NETWORK MANAGEMENT

ANALISA SNMP

Oleh

EKO PRATAMA

09011181320004

PROGRAM STUDI SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2016

SNMP (Simple Network Management Protocol) sebuah protocol yang dirancang untuk memberikan kemampuan pengguna untuk mengatur dan memantau jaringan komputer secara sistematis sementara MIB atau manager information base dapat dikatakan sebagai struktur basis data variable dari elemen jaringan yang dikelola. Struktur ini bersifat hierarki dan memiliki aturan sedemi8kian rupa sehingga informasi setiap variable dapat dikelola atau ditetapkan dengan mudah

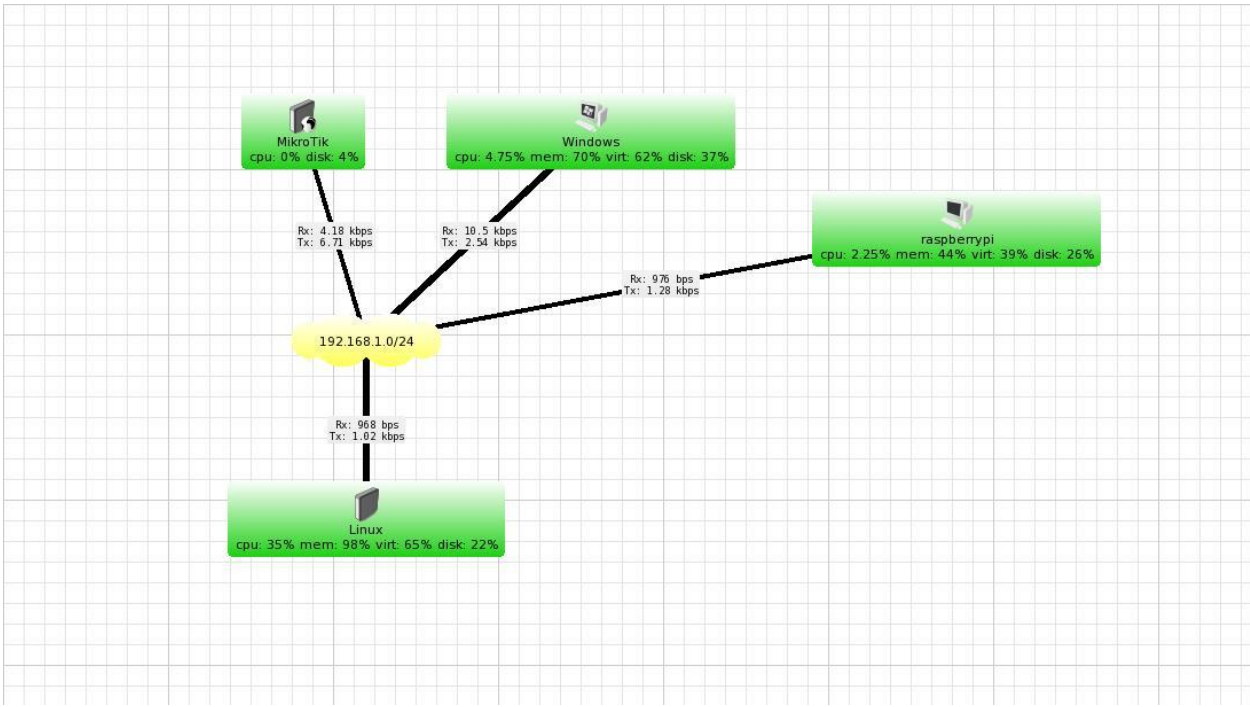
MIB mempunyai bebearapa struktur diantaranya**:**

• Setiap object mempunyai ID unik (OID)

• MIB mengasosiasikan setiap OID menggunakan label dan parameter lain.

