NETWORK MANAGEMENT

Analisis Paket Data Jaringan Simple Network Manajemen Protocol (SNMP) Menggunakan Wireshark

Oleh :

Dinar Agustina

09011181520023

PROGRAM STUDI SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

1. Simple Network Management Protocol

Simple Network Management Protocol (SNMP) adalah sebuah aplikasi protokol yang menawarkan pelayanan manajemen jaringan pada Internet protokol suite-nya dan dirancang untuk memberikan kemampuan pengguna untuk mengatur dan memantau jaringan komputer secara sistematis. SNMP telah diterbitkan pada beberapa Cetakan RFCs pada awal tahun 1990. Selama beberapa tahun belakangan, SNMP telah diadaptasi oleh beberapa vendor perlengkapan jaringan sebagai management interface utama mereka ataupun sebagai perangkat cadangan.

Dengan adanya SNMP kita tidak perlu memeriksa satu-persatu setiap server, tetapi kita cukup mengakses satu komputer untuk melihat kondisi seluruh server dan router. Hal ini disebabkan server dan router akan bertindak sebagai SNMP-server yang bertugas untuk menyediakan request SNMP dari komputer lain. Satu PC akan bertindak sebagai SNMP Agent yaitu komputer yang mengumpulkan informasi-informasi dari SNMP-server.

SNMP menggambarkan sebuah relasi antara Client/Server. Program Client (disebut Network Manager) membuat koneksi virtual ke sebuah program server (disebut SNMP Agent) mengeksekusinya dalam remote network device. Database yang dikontrol oleh SNMP Agent akan diarahkan ke sebagai SNMP Management Information Base (MIB), dan merupakan sebuah standar dari set statistik dan kontrol nilai. Selain itu SNMP mengizinkan perpanjangan dari nilai-nilai standar dengan nilai-nilai spesifik ke agent tertentu melalui penggunaan private MIB.

Sebelum melanjutkan ada baiknya kita mengetahui apa itu Manager, MIB, dan Agent, berikut penjelasannya :

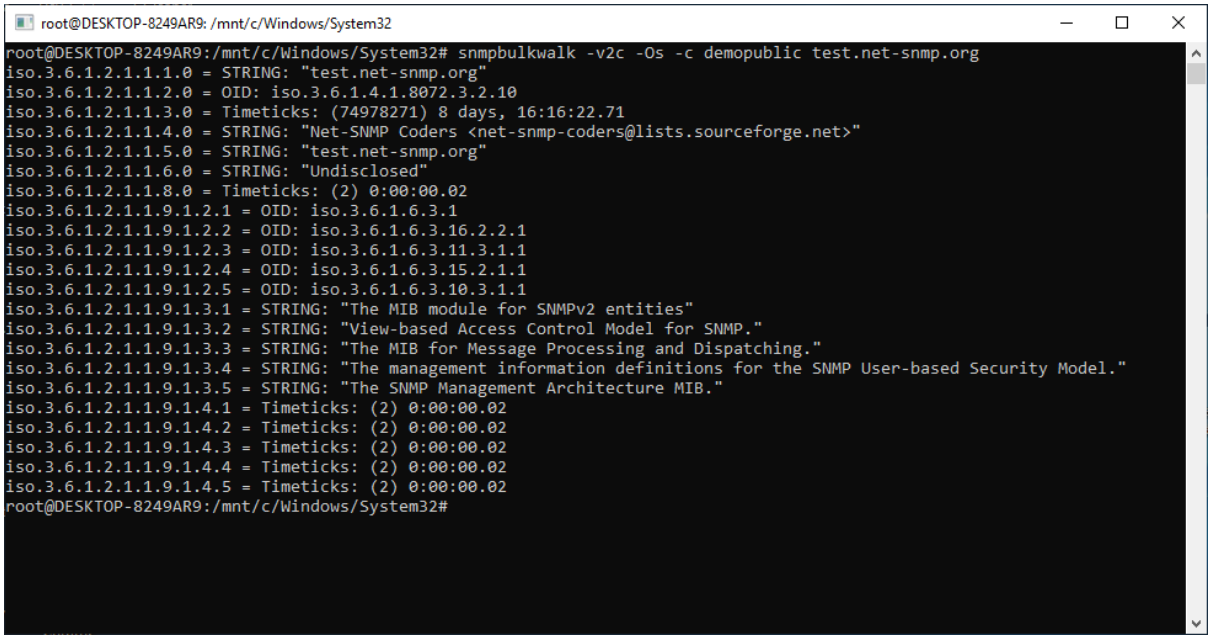
- Manager, yaitu bertugas sebagai manajemen jaringan yang mengumpulkan data informasi dari elemen-elemen jaringan yang ingin dimonitoring. Bentuk dari manager ini berupa perangkat lunak yang memiliki fungsi antarmuka yang baik bagi penggunanya dalam hal ini network administrator jaringan.
- MIB (Management 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.
- Agent, 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.

