

# How to transform pcaps to nfcaps and then in csv in Ubuntu

## How to Install nfdump in ubuntu

```

root@meteye:~# nfdump -R /var/lib/meteye/nfsen/flows-data/live/D02_021 -t -R 2015-08-24/nfcapd.201508240000:2015-08-24/nfcapd.201508240000 -n 10 -s
port:proto:bytes -N
top 10 port all flows ordered by bytes:
date first seen      duration proto      port    flows(%)  packets(%)  bytes(%)  pps    bps    min bps    max bps    bpps
2015-08-23 23:59:10.130 14705.776 17      8116     980( 0.2) 10359025(25.3) 648504086( 3.2) 764    377813 73695    115289    67
2015-08-23 23:58:59.072 14750.048 6       443     136763(14.3) 2710998( 6.6) 560209130( 4.2) 183    307719 384    239449    266
2015-08-23 23:58:59.008 14738.760 6       80      71633(12.7) 2786411( 6.8) 413110183( 3.1) 189    224230 294    1319576   148
2015-08-23 23:59:08.008 14736.592 50      0       5366( 1.0) 1848526( 4.6) 39718086( 3.0) 124    212415 2550   207275    208
2015-08-23 23:59:17.520 14735.912 6       49154   1475( 0.3) 315514( 0.8) 344863857( 2.6) 21    187223 765    762221    1093
2015-08-23 23:59:26.072 14727.368 6       57739   249( 0.0) 260103( 0.5) 246722955( 1.8) 14    134821 221    253288    1179
2015-08-23 23:59:03.100 14683.432 6       25      5631( 1.0) 264644( 0.5) 175067344( 1.3) 13    95293 1111    497253    855
2015-08-23 23:59:02.200 8637.152 6       62639   63( 0.0) 251456( 0.6) 148767649( 1.1) 29    137793 454    1319576   591
2015-08-23 23:59:47.126 14663.904 17      18397   981( 0.2) 1468081( 3.6) 88132968( 0.7) 186    40081 1166    53164    66
2015-08-23 23:59:46.504 14659.048 6       63016   250( 0.0) 76356( 0.2) 87383381( 0.7) 5     47688 355    762221    1144

Summary: total flows: 562074, total bytes: 13348059048, total packets: 40872324, avg bps: 7231853, avg pps: 2769, avg bpps: 326
Time window: 2015-08-23 23:58:58 - 2015-08-24 04:04:57
Total flows processed: 562074, blocks skipped: 0, bytes read: 92201548
Sys: 0.378s flows/second: 1483271.8 Wall: 0.377s flows/second: 1489446.7
root@meteye:~#

```

First, you have to install nfdump, that is the tool that can let you transform .pcaps into nfcaps

```

sudo apt-get update
sudo apt-get install nfdump

```

Then, you have to go to the nfdump folder with this command :

```
cd nfdump
```

## Enable nfcapd option in nfdump

You have to put the `--enable-nfcapd` in true , so introduce this command

```
./configure --enable-nfcapd
```

then :

```
make
```

```
sudo make install
```

Then, nfcapd have to be enable and ready to use it

## Transform pcap to nfcapd (binary)

Create a directory (if you want!), to save the nfcaps records

```
mkdir repository
```

then, to transform :

```
nfcapd -l directory-name -r directory-pcap-location
```

if you want to define a time of creation between nfcaps (example 5 minutes):

```
mfpcapd -l directory-name -r directory-pcap-location -t (minutes*60)
```

## Transform nfcapd to .csv

Use this command :

```
nfdump -r file -o csv > output.csv
```

## Bibliography

<https://github.com/hbhzwj/pcap-converter>

<https://github.com/vasiqmz/netflow2csv>

<https://stackoverflow.com/questions/33706028/how-to-convert-pcap-file-to-nfcapd-file>

<https://askubuntu.com/questions/687659/how-to-install-nfdump>

[https://nsrc.org/workshops/2017/sanog29-cndo/networking/cndo/en/labs/9.31\\_setting\\_up\\_nfsen.html](https://nsrc.org/workshops/2017/sanog29-cndo/networking/cndo/en/labs/9.31_setting_up_nfsen.html)

<https://github.com/phaag/nfdump>

<https://github.com/phaag/nfdump/issues/75>

<https://stackoverflow.com/questions/33706028/how-to-convert-pcap-file-to-nfcapd-file>

<https://www.first.org/resources/papers/conference2006/haag-peter-papers.pdf>

<https://stackoverflow.com/questions/8092380/export-pcap-data-to-csv-timestamp-bytes-uplink-downlink-extra-info>

<https://github.com/urcuqui/WhiteHat/wiki/Netflow-analytics>