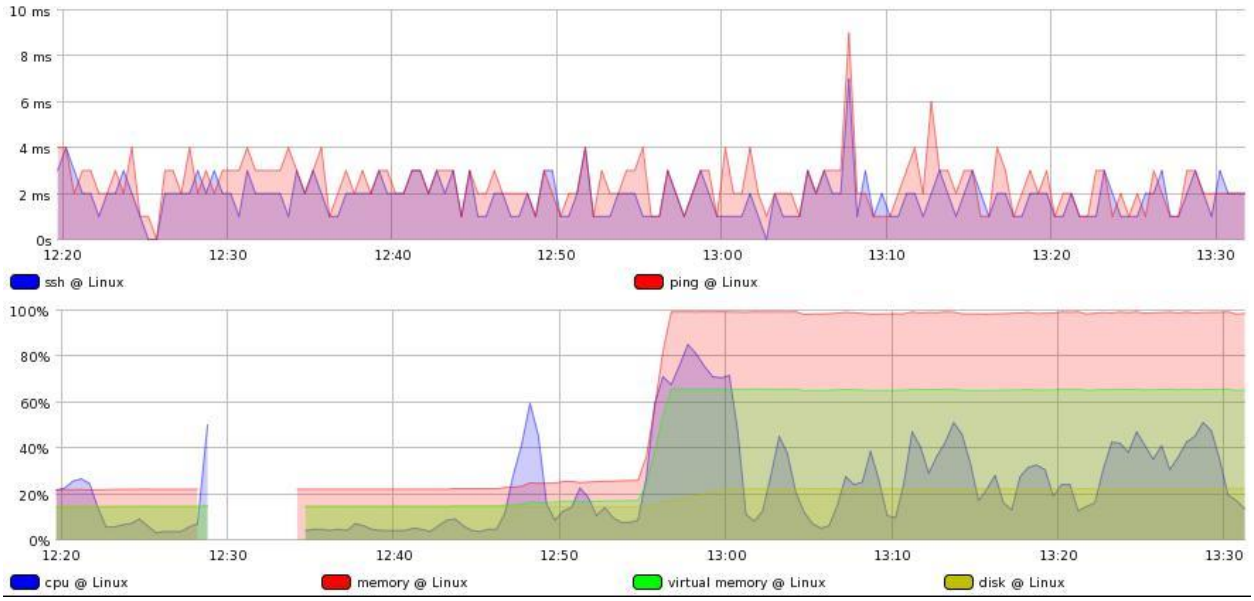
• MIB bertindak sebagai kamus data yang digunakan untuk menyusun terjemahan pesan SNMP

TUGAS *: menganalisa SNMP point point protokol SNMP sesuai dengan point di manager dan agent*



