

Visualisasi dan monitoring aktifitas jaringan menggunakan lanmap dan etherape

By Henry Saptono <boypyt@gmail.com>

Nov 2009

Anda membutuhkan visualisasi peta jaringan dan monitoring traffic jaringan lokal ? tak perlu membuat diagram jaringan komputer Anda secara manual, Anda dapat memanfaatkan fungsi dari lanmap dan Anda dapat menggunakan etherape untuk monitoring traffic atau aktifitas jaringan secara real time. Lanmap adalah sebuah aplikasi dalam bentuk perintah (command) yang tersedia untuk distro linux Ubuntu yang akan memantau traffic jaringan Anda dan membuat gambar 2D dari gambaran aktifitas jaringan Anda secara otomatis. Gambar 2D yang dihasilkan oleh lanmap berisikan informasi tentang nama komputer, ip address, mac address, dan protokol. Etherape menampilkan visualisasi aktifitas jaringan Anda dalam mode grafik secara real time.

Dalam artikel kali ini penulis akan menjelaskan penggunaan lanmap dan etherape secara singkat dan jelas. Agar mudah dalam proses instalasi kedua software tersebut maka penulis menggunakan distro linux ubuntu 8.10 (kemungkinan besar berlaku juga jika Anda menggunakan ubuntu versi lainnya yang terbaru)

Instalasi lanmap dan etherape

Agar proses instalasi lanmap lebih mudah maka penulis menggunakan perintah apt-get untuk instalasi, tidak menggunakan aplikasi synaptic mode grafik. Berikut ini perintah instalasi paket lanmap dan etherape.

```
$ sudo apt-get install lanmap etherape
```

atau jika Anda langsung bekerja sebagai user root :

```
# apt-get install lanmap etherape
```

Menjalankan lanmap

Untuk menjalankan lanmap gunakan perintah berikut ini:

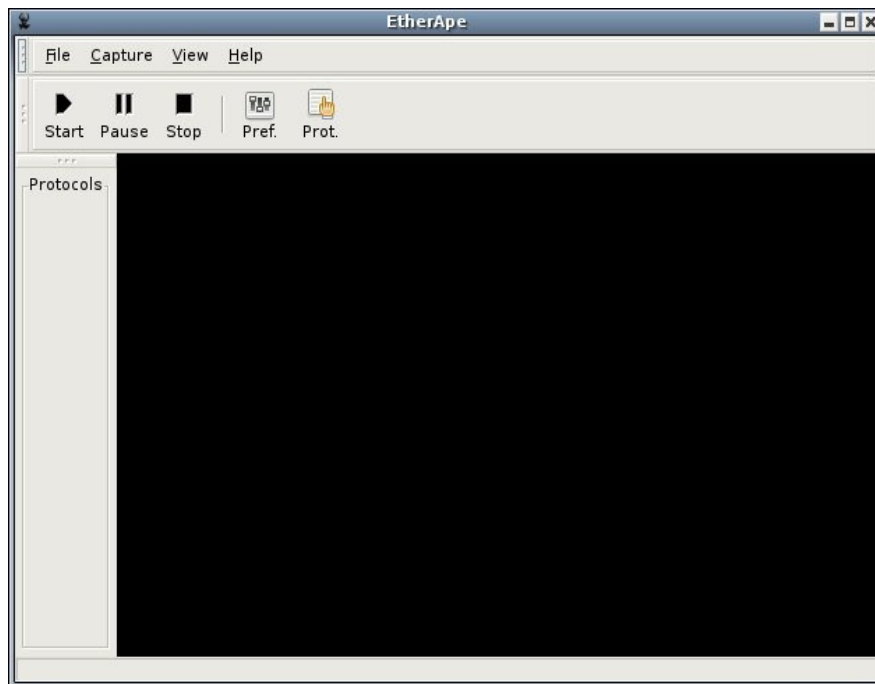
```
$ sudo lanmap -i eth0 -T png -o /tmp
```

atau jika ingin dijalankan dibackground sebagai berikut:

