MANAGEMENT JARINGAN

(TRAFFIC SNMP)

NOVIT HARDIANTO

09011281520086

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

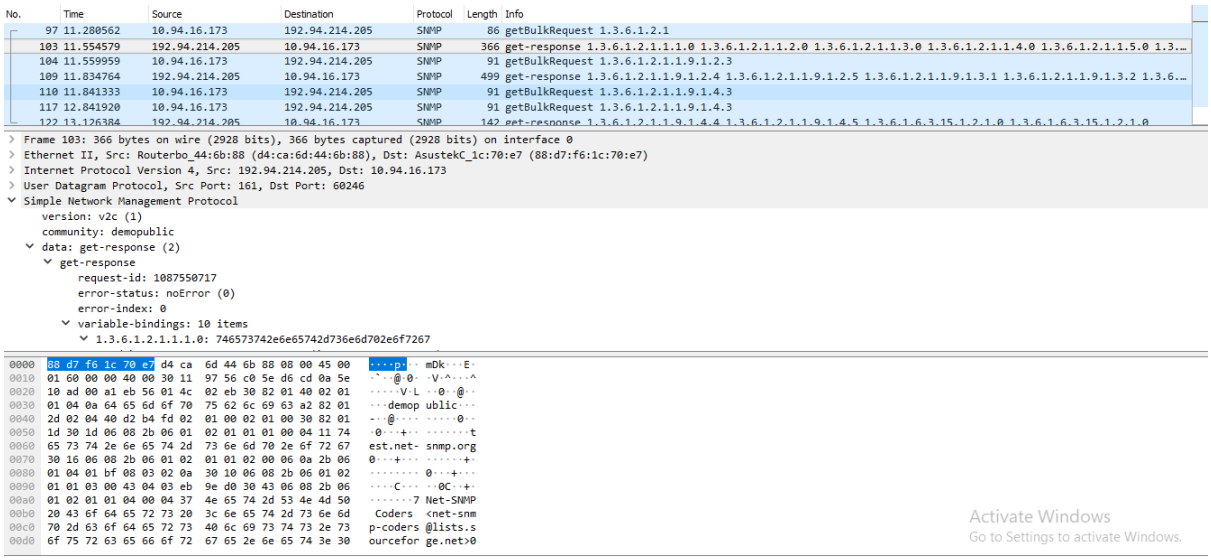
2018

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

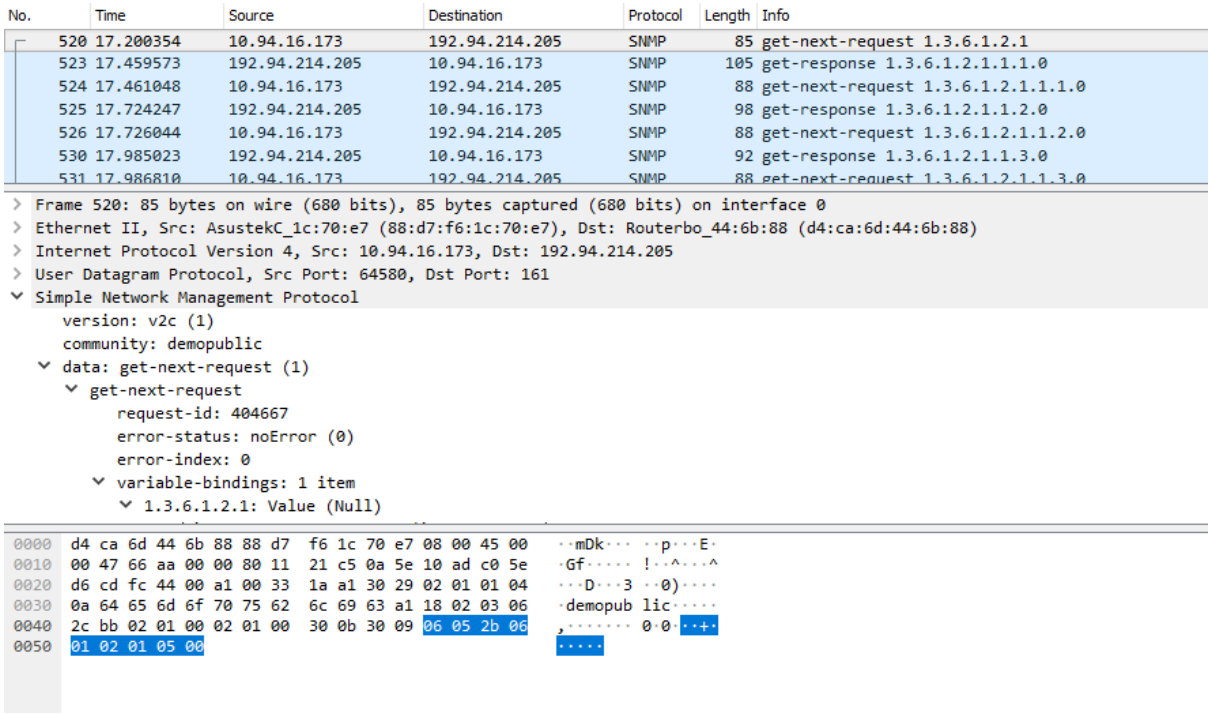
Wireshark merupakan salah satu dari tool Network Analyzer yang biasa digunakan oleh Network Administrator pemecahan masalah jaringan, analisis, perangkat lunak dan pengembangan protokol komunikasi, dan pendidikan. Awalnya bernama Ethereal, dan pada Mei 2006 proyek ini berganti nama menjadi WIreshark karena masalah merek dagang. Bahasa Pemrograman yang digunakan adalah bahasa C dengan lisensi public umum GNU. Wireshark banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis. Seperti namanya, Wireshark mampu menangkap paket-paket data/informasi yang bertebaran dalam jaringan yang kita “intip”. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tidak jarang tool ini juga dapat dipakai untuk sniffing (memperoleh informasi penting spt password email atau account lain) dengan menangkap paket-paket yang berseliweran di dalam jaringan dan menganalisanya. Untuk menggunakan tool ini pun cukup mudah. Kita cukup memasukkan perintah untuk mendapatkan informasi yang ingin kita capture (yang igin diperoleh) dari jaringan kita.