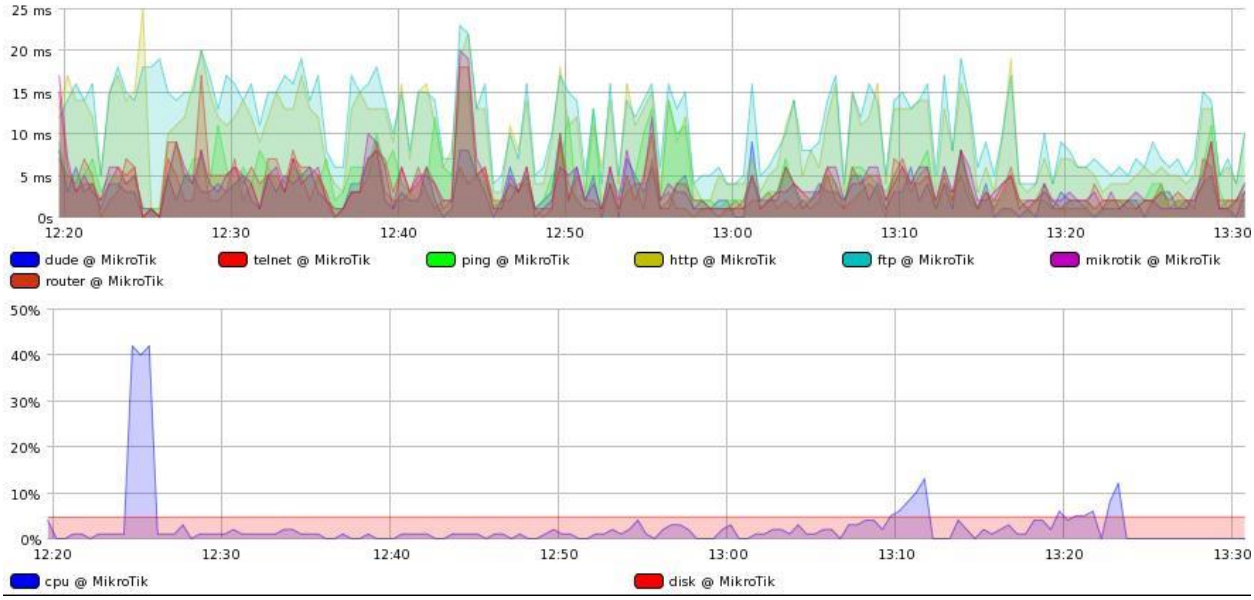
Gambar 1.1 Topologi jaringan SNMP

Pada Gambar 1.1 diatas dapat terlihat bahwa topologi jaringan SNMP (Simple Network Management Protocol) bahwa IP 192.168.1.0 melakukan pengiriman data dan melakukan traffic dengan perangkat perangkat seperti Mikrotik,windows,raspberrypi dan Linux untuk melihat traffic yang terjadi dari protokol SNMP.



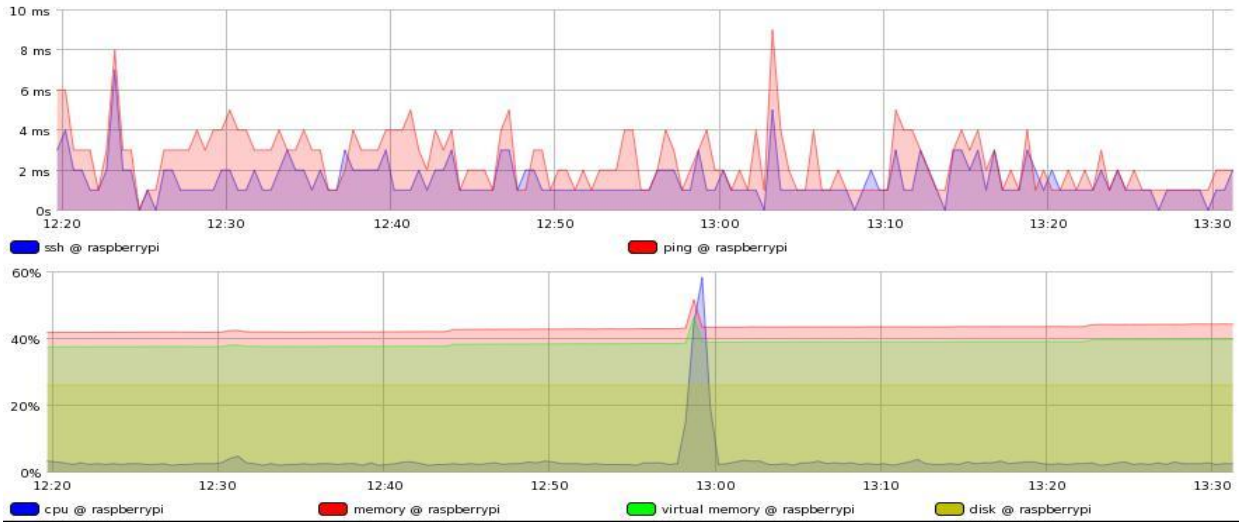
Gambar 1.2 Traffic data pada Linux

Dari gambar 1.2 yang menjelaskan tentang traffic data yang terjadi pada Linux dalam hal ini traffic pada ssh ditandai dengan warna biru. Digambar 1.2 yang bagian atas Pada pukul 13.08 terlihat terjadi pelonjakan traffic yang sangat tinggi yang merupakan traffic tertinggi. Jika pada pukul 13.08 merupakan traffic tertinggi lain halnya yang terjadi pada pukul 12.25 yang merupakan traffic terendah hingga kecepatanya 0 ms, sementara untuk gambar 1.2 bagian bawah dapat dilihat beberapa indicator seperti warna biru yaitu cpu, warna merah yang merupakan memory warna hijau terang yaitu virtual memory dan hijau gelap yang meupakan disk. Dapat terlihat pada pukul 12.20 hingga 12.25 terjadi traffic yang normal dengan presentase kurang lebih 20% pada pukul ke 12.30 hingga 12.34 tiba tiba traffic mengalami penurunan hingga 0% ang menandakan linux sedang tidak bekerja. Traffic teringgi ada pada pukul 12.55 hingga 13.30 dengan presentase 100%.



