Visualisasi Traffik SNMP (*Simple Network Management Protocol*) di Kondisi Jaringan *WiFi* Publik Fakultas Ilmu Komputer Universitas Sriwijaya dengan Wireshark, Rumint, dan Orange

(Tugas Mata Kuliah Manajemen Jaringan)

Nama: Azwar Hidayat

NIM: 09011281520126

Jurusan Sistem Komputer

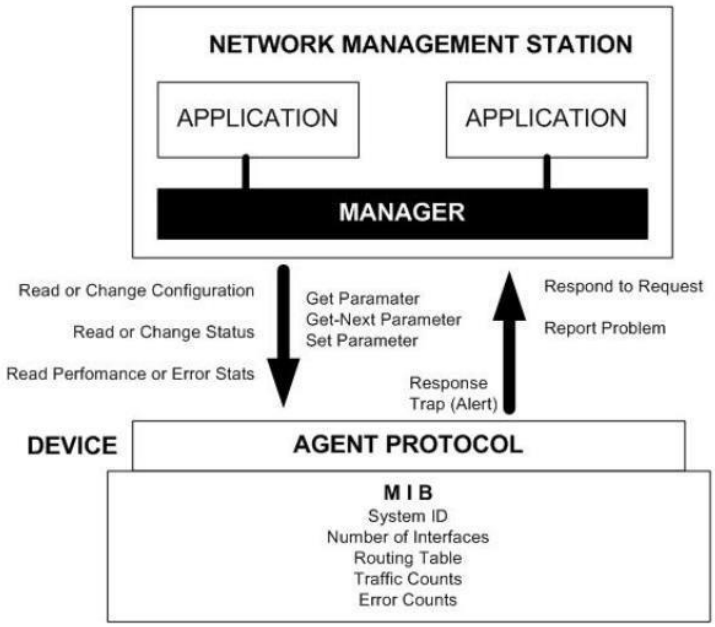
Fakultas lmu Komputer

Universitas Sriwijaya

2018

A. Teori Dasar

Elemen-elemen SNMP



Gambar 1. Interaksi Agent dengan Manager

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 (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:

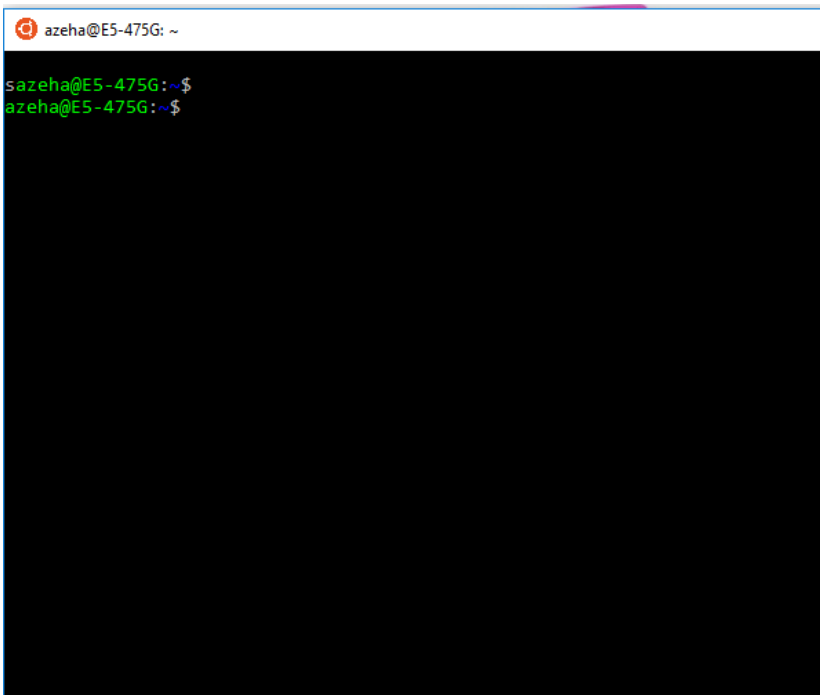
- Setiap object mempunyai ID unik (OID).
- MIB mengasosiasikan setiap OID menggunakan label dan parameter lain.
- MIB bertindak sebagai kamus data digunakan untuk menyusun terjemahan pesan SNMP.

