NETWORK MANAGEMENT

Analisis Paket Data Jaringan Simple Network Manajemen Protocol (SNMP) Menggunakan Wireshark

Oleh :

Abdul Wahid Sempurna

09011181520014

PROGRAM STUDI SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

A. Pendahuluan

1. Latar Belakang

Perkembangan teknologi telekomunikasi yang sangat cepat akan menghadirkan beragam bentuk layanan bagi konsumen. Hal tersebut berbanding lurus dengan bisnis untuk membangun jaringan yang lebih besar dan lebih baik dengan harga yang lebih terjangkau. Dengan peningkatan ukuran dan jumlah perangkat jaringan maka akan maka semakin tinggi resiko terjadi gangguan jaringan. Manajemen jaringan terutama sistem monitoring menjadi sesuatu yang penting dilakukan.

Simple Network Management Protocol (SNMP) adalah sebuah protokol aplikasi pada jaringan TCP/IP yang dapat digunakan untuk pengelolaan dan pemantauan sistem jaringan komputer. Hampir semua peralatan jaringan telah mendukung penggunaan SNMP untuk pemantauannya. SNMP akan mempermudah proses monitoring dan manajemen jaringan karena dengan menggunakan SNMP akan dapat diketahui tentang kondisi perangkat jaringan yang diamati. Tetapi layanan dan informasi SNMP hanya dapat diakses melalui tampilan pada command prompt atau terminal sehingga dalam penggunaannya tidak efektif dan sulit dilakukan karena masih membutuhkan pengolahan dan tampilannya sulit dimengerti.

Solusi yang pernah dilakukan adalah membuat Grapical User Interface (GUI) sebagai perantara untuk mengambil dan menampilkan nilai SNMP. Tetapi solusi yang ditawarkan masih mempunyai kekurangan, karena hasil yang ditampilkan hanya sebatas informasi kondisi jaringan pada saat itu dan masih belum ada sistem untuk menyimpan dan mengolah nilai SNMP lebih lanjut. Padahal jika data tersebut diolah akan dihasilkan laporan tentang kondisi jaringan sehingga mempermudah administrator jaringan dalam pemantauan kondisi jaringan dan menganalisis kebutuhan serta pengembangan jaringan yang akan datang. Solusi yang dapat dilakukan adalah menyediakan sistem database untuk menyimpan nilai-nilai kondisi jaringan yang didapat dari pesan SNMP dan mengolah lebih lanjut.

Pada tugas akhir ini akan dilakukan perancangan dan pembuatan aplikasi monitoring jaringan yang dapat digunakan sebagai perantara untuk mengambil dan mengolah nilai SNMP sekaligus terdapat sistem penyimpanan atau database sehingga dapat ditampilkan laporan informasi tentang kondisi jaringan yang meliputi availability perangkat dan trafik pada transport TCP.

2. Rumusan Masalah

Dengan berkembangnya teknologi informasi, khususnya jaringan memungkinkan terjadinya pertukaran informasi yang cepat dan semakin kompleks. Pengaturan jaringan yang baik tentu akan memaksimalkan pemanfaatan informasi tersebut. karena semakin besar dan luas sistem jaringan maka akan semakin sulit untuk mengatur dan mengawasinya.

3. Tujuan

- Memantau jaringan agar pengiriman atau pertukaran informasi dapat berjalan dengan baik.
- Mengumpulkan informasi manajemen jaringan mengenai keadaan perangkat jaringan.
- Menyimpan dan mengambil informasi manajemen yang didefinisikan di MIB.
- Memberikan sinyal sebuah event ke Manager.
- Bekerja sebagai proxy untuk beberapa node jaringan yang tidak mendukung SNMP.

B. Hasil dan Pembahasan

SNMP merupakan sebuah protokol yang digunakan sebagai standar untuk melakukan pengaturan perangkat-perangkat jaringan[2]. SNMP dapat digunakan untuk mengkonfigurasi device yang jauh, menyediakan sekumpulan operasi yang dapat melakukan pengelolaan beberapa perangkat jaringan secara jarak jauh sehingga monitoring dapat dilakukan tidak hanya pada Local Area Network (LAN) tapi juga dapat dioperasikan pada skala jaringan yang lebih luas seperti Wide Area Network (WAN), mendeteksi kesalahan jaringan atau akses yang tidak cocok, dan mengaudit pemakaian jaringan[1,2]. SNMP adalah protocol pada level aplikasi yang merupakan bagian dari protokol TCP/IP, menggunakan model UDP untuk membentuk fungsi transport[3]. Sampai sekarang terdapat versi dari SNMP: versi 1 (SNMPv1) dan versi 2 (SNMPv2), dan versi 3 (SNMPv3). ketiganya mempunyai fungsi dasar yang sama, tetapi semakin mengalami peningkatan versi, kemampuan dan fungsi yang dimiliki bertambah[3].