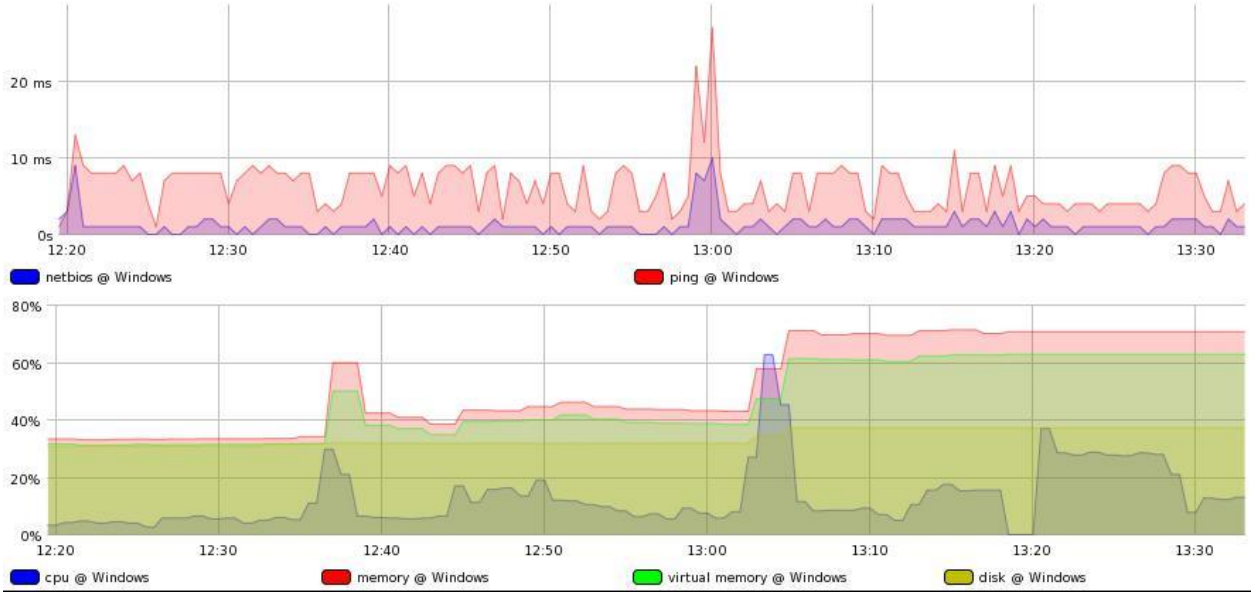
Gambar 1.3 Traffic data pada Mikrotik

Pada gambar 1.3 diatas yang merupakan traffic pada mikrotik dapat terlihat beberapa indicator biru merupakan dude, merah telnet, hijau terang ping dan idicator indicator lainnya dimana pada traffic mikrotik yang pertama terlihat traffic tertinggi pada pukul 12.24 dengan kecepatan kisaran 20-22 MS dan traffic terendah ada pada pukul 13.00 dengan kecepatan hanya 2 MS, sementara pada gambar 1.3 yang bawah terlihat 2 indikator yaitu biru sebagai cpu dan merah sebagai disk pada traffic ini traffic disk terlihat konstan denagn presentase 5% sementara pada CPU terjadi pelonjakan traffic yang tinggi pada pukul 12.25 yang mencapai 40%