2. Analisa Paket Data Menggunakan Wireshark

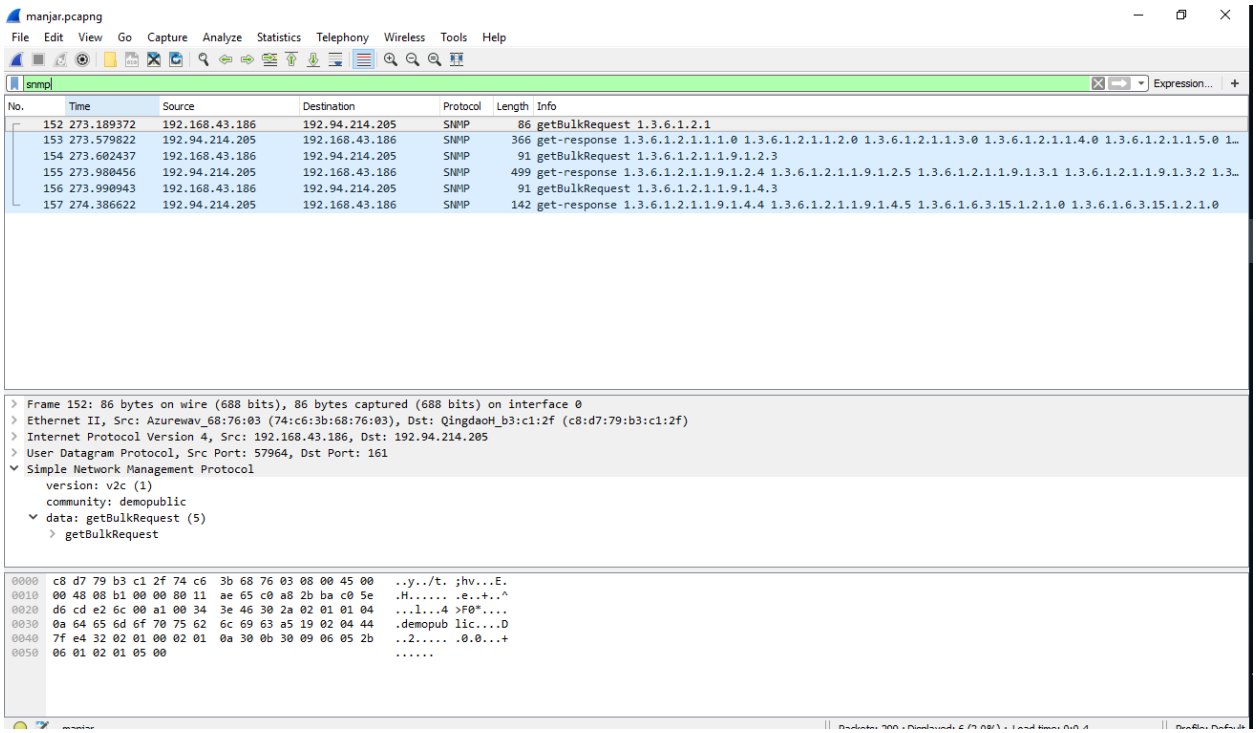
Tapping data dengan wireshark untuk mencari traffick SNMP saya lakukan menggunakan jaringan wifi, terlebih dahulu menginstal program snmp (*get apt install snmp*) pada terminal bash.

