MANAGEMENT JARINGAN

(TAPPING DATA SNMP MENGUNAKAN WIRESHARK)

Nama : M. Kadapi

Nim : 09011181520119

Kelas : SK7B

Dosen Pengampuh : Dr. Deris Stiawan, M.T., P.HD

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

SNMP merupakan sebuah protokol jaringan yang didesain bagi pengguna khususnya administrator jaringan untuk memonitor aktifitas jaringan komputer dan mengontrol sebuah komputer atau server secara sistematis dari jarak jauh. SNMP bekerja dengan mengumpulkan data informasi dari elemen-elemen jaringan dengan parameter dan variabel tertentu dan menyimpannya dalam sebuah database.

SNMP terdiri atas tiga elemen sebagai berikut:

- **Manager** yaitu bertugas sebagai manajemen jaringan yang mengumpulkan data informasi dari elemen-elemen jaringan yang ingin dimonitoring dan atau dikontrol. Bentuk dari manager ini berupa perangkat lunak yang didesain sedemikian rupa sekaligus memiliki fungsi antarmuka yang baik bagi penggunanya dalam hal ini network administrator jaringan. Perangkat lunak manager ini bisa di install di server yang sekaligus sebagai database server bagi data informasi SNMP, namun juga bisa di install pada dekstop atau laptop bahkan *mobile device* dengan syarat server databasenya terpisah.

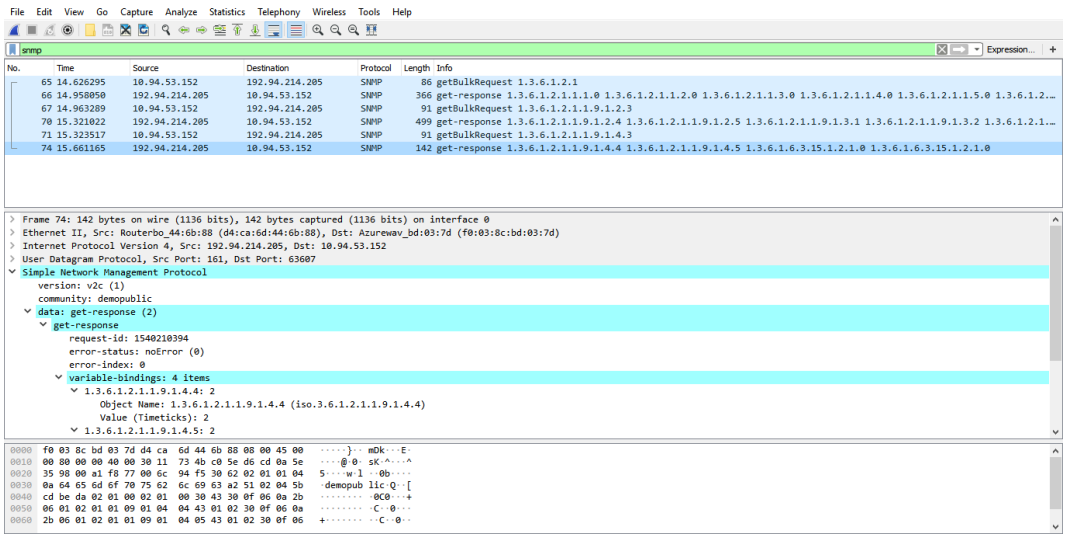
- **MIB (*Management Information Base*)** yaitu database dari data informasi yang dikumpulkan oleh manager dari agen yang tersimpan dalam database server. Struktur data dalam MIB ini bersifat hirarki dan memiliki aturan sedemikian rupa sehingga informasi setiap variabel dapat dikelola atau ditetapkan dengan mudah.