Taping data respons



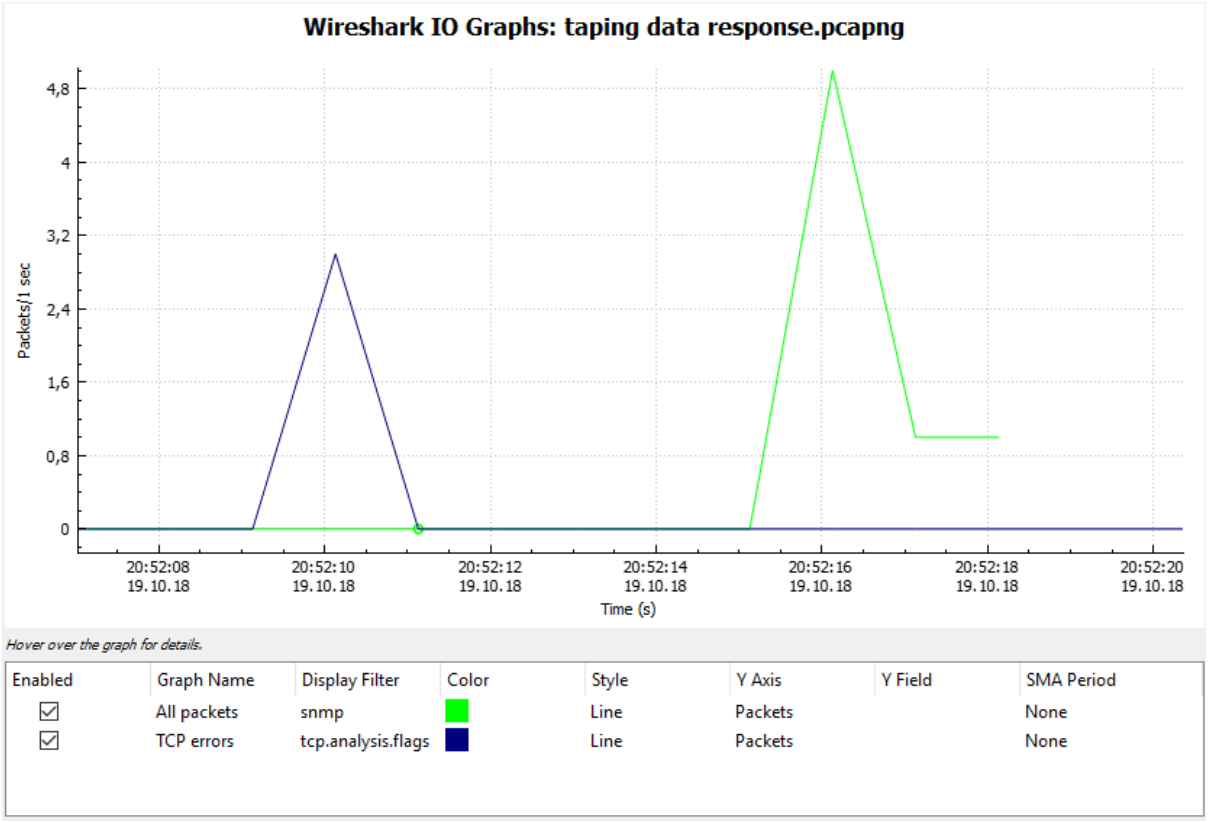
Dari taping data dia atas dapat kita simpulkan bahwa saya menggunakan aplikasi whireshark dimana pada gambar tersebut menjelaskan tentang bagaimana IP melakukan response. Dari capturan diatas IP source 192.94.214.205 dan IP destination 10.94.16.173 dan menggunakan protocol SNMP. Cara perhittungan variable sama dengan saat IP melakukan request

