TCPDUMP Analyser User guide

1 Prerequisites

TCPDUMP analyser needs different softwares to work:

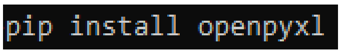
- **Python:**

You can download python on the python site:

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

- **Openpyxl:**

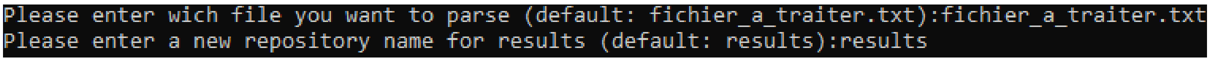
If you want to have results formatted in excel from your tcpdump file, you'll need to install the openpyxl library. Once you have installed python, you'll need to open a terminal and write:



```
pip install openpyxl
```

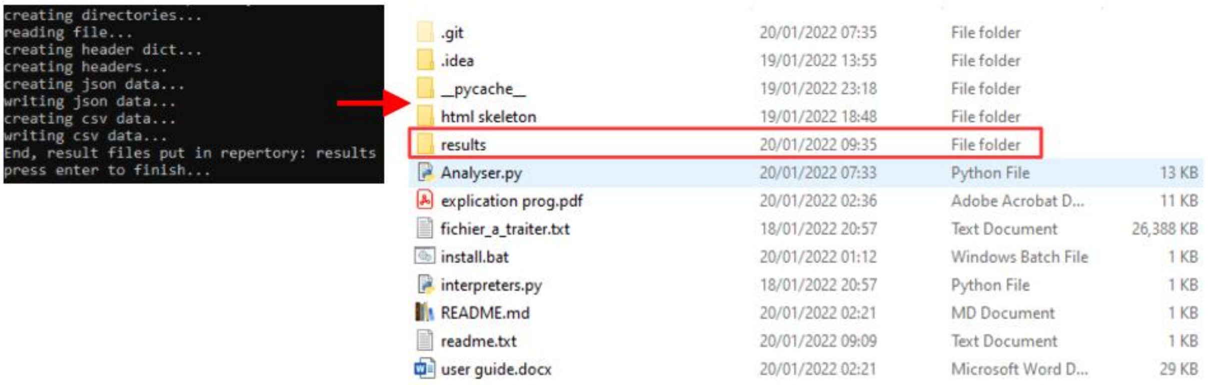
2 Usage

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



```
Please enter wich file you want to parse (default: fichier_a_traiter.txt):fichier_a_traiter.txt
Please enter a new repository name for results (default: results):results
```

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.



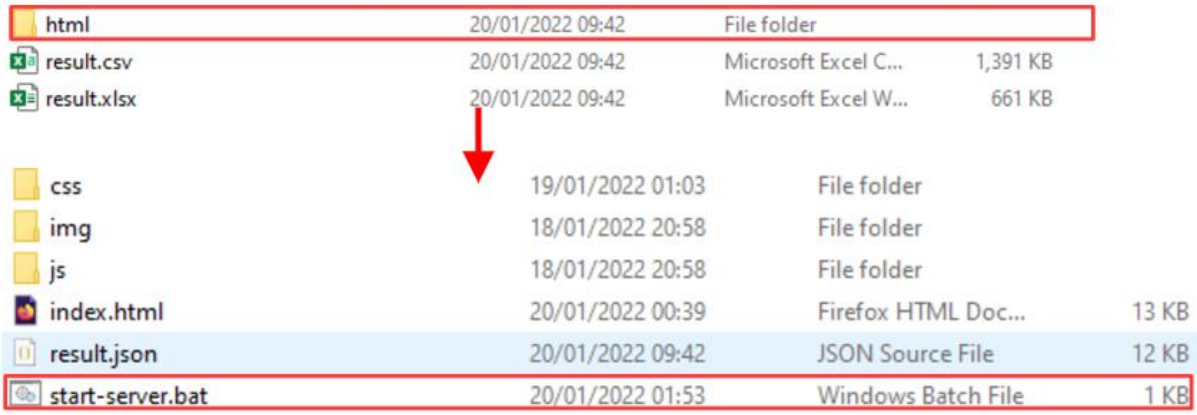
```
creating directories...
reading file...
creating header dict...
creating headers...
creating json data...
writing json data...
creating csv data...
writing csv data...
End, result files put in repertory: results
press enter to finish...
```