- **Agen** yaitu suatu elemen jaringan yang dimonitoring atau dikontrol oleh manager. Pada umumnya perangkat jaringan seperti router dan server difungsikan sebagai agen dalam sistem manajemen jaringan. Hal ini disebabkan lalu lintas trafik data dengan jumlah yang besar melalui atau bermuara pada kedua perangkat jaringan tersebut. Setiap agen mempunyai database yang bersifat lokal dengan variabel-variabel tertentu, artinya secara default informasi disimpan dalam disk lokal dan digunakan oleh sistem operasi internal. Protokol SNMP yang diaktifkan pada suatu agen

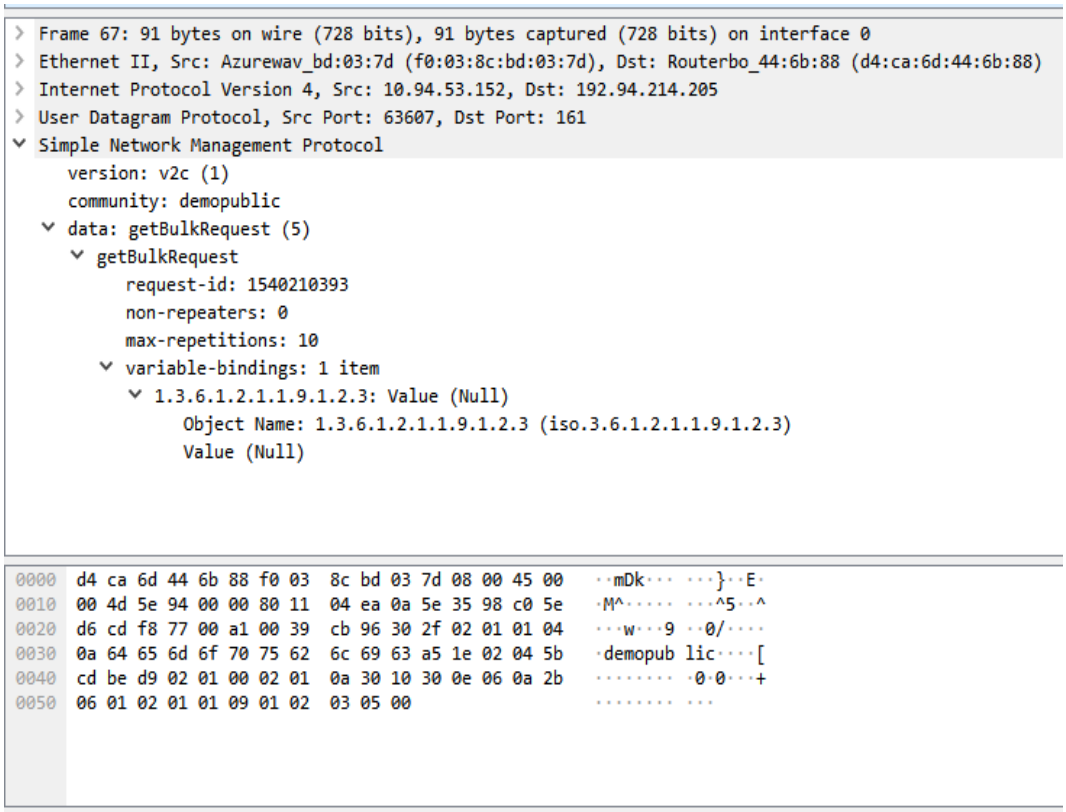
akan menjadikan data informasi agen seperti aktifitas trafik, dan keadaan proses di sistem internal dan kapasitas sistem dapat dikirim ke manager untuk dikelola lebih lanjut.

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. Struktur komunikasi antar elemen SNMP dapat dilihat pada gambar 1, yaitu Agen yang memiliki MIB akan memberikan data informasi yang diperlukan tapi tidak semua oleh manager menggunakan transport UDP yang berorientasi pada kecepatan pengiriman.

