**Tugas Manajemen Jaringan**

**Analisa Packet Simple Network Manajemen Protocol**

****

**Nama : M Rasyid Darmawan**

**NIM : 09011281520108**

**JURUSAN SISTEM KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**2018**

**Analisa File Pcap Protokol SNMP**

**1. Pendahuluan**

Sistem informasi merupakan bagian yang sangat penting untuk setiap organisasi[1]. Perkembangan teknologi informasi, khususnya jaringan memungkinkan terjadinya pertukaran informasi yang cepat dan semakin kompleks . Pengaturan jaringan yang baik tentu akan memaksimalkan pemanfaatan informasi tersebut. Oleh sebab itu jaringan harus diatur dan dipantau, sehingga kelancaran pengiriman informasi dapat berjalan baik.

Pada saat ini, pemantauan jaringan menjadi suatu hal yang cukup sulit dilakukan apabila jaringan komputer pada lingkungan suatu lembaga sudah menjadi sangat luas dan kompleks. Masalah-masalah jaringan yang sering terjadi salah satunya adalah kerusakan elemen jaringan seperti hub, bridge, router, Transmission Facilities dan sebagainya, dimana kesalahannya tidak diketahui oleh pemantau jaringan secara manual dan pemeriksaan jaringan yang terlalu lama. Karena pentingnya jaringan komputer pada kehidupan sekarang, perlu adanya kestabilan jaringan komputer yang digunakan. Disinilah seorang network administrator jaringan memposisikan diri menjaga stabilitas jaringan komputer. Monitoring jaringan komputer adalah metode utama untuk menjaga stabilitas jaringan komputer. Dengan monitoring diharapkan jika terjadi permasalahan pada jaringan dapat diperbaiki dengan cepat dan mudah oleh administrator.

Banyaknya *device* yang digunakan dalam infrastruktur jaringan, maka diperlukanlah suatu manajemen jaringan yang baik dan sistem monitoring yang mampu memantau kinerja dari jaringan tersebut, kemudian sistem monitoring yang didesain untuk memantau status infrastuktur LAN/WAN, memastikan *device* tersebut dalam kondisi normal dan aktif, dapat melihat statistik dalam bentuk grafik, pengecekan kondisi sinyal, dapat memprediksi masalah yang akan muncul atau dapat memantau paket data yang lewat di trafik jaringan[2] .

Protokol yang populer digunakan untuk manajemen jaringan adalah Simple Network Management Protocol (SNMP). SNMP merupakan sebuah protokol yang digunakan sebagai standar untuk melakukan pengaturan perangkat-perangkat jaringan[2]. 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) tapi juga dapat dioperasikan pada skala jaringan yang lebih luas seperti *Wide Area Network* (WAN), mendeteksi kesalahan jaringan atau akses yang tidak cocok.

**2. Dasar Teori**

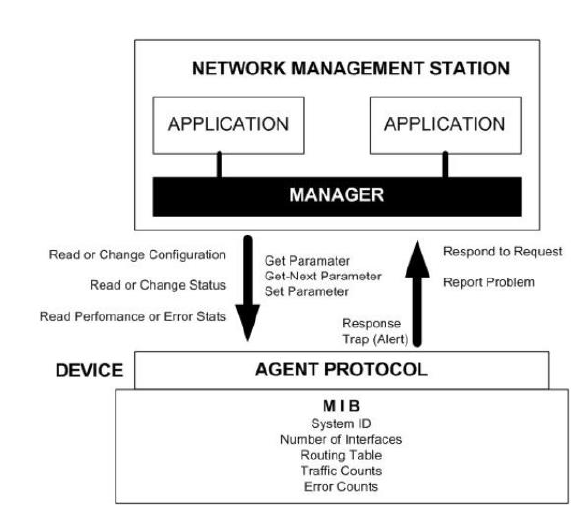
Simple Network Management Protocol (SNMP) merupakan protokol aplikasi yang mampu menjalankan tugas untuk memonitoring kondisi jaringan (Pradikta. dkk, 2013). SNMP akan mempermudah proses monitoring dan manajemen jaringan karena dengan menggunakan SNMP akan dapat diketahui informasi tentang kondisi perangkat jaringan yang diamati.