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.

B. Langkah – Langkah

1. Pada percobaan kali ini, saya menggunakan os windows dan menggunakan tools windows for linux



Gambar 2. Linux For windows

2. Menghubungkan dengan jaringan publik yang dimana pada percobaan ini menggunakan wifi Fakultas Ilmu Komputer Universitas Sriwijaya Kampus Indralaya.
3. Menginstall snmp dengan command **sudo apt install snmp**.

```
azeha@E5-475G:~$ sudo apt install snmp
Reading package lists... Done
Building dependency tree
Reading state information... Done
snmp is already the newest version (5.7.3+dfsg-1.8ubuntu3).
The following package was automatically installed and is no longer required:
  libfreetype6
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Gambar 3. Sudo apt Install snmp

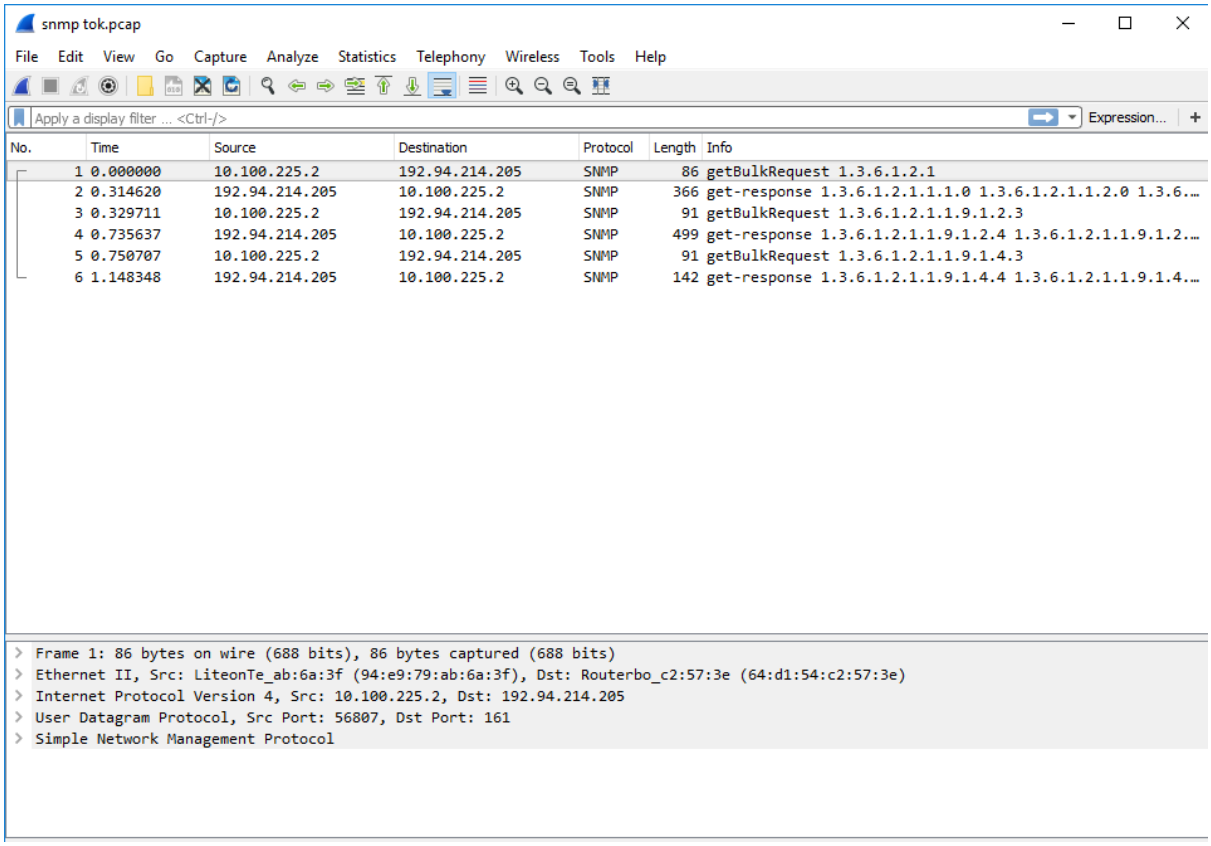
4. Melakukan SNMP bulkwalk. Snmpbulkwalk adalah Aplikasi dari SNMP yang menggunakan SNMP GETBULK request untuk melakukan query ke entitas secara efficient untuk serangkaian list Informasi. Secara konseptual, sistem akan mencari OID

(Object identifier) yang memberikan spesifikasi yang dapat dicari menggunakan request GETBULK. Seluruh variabeldi subtree dibawah OID akan di query dan nilainya akan di tampilkan kepada user. Apabila OID tidak ditemukan, maka snmpbulkwalk akan mencarinya di MIB-2. Command yang digunakan adalah **snmpbulkwalk –v2c –Os demopublic test.net-snmp.org**

