Table of Contents

Cara Memonitor Traffic Jaringan di Linux

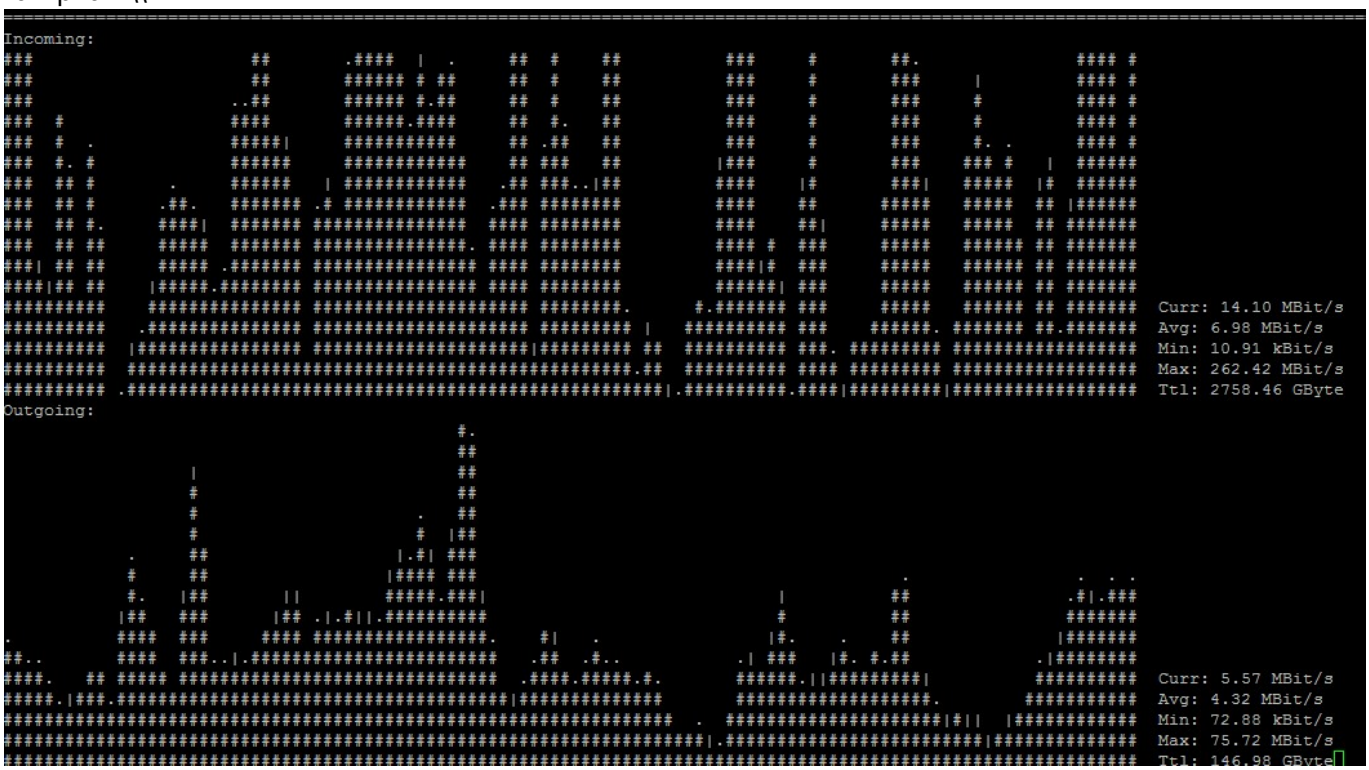
Berikut ini adalah daftar linux command / applikasi yang dapat digunakan untuk memonitor traffic networking.

NLOAD

Perintah

```
nload
```

tampilan \\



cara install

```
# fedora or centos
$ yum install nload -y

# ubuntu/debian
$ sudo apt-get install nload
```

HTTPRY

Untuk dapat menggunakan httpry anda harus menginstall paket epel

```
yum install epel-release -y
yum install httpry -y
```

