MANAJEMEN JARINGAN
ANALISIS TRAFFIC SNMP

ROFBY HIDAYADI
09011281520132

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2018

BAB I
PENDAHULUAN

1.1 Latar Belakang

Salah satu protokol yang digunakan untuk manajemen jaringan adalah *Simple Network Management Protocol* (SNMP). SNMP merupakan sebuah protokol yang digunakan sebagai standar untuk melakukan pengaturan perangkat-perangkat jaringan. SNMP dapat digunakan untuk mengkonfigurasi perangkat-perangkat yang jauh, karena SNMP menyediakan sekumpulan operasi yang dapat melakukan pengelolaan beberapa perangkat jaringan secara jarak jauh sehingga monitoring dapat dilakukan tidak hanya pada *Local Area Network* (LAN). Akan tetapi, dapat juga dioperasikan pada skala jarignan yang lebih luas seperti *Wide Area Network* (WAN). Dapat juga digunakan untuk mendeteksi kesalahan jaringan atau akses yang tida cocok, dan mengaudit pemakain jaringan. Ada beberapa versi dari SNMP, diantaranya sebagai berikut : SNMPv1, SNMPv2, SNMPv3. Ketiganya memmpunya fungsi dasar yang sama, akan tetapi, semakin mengalami peningkatan versi maka, kemampuan dan fungsi yang dimiliki semakin baik. [1]

Traffic SNMP didapat dari SNMP pcap dataset yang merupakan hasil capturing data SNMP pada jaringan komputer menggunakan aplikasi Wireshark, yang kemudian disimpan untuk digunakan dalam berbagai hal seperti analisis lebih lanjut mengenai SNMP yang ada pada jaringan tersebut. Wireshark merupakan aplikasi analyzer berbasis open source yang digunakan untuk network troubleshooting, network analysis, ataupun sebagai sarana edukasi [2].

Rumint merupakan aplikasi berbasis open source yang digunakan sebagai sarana network visualization tool. Nantinya pcap dataset yang didapat akan dijadikan data source visualization. [3]

Oleh karena itu, dalam tugas kali ini penulis menggunakan aplikasi Wireshark sebagai sarana capturing data SNMP lalu divisualisasikan menggunakan aplikasi Rumint.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang penulis buat, maka diperoleh rumusan masalah sebagai berikut :

1. Apa itu SNMP?
2. Bagaimana capturing data SNMP menggunakan Wireshark?
3. Bagaimana proses visualisasi SNMP pcap dataset menggunakan Rumint?

1.3 Tujuan

Adapun tujuan penulis sebagai berikut :

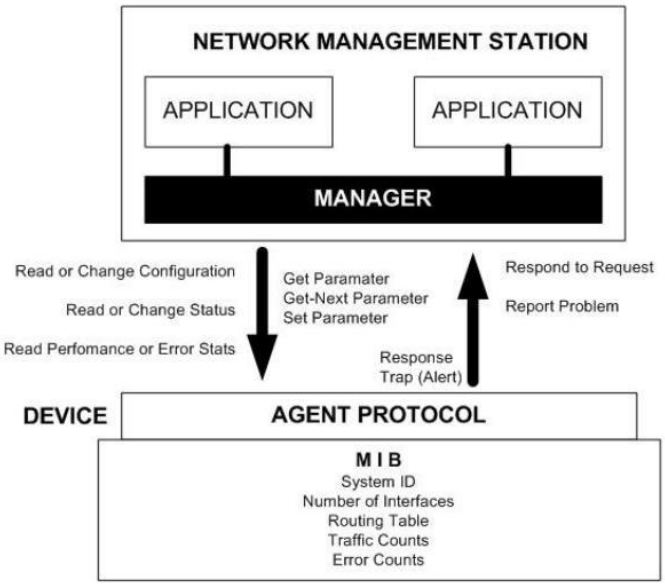
1. Mengetahui apa itu SNMP.
2. Mengetahui proses capturing data SNMP menggunakan Wireshark.
3. Mengetahui cara menggunakan SNMP pcap dataset dalam Rumint.
4. Mengetahui proses visualisasi SNMP pcap dataset menggunakan Rumint.