```
azeha@E5-475G:~$ snmpbulkwalk -v2c -Os -c demopublic test.net-snmp.org
iso.3.6.1.2.1.1.1.0 = STRING: "test.net-snmp.org"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (73743740) 8 days, 12:50:37.40
iso.3.6.1.2.1.1.4.0 = STRING: "Net-SNMP Coders <net-snmp-coders@lists.sourceforge.net>"
iso.3.6.1.2.1.1.5.0 = STRING: "test.net-snmp.org"
iso.3.6.1.2.1.1.6.0 = STRING: "Undisclosed"
iso.3.6.1.2.1.1.8.0 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The management information definitions for the SNMP User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (2) 0:00:00.02
```

Gambar 4. Hasil dari snmpbulkwalk

5. Lakukan filtering paket di wireshark hasil dari capture selama kita melakukan bulkwalk tadi dan akan didapatkan hasil seperti ini.



Gambar 5. PCAP SNMP

Berdasarkan gambar 5, 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. Pada percobaan ini, SNMP yang didapatkan adalah snmp v2.

Beberapa pesan umum snmp :

Inform-request : Pesan manajer ke manajer yang menjelaskan MIB lokal

Set-request : Memperbarui sebuah variabel atau lebih

Get-bulk-request : Mengambil sebuah tabel berukuran besar

Get-next-request : Meminta variabel setelah saat itu