Berikut ini adalah cara penggunaan httpry untuk memonitor traffic pada port 80

```
httpry -i eth0
```

dan outputnya kurang lebih seperti ini

```
[root@uvcms1 abuse]# httpry -i eth0
httpry version 0.1.8 -- HTTP logging and information retrieval tool
Copyright (c) 2005-2014 Jason Bittel <jason.bittel@gmail.com>
Starting capture on eth0 interface
2020-09-26 15:47:53     139.99.53.101   36.77.47.183    <       -       -
-       HTTP/1.1        403     Forbidden
2020-09-26 15:47:53     36.77.47.183    139.99.53.101   >       GET
kediripost.co.id        /wp-
content/themes/korankoran/includes/sharrre.php?url=http%3A%2F%2Fkediripost.c
o.id%2F2020%2F09%2F26%2Fdhito-tiba-tiba-datang-ke-nu%2F&type=googlePlus
HTTP/1.1        -       -
2020-09-26 15:47:53     36.77.47.183    139.99.53.101   >       GET
kediripost.co.id        /wp-
content/themes/korankoran/includes/sharrre.php?url=http%3A%2F%2Fkediripost.c
o.id%2F2020%2F09%2F26%2Fdhito-tiba-tiba-datang-ke-nu%2F&type=stumbleupon
HTTP/1.1        -       -
2020-09-26 15:47:53     139.99.53.101   143.204.82.117  >       GET
www.stumbleupon.com     /services/1.01/badge.getinfo?
```

</code>

Anda bisa menghilangkan keterangan header httpry version degan cara menambahkan **-q**

```
httpry -q -i eth0
```

Apabila anda hanya ingin mengambil traffic 50 baris anda bisa menggunakan

```
httpry -q -i eth0 -n 30
```

Anda juga dapat menyimpan output pada file dengan cara

```
httpry -q -i eth0 -n 30 -o /path/nama-file.txt
```

atau bisa juga

```
httpry -q -i eth0 -n 30 >> /path/nama-file.txt
```

Apabila anda ingin memfilter post,get,head anda bisa menggunakan

```
httpry -q -i eth0 -n 30 -m post,head
```

Apabila anda ingin memfilter source traffic dari ip tertentu berikut ini perintahnya

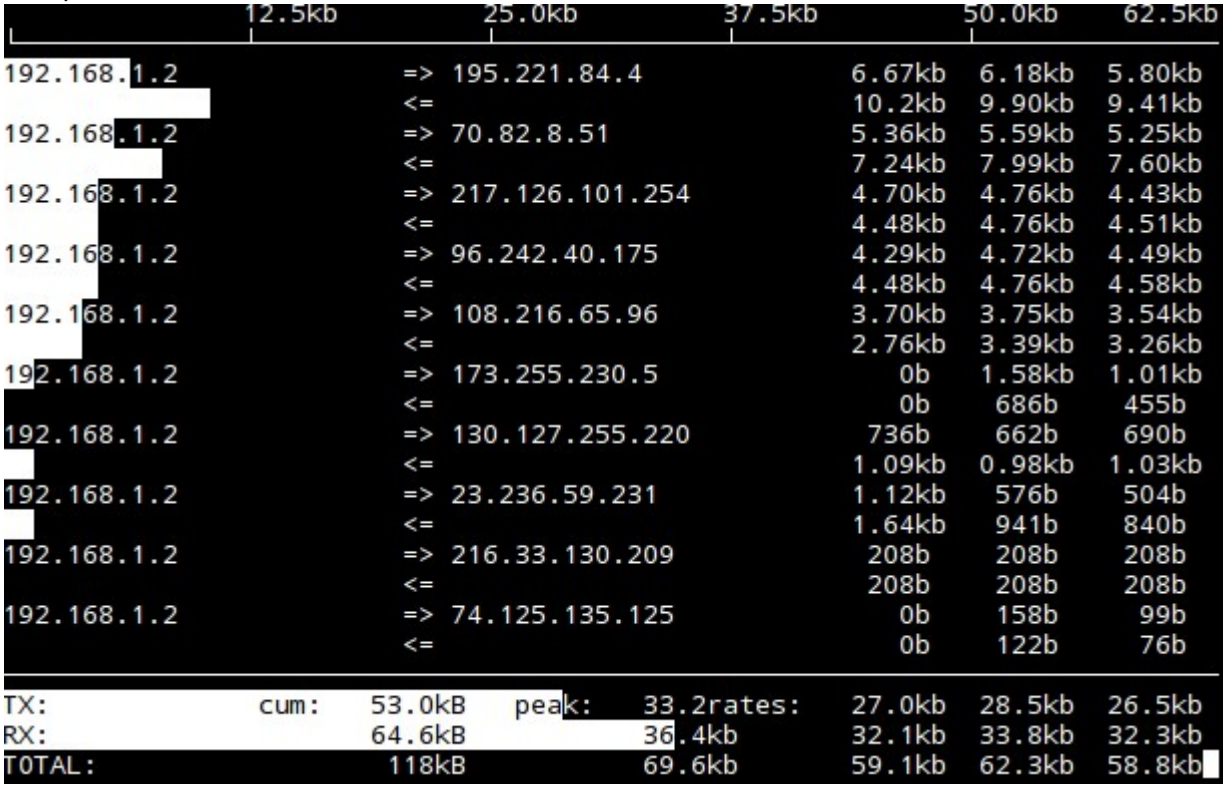
```
httpry -q -i eth0 -n 30 'src host 139.99.53.101'
```