SNMP bukanlah perangkat lunak untuk melakukan menajemen jaringan, melainkan protokol ini menjadi basis pembuatan perangkat lunak manajemen jaringan (Ohara, 2005).

Untuk menjaga agar kondisi jaringan tetap dapat digunakan secara maksimal, maka diperlukan adanya monitoring perangkat jaringan seperti pada objek penelitian monitoring perangkat jaringan berbasis SNMP untuk kemudian monitoring tersebut juga dapat ditampilkan dalam bentuk web yang bertujuan mempermudah administrator dalam melakukan tugas monitoring jaringan.

SNMP adalah protocol pada level aplikasi yang merupakan bagian dari protokol TCP/IP, menggunakan model UDP untuk membentuk fungsi transport. 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**



**a. 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.

**b. 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.

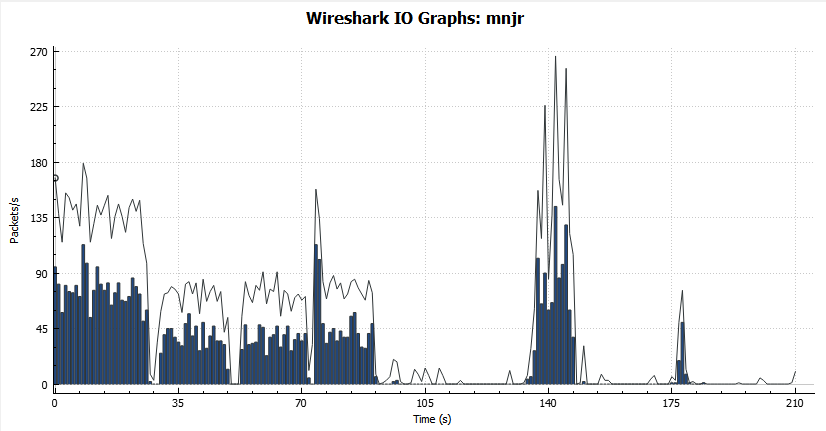
**c. Agent**

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.

**3. Hasil dan Pembahasan**

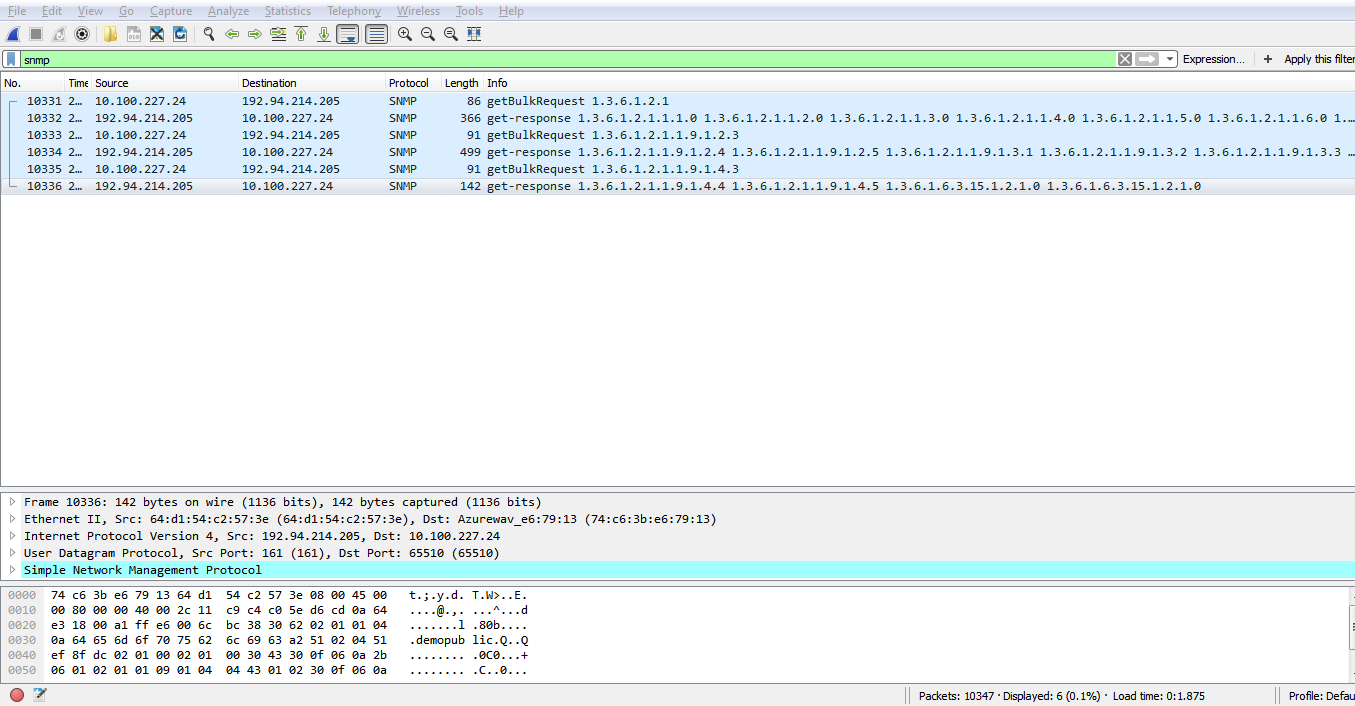
Untuk mendapatkan hasil pcap traffic jaringan berbasis SNMP dan untuk mengetahui lebih dalam lagi mengenai SNMP, maka telah dilakukan tapping data di wilayah sekitar Fakultas Ilmu Komputer Universitas Sriwijaya menggunakan aplikasi wireshark untuk mendapatkan traffic jaringan.