Elemen-elemen 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. Berikut adalah struktur dari MIB, yaitu:

- Setiap object mempunyai ID unik (OID).
- MIB mengasosiasikan setiap OID menggunakan label dan parameter lain.
- MIB bertindak sebagai kamus data 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.

SNMP menggunakan protokol transport UDP (*User Datagram Protocol*) di port 161 untuk mengirimkan permintaan dari manager ke agen dan menerima jawaban dari agen ke manager. Agen yang memiliki MIB akan memberikan data informasi yang diperlukan tapi tidak semua oleh manager menggunakan transport UDP yang berorientasi pada kecepatan pengiriman.

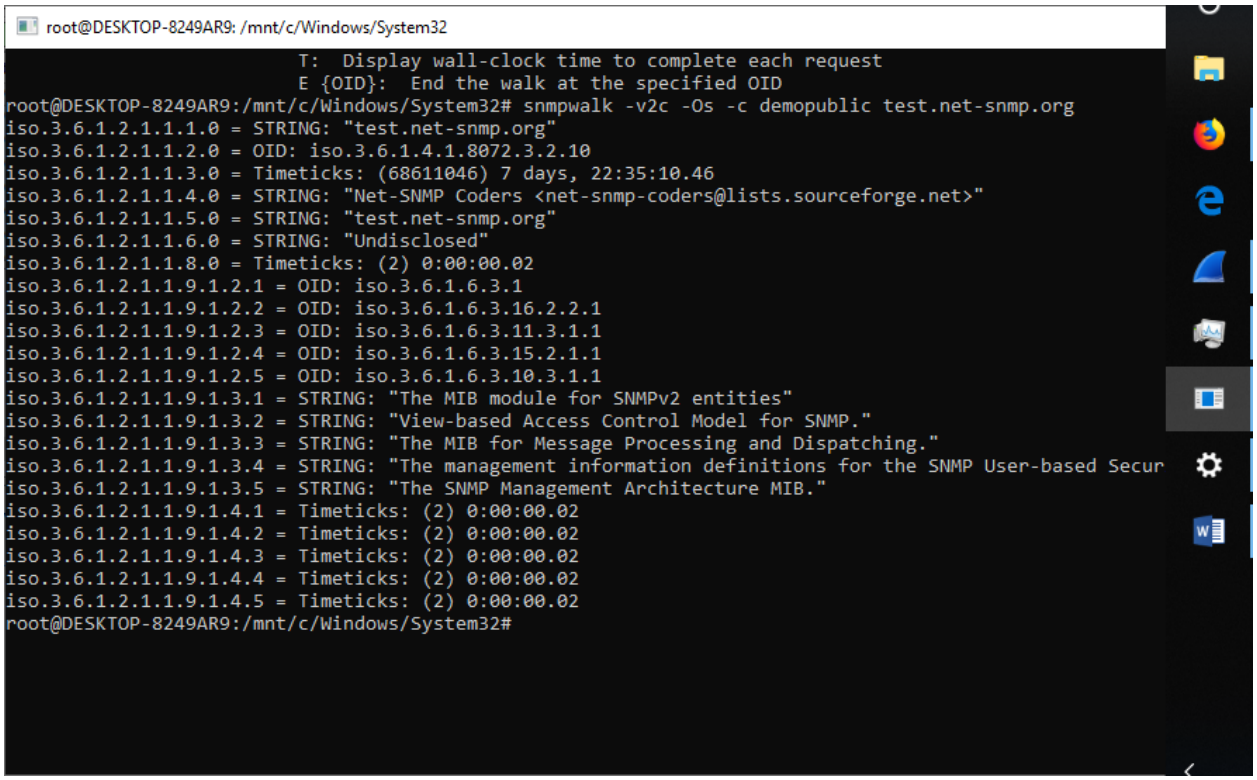
Tipe Paket dari Manager dan Agent

Gambar 1 Tipe Paket dari Manager dan agent

- **Get Request** : Manajer SNMP mengirim permintaan ke agen SNMP untuk mengumpulkan satu atau lebih variabel MIB pada objek tertentu.
- **Get Next Request**: Permintaan ini dibuat setelah yang sebelumnya saja. Manajer SNMP mengirim permintaan ke agen SNMP untuk mengumpulkan satu atau lebih variabel MIB pada objek berikutnya dalam hierarki MIB. Perintah ini memungkinkan permintaan pemindaian pada objek tabel yang diindeks.
- **Get Bulk Request** : Hanya di versi 2 SNMP, permintaan ini disetel GET dan GETNEXT dan memungkinkan untuk mendapatkan variabel MIB di beberapa objek dalam satu tembakan.
