Analisis Protocol SNMP dengan Wireshark

serta Visualisasi Menggunakan Oange dan RapidMiner

Disusun Oleh:

Nama : M. Andre Sofyan

NIM : 09011181520130

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

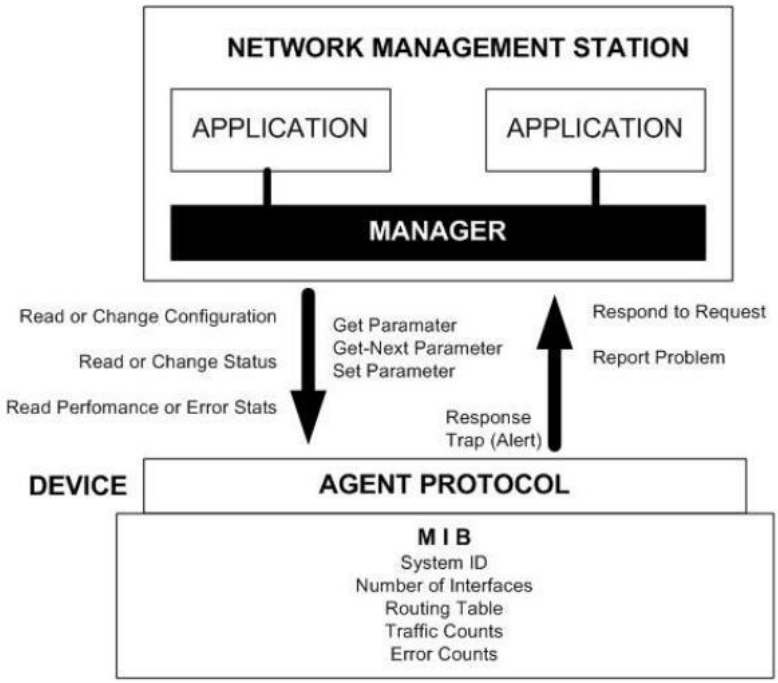
UNIVERSITAS SRIWIJAYA

2018

1. Pengertian SNMP

Salah satu protokol yang populer digunakan untuk manajemen jaringan adalah Simple Network Management Protocol (SNMP). SNMP merupakan sebuah protokol yang digunakan sebagai standar untuk melakukan pengaturan perangkat-perangkat jaringan.

2. Elemen yang terdapat di dalam SNMP



1) Manager

Manager adalah pelaksana dan manajemen jaringan. Pada kenyataannya manager ini merupakan komputer biasa yang ada pada jaringan yang mengoperaksikan perangkat lunak untuk manajemen jaringan. Manager ini terdiri atas satu proses atau lebih yang berkomunikasi dengan agen-agennya dan dalam jaringan. Manajer akan mengumpulkan informasi dari agen dari jaringan yang diminta oleh administrator saja bukan semua informasi yang dimiliki agen.

2) MIB atau Manager Information Base

Dapat dikatakan sebagai struktur basis data variabel dari elemen jaringan yang dikelola. Struktrur ini bersifat hierarki dan memiliki aturan sedemikian rupa sehingga informasi setiap variabel dapat dikelola atau ditetapkan dengan mudah.