Get-request : Meminta nilai sebuah variabel atau lebih

SNMPv2-trap : Laporan tiap agen ke manager

Beberapa Kelebihan dari SNMP v2 yaitu:

- komunikasi antar NMS yang meningkatkan fleksibilitas dan skalabilitas dari suatu jaringan yang dikelola
- Peningkatan keamanan dengan adanya Enkripsi (DES), Autentikasi, dan Otorisasi
- Peningkatan efisiensi dan performa dengan adanya bulk transfer yang menyebabkan manajemen jaringan dapat dijalankan pada jaringan WAN dengan bandwidth kecil.
- mendukung protokol jaringan selain UDP/IP, seperti OSI, NetWare IPX/SPX, dan Appletalk.

Perbedaan antara SNMPv1 dengan SNMPv2 :

Perbedaan utama antara V1 dan V2 adalah SNMPv2 menambahkan beberapa paket, seperti GETBULK-PDU yang memungkinkan kita untuk meminta sejumlah besar paket **GetNext** atau dalam satu paket. SNMPv1 juga telah ditetapkan untuk menggunakan original SMI, tetapi SNMPv2 menggunakan SMIv2 yang lebih baik, dengan lebih banyak jenis data seperti 64-bit counter. Tapi sebagian besar perbedaan antara V1 dan V2 adalah berupa hal yang bersifat internal dan pengguna akhir mungkin tidak akan melihat adanya perbedaan antara keduanya.

Branch	OID	RFIC