Gambar 1.4 Traffic data pada raspberry pi

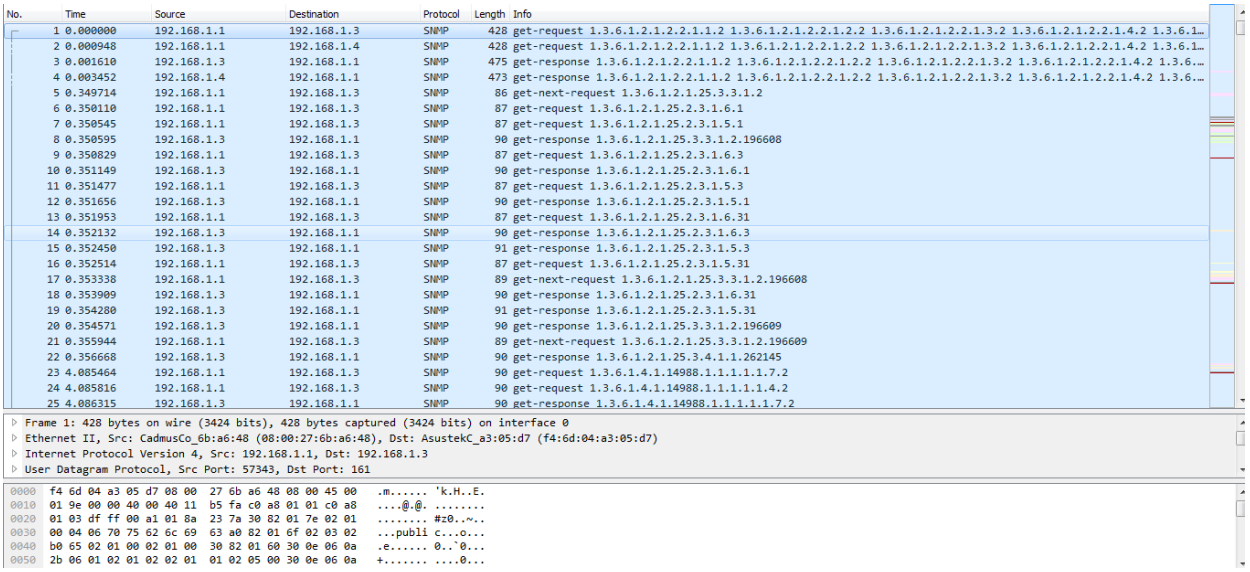
Pada gambar 1.4 traffic data pada raspberry pi atas, warna biru adalah statistik ssh dan warna merah statistik ping. Pada statistik ssh, statistik tertinggi pada jam lebih dari jam 12:20 dengan kecepatan data yang diperoleh sebesar lebih dari 6 ms dan statistik terendah pada jam kurang dari 12:30, kurang dari jam 13:10 dan kurang dari jam 13:20 dengan kecepatan data yang diperoleh sebesar 0 ms sedangkan statistik netral pada kecepatan kurang dari 2 ms. Sementara Pada trafik bawah, warna biru adalah statistik cpu, warna merah statistik memory, warna hijau statistik virtual memory dan warna kuning statistik disk. Pada cpu, statistik tertinggi pada jam 13:00 dengan presentase data yang diterima sebesar kurang dari 60%. Pada memory, statistik tertinggi pada jam 13:00 dengan presentase data yang diterima sebesar kurang dari 60% dan statistik terendah pada jam 12:20 dengan presentase data yang diterima sebesar 40%.



