solunet.com.ar	184.107.43.74	120	[S]	36	512	556803824:556803944	
190-0-175-100.gba.solunet.com.ar	184.107.43.74	120	[S]	36	512	1921632185:1921632305	

Then select as delimiter the comma and finally press the loader.

Here is the first page containing the useful informations of the sorted tcpdump.

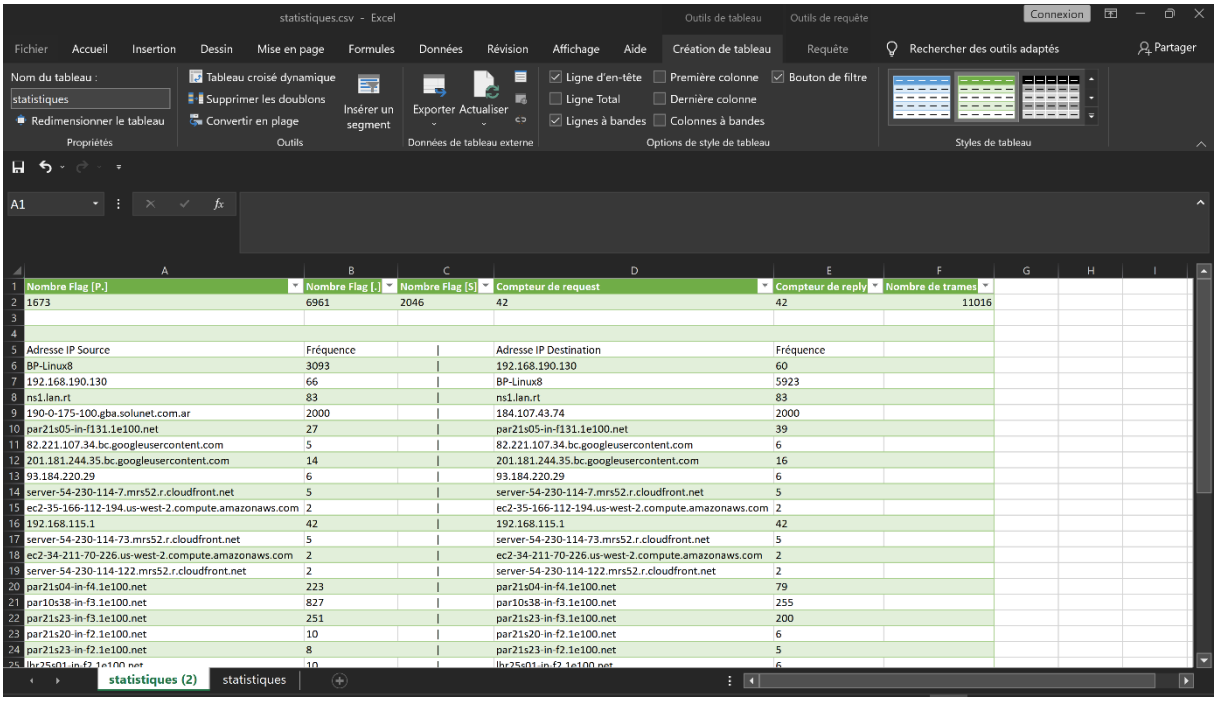


donnees.csv - Excel

IP source	IP destination	Length	Flag	Numéro ACK	Numéro WIN	Numéro seq	ICMP Request/Reply
BP-Linux8	192.168.190.130	108	[P.]	1972915080	312	2243505564:2243505672	
BP-Linux8	192.168.190.130	36	[P.]	1	312	108:144	
BP-Linux8	192.168.190.130	108	[P.]	1	312	144:252	
BP-Linux8	192.168.190.130	36	[P.]	1	312	252:288	
192.168.190.130	BP-Linux8	0	[.]	108	7319		
192.168.190.130	BP-Linux8	0	[.]	144	7318		
192.168.190.130	BP-Linux8	0	[.]	252	7316		
192.168.190.130	BP-Linux8	0	[.]	288	7320		
BP-Linux8	ns1.lan.rt	36	[P.]	1851233244	2048		
ns1.lan.rt	BP-Linux8	36	[P.]	36	291		
192.168.190.130	BP-Linux8	116	[P.]	36	291	1601828178:1601828214	
BP-Linux8	192.168.190.130	36	[P.]	36	291	1:37	
BP-Linux8	ns1.lan.rt	120	[S]	37	512		
ns1.lan.rt	BP-Linux8	120	[S]	512	512		
BP-Linux8	192.168.190.130	120	[S]	512	512	37:153	
BP-Linux8	192.168.190.130	120	[S]	153	512	153:189	
190-0-175-100.gba.solunet.com.ar	184.107.43.74	120	[S]	189	512	326991629:326991749	
190-0-175-100.gba.solunet.com.ar	184.107.43.74	120	[S]	36	512	920517760:920517880	
190-0-175-100.gba.solunet.com.ar	184.107.43.74	120	[S]	36	512	556803824:556803944	
190-0-175-100.gba.solunet.com.ar	184.107.43.74	120	[S]	36	512	1921632185:1921632305	
190-0-175-100.gba.solunet.com.ar	184.107.43.74	120	[S]	225	512	1170972654:1170972774	
190-0-175-100.gba.solunet.com.ar	184.107.43.74	120	[S]	585	512	754504426:754504546	
190-0-175-100.gba.solunet.com.ar	184.107.43.74	120	[S]	653	512	669863147:669863267	