BAB II
PEMBAHASAN

2.1 Pengertian SNMP, Wireshark, dan Rumint

SNMP merupakan sebuah protokol yang digunakan sebagai standar untuk melakukan pengaturan perangkat-perangkat jaringan. SNMP dapat digunakan untuk mengkonfigurasi perangkat-perangkat yang jauh, karena SNMP menyediakan sekumpulan operasi yang dapat melakukan pengelolaan beberapa perangkat jaringan secara jarak jauh sehingga monitoring dapat dilakukan tidak hanya pada *Local Area Network* (LAN). Akan tetapi, dapat juga dioperasikan pada skala jarignan yang lebih luas seperti *Wide Area Network* (WAN). Dapat juga digunakan untuk mendeteksi kesalahan jaringan atau akses yang tida cocok, dan mengaudit pemakain jaringan. Ada beberapa versi dari SNMP, diantaranya sebagai berikut : SNMPv1, SNMPv2, SNMPv3. Ketiganya memmpunya fungsi dasar yang sama, akan tetapi, semakin mengalami peningkatan versi maka, kemampuan dan fungsi yang dimiliki semakin baik. [1]

Adapun untuk elemen-elemen yang terdapat pada SNMP dapat dilihat pda gambar berikut :



Gambar 1. Interaksi Manager dan Agent

1. **Manager**

   Pada kenyataannya manager ini merupakan komputer biasa yang ada pada jaringan yang mengoperasikan perangkat lunak untuk manajemen jaringan. Manager ini terdiri satu proses atau lebih yang berkomunikasi dengan agen-agennya dan dalam jaringannya. Manager akan mengumpulkan informasi dari agen yang ada pada jaringan yang diminta oleh administrator.

2. **Manager Information Base (MIB)**

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

   a. Setiap object mempunyai ID unik (OID).
   b. MIB mengasosiasikan setiap OID menggunakan label da parameter yang lain.
   c. MIB bertindak sebagai kamus data yang digunakan untuk menyusun terjemahan pesan SNMP.

3. **Agent**

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

Wireshark merupakan aplikasi analyzer berbasis open source yang digunakan untuk network troubleshooting, network analysis, ataupun sebagai sarana edukasi [2]. Wireshark merupakan salah satu program untuk menganalisis suatu jaringan, baik jaringan kabel ataupun nirkabel yang sering digunakan untuk *troubleshooting*, memeriksa keamanan jaringan dan lain-lain. Wireshark akan menangkap paket data pada jaringan yang kemudian, data yang ditangkap tersebut ditampilkan sedetail mungkin [4]. Adapun fungsi dari wireshark itu sendiri, sebagai berikut [5] :

1. Menganalisa jaringan.
2. Menangkap paket data atau informasi dalam jaringan yang terlihat.
3. Dapat digunakan untuk proses sniffing.
4. Membaca serta menganalisa transmisi paket data dalam jaringan, proses koneksi, dan transmisi paket data antar komputer.

Rumint merupakan aplikasi berbasis open source yang digunakan sebagai sarana network visualization tool. Nantinya pcap dataset yang didapat akan dijadikan data source visualization. Adapun fungsi dari Rumint antara lain sebagai berikut : [3]

1. Sarana visualisasi jaringan.
2. Analisa paket data dalam jaringan.
3. Filterisasi paket data dalam jaringan.

2.2 Capturing Data SNMP menggunakan Wireshark

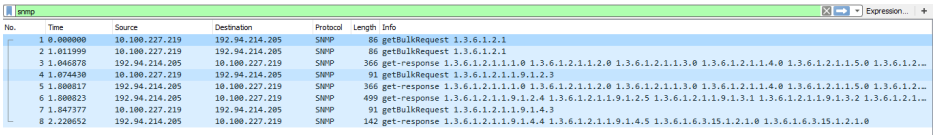
Capturing data SNMP menggunakan Wireshark nantinya akan dijadikan SNMP pcap dataset, yang kemudian akan dianalisis lebih lanjut lalu divisualisasikan menggunakan Rumint. Adapun cara mendapatkan SNMP pcap dataset menggunakan Wireshark adalah sebagai berikut :