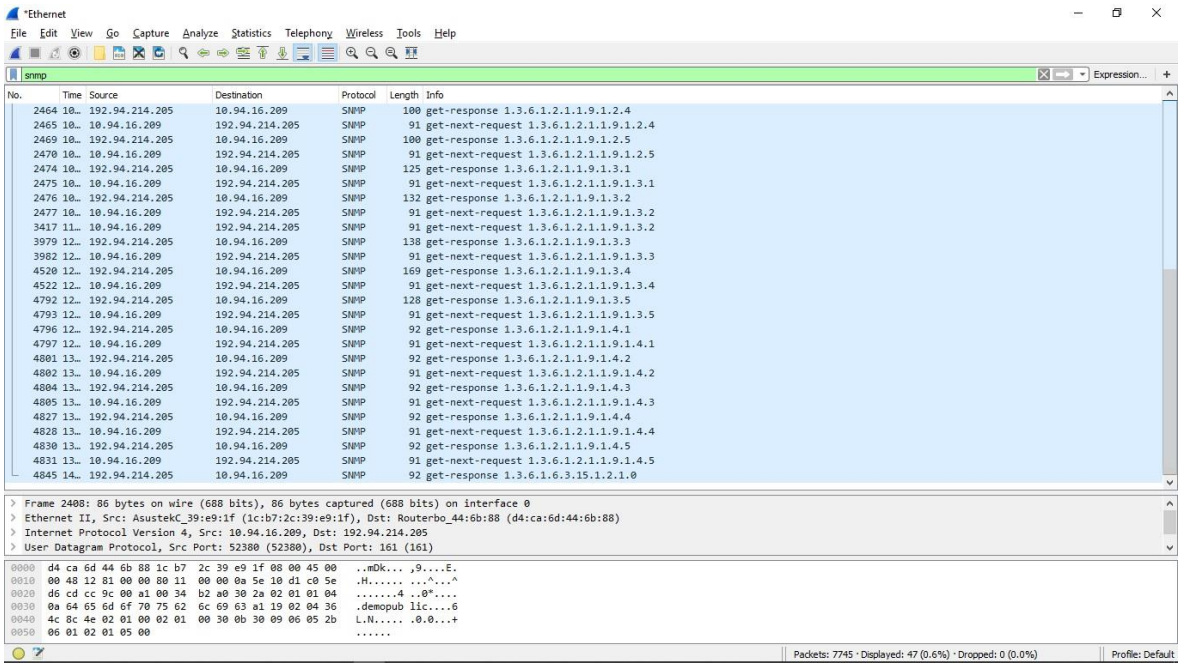
MIB mempunyai bebearapa struktur diantaranya:

- 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

3) Agent

Agent merupakan perangkat lunak yang dijalankan disetiap elemen jaringan yang dikelola. Setiap agen mempunyai basis data variabel yang bersifat lokal yang menerangkan keadaan dan berkas aktivitasnya dan pengaruhnya terhadap operasi.