Setelah melakukan tapping data menggunakan wireshark didapatkan grafik traffic secara keseluruhan sebagai berikut yang telah di visualkan ke dalam Input/Output Graph



(Wireshark I/O Graph)

Dari keseluruhan hasil capture data menggunakan Wireshark didapatkan juga Protokol SNMP



(Capture packet data SNMP)

Berdasarkan gambar (sekian), 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[4].

Arsitektur SNMP mendefinisikan tipe pesan dari PDU sebagai berikut :

***1. Get-Request PDU* :** dikirim oleh SNMP manager untuk mengambil satu atau lebih variabel MIB yang diminta yang telah ditentukan oleh PDU.

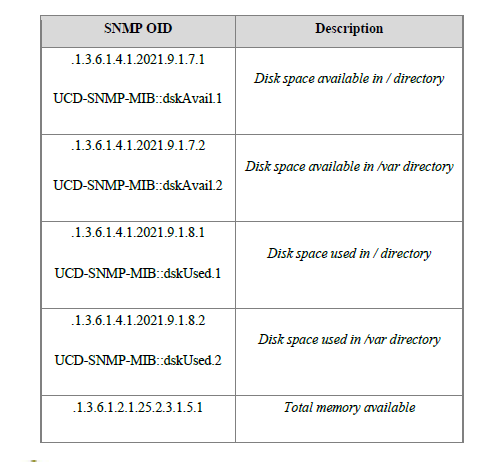
***2. Get-Next-Request PDU* :** dikirim oleh SNMP manager untuk mengambil variabel MIB berikutnya. Anda dapat memiliki beberapa pernintaan di PDU.

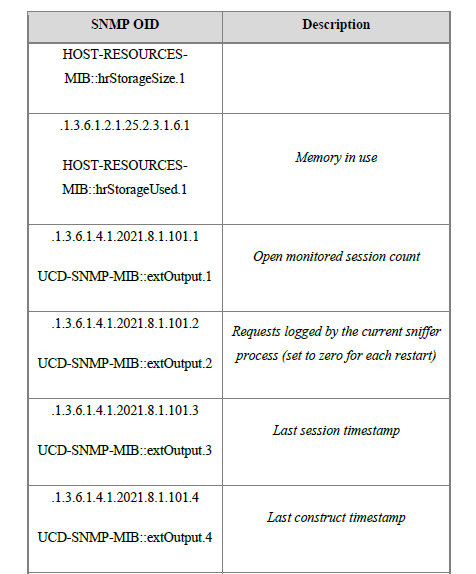
***3. Set-Request PDU* :** dikirim oleh SNMP manager untuk mengatur satu atau lebih variabel MIB dengan nilai yang telah ditentukan dalam PDU.