- **Set Request**: Mengaktifkan pengelola SNMP untuk mengubah satu atau lebih variabel MIB. Semua variabel MIB tidak dapat diatur, beberapa di antaranya hanya bisa dibaca.
- **Get Response** : Digunakan oleh agen untuk menanggapi permintaan pengelola.
- **Trap**: Agen dapat mengirim paket tanpa pengawasan ini untuk memberi tahu manajer tentang kejadian khusus yang mendesak (perubahan status tautan, kegagalan). Manajer tidak akan membebaskan paket ini.
- **Notification**: Memperkenalkan dengan SNMP versi 2, pemberitahuan dikirim oleh agen kepada manajer untuk menginformasikan peristiwa khusus yang bersifat mendesak (perubahan status tautan, kegagalan). Manajer tidak akan membebaskan paket ini.
- **Inform**: Perkenalkan dengan versi 2, tujuan utama dari paket ini adalah untuk memungkinkan manajer mengelola komunikasi.

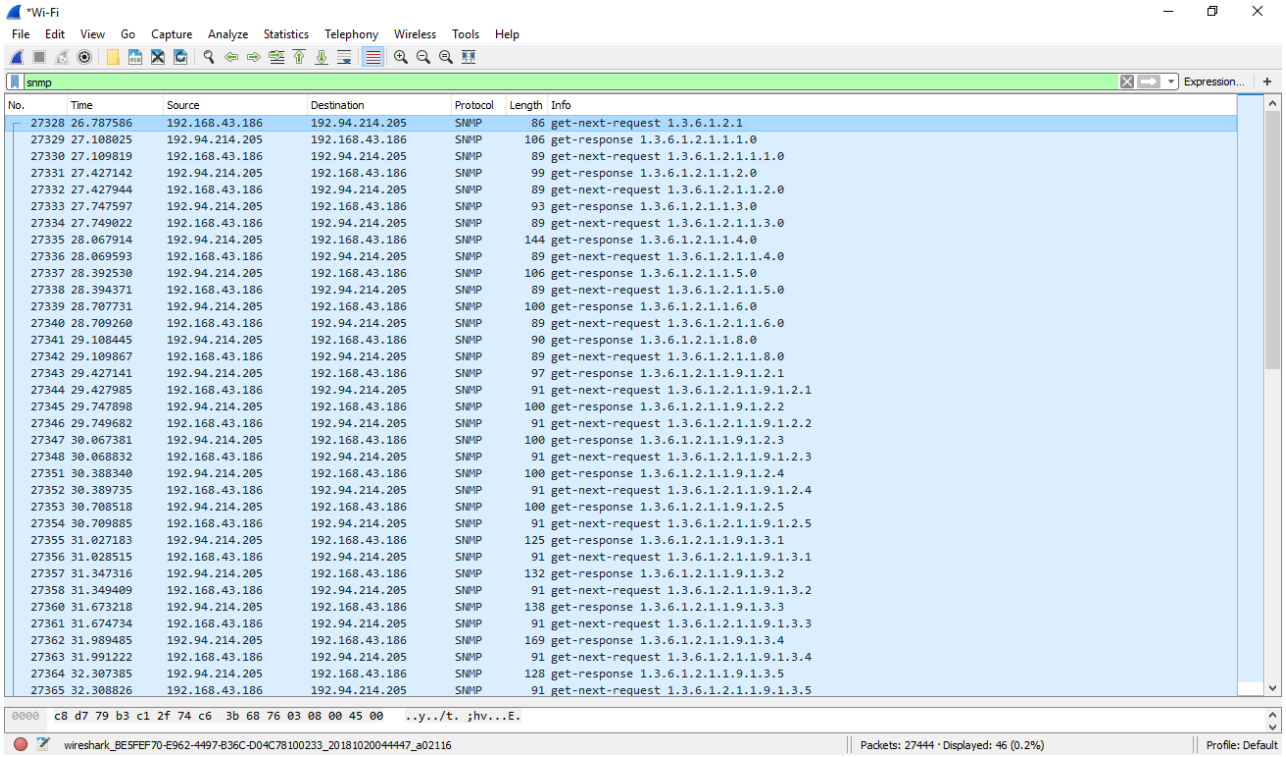
Tapping data dengan wireshark untuk mencari traffick SNMP saya lakukan menggunakan jaringan wifi yang menggunakan tathering dari hangphone saya, terlebih dahulu menginstal program snmp (*get apt install snmp*) pada terminal bash. Pada terminal bash saya menggunakan command : snmpwalk -v2c -On -c demopublic test.net-snmp.org. command tersebut saya gunakan untuk menapilkan protocol snmp pada jaringan yang saya gunakan.