Pertama saya masuk ke windows update setting terus kita pilih “for development” kemudian pilih “Develover mode”, setelah itu kita menunggu beberapa saat dia mengistall, apabila sudah selesai selanjutnya kita menginstall Ubuntu pada windows. Fungsi kita menginstall Fungsi dari Ubuntu tersebut adalah untuk menuliskan commen atau perintah yang berfungsi agar SNMP itu bias terbaca pada saat kita tapping. Saya melakukan tapping data dengan wireshark dengan menggunakan wifi public di perpustakaan Unuversitas Sriwijaya.

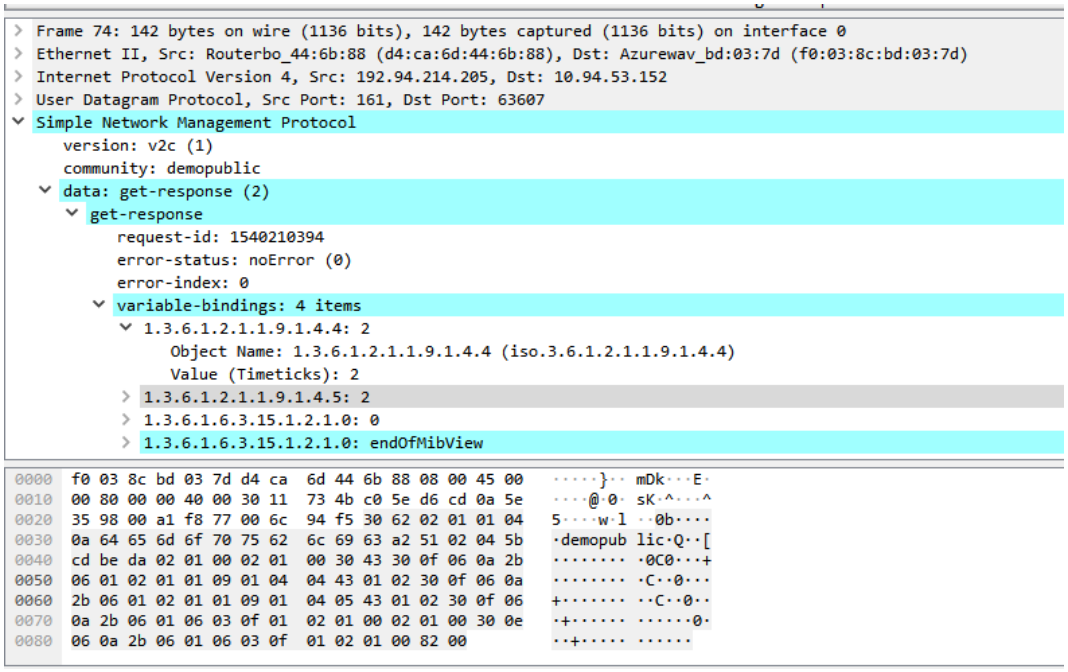


Gambar 1 Tapping Data



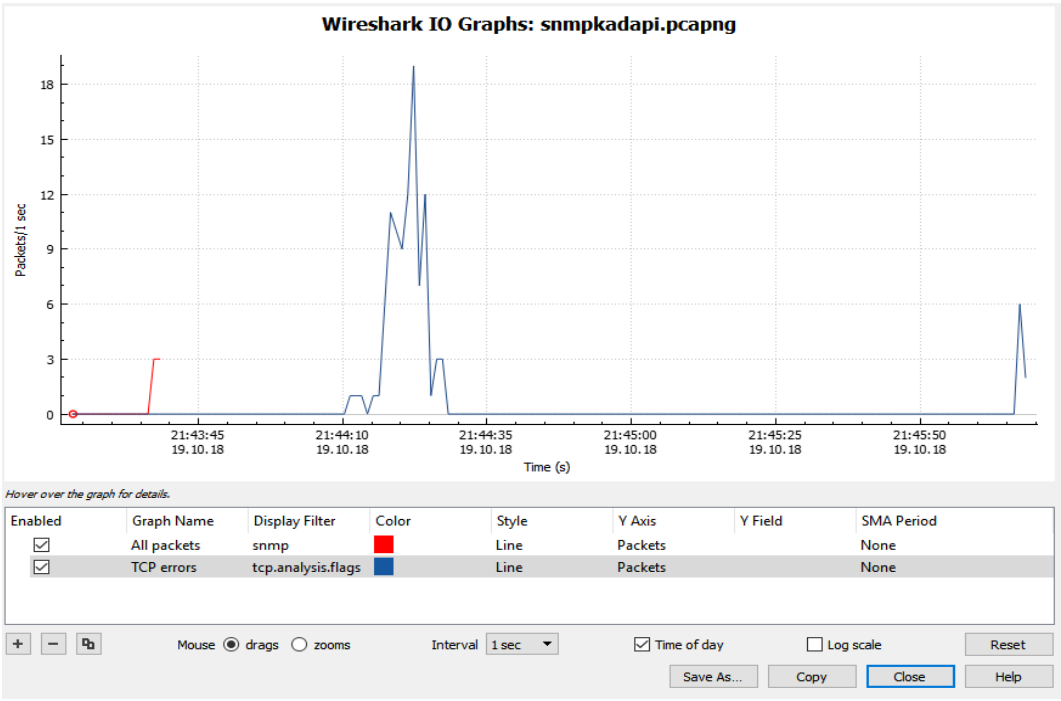
Gambar 2 IP Request

Gambar diatas merupakan sebuah capturan dari pcaps menggunakan aplikasi wireshark dimana pada gambar tersebut menjelaskan tentang bagaimana IP melakukan request. Dari capturan diatas IP source 192.94.214.205 dan IP destination 10.94.53.152 dan menggunakan protocol SNMP dengan