Snmpv2	**{1.3.6.1.6}**	1442
SnmpDomains	**{1.3.6.1.6.1}**	1442,1902,1906
SnmpProxys	**{1.3.6.1.6.2}**	1442,1902,1906

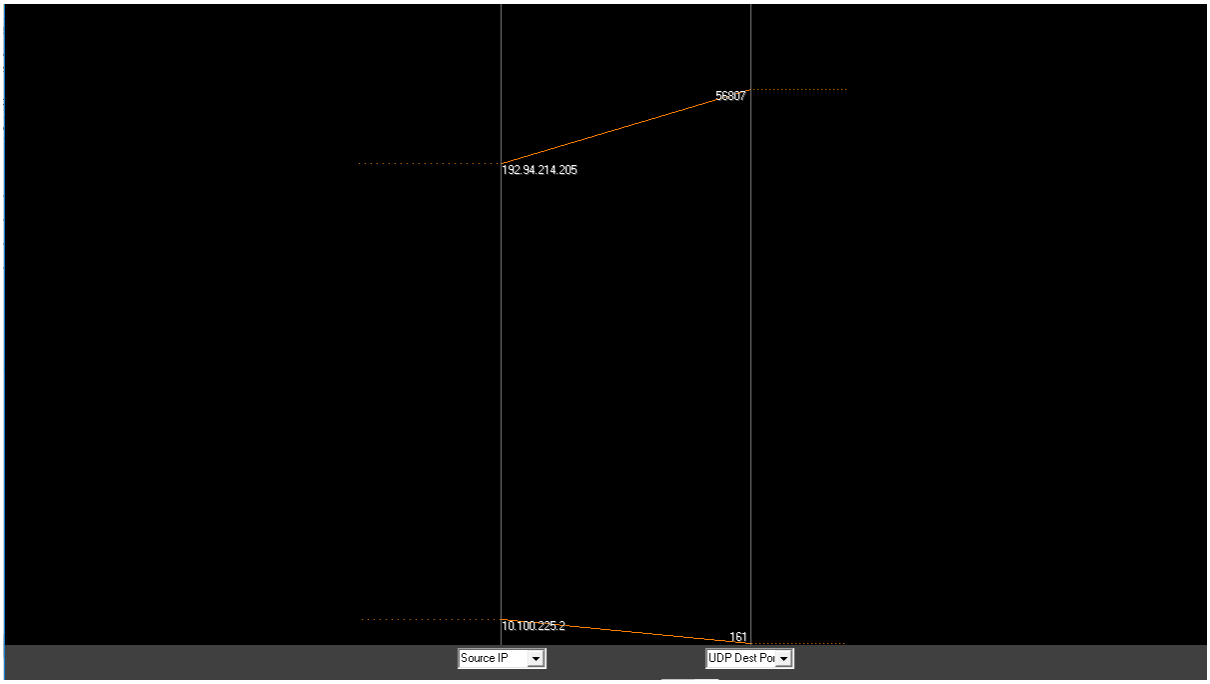
snmpModules	**{1.3.6.1.6.3}**	1442,1902
snmpMIB	**{1.3.6.1.6.3.1}**	1450, 1907
snmpM2M	**{1.3.6.1.6.3.2}**	1451
partyMIB	**{1.3.6.1.6.3.3}**	1447

Hasil tersebut kemudian di visualisasikan dengan menggunakan 2 tools yaitu orange dan rumint.

Hasil visualisasi Traffic dengan rumint

1. Load file Pcap ke dalam *rumint*
2. Lalu klik ***loop*** dan ***play*** maka paket akan berjalan secara *loop*
3. Lalu pilih ***view – combined***

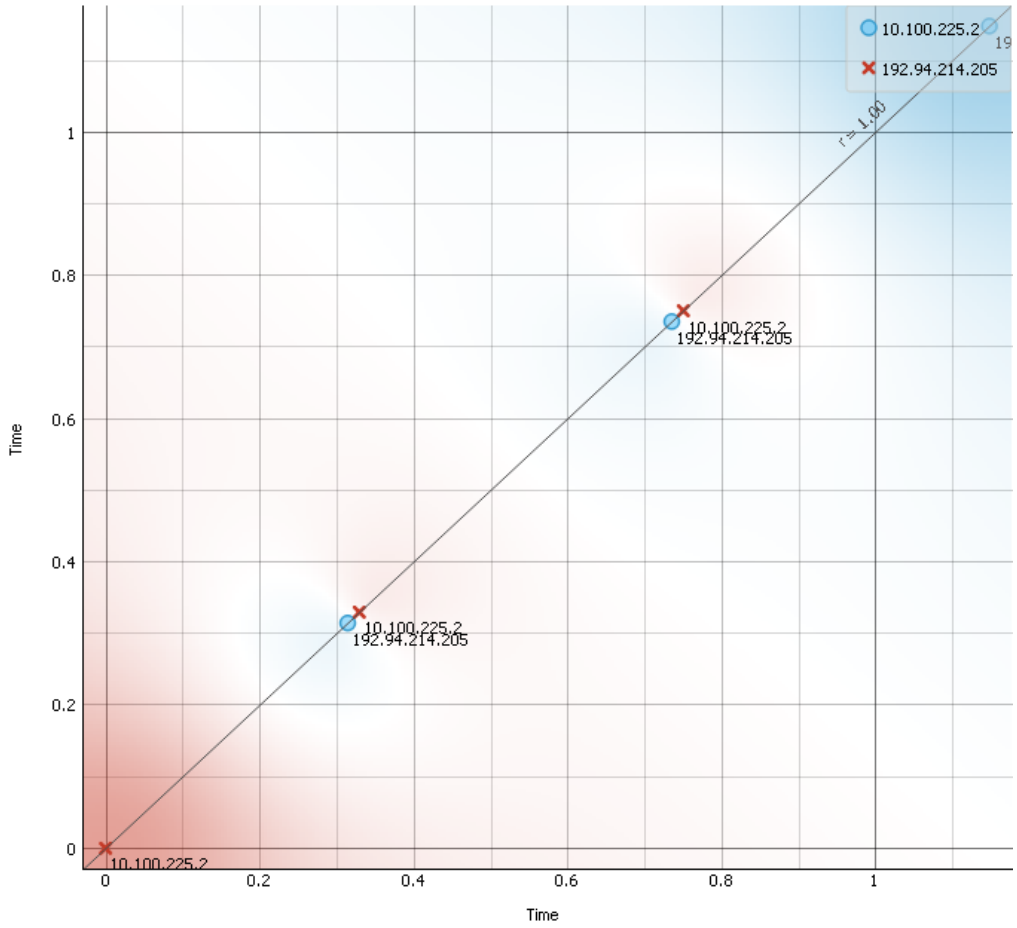
Disini saya memilih source ip dan udp destination untuk di tampilkan :



Gambar 6. Hasil Visualisasi Dengan Rumint

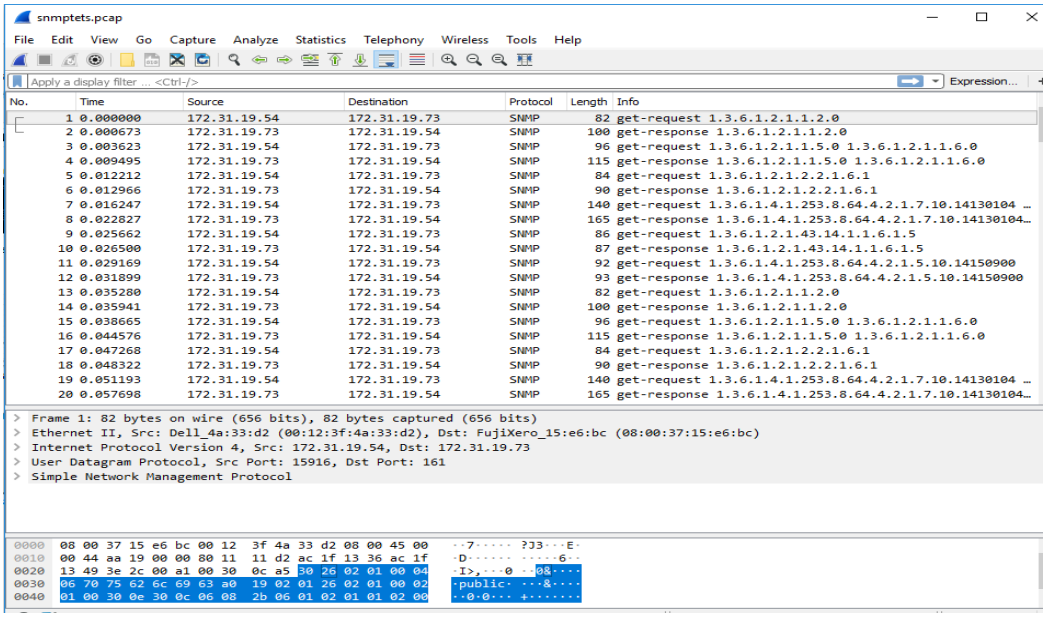
Hasil Visualisasi dengan *orange :*

1. Ubah file *pcap* menjadi *csv*
2. Import data csv ke orange dan memilih komponen yang akan di visualkan. Disini, saya mengambil time, source ip dan source destination.

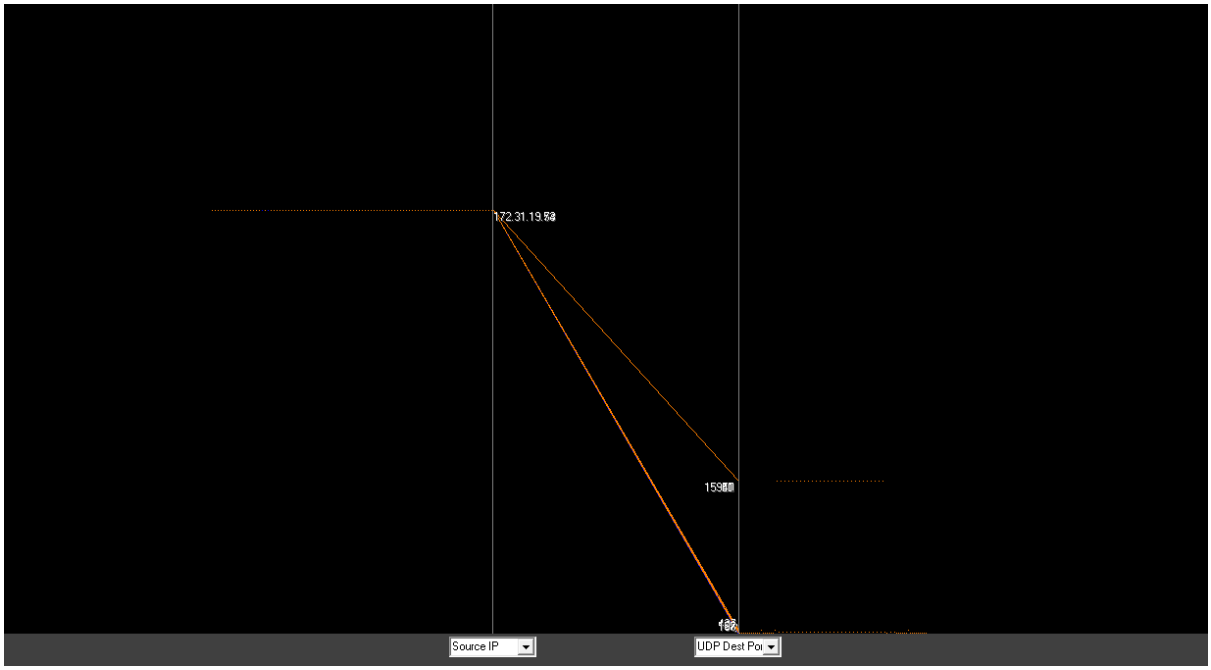


Gambar 7. Hasil Visualisasi dengan Orange

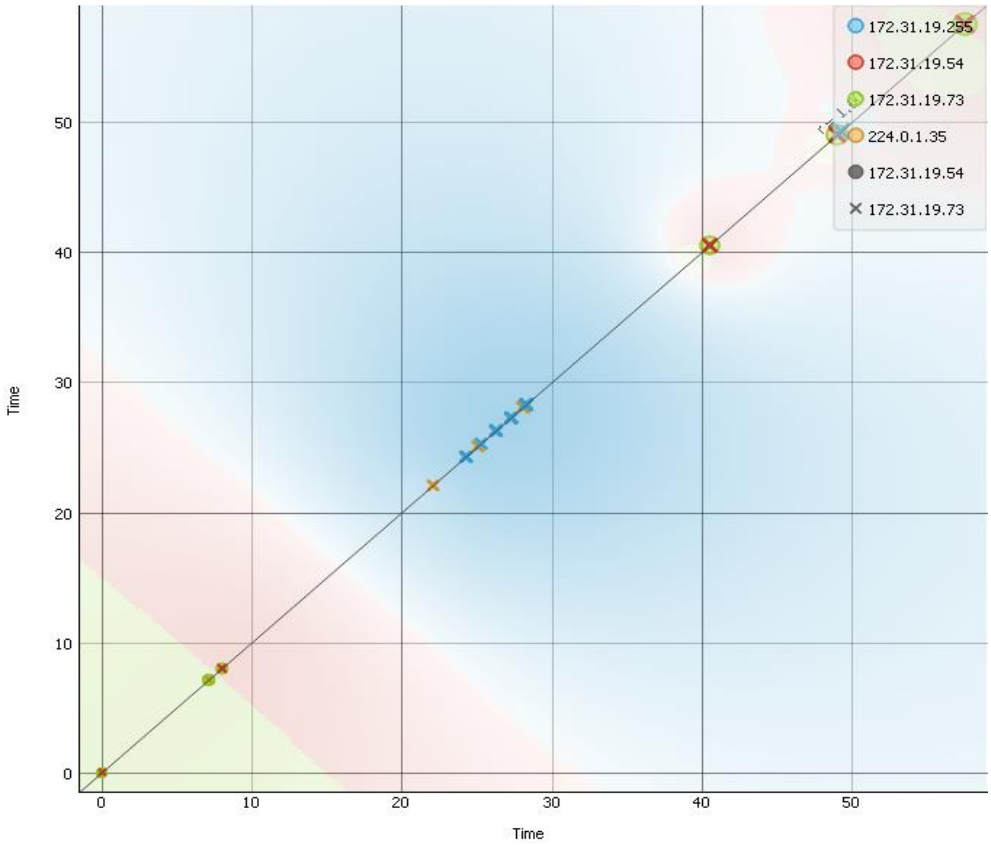