Berikut gambar hasil comandnya



Gambar 2 comand pada terminal bash

Berikut hasil capture trafick pada wireshark yang telah di filter pada bagian snmp



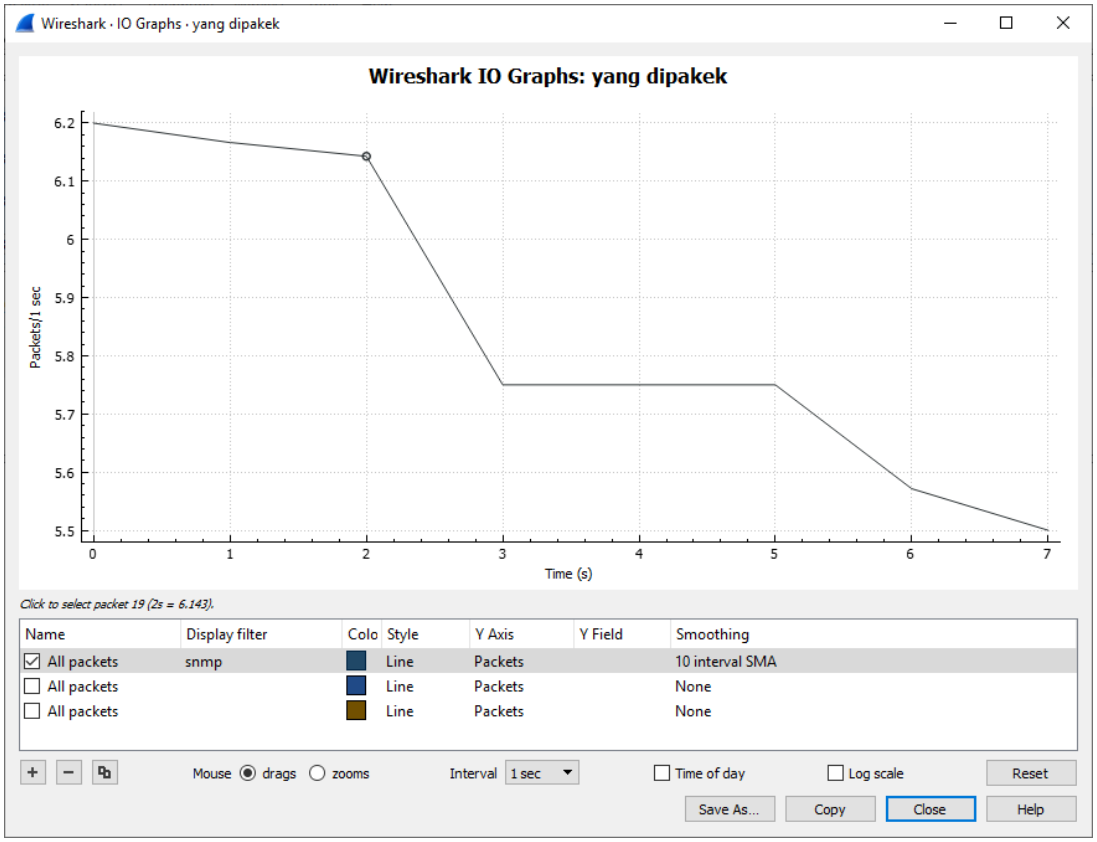
Gambar 3 hasil capture trafick di wireshark

Pada gambar 2 bisa kita lihat bahwa saya menggunakan terminal bash untuk menajalankan command yang nantinya akan membuat service snmpnya berjalan pada pc.

Pada gambar 3 tersebut terlihat hasil filtering dengan keyword “snmp” yang kita masukkan, terlihat beberapa caption sperti *no*, *time*, *source*, *destination*, *protocol*, *data length* dan juga info. Deretan tupple ini memperlihatkan *handshake* yang dilakukan antara kedua alamat. Address pertama 192.168.43.186 merupakan alamat ip manajer sedangkan alamat kedua 192.94.214.205 merupakan alamat router atau agen. Manajer melakukan *request* kepada *agen* berupa *get-next-request (Meminta komponen objek berikutnya dari suatu table atau daftar dari suatu agen)* dan nomor OID yang terlihat pada info, kemudian agen memberikan pesan *get-response (Merespon semua permintaan)* menuju manajer. Proses *trap* ini dilakukan terus menerus.