1. Install bash terminal terlebih dahulu dengan cara : open menu settings – windows update – checklist developer mode – restart – open program and features – turn windows features on or off – checklist windows subsystem for linux – klik ok – restart – open microsoft store – install ubuntu – open ubuntu lalu tunggu installasi sampai selesai – finish
2. Connect ke salah satu Wi-Fi publik dalam hal ini penulis menggunakan jaringan Wi-Fi Fasilkom Unsri Indralaya, kemudian buka aplikasi Wireshark.
3. Capturing data pada jaringan Wi-Fi tersebut.
4. Lalu open bash terminal (ketikkan bash pada search engine), kemudian ketikkan perintah sebagai berikut dalam mode root :
   snmpbulkwalk -v2c -Os -c demopublic test.net-snmp.org

```
root@LENOVO-PC:/mnt/c/Windows/System32# snmpbulkwalk -v2c -Os -c demopublic test.net-snmp.org
Created directory: /var/lib/snmp/mib_indexes
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: (63451514) 7 days, 8:15:15.14
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
root@LENOVO-PC:/mnt/c/Windows/System32#
```

Jika *snmpbulkwalk* command tidak tersedia, maka install terlebih dahulu dengan cara ketikkan : *apt install snmp*

5. Setelah itu buka kembali aplikasi Wireshark lalu stop capturing data.
6. Lakukan filterisasi SNMP, sehingga data yang tampil hanya data SNMP.

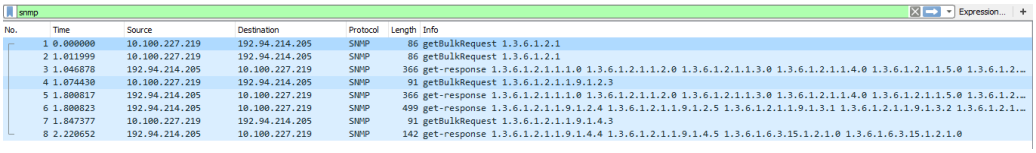


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.100.227.219	192.94.214.205	SNMP	86	getBulkRequest 1.3.6.1.2.1
2	1.011999	10.100.227.219	192.94.214.205	SNMP	86	getBulkRequest 1.3.6.1.2.1
3	1.046878	192.94.214.205	10.100.227.219	SNMP	366	get-response 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.1.4.0 1.3.6.1.2.1.1.5.0 1.3.6.1.2…
4	1.074430	10.100.227.219	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.2.3
5	1.800817	192.94.214.205	10.100.227.219	SNMP	366	get-response 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.1.4.0 1.3.6.1.2.1.1.5.0 1.3.6.1.2…
6	1.800823	192.94.214.205	10.100.227.219	SNMP	499	get-response 1.3.6.1.2.1.1.9.1.2.4 1.3.6.1.2.1.1.9.1.2.5 1.3.6.1.2.1.1.9.1.3.1 1.3.6.1.2.1.1.9.1.3.2 1.3.6.1.2.1.…
7	1.847377	10.100.227.219	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.4.3
8	2.220652	192.94.214.205	10.100.227.219	SNMP	142	get-response 1.3.6.1.2.1.1.9.1.4.4 1.3.6.1.2.1.1.9.1.4.5 1.3.6.1.6.3.15.1.2.1.0 1.3.6.1.6.3.15.1.2.1.0

7. Selanjutnya simpan data tersebut dengan cara : file – export specified packets – simpan dengan extension .pcap

2.3 Analisis Data SNMP

Setelah mendapatkan SNMP pcap dataset, selanjutnya adalah menganalisis data tersebut. Dari gambar tersebut dapat diketahui bahwa terdapat informasi pada setiap pesan SNMP terdapat Protocol Data Unit (PDU). PDU merupakan unit data yang terdiri atas sebuah header dan beberapa daya yang ditempelkan. SNMP PDU digunakan antara manager SNMP dan agent SNMP [1]. Berikut adalah analisis dari data SNMP tersebut :



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.100.227.219	192.94.214.205	SNMP	86	getBulkRequest 1.3.6.1.2.1
2	1.011999	10.100.227.219	192.94.214.205	SNMP	86	getBulkRequest 1.3.6.1.2.1
3	1.046878	192.94.214.205	10.100.227.219	SNMP	366	get-response 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.1.4.0 1.3.6.1.2.1.1.5.0 1.3.6.1.2…
4	1.074430	10.100.227.219	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.2.3
5	1.800817	192.94.214.205	10.100.227.219	SNMP	366	get-response 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.1.4.0 1.3.6.1.2.1.1.5.0 1.3.6.1.2…
6	1.800823	192.94.214.205	10.100.227.219	SNMP	499	get-response 1.3.6.1.2.1.1.9.1.2.4 1.3.6.1.2.1.1.9.1.2.5 1.3.6.1.2.1.1.9.1.3.1 1.3.6.1.2.1.1.9.1.3.2 1.3.6.1.2.1.…
7	1.847377	10.100.227.219	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.4.3
8	2.220652	192.94.214.205	10.100.227.219	SNMP	142	get-response 1.3.6.1.2.1.1.9.1.4.4 1.3.6.1.2.1.1.9.1.4.5 1.3.6.1.6.3.15.1.2.1.0 1.3.6.1.6.3.15.1.2.1.0