3. Hasil Percobaan Menggunakan Wireshark

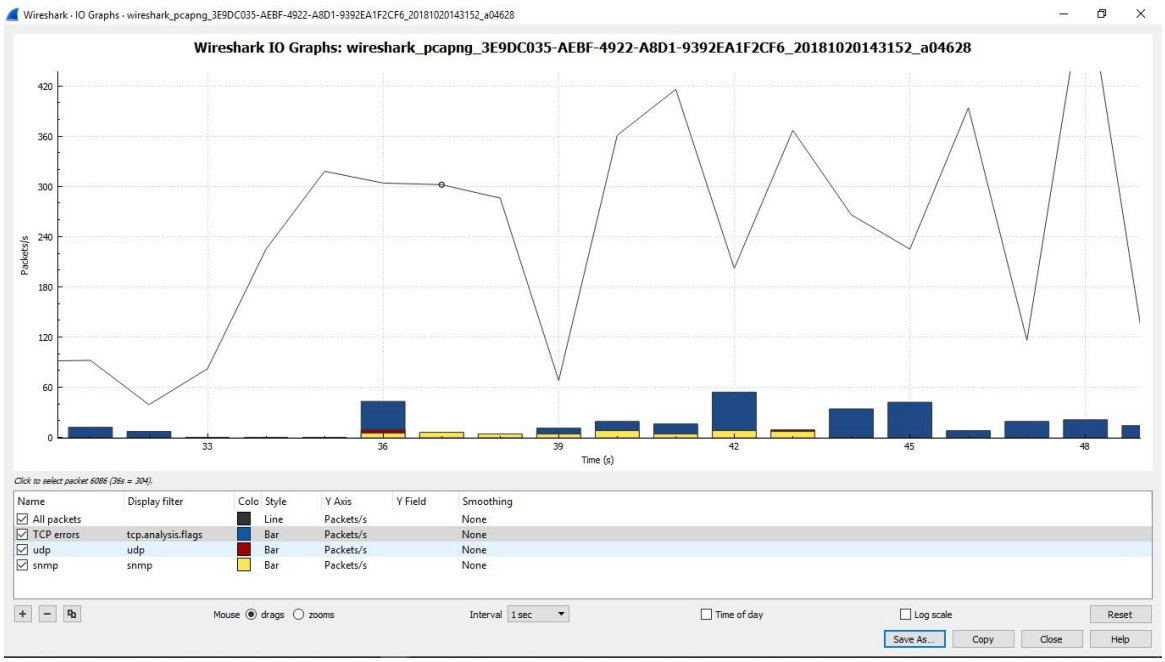


Gambar diatas menjelaskan tentang beberapa IP yang sedang melakukan traffic data dengan request dan response, dalam aplikasi Wireshark inilah kita dapat menganalisa IP mana yang sedang melakukan request dan melakukan response.

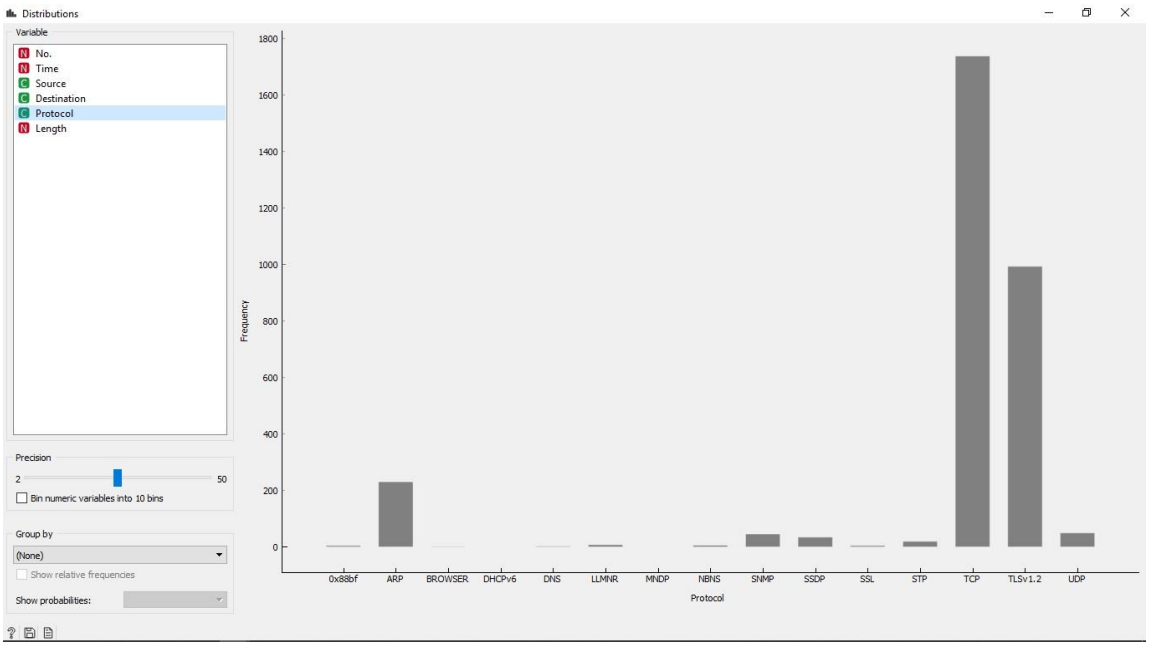
Berdasarkan gambar (sekian), dapat kita lihat pada bagian INFO bahwa setiap pesan SNMP terdapat Protocol Data Unit (PDU). PDU merupakan unit data yang terdiri atas sebuah header dan beberapa data yang ditempelkan. SNMP PDU digunakan untuk komunikasi antara manager SNMP dan agent SNMP.