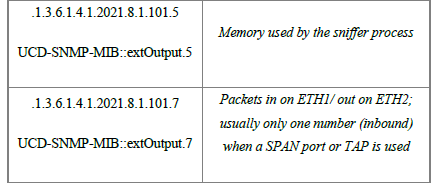
***4. Get-Response PDU* :** dikirim oleh SNMP agent dalam menanggapi *Get-Request PDU, Get-Next-Request PDU* atau *Set-Request PDU*

***5. Trap PDU* :** berisikan pesan yang tidak diinginkan yang dikirim oleh SNMP agent untuk memberitahu SNMP manager tentang peristiwa penting yang terjadi di agent.

Kemudian pada bagian INFO terdapat juga OID dari MIB. OID adalah angka unik yang dipisahkan oleh titik-titik. Setiap OID memiliki arti masing-masing. Untuk mengetahui artinya, lihat tabel dibawah ini:

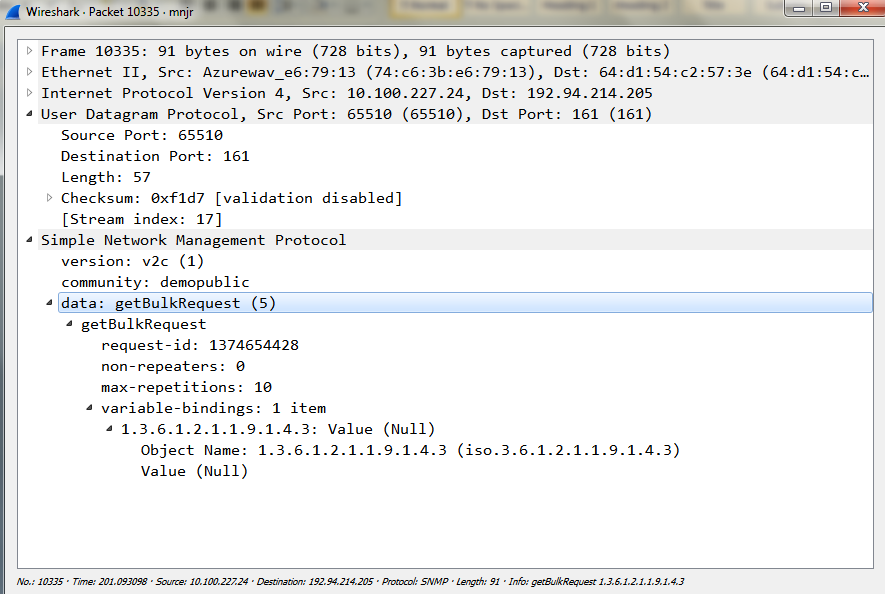






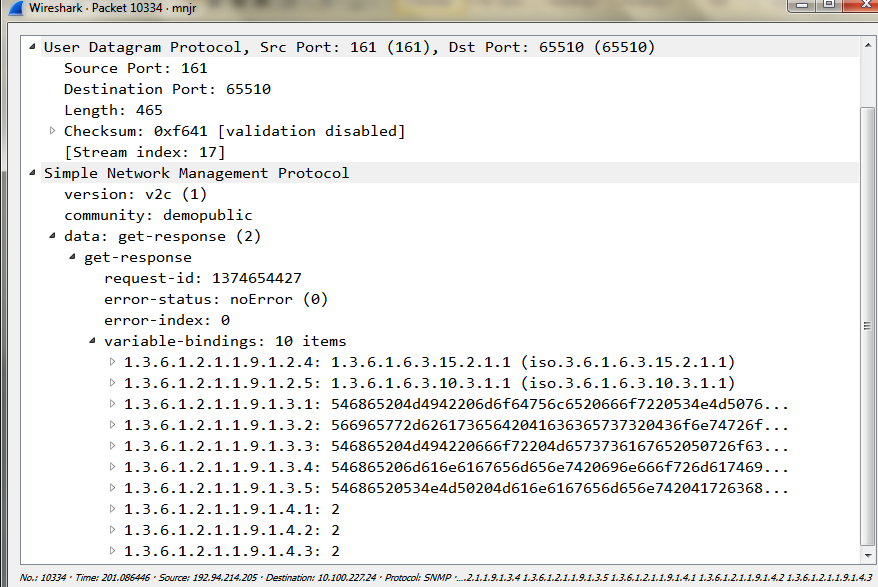
Sebagai sampel analisa pcap SNMP, penulis memilih relasi antara manager (IP Address *Souce* 10.100.227.24) dan agent (IP *Address Destination* 192.94.214.205). Pada pcap SNMP kita dapat melihat MAC *Address Source* yaitu 64:d1:54:c2:57:3e dan MAC *Address Destination* yaitu 74:c6:3b:36:79:13.