Gambar 2. Data SNMP

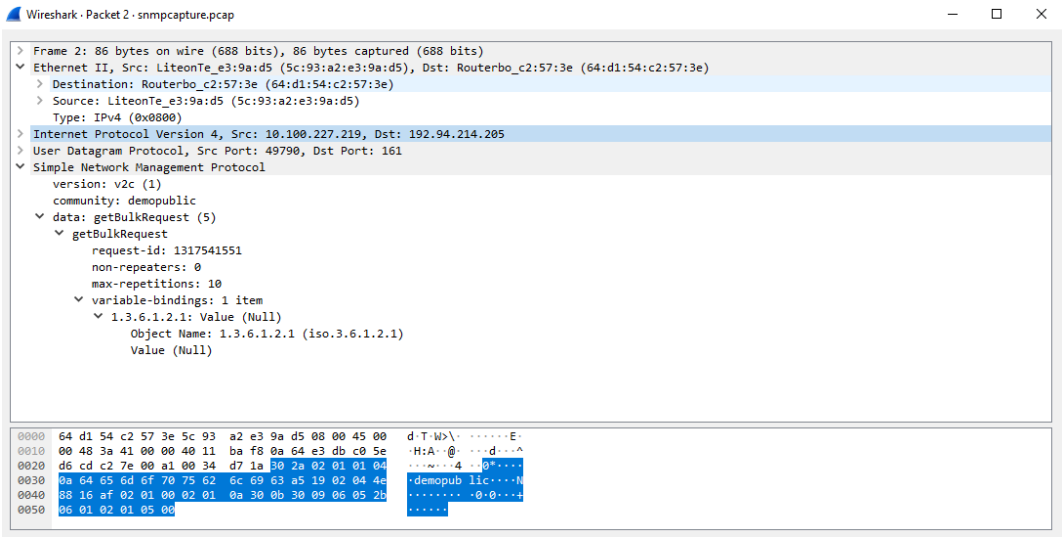
1. **GetBulk-Request**

   Pada SNMPv2 *GetBulk-Request* sama seperi *Get-Request* pada SNMPv1. GetBulk-Request dikirim oleh SNMP manager untuk mengambil satu atau lebih variabel MIB yang telah ditentukan oleh PDU.

2. **Get-Response**

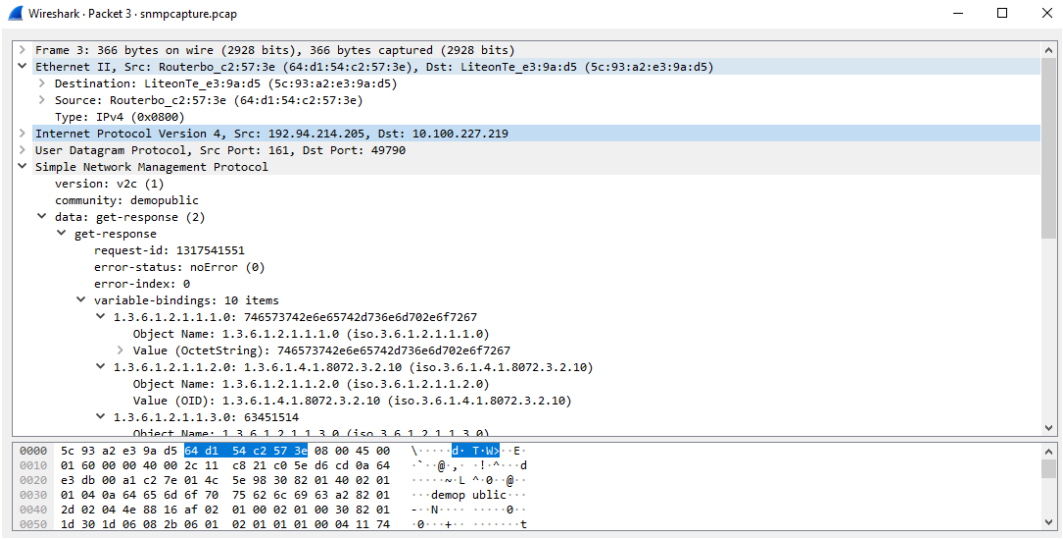
   Dikirim oleh SNMP agent dalam hal menanggapi *GetBulk-Request*.