Gambar 1.5 Traffic data pada windows 8

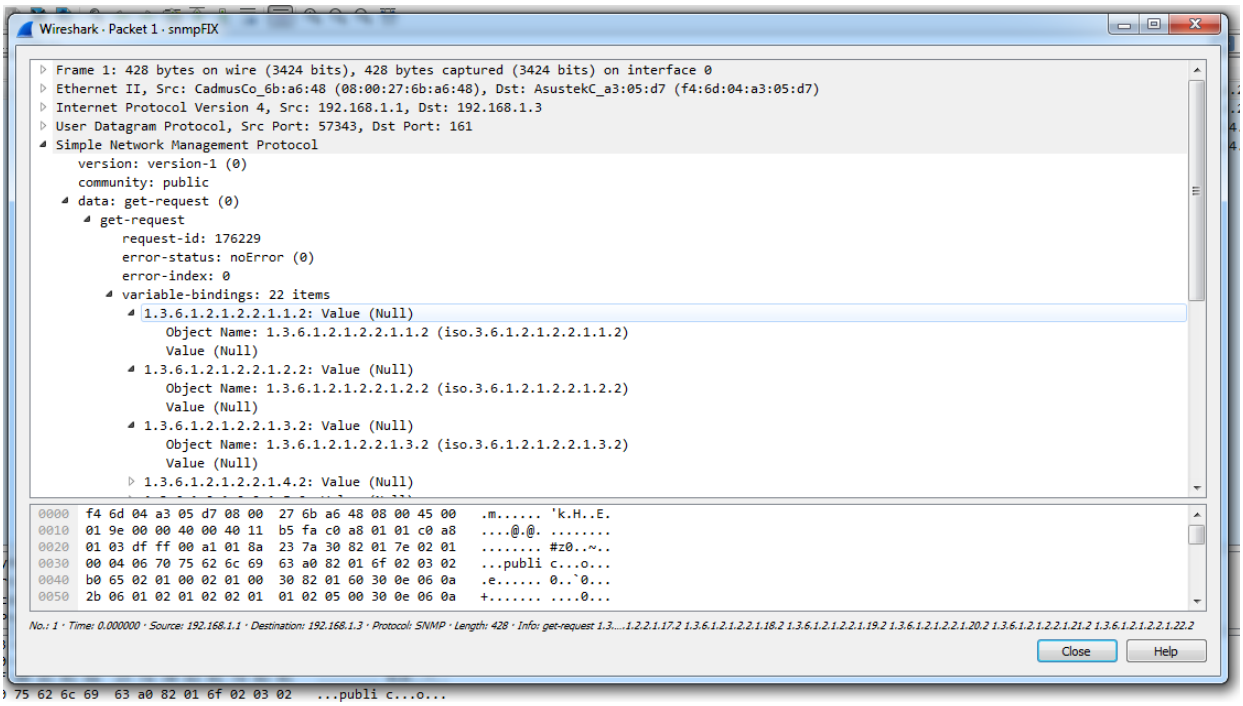
Pada gambar 1.5 yang merupakan traffic yang terjadi pada windows 8 terlihat beberapa indicator biru dan merah dengan biru sebagai netbios dan merah ping. Traffic tertinggi terjadin pada pukul 13.00 dengan kecepatan 25 MS dan traffic terendah pada pukul 12.25 dengan kecepatan 2 MS pada gambar yang bawah warna biru menunjukkan statistik cpu, warna merah statistic memory, warna hijau statistik virtual memory dan warna kuning statistik disk. Pada cpu, statistik tertinggi pada jam lebih dari 13:00 dengan presentase data yang diperoleh sebesar lebih dari 60 % dan statistik terendah pada jam 13:20 dengan presentase data yang diperoleh sebesar 0%. Pada memory, statistik tertinggi pada jam kurang dari 13:10 dengan presentase data yang diperoleh

sebesar lebih dari 60% sedangkan statistik terendah pada jam 12:20 sampai dengan jam kurang dari 12:40 dengan presentase data yang diperoleh sebesar kurang dari 40%. Pada virtual memory, statistik tertinggi pada jam lebih dari 13:10 sampai dengan jam 13:30 dengan presentase data yang diperoleh sebesar lebih dari 60% dan statistic terendah pada jam lebih dari 12:40 dengan presentase data yang diperoleh sebesar kurang dari 40%. Sedangkan pada disk, statistik tertinggi pada jam kurang dari 13:10 sampai dengan jam 13:30 dengan presentase data yang diperoleh sebesar kurang dari 40% dan statistik terendah pada jam 12;20 sampai dengan jam lebih dari 13:00 dengan presentase data yang diperoleh sebesar lebih dari 20%