Arsitektur SNMP Versi 1 mendefinisikan tipe pesan dari PDU sebagai berikut :

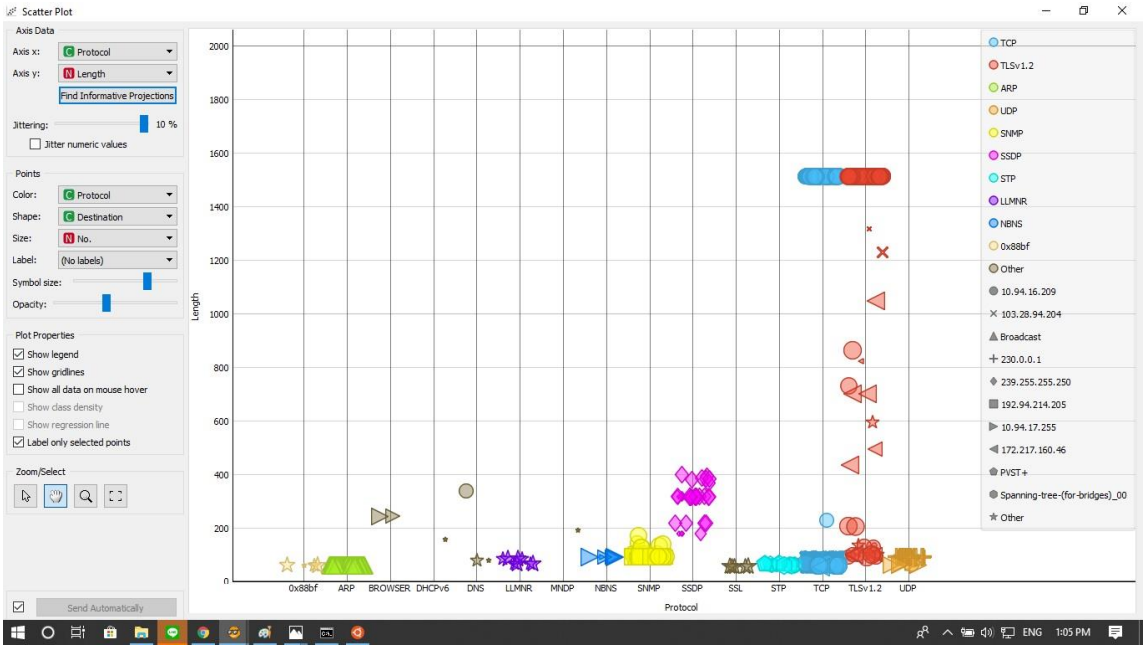
a) Get-Request PDU : dikirim oleh SNMP manager untuk mengambil satu atau lebih variabel MIB yang diminta yang telah ditentukan oleh PDU.
b) Get-Next-Request PDU : dikirim oleh SNMP manager untuk mengambil variabel MIB berikutnya. Anda dapat memiliki beberapa pernintaan di PDU.
c) Set-Request PDU : dikirim oleh SNMP manager untuk mengatur satu atau lebih variabel MIB dengan nilai yang telah ditentukan dalam PDU.
d) Get-Response PDU : dikirim oleh SNMP agent dalam menanggapi Get-Request PDU, Get-Next-Request PDU atau Set-Request PDU
e) Trap PDU : berisikan pesan yang tidak diinginkan yang dikirim oleh SNMP agent untuk memberitahu SNMP manager tentang peristiwa penting yang terjadi di agent