Berikut hasil command yang saya gunakan



Gambar 1 comand untuk mengaktifkan protocol snmp

Berikut gambar Capture traffick data SNMP di wireshark:

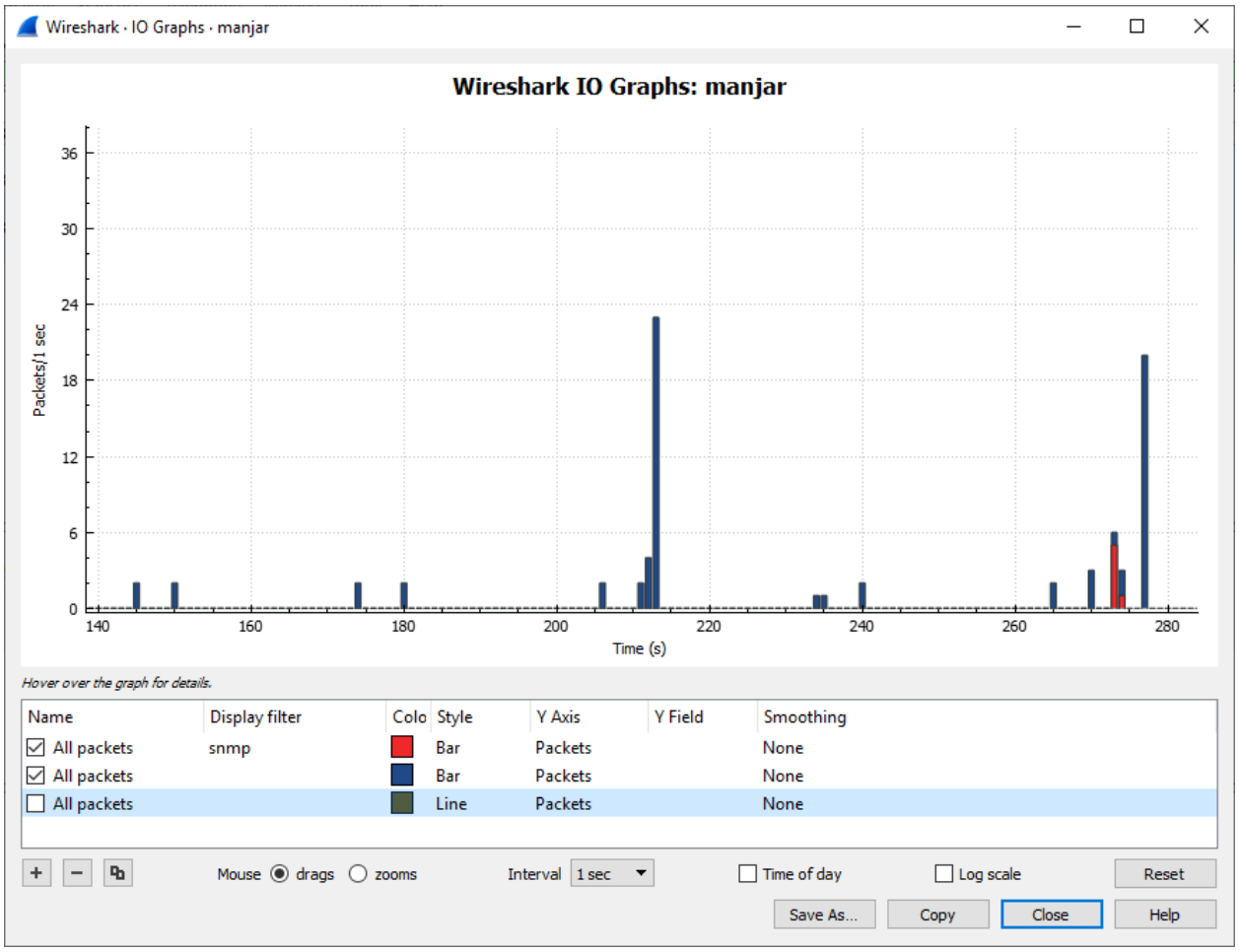


Gambar 2 capture traffic wireshark dengan filter snmp

Pada gambar tersebut terlihat hasil filtering dengan keyword “snmp” yang kita masukkan, terlihat beberapa caption sperti *no*, *time*, *destination*, *protocol*, *data length* dan juga info. Deretan tupple ini memperlihatkan *handshake* yang dilakukan antara kedua alamat. Address pertama 192.168.43.186 merupakan alamat ip manajer sedangkan alamat kedua 192.94.214.205 merupakan alamat router atau agen. Manajer melakukan *request* kepada *agen* berupa *get-next-request (Meminta komponen objek berikutnya dari suatu table atau daftar dari suatu agen)* dan nomor OID yang terlihat pada info, kemudian agen memberikan pesan *get-response (Merespon semua permintaan)* menuju manajer. Proses *trap* ini dilakukan terus menerus.

perlu kita ketahui bahwa bagian INFO pada setiap permintaan 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.

Berikut gambar trafik snmp beserta trafik protocol lainnya



Gambar 3 grafik snmp di dalam traffic jaringan

```
> Frame 152: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
> Ethernet II, Src: Azurewav_68:76:03 (74:c6:3b:68:76:03), Dst: QingdaoH_b3:c1:2f (c8:d7:79:b3:c1:2f)
> Internet Protocol Version 4, Src: 192.168.43.186, Dst: 192.94.214.205