Berikut ini adalah informasi SNMP ***Get-Request PDU*** dari manager ke agent pada Packet 1 yang penulis pilih sebagai sampel analisa. Pada isi pesan tersebut kita dapat mengetahui *request-id* adalah 1374654428, dengan *variable-bindings* berjumlah 1 item, yaitu: *1.3.6.1.2.1.1.9.1.4.3*



(Isi informasi *Get-Request 1.3.6.1.2.1.1.9.1.4.3)*

Setelah diperhatikan, ketika manager telah mengirim *Get-Request 1.3.6.1.2.1.1.9.1.4.3* kepada agent, maka agent akan mengirim *Get-Respone 1.3.6.1.2.1.1.9.1.4.3* (dapat dilihat pada paket 5 file pcap pada SNMP)*.* ***Get-Respone PDU*** dikirim oleh SNMP agent untuk menanggapi *Get-Request PDU, Get-Next-Request PDU* atau *Set-Request PDU.*

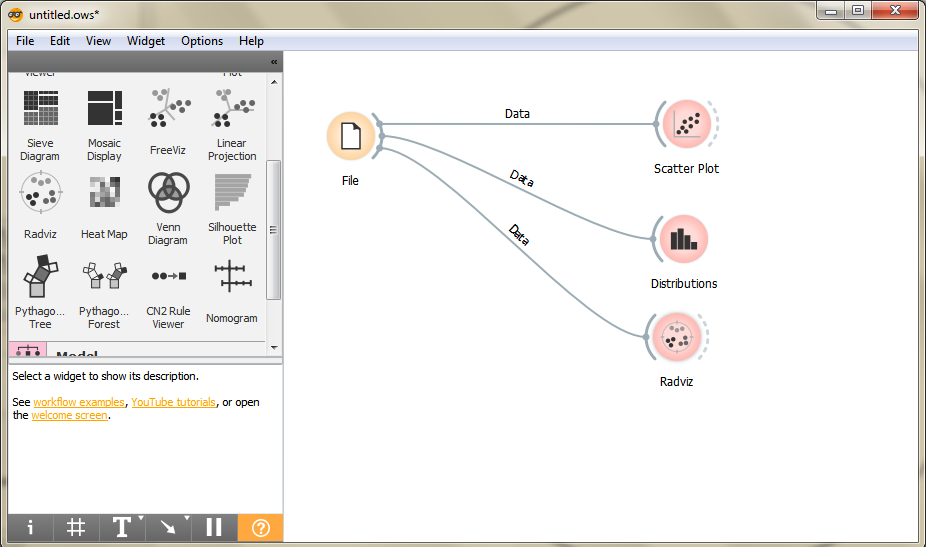


(Bukti bahwa agent telah mengirim *Get-Response* 1.3.6.1.2.1.1.9.1.4.3 kepada manager)