Pada gambar 2 dapat kita ketahui bahwa ada dua IP address yaitu 10.100.227.219 dan 192.94.214.205 yang sedang melakukan traffic data dengan bulkrequest dan response. Sebagai sampel analisa SNMP pcap dataset, penulis memilih paket 2 dan 3 untuk dianalisa, dimana paket 2 berupa informasi SNMP *GetBulk-Request* dan paket 3 berupa informasi SNMP *Get-Response*.



Gambar 3. Paket 2 *GetBulk-Request*

Pada paket 2 *GetBulk-Request* dapat diketahui bahwa manager (IP address source 10.100.227.219 dan MAC address 5c:93:a2:e3:9a:d5) dan agent (IP address destination 192.94.214.205 dan MAC address 64:d1:54:c2:57:3e). Pada isi paket tersebut juga dapat ketahui *request-id* adalah 1317541551, dengan *variable-bindings* berjumlah 1 item, yaitu 1.3.6.1.2.1: Value (Null) dan Object Name yaitu 1.3.6.1.2.1 (iso.3.6.1.2.1).



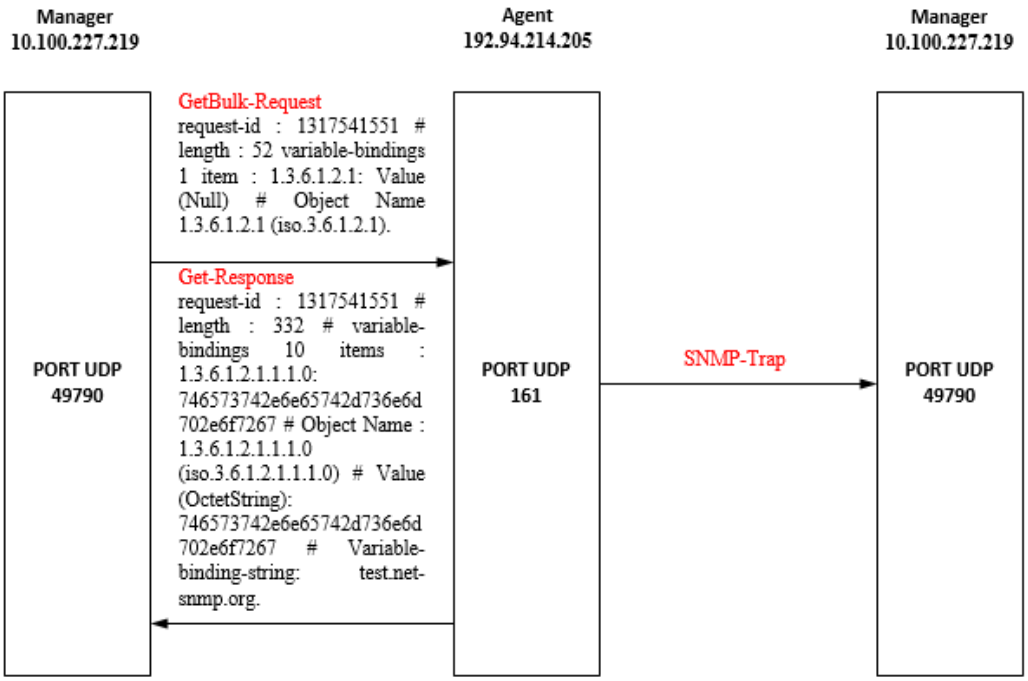
Gambar 3. Paket 3 *Get-Response*

Pada paket 3 *Get-Response* dapat diketahui bahwa agent (IP address source 192.94.214.205 dan MAC address 64:d1:54:c2:57:3e) dan manager (IP address destination 10.100.227.219 dan MAC address 5c:93:a2:e3:9a:d5). Pada isi paket tersebut juga dapat ketahui *request-id* adalah 1317541551, dengan *variable-bindings* berjumlah 10 items, yaitu salah satunya 1.3.6.1.2.1.1.1.0: 746573742e6e65742d736e6d702e6f7267 dan Object Name yaitu 1.3.6.1.2.1.1.1.0 (iso.3.6.1.2.1.1.1.0) Value (OctetString): 746573742e6e65742d736e6d702e6f7267 Variable-binding-string: test.net-snmp.org.