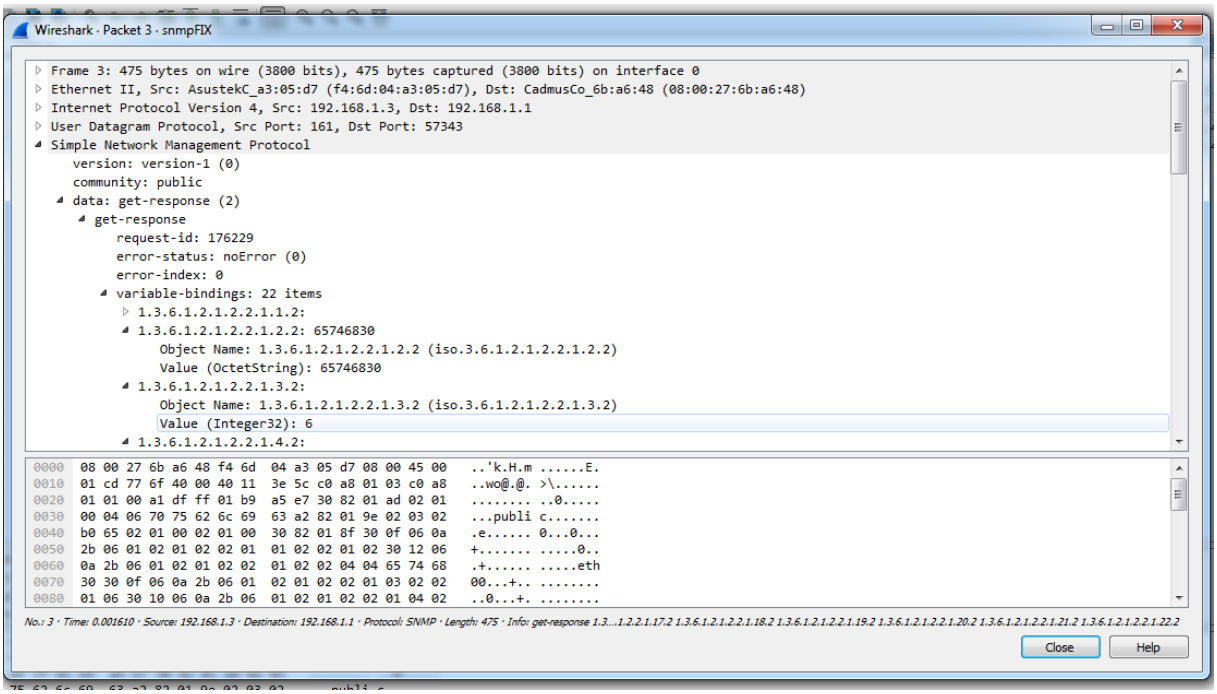
Gambar 1.6 hasil pcaps tentang SNMP

Gambar 1.6 menjelaskan tentang beberapa IP yang sedang melakukan traffic data dengan request dan response dalam aplikasi inilah kita dapat menganalisa IP mana yang sedang melakukan request dan melakukan response dimenit keberapa



Gambar 1.7 IP request

Pada Gambar 1.7 merupakan sebuah capturan dari pcaps menggunakan aplikasi whireshark dimana pada gambar tersebut menjelaskan tentang bagaimana IP melakukan request. Dari capturan diatas IP source 192.168.1.1 dan IP destination 192.168.1.3 dan menggunakan protocol SNMP dengan request-id: 176229 pada variable binding terdapat 22 items dan saya ambil 1 contoh 1.3.6.1.2.1.2.2.1.1.2: Value (Null) dan Object Name: 1.3.6.1.2.1.2.2.1.1.2 (iso.3.6.1.2.1.2.2.1.1.2) maksud dari angka 1.3.6.1.2.1.2.2.1.1.2 yaitu 1 merupakan ISO, 3 merupakan identification ISO 6 US dod, 1 merupakan angka internet, 2 merupakan management, 1 merupakan MIB , kemudian 1 lagi merupakan protocol SNMP dan 2 merupakan datagram dari SNMP, nah dari variable variable diatas terbentuklah satu kesatuan variable saat IP meminta request



Gambar 1.8 IP response

Pada Gambar 1.8 merupakan sebuah capturan dari pcaps menggunakan aplikasi whireshark dimana pada gambar tersebut menjelaskan tentang bagaimana IP melakukan response. Dari capturan diatas IP source 192.168.1.3 dan IP destination 192.168.1.1 dan menggunakan protocol SNMP. Cara perhittungan variable sama dengan saat IP melakukan request