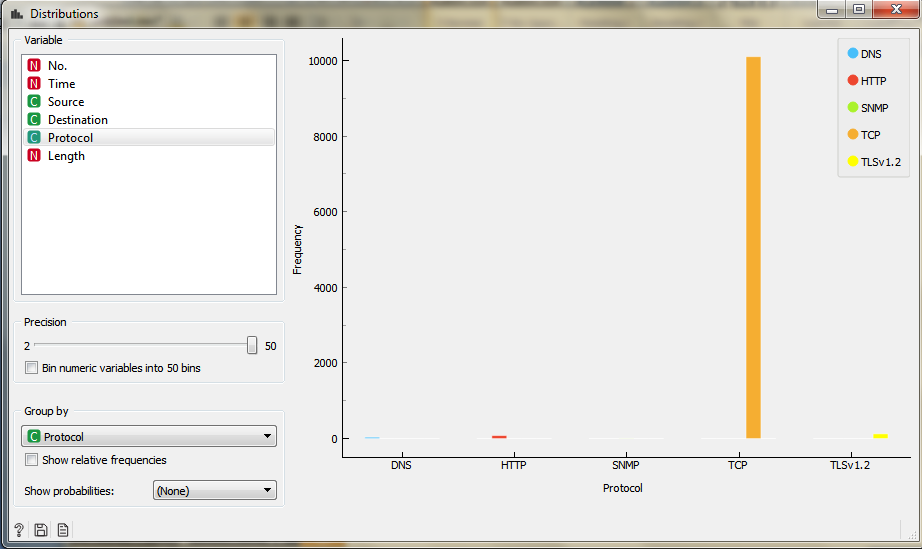
Perbedaan antara ***Get-Request*** dan ***Get-Respone*** terdapat pada nilai *Value*-nya. Pada saat pertama kali manager mengirim *Get-Request* kepada agent, nilai *Value* yaitu Null. Kemudian agent menanggapi permintaan dari manager. maka agent akan mengirimkan *Get-Respone* ke manager.

