Instruction for use

Program code

```
import re
import os
import csv
from collections import Counter
import matplotlib.pyplot as plt
import pandas as pd
import numpy as np

file = open('sae15.txt', 'r')

lines = "DATE, IP SOURCE, IP DESTINATION, FLAG, SEQUENCE, ACK, WIN, OPTION, LENGTH \n"
for line in file:
    m = re.findall("..:..:..", line)
    for x in m:
        lines +=  line

lines = lines.replace(">", "")
lines = lines.replace("Flags", "")
lines = lines.replace("seq", "")
lines = lines.replace("ack", "")
lines = lines.replace("win", "")
lines = lines.replace("option", "")
lines = lines.replace("length", "")
lines = lines.replace("IP", "")

lines = lines.replace(",", " ")
lines = lines.replace("  ", ",")

lines = lines.replace(" ", "")



myText = open(r'lines.csv', 'w')
myText.write(lines)
myText.close()
```

```
file = open('lines.csv')
reader = csv.reader(file)

ip_source = []
ip_destination = []

for line in reader:
    source = line[1]
    destination = line[2]
    source = line[1].rsplit(".",1)[0]
    destination = line[2].rsplit(".",1)[0]

    ip_source.append(source)
    ip_destination.append(destination)



src = Counter(ip_source)
tri_src = {val[0] : val[1] for val in sorted(src.items(), key = lambda x: (-x[1], x[0]))}
print(list(tri_src.items())[:5])


dst = Counter(ip_destination)


tri_dest = {val[0] : val[1] for val in sorted(dst.items(), key = lambda x: (-x[1], x[0]))}
print(list(tri_dest.items())[:5])
```

Choosing input and output

- In the variable file, in the open function between the ‘ ’, you need to put the name of the tcp dump file. (sae15.txt in my case)

```
file = open('sae15.txt', 'r')
```

- In the variable myText, in the open function between the ‘ ’, you can choose the output csv file name. (lines.csv in my case)

```
myText = open(r'lines.csv', 'w')
```

Example of output in csv :

	A	B	C	D	E	F	G	H	
1	DATE	SOURCE	DESTINATION	FLAG	SEQUENCE	ACK	WIN	OPTION	LENGT
2	11:42:04.766656	BP-Linux8.ssh	192.168.190.13(	[P.]	2243505564:224	1972915080	312	s[nopnopTSval1	
3	11:42:04.766694	BP-Linux8.ssh	192.168.190.13(	[P.]	110:24:00	1	312	s[nopnopTSval1	
4	11:42:04.766723	BP-Linux8.ssh	192.168.190.13(	[P.]	148:12:00	1	312	s[nopnopTSval1	
5	11:42:04.766744	BP-Linux8.ssh	192.168.190.13(	[P.]	256:48:00	1	312	s[nopnopTSval1	
6	11:42:04.785366	192.168.190.13(	BP-Linux8.ssh:	[.]	108	7319	s[nopnopTSval3	0	
7	11:42:04.785384	192.168.190.13(	BP-Linux8.ssh:	[.]	144	7318	s[nopnopTSval3	0	
8	11:42:04.785406	192.168.190.13(	BP-Linux8.ssh:	[.]	252	7316	s[nopnopTSval3	0	
9	11:42:04.785454	192.168.190.13(	BP-Linux8.ssh:	[.]	288	7320	s[nopnopTSval3	0	
10	11:42:05.768334	BP-Linux8.5846(	ns1.lan.rt.domain:16550+PTR?130.190.168.192.in-addr.arpa.(46)						
11	11:42:05.769075	ns1.lan.rt.domai	BP-Linux8.58466:16550NXDomain0/1/0(112)						
12	11:42:06.669393	192.168.190.13(	BP-Linux8.ssh:	[P.]	1601828178:160	1851233244	2048	s[nopnopTSval3	
13	11:42:06.669906	BP-Linux8.ssh	192.168.190.13(	[P.]	01:37	36	291	s[nopnopTSval1	
14	11:42:06.679262	BP-Linux8.5322(	ns1.lan.rt.domain:54801+A?lacampora.org.(31)						
15	11:42:06.679971	ns1.lan.rt.domai	BP-Linux8.53220:548011/0/0A184.107.43.74(47)						
16	11:42:06.681188	BP-Linux8.ssh	192.168.190.13(	[P.]	39:33:00	36	291	s[nopnopTSval1	
17	11:42:06.681222	BP-Linux8.ssh	192.168.190.13(	[P.]	156:09:00	36	291	s[nopnopTSval1	
18	11:42:06.681248	190-0-175-100.g	184.107.43.74.h	[S]	326991629:3269	512	120:HTTP		
19	11:42:06.681274	190-0-175-100.g	184.107.43.74.h	[S]	920517760:9205	512	120:HTTP		
20	11:42:06.681294	190-0-175-100.g	184.107.43.74.h	[S]	556803824:5568	512	120:HTTP		
21	11:42:06.681312	190-0-175-100.g	184.107.43.74.h	[S]	1921632185:192	512	120:HTTP		
22	11:42:06.681328	190-0-175-100.g	184.107.43.74.h	[S]	1170972654:117	512	120:HTTP		
23	11:42:06.681345	190-0-175-100.g	184.107.43.74.h	[S]	754504426:7545	512	120:HTTP		
24	11:42:06.681362	190-0-175-100.g	184.107.43.74.h	[S]	669863147:6698	512	120:HTTP		
25	11:42:06.681379	190-0-175-100.g	184.107.43.74.h	[S]	1036593434:103	512	120:HTTP		

In the output you will also see the number of duplicate

example :

```
========================= RESTART: /Users/shaku/Desktop/sae15/sae15.py =========================
[('BP-Linux8', 3093), ('www.aggloroanne.fr', 2130), ('190-0-175-100.gba.solunet.com.ar', 2000
), ('mauves.univ-st-etienne.fr', 1687), ('par10s38-in-f3.1e100.net', 827)]


[('BP-Linux8', 5813), ('184.107.43.74', 2000), ('www.aggloroanne.fr', 1022), ('mauves.univ-st
-etienne.fr', 751), ('par10s38-in-f3.1e100.net', 255)]
```