Selain paket yang penulis tapping sendiri, penulis juga melakukan perbandingan dengan menggunakan PCAP dari SNMP dataset dari wikiwireshark.



Gambar 8. SNMP Pcap dari dataset



Gambar 9. Visualisasi SNMP Dataset dengan Rumint



Gambar 10. Visualisasi SNMP dataset dengan Orange

Arsitektur SNMP mendefinisikan tipe pesan dari PDU sebagai berikut :

- GetRequest-PDU

GetRequest-PDU dihasilkan dan dikirim atas permintaan yang datang dari aplikasi SNMPv2. Setelah menerima GetRequest-PDU, proses SNMPv2 entitas mengikat setiap variabel-variabel ke daftar untuk menghasilkan Response-PDU.

- GetNextRequest-PDU

Setelah menerima GetNextRequest-PDU, proses SNMPv2 entitas akan mengikat setiap variabel-variabel ke daftar yang akan menghasilkan Response-PDU.

- GetBulkRequest-PDU

GetBulkRequest-PDU dihasilkan dan dikirim atas permintaan dari aplikasi SNMPv2. Tujuan GetBulkRequest-PDU adalah untuk meminta transfer dalam jumlah data yang besar, namun tidak terbatas pada keefisiensian dan cepat dari media, contohnya tabel yang besar. Setelah menerima GetBulkRequest-PDU, proses dalam SNMPv2 entitas mengikat setiap variabel-variabel ke daftar yang akan menghasilkan Respon-PDU dengan permintaan id yang sama nilai seperti pada permintaan.