IFTOP

Perintah Command

```
$ sudo iftop -n
```

Tampilan



Installasi

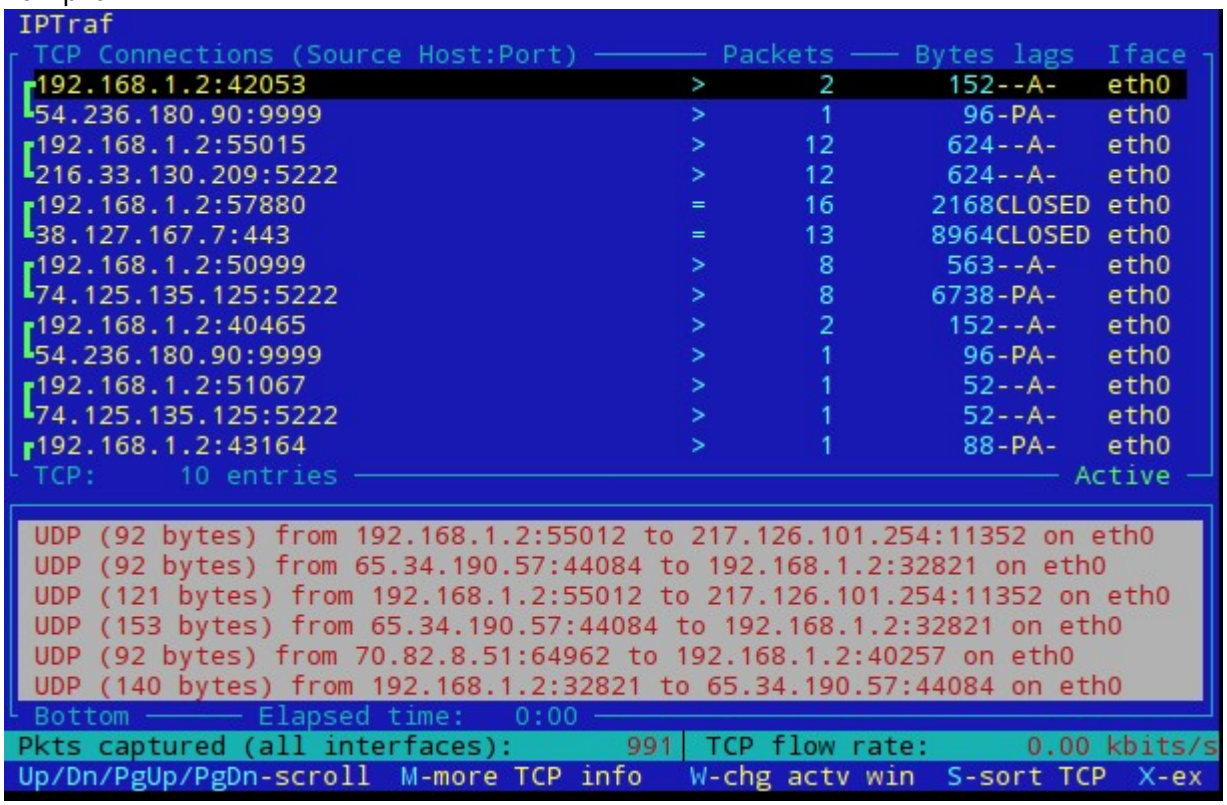
```
# fedora or centos
yum install iftop -y

# ubuntu or debian
$ sudo apt-get install iftop
```

IPTRAF

Perintah

```
$ sudo iptraf
```

Tampilan



Install

```
# Centos (base repo)
$ yum install iptraf

# fedora or centos (with epel)
$ yum install iptraf-ng -y

# ubuntu or debian
$ sudo apt-get install iptraf iptraf-ng
```