Berdasarkan gambar 1 dapat kita lihat pada bagian INFO bahwa setiap permintaan 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.

Berikut gambar grafik yang di dapat dari capture trafik di wireshark



Gambar 4 grafik data snmp

```
> Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
> Ethernet II, Src: Azurewav_68:76:03 (74:c6:3b:68:76:03), Dst: QingdaoH_b3:c1:2f (c8:d7:79:b3:c1:2f)
> Internet Protocol Version 4, Src: 192.168.43.186, Dst: 192.94.214.205
> User Datagram Protocol, Src Port: 49709, Dst Port: 161
v Simple Network Management Protocol
    version: v2c (1)
    community: demopublic
  v data: get-next-request (1)
    v get-next-request
        request-id: 1016188932
        error-status: noError (0)
        error-index: 0
      v variable-bindings: 1 item
        v 1.3.6.1.2.1: Value (Null)
            Object Name: 1.3.6.1.2.1 (iso.3.6.1.2.1)
            Value (Null)
```

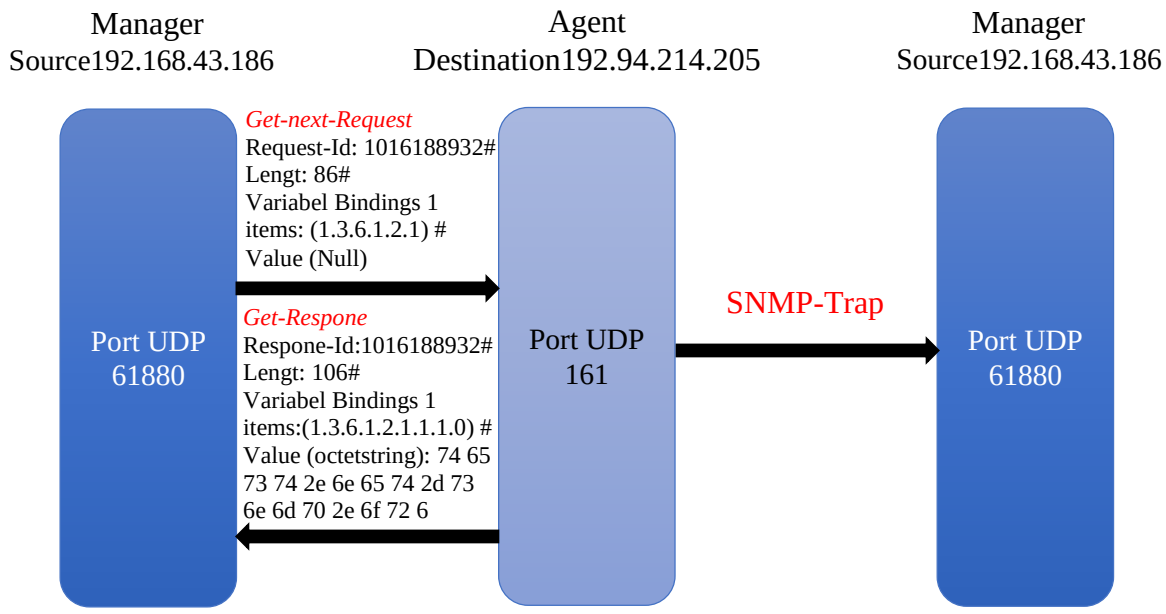
Gambar 5 info detail get-next-request

```
> Frame 32: 169 bytes on wire (1352 bits), 169 bytes captured (1352 bits)
> Ethernet II, Src: QingdaoH_b3:c1:2f (c8:d7:79:b3:c1:2f), Dst: Azurewav_68:76:03 (74:c6:3b:68:76:03)
> Internet Protocol Version 4, Src: 192.94.214.205, Dst: 192.168.43.186
> User Datagram Protocol, Src Port: 161, Dst Port: 49709
v Simple Network Management Protocol
    version: v2c (1)
    community: demopublic
  v data: get-response (2)
    v get-response
        request-id: 1016188947
        error-status: noError (0)
        error-index: 0
      v variable-bindings: 1 item
        v 1.3.6.1.2.1.1.9.1.3.4: 546865206d616e6167656d656e7420696e666f726d617469...
            Object Name: 1.3.6.1.2.1.1.9.1.3.4 (iso.3.6.1.2.1.1.9.1.3.4)
            Value (OctetString): 546865206d616e6167656d656e7420696e666f726d617469...
```