Taping data request



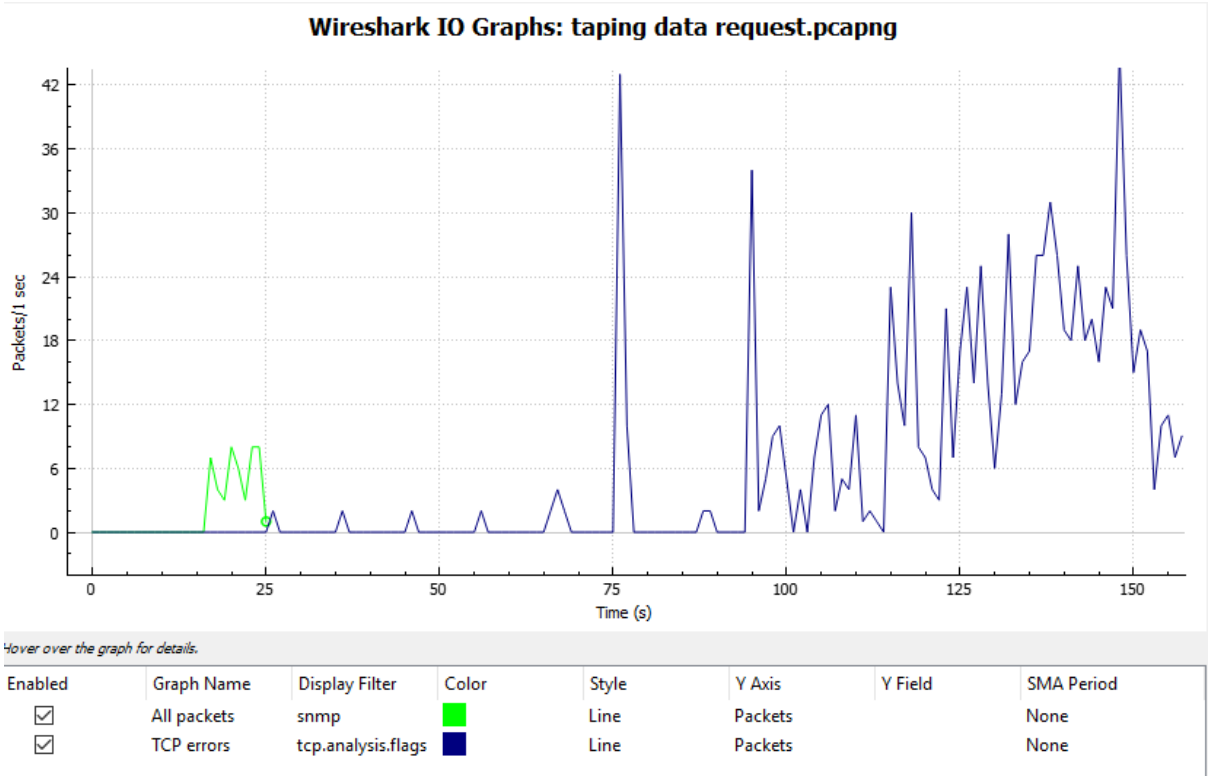
Dari gambar di atas merupakan sebuah capturan dari pcaps menggunakan aplikasi whireshark dimana pada gambar tersebut menjelaskan tentang bagaimana IP melakukan request. Dari capturan diatas IP source 10.94.16.173 dan IP destination 192.94.214.205 dan menggunakan protocol SNMP dengan request-id: 404667 pada variable binding terdapat 1 items dan saya ambil 1 contoh 1.3.6.1.2.1: Value (Null) dan Object Name: 1.3.6.1.2.1 (iso.3.6.1.2.1) maksud dari angka 1.3.6.1.2.1 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.