- Response-PDU

Response-PDU yang dihasilkan oleh entitas SNMPv2 hanya atas penerimaan dari PDU :

- GetRequest-PDU
- GetNextRequest-PDU
- GetBulkRequest-PDU
- SetRequest-PDU
- InformRequest-PDU.

Jika kesalahan-status pada Response-PDU ini adalah tidak nol, nilai bidang variabel dalam daftar variabel yang terikat akan diabaikan.

- SetRequest-PDU

SetRequest-PDU dihasilkan dan dikirim atas permintaan yang datang dari aplikasi SNMPv2.

- Jika variabel terikat menentukan nama yang sudah ada atau non -variabel yang ada untuk permintaan ini adalah / akan dapat mengakses karena / tidak akan di MIB melihat sesuai, maka Respons dari nilai-PDU dari kesalahan-status lapangan diatur ke `noAccess', dan nilai dari kesalahan-indeks bidang diatur ke indeks dari variabel gagal mengikat.
- Jika tidak, jika tidak ada variabel yang sama berbagi Object Identifier variabel nama, dan yang dapat dibuat atau diubah dengan nilai baru sudah ditentukan, maka

nilai dari Respon-PDU dari kesalahan-status akan diset ke 'notWritable ', dan nilai dari kesalahan-indeks akan diset ke indeks dari variabel tersebut.

- Trap-PDU