Setelah diperhatikan, ketika manager mengirim *GetBulk-Request* 1.3.6.1.2.1: Value (Null) dan Object Name yaitu 1.3.6.1.2.1 (iso.3.6.1.2.1) kepada agent, maka agent akan mengirim *Get-Response* berupa 1.3.6.1.2.1.1.1.0: 746573742e6e65742d736e6d702e6f7267 dan Object Name yaitu 1.3.6.1.2.1.1.1.0 (iso.3.6.1.2.1.1.1.0) Value (OctetString): 746573742e6e65742d736e6d702e6f7267 Variable-binding-string: test.net-snmp.org. Hal tersebut dapat dilihat pada 10 items *Get-Response*.

Perbedaan antara *GetBulk-Request* dan *Get-Response* adalah pada nilai value nya. Pada saat manager mengirim *GetBulk-Request* kepada agent, nilai valuenya NULL. Kemudian, agent menanggapi permintaan dari manager, maka, agent akan mengirimkan *Get-Response* ke manager. Pada detai informasi paket *Get-Response*, kita dapat melihat bahwa nilai valuenya adalah

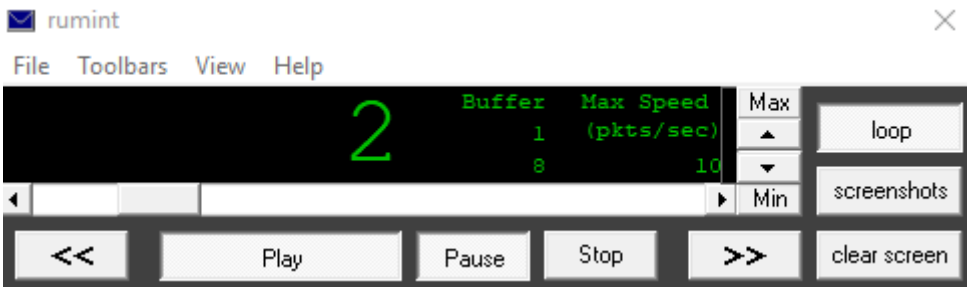
46573742e6e65742d736e6d702e6f7267 yang bertipe OctetString, lalu nilai value itulah yang akan dikirim ke manager. Berikut adalah *Three Way Handshake* SNMP tersebut :