Menjalankan etherape

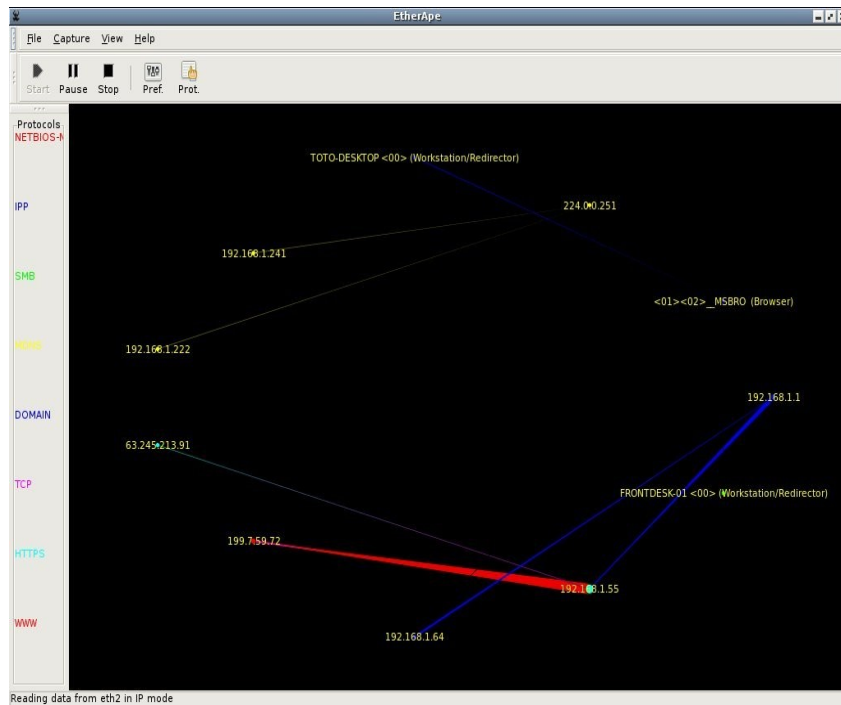
Berbeda dengan lanmap yang dijalankan dalam mode perintah dan hanya menghasilkan output berupa file image 2D, etherape tidak menghasilkan file image 2D namun etherape mampu melakukan visualisasi secara real time tentang aktifitas jaringan dalam tampilan yang mudah dibaca dan dipahami. Etherape berjalan dalam environment Desktop (GUI), Anda tidak akan bisa menjalankan etherape dalam environment text mode.

Untuk menjalankan etherape pada main menu pilih **Applications | Internet | EtherApe (as root)** , maka akan muncul pada desktop Anda window seperti gambar -2 berikut ini.



Gambar-2. Window utama etherape

Kemudian Anda pilih pada interface manakah etherape akan melakukan capture traffic dengan memilih menu **Capture | Intefaces | eth0** pada window utama etherape. Selanjutnya akan muncul window seperti tampak pada gambar-3.



Gambar-3. Network traffic visualisasi

Pada gambar-3 tampak visualisasi aktifitas jaringan Anda yang menunjukkan adanya koneksi atau hubungan jaringan yang dilakukan oleh komputer komputer dalam jaringan , koneksi atau hubungan tersebut direpresentasikan dalam bentuk garis-garis berwarna, yang masing masing warna memiliki asosiasi dengan protokol-protokol komunikasi TCP/IP (HTTP, SMB, SMTP, FTP dll). Untuk menampilkan informasi statistik setiap traffic berdasarkan protokol pilih menu **View | Protocols** sehingga akan muncul window seperti tampak pada gambar-4.

The screenshot shows the 'EtherApe: Protocols' window with a table of traffic statistics. The table has columns for Protocol, Inst Traffic, Accum Traffic, Last Heard, and Packets.

Protocol	Inst Traffic	Accum Traffic	Last Heard	Packets
DOMAIN	0 bps	2.288 Kbytes	1'44" ago	18
IPP	0 bps	14.287 Kbytes	19" ago	75
NETBIOS-NS	0 bps	4.877 Kbytes	1'4" ago	49
SMB	0 bps	6.547 Kbytes	1'12" ago	26
TCP-Unknown	0 bps	3.331 Kbytes	9'54" ago	4

Gambar-4. Statistik traffic berdasarkan protokol

etherape dapat juga difungsikan sebagai interpreter file ouput dari aplikasi tcpdump. Untuk membaca

file hasil tcpdump, tentunya Anda harus melakukan capture traffic terlebih dahulu dengan menggunakan tcpdump, dengan perintah berikut ini:

```
$ sudo tcpdump -i eth0 -n -w /tmp/tcpdump.out
```

Selanjutnya jika file hasil tcpdump sudah terbentuk dan telah menyimpan sejumlah informasi traffic , Anda dapat membuka atau membaca file tersebut menggunakan etherape dengan memilih menu **File | Open** kemudian pilihlah file **/tmp/tcpdump.out** .



gambar-5. Window dialog open file