J-Trap SNMPv2-PDU dihasilkan dan dikirimkan oleh sebuah entitas SNMPv2 yang akan bertindak sebagai agen ketika situasi yang tidak biasa terjadi. Tujuan dalam Trap pada PDU ini dikirim dan ditentukan pelaksanaannya tergantung oleh SNMPv2 entitas.

- InformRequest-PDU

InformRequest-PDU dihasilkan dan dikirimkan atas permintaan aplikasi di SNMPv2 entitas bertindak dalam peran seorang manajer, yang memberitahukan aplikasi lain (dalam SNMPv2 entitas lain juga bertindak dalam peran seorang manajer) dari informasi dalam MIB dalam hal penerimaan aplikasi.

Kesimpulan :

1. Akan selalu ada proses threeways Handshake Antara Manager dan Agent SNMP (Manager > Agent > Manager)
2. SNMP yang didapatkan adalah SNMP V.2 Seperti yang terlihat dari Wireshark.
3. Traffic SNMP berbeda dengan traffic protocol yang lain yang mana memerlukan perlakuan khusus agar dapat terdeteksi oleh wireshark/

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. https://wiki.wireshark.org/SNMP
3. G. D. Harmawan and U. Gunadarma, “Aplikasi Pemantauan Jaringan Dengan Agen SNMP Menggunakan Pemrograman TCL Dengan Perluasan Scotty.”
4. Mardhana,Fadly. SNMP V2. 2009
5. Fepiliana, “ Analisa File PCAP Protokol SNMP”.2016. Palembang : Universitas Sriwijaya.