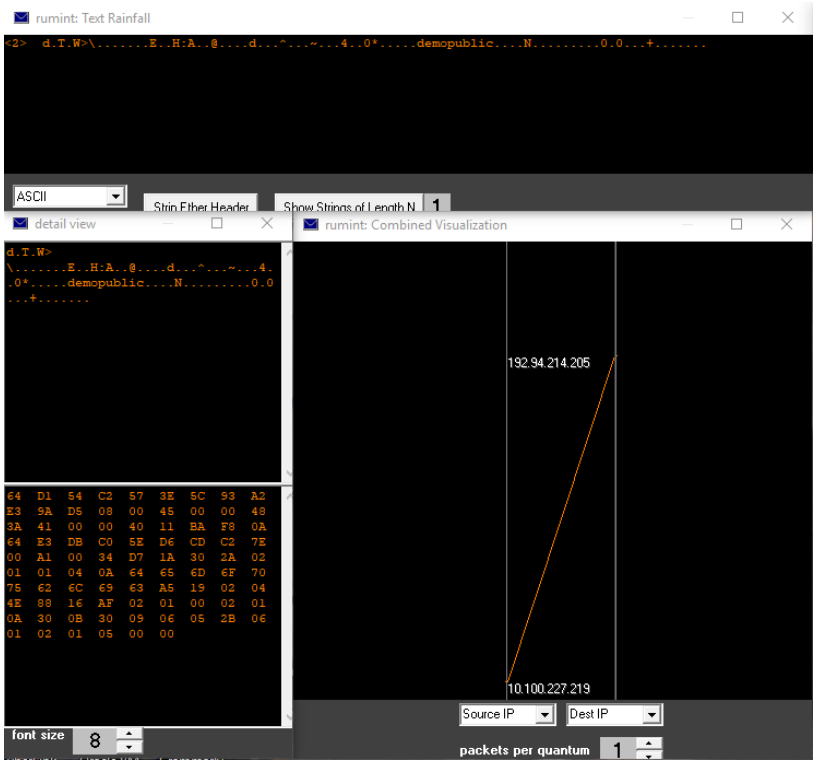
Gambar 4. Three Way Hand Shake SNMP

2.4 Visualiasi Data SNMP

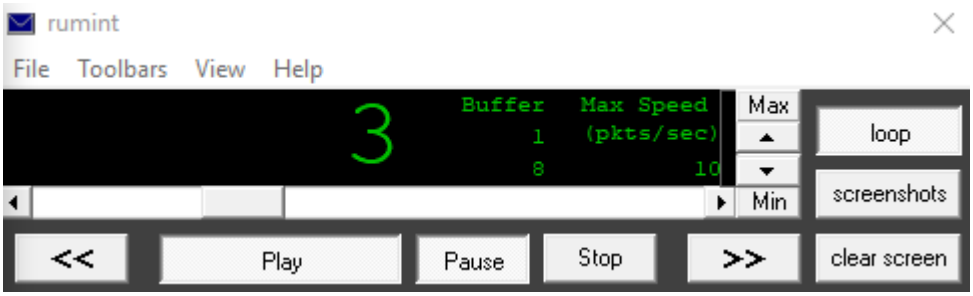
Untuk melakukan visualisasi data SNMP yang telah didapat sebelumnya, digunakan aplikasi Rumint. Adapun hasil visualisasi SNMP pcap dataset yang telah didapat adalah sebagai berikut :



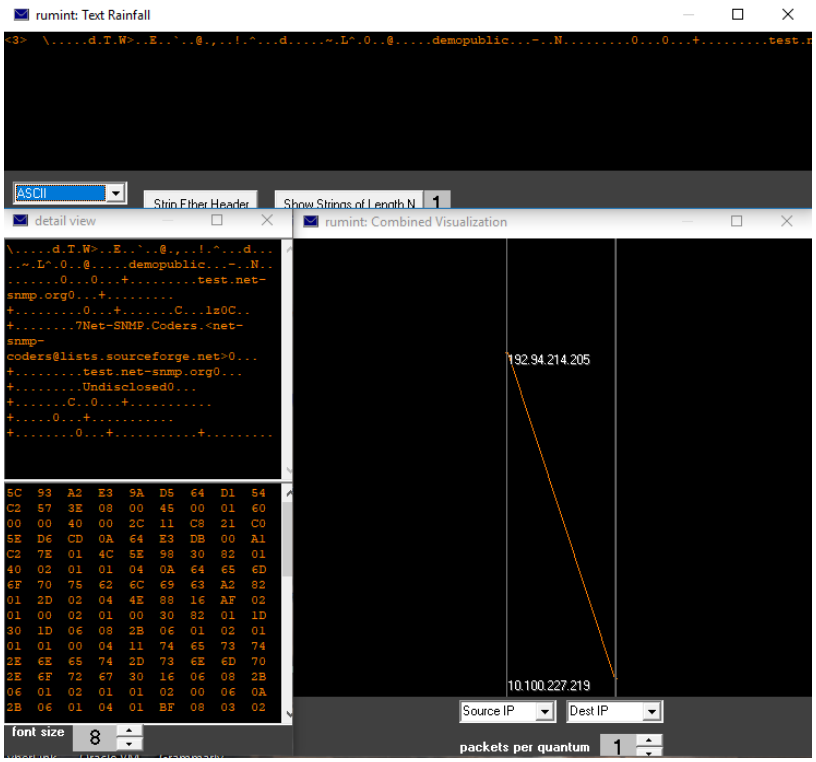
Gambar 5. Load SNMP Pcap Dataset Paket 2 *GetBulk-Request*