> User Datagram Protocol, Src Port: 57964, Dst Port: 161
v Simple Network Management Protocol
    version: v2c (1)
    community: demopublic
  v data: getBulkRequest (5)
    v getBulkRequest
        request-id: 1149232178
        non-repeaters: 0
        max-repetitions: 10
      v variable-bindings: 1 item
        v 1.3.6.1.2.1: Value (Null)
            Object Name: 1.3.6.1.2.1 (iso.3.6.1.2.1)
            Value (Null)
```

Gambar 4 Info Detail GetBbulkRequest

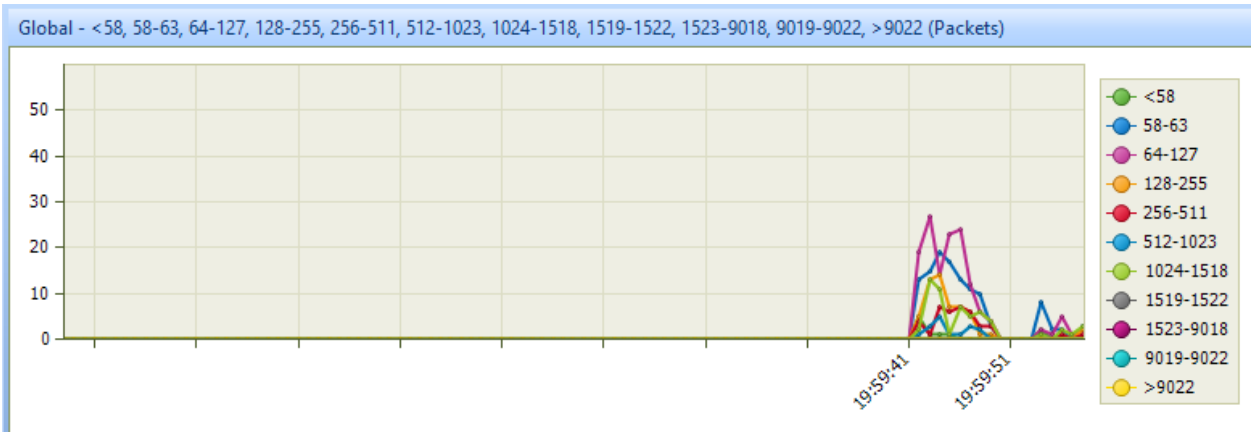
```
> Frame 153: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits) on interface 0
> Ethernet II, Src: QingdaoH_b3:c1:2f (c8:d7:79:b3:c1:2f), Dst: Azurewav_68:76:03 (74:c6:3b:68:76:03)
> Internet Protocol Version 4, Src: 192.94.214.205, Dst: 192.168.43.186
> User Datagram Protocol, Src Port: 161, Dst Port: 57964
v Simple Network Management Protocol
    version: v2c (1)
    community: demopublic
  v data: get-response (2)
    v get-response
        request-id: 1149232178
        error-status: noError (0)
        error-index: 0
      v variable-bindings: 10 items
        v 1.3.6.1.2.1.1.1.0: 746573742e6e65742d736e6d702e6f7267
            Object Name: 1.3.6.1.2.1.1.1.0 (iso.3.6.1.2.1.1.1.0)
          > Value (OctetString): 746573742e6e65742d736e6d702e6f7267
        v 1.3.6.1.2.1.1.2.0: 1.3.6.1.4.1.8072.3.2.10 (iso.3.6.1.4.1.8072.3.2.10)
            Object Name: 1.3.6.1.2.1.1.2.0 (iso.3.6.1.2.1.1.2.0)
```