request-id: 1540210393 pada variable binding terdapat 1 items dan saya ambil 1 contoh 1.3.6.1.2.1.1.9.1.2.3: Value (Null) dan Object Name: 1.3.6.1.2.1.1.9.1.2.3 (iso.3.6.1.2.1.1.9.1.2.3 maksud dari angka 1.3.6.1.2.1.1.9.1.2.3 yaitu 1 merupakan ISO, 3 merupakan identification ISO 6 US dod, 1 merupakan angka internet, 2 merupakan management, 1 merupakan MIB , kemudian 2 lagi merupakan protocol SNMP dan 3 merupakan datagram dari SNMP, nah dari variable variable diatas terbentuklah satu kesatuan variable saat IP meminta resquest.



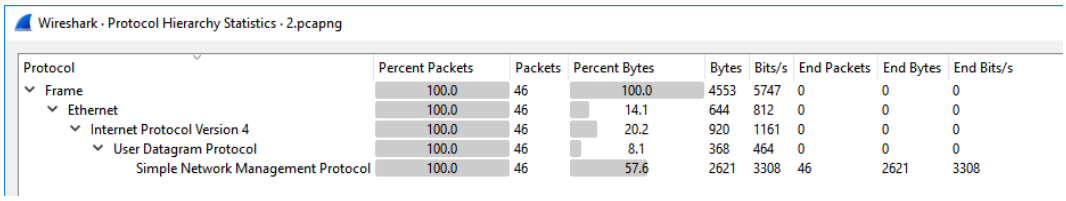
Gambar 3. IP Response

Gambar 3 merupakan sebuah capturan dari pcaps menggunakan aplikasi whiresharkdimana pada gambar tersebut menjelaskan tentang bagaimana IP melakukan response. Dari capturan diatas IP source 192.94.214.205 dan IP destination 10.94.53.152 dan menggunakan protocol SNMP. Cara perhittungan variable sama dengan saat IP melakukan request.