Gambar 6. Visualisasi SNMP Pcap Dataset Paket 2 *GetBulk-Request*

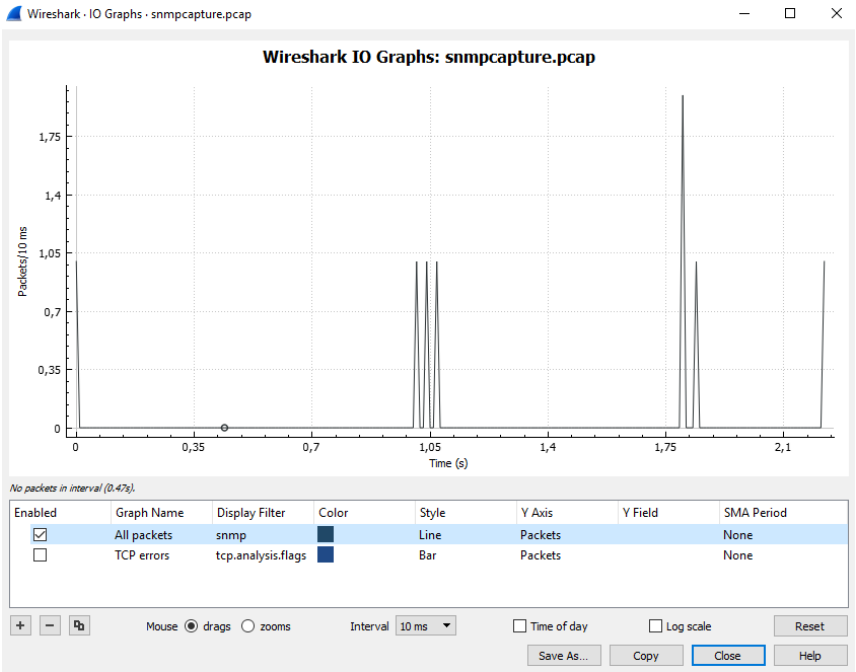


Gambar 7. Load SNMP Pcap Dataset Paket 3 *Get-Response*



Gambar 7. Visualisasi SNMP Pcap Dataset Paket 3 *Get-Response*

Selain itu juga didapat grafik yang diperoleh dari aplikasi Wireshark, sebagai berikut :



Gambar 8. Grafik Paket Data SNMP

BAB III
PENUTUP

3.1 Kesimpulan

Adapun kesimpulan dari pembahasan kali ini, sebagai berikut :

1. Wireshark merupakan aplikasi analyzer berbasis open source yang digunakan untuk network troubleshooting, network analysis, ataupun sebagai sarana edukasi.
2. Rumint merupakan aplikasi berbasis open source yang digunakan sebagai sarana network visualization tool.
3. Traffic SNMP didapat dari SNMP pcap dataset merupakan hasil capturing data SNMP pada jaringan komputer menggunakan aplikasi Wireshark, yang kemudian disimpan untuk digunakan dalam berbagai hal seperti analisis lebih lanjut mengenai SNMP yang ada pada jaringan tersebut.
4. Pada SNMPv2 *GetBulk-Request* sama seperi *Get-Request* pada SNMPv1. GetBulk-Request dikirim oleh SNMP manager untuk mengambil satu atau lebih variabel MIB yang telah ditentukan oleh PDU.
5. Get-Response dikirim oleh SNMP agent dalam hal menanggapi *GetBulk-Request*.
6. Perbedaan antara *GetBulk-Request* dan *Get-Response* adalah pada nilai value nya. Pada saat manager mengirim *GetBulk-Request* kepada agent, nilai valuenya NULL. Kemudian, agent menanggapi permintaan dari manager, maka, agent akan mengirimkan *Get-Response* ke manager. Pada detai informasi paket *Get-Response*, kita dapat melihat bahwa nilai valuenya adalah 46573742e6e65742d736e6d702e6f7267 yang bertipe OctetString, lalu nilai value itulah yang akan dikirim ke manager.

DAFTAR PUSTAKA

[1] Fepiliana. 2016. “Analisa File Pcap Protokol SNMP”. Sistem Komputer Universitas Sriwijaya.

[2] Anonim. 2018. “Wireshark”. (online) https://en.wikipedia.org/wiki/Wireshark . Diakses pada tanggal 14 Oktober 2018.

[3] Anonim. 2018. “Rumint”. (online) http://rumint.org/ . Diakses pada tanggal 14 Oktober 2018.

[4] Hidayadi, Rofby. 2017. “Capturing dan Analisa Paket Data menggunakan Wireshark dan Command Prompt”. (online) http://edocs.ilkom.unsri.ac.id/id/eprint/1477. Diakses pada tanggal 14 Oktober 2018.

[5] Phyong, Fiya. 2010. “Fungsi Wireshark dan Kegunaannya”. (online) http://fiyaphyong.blogspot.co.id/2010/10/wireshark-fungsi-dan-kegunaanya.html. Diakses pada tanggal 14 Oktober 2018.