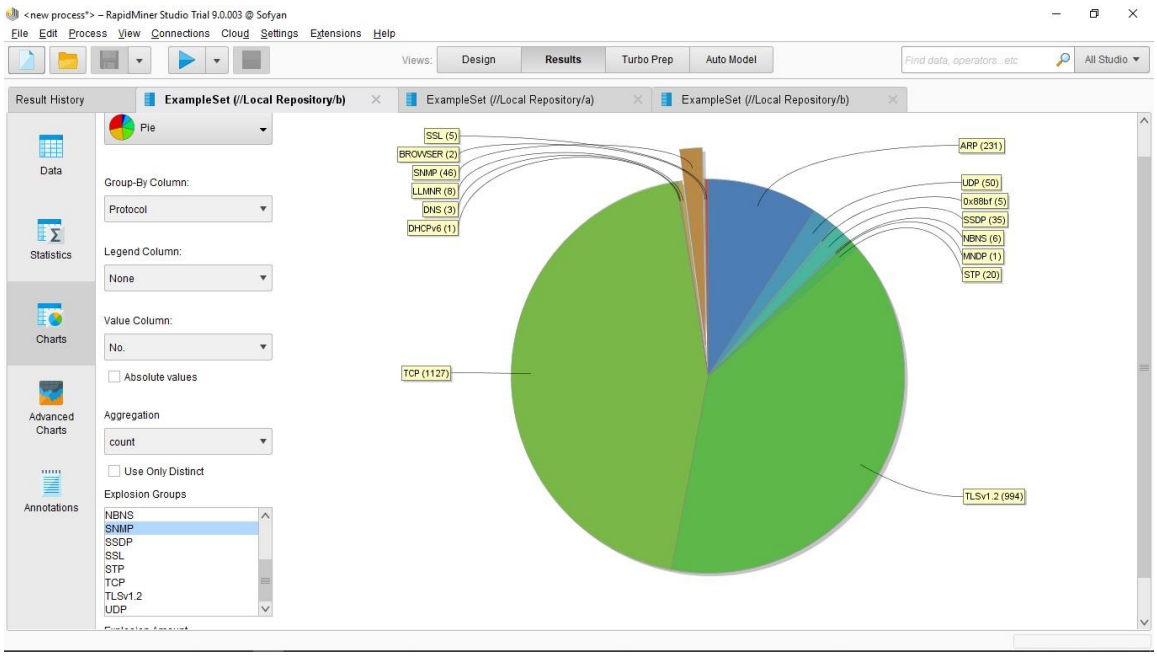
Gambar diatas adalah grafik dari traffic paket protokol SNMP, udp, TCP errors, dan semua paket lainnya yang ditampilkan melalui Wireshark I/O Grafik. Traffic SNMP ditunjukkan dengan bar berwarna kuning, semua paket ditandai dengan grafik line berwarna hitam, udp ditandai dengan bar berwarna merah, dan TCP ditandai dengan bar berwarna hijau biru.



Gambar diatas merupakan hasil Visualisasi bentuk distribusi table bar dari aplikasi Orange yang menampilkan banyak jumlah SNMP pada hasil capturing yang dilakukan oleh wireshark. Dengan skala 200, dapat terlihat Jumlah SNMP tidak sampai dengan 200 sesuai dengan hasil capturing di Wireshark yang terdapat hanya 46.



Gambar diatas merupakan hasil Visualisasi bentuk scatter plot dari aplikasi Orange yang menampilkan banyak jumlah SNMP juga pada hasil capturing yang dilakukan oleh wireshark. Disitu juga terdapat bentuk warna untuk menandai yang mana destination, source, protocol dan sebagainya.



Gambar diatas merupakan hasil Visualisasi dari aplikasi RapidMiner yang menampilkan banyak jumlah SNMP pada hasil capturing yang dilakukan oleh wireshark. Disitu terdapat 46 SNMP dan data yang lain juga bias dilihat disitu melalui hasil visualisasi berbentuk Pie.

4. Kesimpulan

SNMP merupakan sebuah protokol yang digunakan sebagai standar untuk melakukan pengaturan perangkat-perangkat jaringan yang dirancang untuk memberikan kemampuan kepada penggunanya dalam hal memantau dan mengatur jaringan komputernya secara sistematis dari jarak jauh atau dalam satu pusat kontrol saja. dengan menggunakan protokol ini kita bisa mendapatkan informasi tentang status dan keadaan dari suatu jaringan. Dan juga perbedaan antara ***Get-Request*** dan ***Get-Respone*** terdapat pada nilai *Value*-nya. Pada saat pertama kali manager mengirim *Get-Request* kepada agent, nilai *Value* yaitu Null. Kemudian agent menanggapi permintaan dari manager. maka agent akan mengirimkan *Get-Respone* ke manager. .

.