Do the same for the second file, so you have to : launch it, click on "Data", then "From a CSV file", select the second the csv file you have just opened, then put the comma as a delimiter and finally "Load".

You should see these stats appear here:



statistiques.csv - Excel

Nombre Flag [P.]	Nombre Flag [.]	Nombre Flag [S]	Compteur de request	Compteur de reply	Nombre de trames
1673	6961	2046	42	42	11016

Adresse IP Source	Fréquence	Adresse IP Destination	Fréquence
BP-Linux8	3093	192.168.190.130	60
192.168.190.130	66	BP-Linux8	5923
ns1.lan.rt	83	ns1.lan.rt	83
190-0-175-100.gba.solunet.com.ar	2000	184.107.43.74	2000
par21s05-in-f131.1e100.net	27	par21s05-in-f131.1e100.net	39
82.221.107.34.bc.googleusercontent.com	5	82.221.107.34.bc.googleusercontent.com	6
201.181.244.35.bc.googleusercontent.com	14	201.181.244.35.bc.googleusercontent.com	16
93.184.220.29	6	93.184.220.29	6
server-54-230-114-7.mrs52.r.cloudfront.net	5	server-54-230-114-7.mrs52.r.cloudfront.net	5
ec2-35-166-112-194.us-west-2.compute.amazonaws.com	2	ec2-35-166-112-194.us-west-2.compute.amazonaws.com	2
192.168.115.1	42	192.168.115.1	42
server-54-230-114-73.mrs52.r.cloudfront.net	5	server-54-230-114-73.mrs52.r.cloudfront.net	5
ec2-34-211-70-226.us-west-2.compute.amazonaws.com	2	ec2-34-211-70-226.us-west-2.compute.amazonaws.com	2
server-54-230-114-122.mrs52.r.cloudfront.net	2	server-54-230-114-122.mrs52.r.cloudfront.net	2
par21s04-in-f4.1e100.net	223	par21s04-in-f4.1e100.net	79
par10s38-in-f3.1e100.net	827	par10s38-in-f3.1e100.net	255
par21s23-in-f3.1e100.net	251	par21s23-in-f3.1e100.net	200
par21s20-in-f2.1e100.net	10	par21s20-in-f2.1e100.net	6
par21s23-in-f2.1e100.net	8	par21s23-in-f2.1e100.net	5

You can now launch your html page, go to where you specified the path, if you did like me it will be on your Desktop, and you just have to double click on it and select your favourite browser if the page doesn't start automatically.

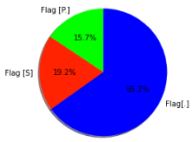
Here's what you should have:

Informations sur le fichier

Nombre de trames au total

Trames dans ce fichier : 11016

Fréquences des flags

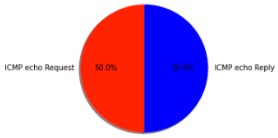


Signification des différents Flags

"S" -> SYN "F" -> FIN "." -> ACK "P" -> PUSH "R" -> STOP

Flag [P.]: 1673 fois
Flag [.]: 6961 fois
Flag [S]: 2046 fois

Nombre de request et de reply



Request : 42 fois
Adresse source : BP-Linux8

Reply : 42 fois
Adresse destination : 192.168.115.1

Légende des fréquences des IP sources et destination

Légende des fréquences des IP sources et destination

Fréquence >= ou égal à 200
Fréquence supérieur à 500
Fréquence supérieur à 1000
Fréquence supérieur à 2000
Fréquence supérieur à 3000

Fréquences des IP sources les plus élevées

BP-Linux8 : 3093 190-0-175-100.gba.solunet.com.ar : 2000 par21s04-in-f4.1e100.net : 223 par10s38-in-f3.1e100.net : 827
par21s23-in-f3.1e100.net : 251 mauves.univ-st-etienne.fr : 1687 www.aggloroanne.fr : 2130

Fréquences des IP destination les plus élevées

BP-Linux8 : 5923 184.107.43.74 : 2000 par10s38-in-f3.1e100.net : 255 par21s23-in-f3.1e100.net : 200
mauves.univ-st-etienne.fr : 751 www.aggloroanne.fr : 1022