.git	20/01/2022 07:35	File folder	
.idea	19/01/2022 13:55	File folder	
__pycache__	19/01/2022 23:18	File folder	
html skeleton	19/01/2022 18:48	File folder	
results	20/01/2022 09:35	File folder	
Analyser.py	20/01/2022 07:33	Python File	13 KB
explication prog.pdf	20/01/2022 02:36	Adobe Acrobat D...	11 KB
fichier_a_traiter.txt	18/01/2022 20:57	Text Document	26,388 KB
install.bat	20/01/2022 01:12	Windows Batch File	1 KB
interpreters.py	18/01/2022 20:57	Python File	1 KB
README.md	20/01/2022 02:21	MD Document	1 KB
readme.txt	20/01/2022 09:09	Text Document	1 KB
user guide.docx	20/01/2022 02:21	Microsoft Word D...	29 KB

3 Results

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

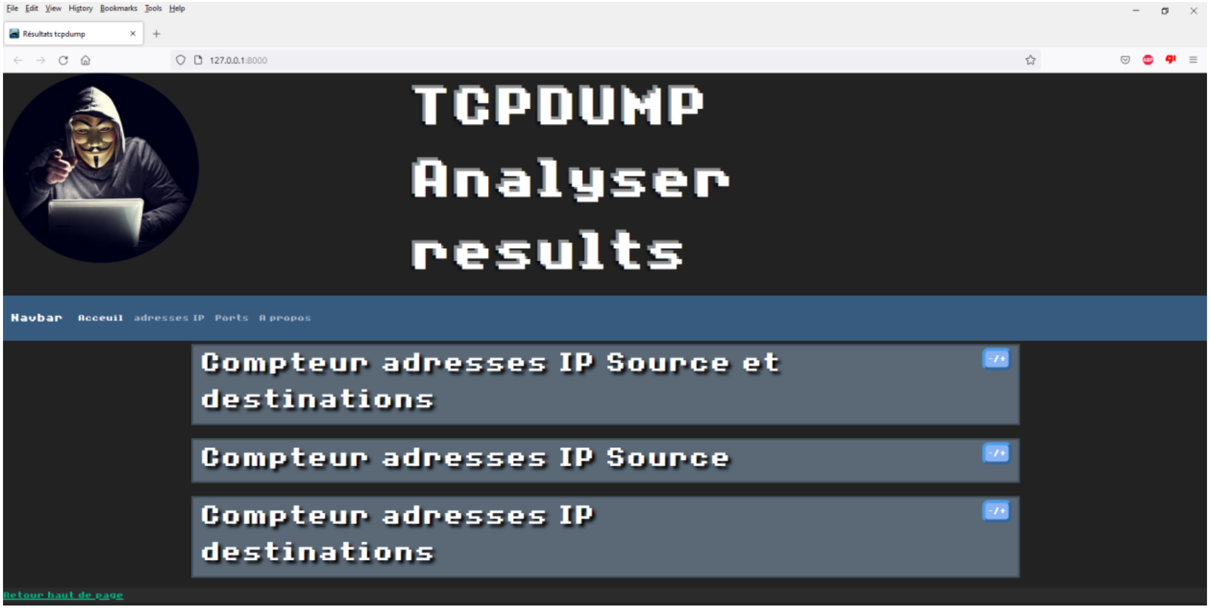
- **HTML results:**



html	20/01/2022 09:42	File folder	
result.csv	20/01/2022 09:42	Microsoft Excel C...	1,391 KB
result.xlsx	20/01/2022 09:42	Microsoft Excel W...	661 KB

css	19/01/2022 01:03	File folder	
img	18/01/2022 20:58	File folder	
js	18/01/2022 20:58	File folder	
index.html	20/01/2022 00:39	Firefox HTML Doc...	13 KB
result.json	20/01/2022 09:42	JSON Source File	12 KB
start-server.bat	20/01/2022 01:53	Windows Batch File	1 KB