Gambar 6 info detail ger-response

Bisa kita lihat pada gambar diatas, bahwa perbedaan dari ***Get-next-Request*** dan ***Get-Respone*** berada pada nilai valuenya. Saat pertama kali menager mengirim Get-request kepada agent, nilai valuenya adalah null. Tapi kemudian ketiaka agent menanggapi permintaan dari manager, maka nilai valuenya berubah menjadi 74:65:73:74:2e:6e:65:74:2d:73:6e:6d:70:2e:6f:72:67 yang bertipe octetsring. Lalu nilai value tersebut akan dikirim ke manager.

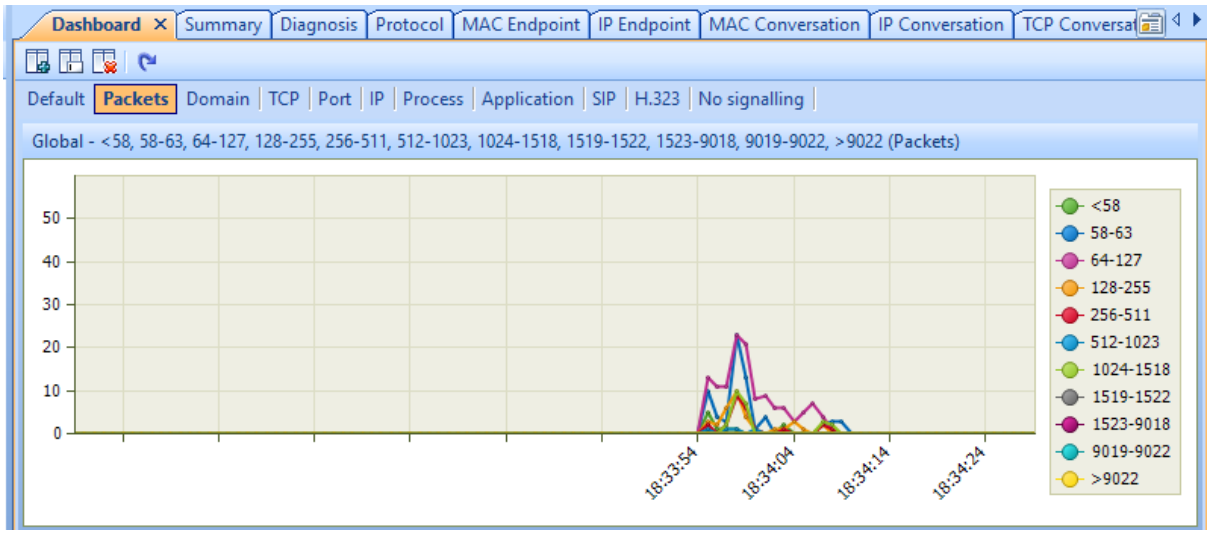
Dibawah ini adalah *three way handshake* SNMP :



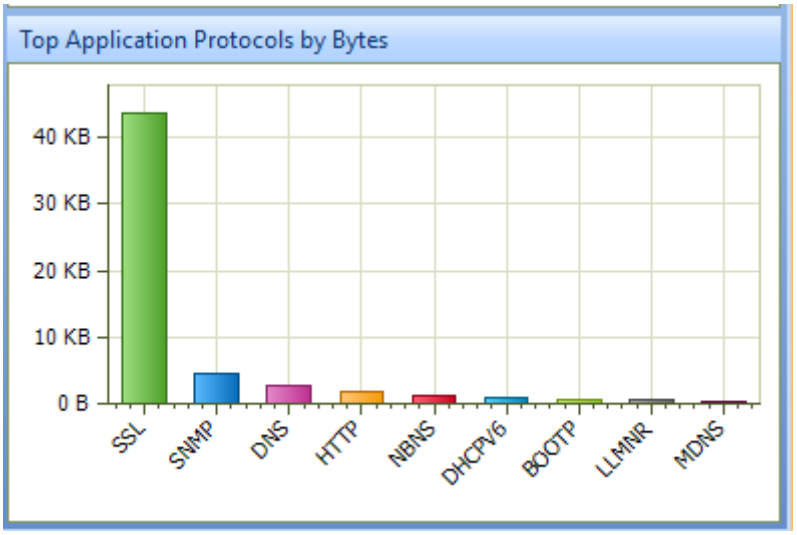
Gambar 7: *Three Way Handshake* SNMP)

