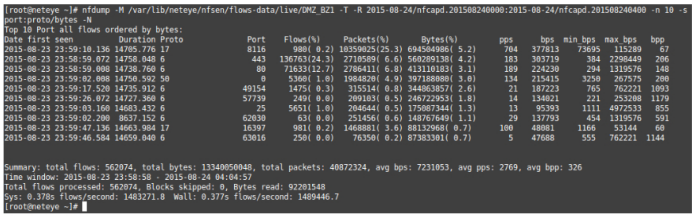
How to transform pcaps to nfpcaps and then in csv in Ubuntu

How to Install nfdump in ubuntu



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 nfpcapd option in nfdump

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

```
./configure --enable-nfpcapd
```

then :

```
make
```

```
sudo make install
```

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

Transform pcap to nfpcapd (binary)

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

```
mkdir repository
```

then, to transform :

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

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

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

Transform nfpcapd 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://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