Gambar 5 Info Detail get-response

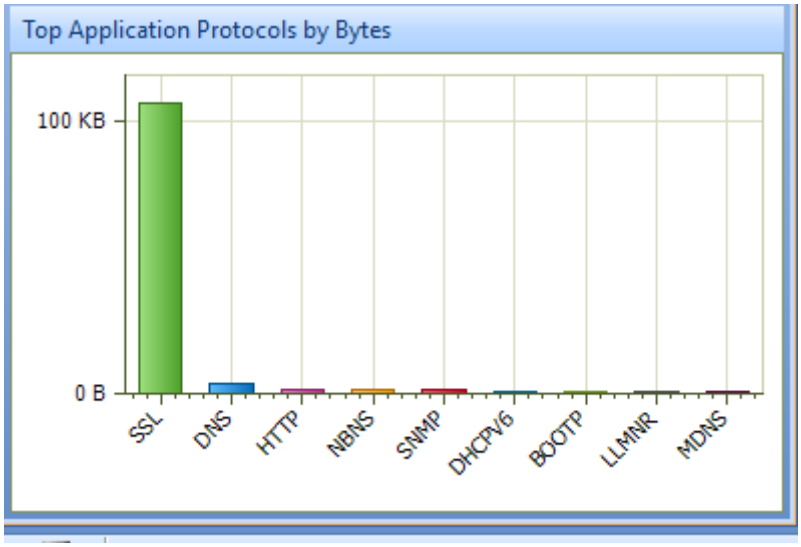
Dilihat pada info detail perbedaan antara **GetBbulkRequest** dan ***Get-Respone*** terdapat pada nilai *Value*-nya. Pada saat pertama kali manager mengirim *Get-Request* kepada agent, nilai *Value* yaitu Null. Kemudian agent menanggapi permintaan dari manager. maka agent akan mengirimkan *Get-Respone* ke manager. Di detail informasi *get-respone*, kita dapat melihat bahwa nilai Value adalah 74:65:73:74:2e:6e:65:74:2d:73:6e:6d:70:2e:6f:72:67 yang bertipe octetstring, nilai Value itulah yang akan di kirim kepada manager.

3. Visualisasi Traffic Menggunakan Colasoft

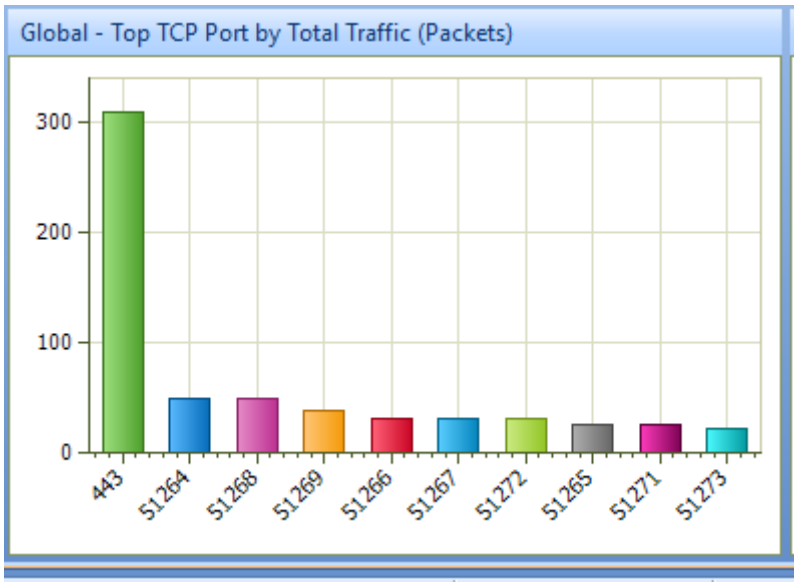
Pada gambar-gambar dibawah ini digunakan software yang berbeda untuk menampilkan traffic dari hasil capture menggunakan wireshark sebelumnya. Software yang digunakan adalah Colasoft Capsa. Jika kita perhatikan, terdapat kemiripan traffic dari software wireshark dan colasoft.