C. Visualisasi Traffic Menggunakan Colasoft

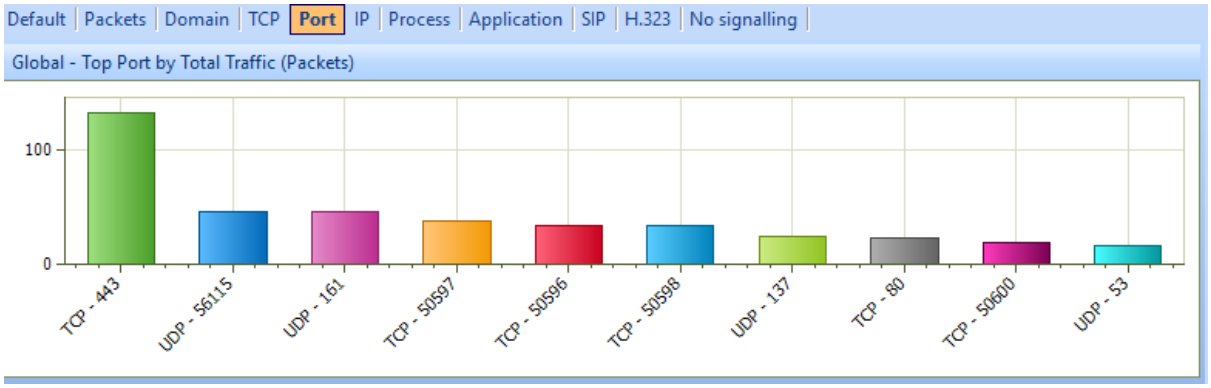
Pada gambar-gambar dibawah ini digunakan software yang berbeda untuk menampilkan traffic dari hasil capture menggunakan wireshark sebelumnya. Software yang digunakan adalah Colasoft Capsa. Jika kita perhatikan, terdapat kemiripan traffic dari software wireshark dan colasoft.



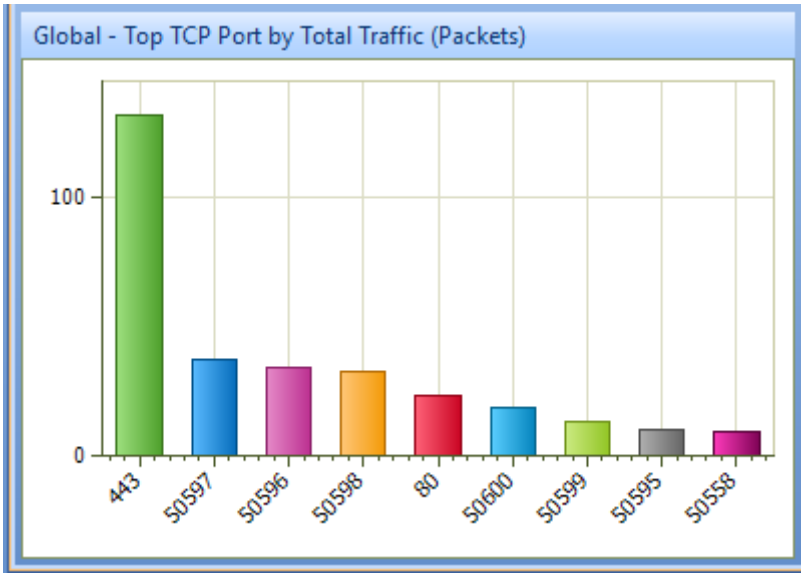
Gambar 8 Traffic data menggunakan Colasoft