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:



TCPDUMP Analyser results

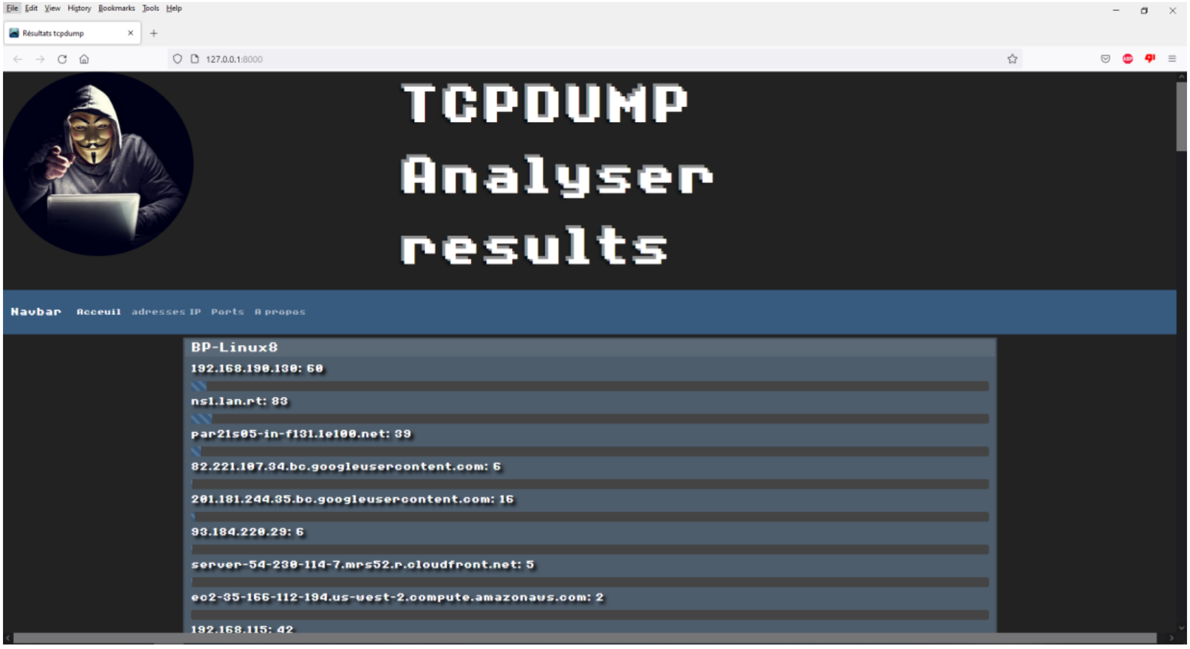
Compteur adresses IP Source et destinations

Compteur adresses IP Source

Compteur adresses IP destinations

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



TCPDUMP Analyser results

Navbar Acceuil adresses IP Ports A propos

BP-Linux8

192.168.190.130: 60

ns1.lan.rt: 83

par21s05-in-f131.1e100.net: 39

82.221.107.34.bc.googleusercontent.com: 6

201.181.244.35.bc.googleusercontent.com: 16

93.184.220.29: 6

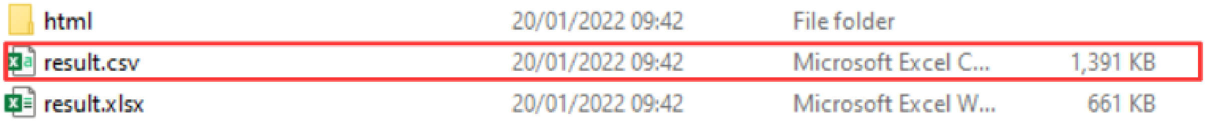
server-54-230-114-7.mrs52.r.cloudfront.net: 5

ec2-35-166-112-194.us-west-2.compute.amazonaws.com: 2

192.168.115: 42

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.