Gambar 4. Grafik SNMP dan All Packet

Pada gambar diatas dapat di lihat grafik perubahan dari paket protocol SNMP dan All Packet yang ada pada jaringan wifi di perpustakaan Universitas Sriwijaya pada jam 21.43.20 – 21.43.50 WIB. Pada garis yang berwarna merah melambangkan paket SNMP yang mana jumlah paket SNMP sebanyak 46 paket karena pada saat mengcapture saya rentan waktunya tidak begitu lama. Untuk garis yang berwarna merah melambangkan paket dari seluruh paket yang melintasi jaringan yang ada pada wifi tersebut.

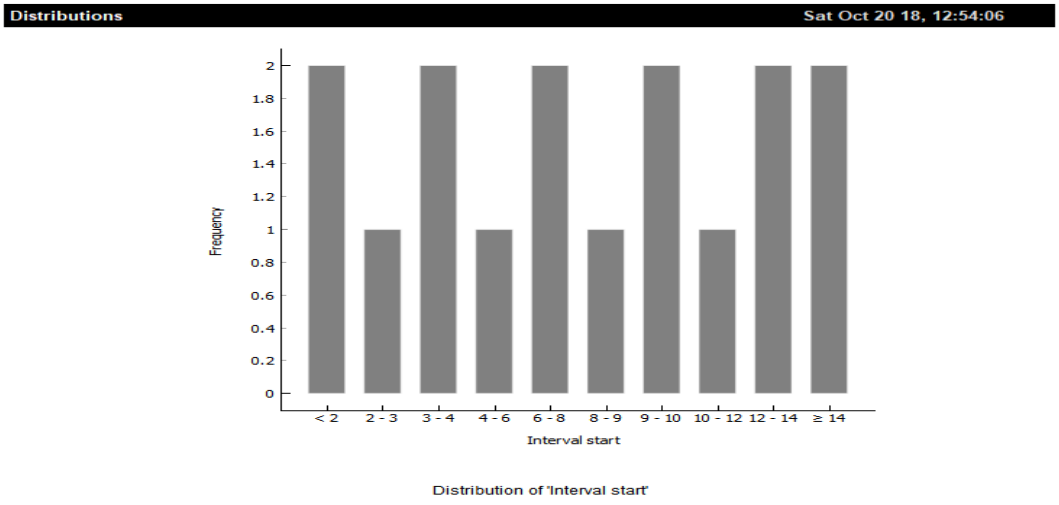

Wireshark · Protocol Hierarchy Statistics · 2.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	46	100.0	4553	5747	0	0	0
Ethernet	100.0	46	14.1	644	812	0	0	0
Internet Protocol Version 4	100.0	46	20.2	920	1161	0	0	0
User Datagram Protocol	100.0	46	8.1	368	464	0	0	0
Simple Network Management Protocol	100.0	46	57.6	2621	3308	46	2621	3308

Gambar 5. Tabel statistik protocol

Pada gambar diatas terdapat 5 protokol dengan persen packet yang sama yaitu 100, dan memiliki packet sebanyak 46. Dan memiliki perbedaan pada present, bytes, bits.

Gambar grafik dibawah ini merupakan hasil dari tapping data yang divisualisasi dengan menggunakan orange. Pada grafik tersebut terdapat ± 14 interval start. Dimana interval <2, 3-4, 6-8, 9-10, 12-14, ≥14 itu memiliki frekuensi sebesar 2Hz. Dan interval 2-3, 4-6, 8-9, 10,12 itu memiliki frekuensi 1Hz.



Gambar 6 grafik distributions orange

Kesimpulan :

1. 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.
2. SNMP merupakan sebuah protokol jaringan yang didesain bagi pengguna khususnya administrator jaringan untuk memonitor aktifitas jaringan komputer dan mengontrol sebuah komputer atau server secara sistematis dari jarak jauh.

Daftar Pustaka

1. http://pasman-pcr.blogspot.com/2014/07/snmp-simple-network-management-protocol_4.html.

2. S. I. Lestariningati and F. Rozak, “Pembangunan Aplikasi Monitoring Jaringan Berbasis Web Menggunakan Simple Network Management Protocol (Snmp),” vol. 12,
no. 2, pp. 211–222, 2012