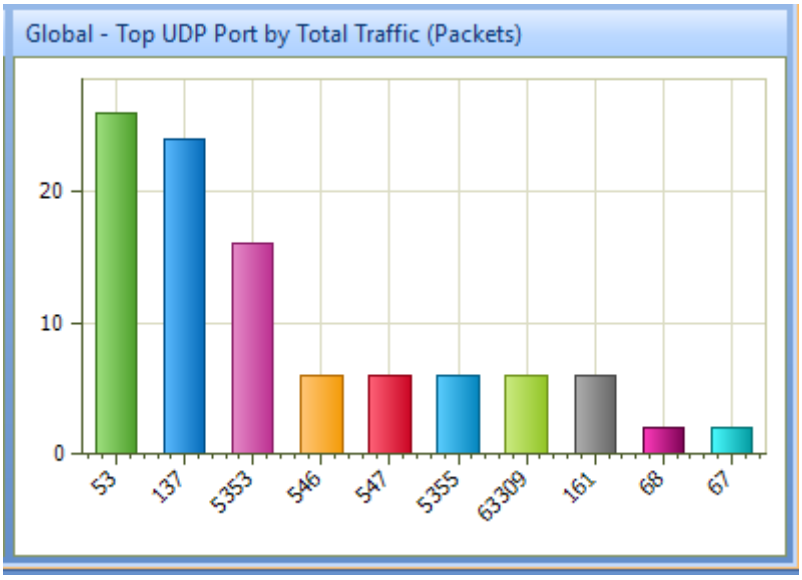
Gambar 6 Traffic data menggunakan Colasoft



Gambar 7 grafik top aplikasi protokol



Gambar 8 grafik top tcp port



Gambar 9 grafik top udp port

Name	Bytes	Packets	bps
Ethernet II	130.12 KB	439	928.000 bps
IP	126.12 KB	396	928.000 bps
TCP	117.89 KB	329	928.000 bps
SSL	106.25 KB	163	35.888 Kbps
HTTPS	106.25 KB	163	35.888 Kbps
HTTP	1.84 KB	5	472.000 bps
UDP	7.41 KB	53	2.376 Kbps
DNS	3.44 KB	26	2.376 Kbps
DNS Response	2.36 KB	13	1.632 Kbps
DNS Query	1.08 KB	13	744.000 bps
NBNS	1.34 KB	12	2.736 Kbps
SNMP	1.27 KB	6	5.952 Kbps
BOOTP	743.00 B	2	5.944 Kbps
DHCP	743.00 B	2	5.944 Kbps

Gambar 10 Tabel Usage setiap protocol

4. Kesimpulan

SNMP merupakan sebuah protokol jaringan yang dibuat agar para administrator jaringan bisa memonitoring perangkat jaringan yang ada pada jaringannya. Bukan hanya memonitoring perangkatnya saja, para administrator juga bisa melihat bagaimana keadaan traffic pada jaringan yang mereka punyai. Protocol ini sangat berguna agar bisa membuat para administrator bisa mengetahui bila terjadi keanehan baik pada trafik jaringan maupun pada perangkat jaringan mereka.

DAFTAR PUSTAKA

1. Admin. “IBM Knowledge Center: Protocol data units (PDUs)” http://www.ibm.com/support/knowledgecenter/SSB23S_1.1.0.13/gtpc1/pdus.htm l (Diakses pada Selasa, 11 Oktober 2016)
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.”