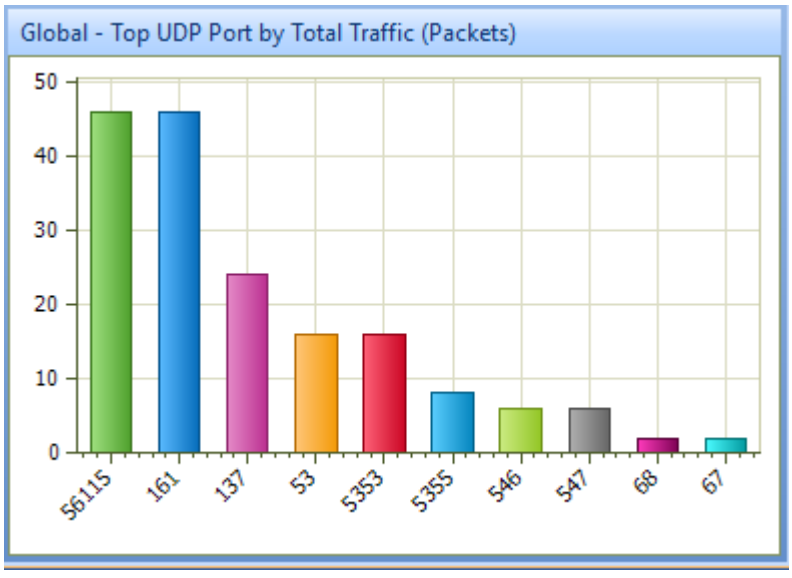
Gambar 9 Tabel Top Applikasi protocol



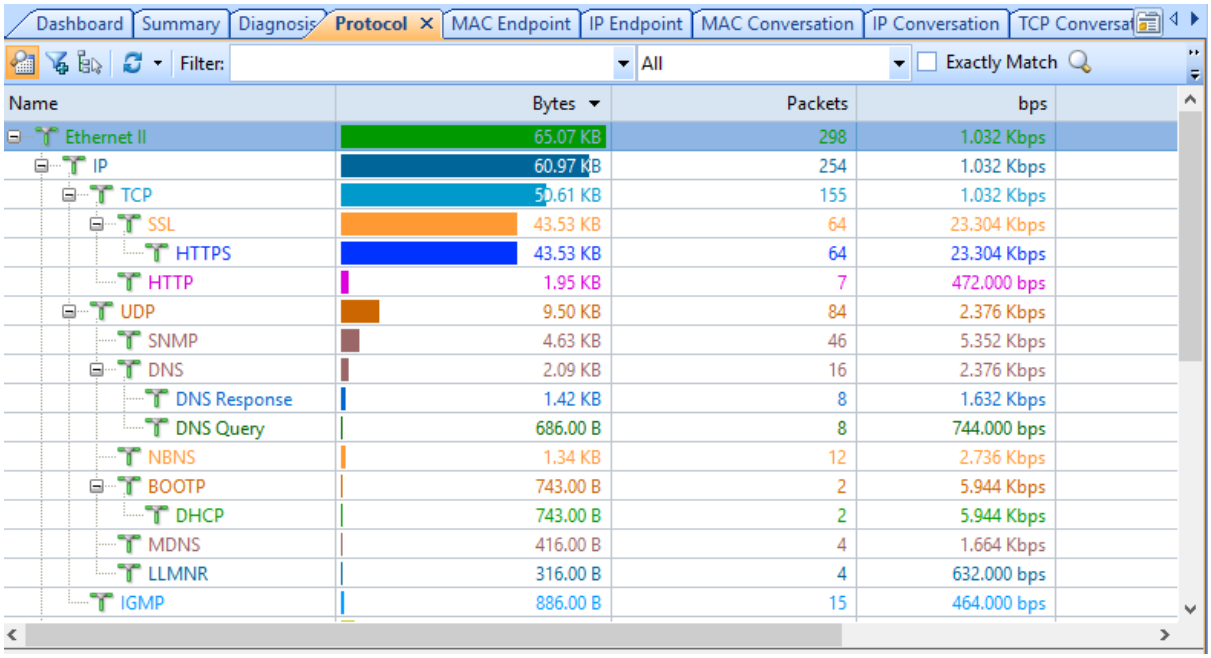
Gambar 10 Top port by total traffic



Gambar 11 Top TCP port by total traffic



Gambar 12 Top UDP port by total traffic



Gambar 13 Tabel Usage setiap protocol

D. Kesimpulan

SNMP merupakan sebuah protokol jaringan yang dibuat agar para administrator jaringan bisa memonitoring perangkat jaringan mereka dari pc mereka secara realtime. SNMP ini akan membantu para administrator untuk mengetahui bagaimana keadaan perangkat yang mereka miliki serta ada tidaknya keanehan pada trafik jaringan mereka.

Daftar Pustaka

[1] M. Rizky, D. Jurusan, T. Elektro, F. Teknologi, and U. Andalas, “IMPLEMENTASI PROTOKOL SNMP UNTUK JARINGAN Abstrak,” vol. 1, no. 1, pp. 15–19, 2013.

[2] D. Stiawan, D. Jurusan, S. Komputer, and F. Unsri, “Network Management : Optimalisasi untuk mencapai High Reliability Sisi Teknis …,” no. i.

[3] G. D. Harmawan and U. Gunadarma, “Aplikasi Pemantauan Jaringan Dengan Agen SNMP Menggunakan Pemrograman TCL Dengan Perluasan Scotty.”