Grafik data respone



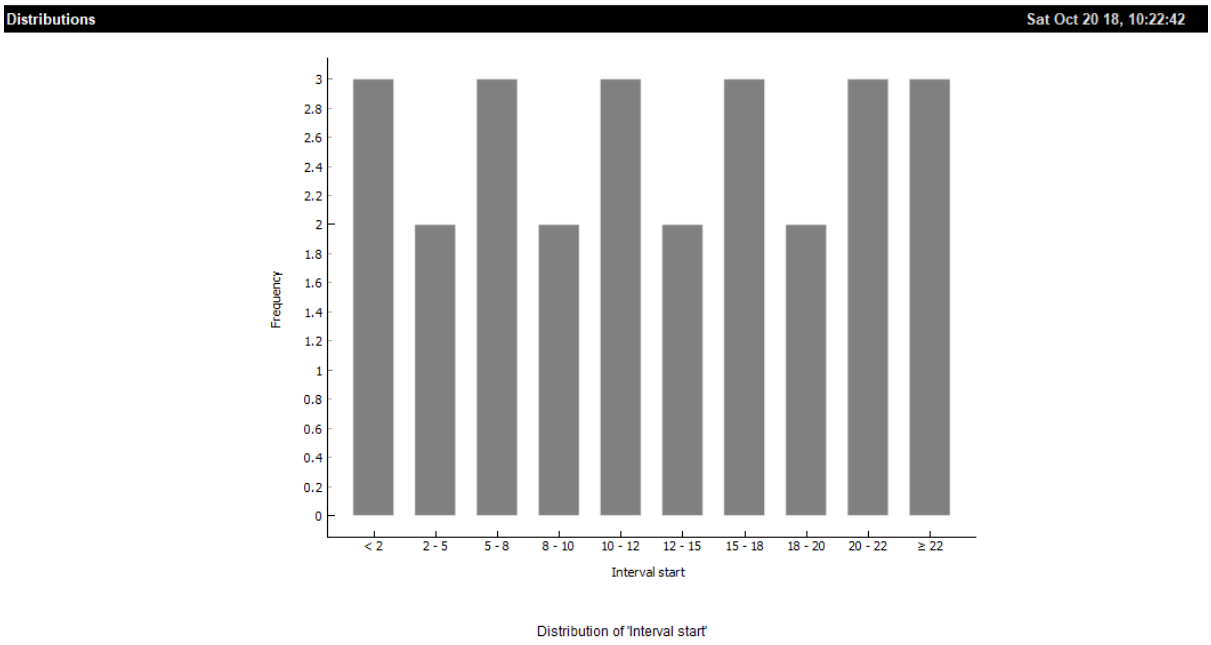
Dari grafik yang dapat di atas mengunakan wifi publik perpustkaan unsri disini dapat dilihat ada dua grafik yaitu (Grafik All packets) dan (Grafik TCP errors), dan All packets tersebut adalah data seluruh pengunaan mengunakan snmp pada wireshark dan dapat dilihat pada gambar di atas pengunaan data snmp banyaknya request dari penguna jaringan dan banyak nya paket yang masuk sebanyak 48 pakets karena saat saya mencapture agak begitu lama . dan garis utuk warna biru melambangkan paket seluruh yang melintas yang ada pada wifi perpustakaan unsri tersebut.

Grafik data request



Dari grafik yang dapat di atas mengunakan wifi publik perpustkaan unsri disini dapat dilihat ada dua grafik yaitu (Grafik All packets) dan (Grafik TCP errors), dan All packets tersebut adalah data seluruh pengunaan mengunakan snmp pada wireshark dan dapat dilihat pada gambar di atas pengunaan data snmp sedikitnya request dari penguna jaringan dan garis utuk warna biru melambangkan paket seluruh yang melintas atau banyak nya request dari penguna yang ada pada wifi perpustakaan unsri tersebut.

Grafik distribution



Dapat di lihat pada grafik diatas menampilkan hasil dari PCAP pada wireshark yang telah di masukkan datanya di orange gambar diatas merupakan tingkat data protocol SNMP yang telah di dapat dari wifi perpustakaan Universitas Sriwijaya. dan hasil pengamatan yang telah dilakukan bahwa dalam protocol SNMP terjadi interaksi antara manager dan agent dengan saling berkirim pesan berupa permintaan manager yang meminta request kepada agent setelah agent menerima permintaan dari manager maka agent akan meresponse permintaan tersebut.

Daftar pustaka

[1] Asep, 2010 “http://jaringankomputer.wordpress.com/2009/07/09/tentang-wireshark-dan-pemakaiannya”

[2] indyawan, farras ” wireshark adalah” https://medium.com/@kitaadmin/wireshark-adalah-pengertian-dan-fungsi-256dc09c8292

[3] J. Schippers and A. Pras, “SNMP Traffic Analysis : Approaches , Tools, and FirstResult,”pp.323-332,2007.