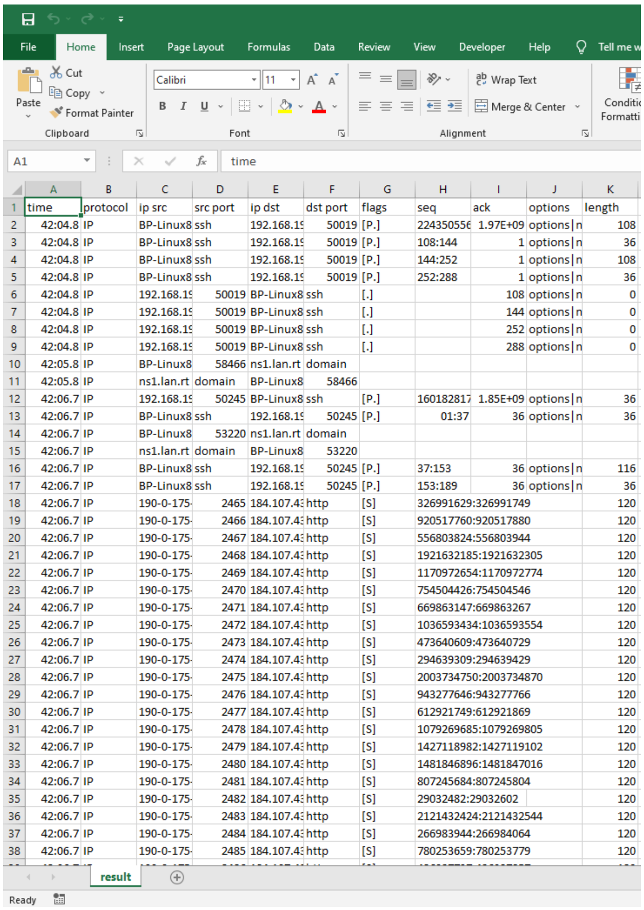
- **CSV file:**



html	20/01/2022 09:42	File folder	
result.csv	20/01/2022 09:42	Microsoft Excel C...	1,391 KB
result.xlsx	20/01/2022 09:42	Microsoft Excel W...	661 KB

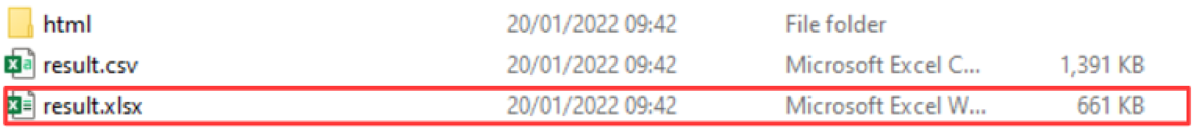
In the csv file you will only find the different packet informations separated in this order:

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



	A	B	C	D	E	F	G	H	I	J	K
1	time	protocol	ip src	src port	ip dst	dst port	flags	seq	ack	options	length
2	42:04.8	IP	BP-Linux8	ssh	192.168.19	50019	[P.]	224350556	1.97E+09	options|n	108
3	42:04.8	IP	BP-Linux8	ssh	192.168.19	50019	[P.]	108:144	1	options|n	36
4	42:04.8	IP	BP-Linux8	ssh	192.168.19	50019	[P.]	144:252	1	options|n	108
5	42:04.8	IP	BP-Linux8	ssh	192.168.19	50019	[P.]	252:288	1	options|n	36
6	42:04.8	IP	192.168.19	50019	BP-Linux8	ssh	[.]		108	options|n	0
7	42:04.8	IP	192.168.19	50019	BP-Linux8	ssh	[.]		144	options|n	0
8	42:04.8	IP	192.168.19	50019	BP-Linux8	ssh	[.]		252	options|n	0
9	42:04.8	IP	192.168.19	50019	BP-Linux8	ssh	[.]		288	options|n	0
10	42:05.8	IP	BP-Linux8	58466	ns1.lan.rt	domain					
11	42:05.8	IP	ns1.lan.rt	domain	BP-Linux8	58466					
12	42:06.7	IP	192.168.19	50245	BP-Linux8	ssh	[P.]	160182817	1.85E+09	options|n	36
13	42:06.7	IP	BP-Linux8	ssh	192.168.19	50245	[P.]	01:37	36	options|n	36
14	42:06.7	IP	BP-Linux8	53220	ns1.lan.rt	domain					
15	42:06.7	IP	ns1.lan.rt	domain	BP-Linux8	53220					
16	42:06.7	IP	BP-Linux8	ssh	192.168.19	50245	[P.]	37:153	36	options|n	116
17	42:06.7	IP	BP-Linux8	ssh	192.168.19	50245	[P.]	153:189	36	options|n	36
18	42:06.7	IP	190-0-175-	2465	184.107.43	http	[S]	326991629:326991749			120
19	42:06.7	IP	190-0-175-	2466	184.107.43	http	[S]	920517760:920517880			120
20	42:06.7	IP	190-0-175-	2467	184.107.43	http	[S]	556803824:556803944			120
21	42:06.7	IP	190-0-175-	2468	184.107.43	http	[S]	1921632185:1921632305			120
22	42:06.7	IP	190-0-175-	2469	184.107.43	http	[S]	1170972654:1170972774			120
23	42:06.7	IP	190-0-175-	2470	184.107.43	http	[S]	754504426:754504546			120
24	42:06.7	IP	190-0-175-	2471	184.107.43	http	[S]	669863147:669863267			120
25	42:06.7	IP	190-0-175-	2472	184.107.43	http	[S]	1036593434:1036593554			120
26	42:06.7	IP	190-0-175-	2473	184.107.43	http	[S]	473640609:473640729			120
27	42:06.7	IP	190-0-175-	2474	184.107.43	http	[S]	294639309:294639429			120
28	42:06.7	IP	190-0-175-	2475	184.107.43	http	[S]	2003734750:2003734870			120
29	42:06.7	IP	190-0-175-	2476	184.107.43	http	[S]	943277646:943277766			120
30	42:06.7	IP	190-0-175-	2477	184.107.43	http	[S]	612921749:612921869			120
31	42:06.7	IP	190-0-175-	2478	184.107.43	http	[S]	1079269685:1079269805			120
32	42:06.7	IP	190-0-175-	2479	184.107.43	http	[S]	1427118982:1427119102			120
33	42:06.7	IP	190-0-175-	2480	184.107.43	http	[S]	1481846896:1481847016			120
34	42:06.7	IP	190-0-175-	2481	184.107.43	http	[S]	807245684:807245804			120
35	42:06.7	IP	190-0-175-	2482	184.107.43	http	[S]	29032482:29032602			120
36	42:06.7	IP	190-0-175-	2483	184.107.43	http	[S]	2121432424:2121432544			120
37	42:06.7	IP	190-0-175-	2484	184.107.43	http	[S]	266983944:266984064			120
38	42:06.7	IP	190-0-175-	2485	184.107.43	http	[S]	780253659:780253779			120

- **Excel file**



html	20/01/2022 09:42	File folder	
result.csv	20/01/2022 09:42	Microsoft Excel C...	1,391 KB
result.xlsx	20/01/2022 09:42	Microsoft Excel W...	661 KB

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