**Visualisasi menggunakan aplikasi Orange**

**Tampilan**

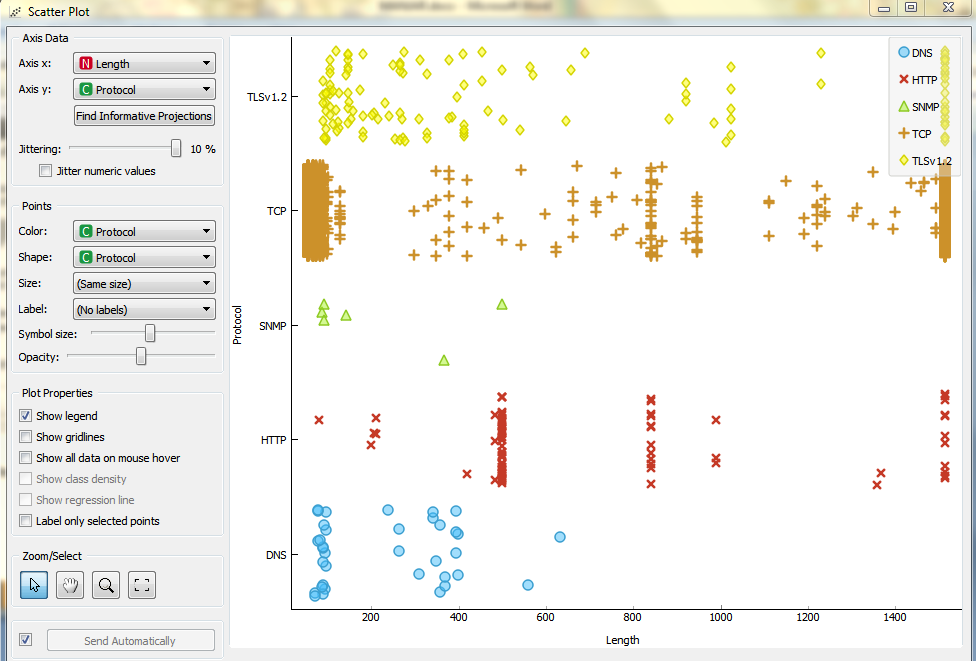
****

**Visualisasi Distributions**

****

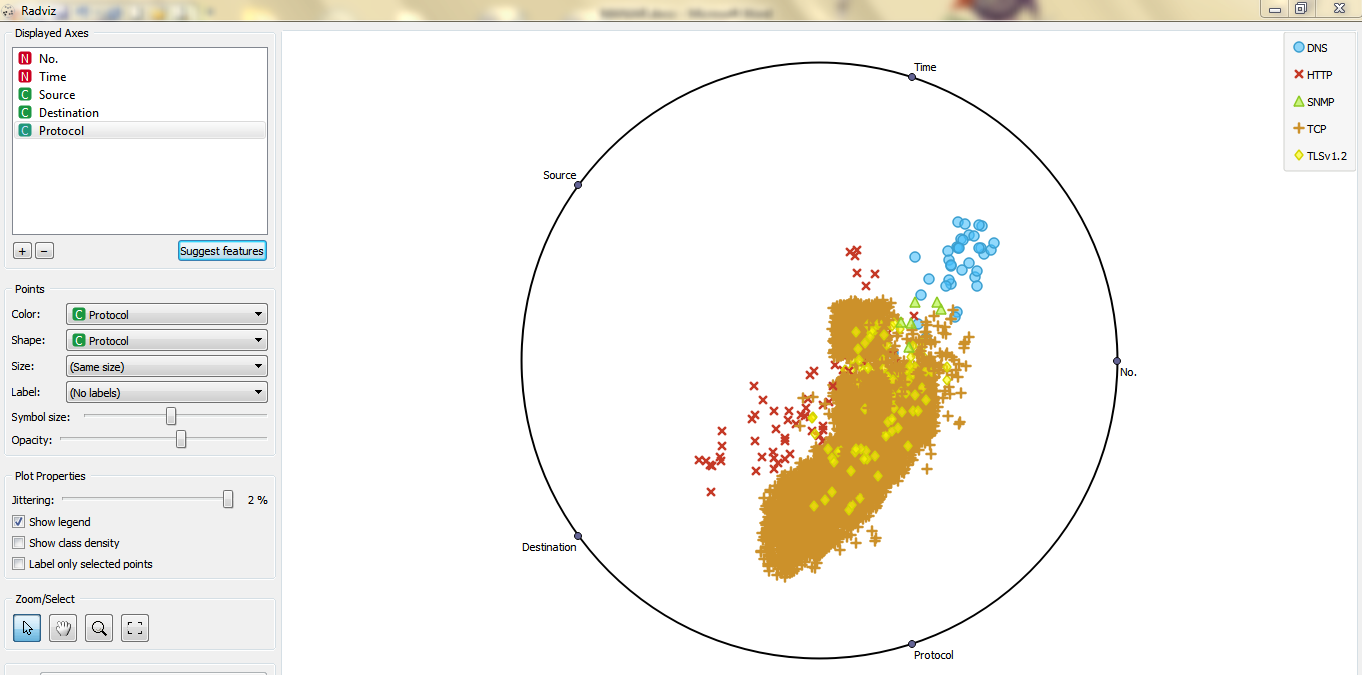
Pada gambar diatas Protocol SNMP seperti tidak nampak dikarenakan Protocol SNMP hanya berjumlah 6 dibandingan dengan protocol yang lain.

**Visualisasi Scatter Plot**

****

Disini terlihat protocol SNMP berjumlah 6 sesuai dengan yang ter capture di wireshark

**Visualisasi Radviz**

****

**DAFTAR PUSTAKA**

[1] M. Reztra, D. Jurusan, T. Elektro, F. Teknologi, and U. Andalas, “IMPLEMENTASI PROTOKOL SNMP UNTUK JARINGAN Abstrak,” vol. 1, no. 1, pp. 15–19, 2015.

[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.”

[4] Admin. “IBM Knowledge Center: Protocol data units (PDUs)” http://www.ibm.com/support/knowledgecenter/SSB23S\_1.1.0.13/gtpc1/pdus.html (Diakses pada Selasa, 11 Oktober 2016 )