

# **Network Management**

## **Analisa Paket Data Jaringan Simple Network Manajemen Protoco (SNMP)**

### **Menggunakan Wireshark**



**OLEH :**

**SYUKRAN RIZKI**

**09011181520019**

**JURUSAN SISTEM KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**2018**

## **Simple Network Management Protocol (SNMP)**

Simple Network Management Protocol (SNMP) merupakan sebuah protokol yang dirancang untuk memberikan kemampuan kepada pengguna untuk memantau dan mengatur jaringan komputernya secara sistematis dari jarak jauh atau dalam satu pusat kontrol saja. Pengolahan ini dijalankan dengan menggumpulkan data dan melakukan penetapan terhadap variabel-variabel dalam elemen jaringan yang dikelola.

Elemen-elemen di SNMP :

- a. Manajer adalah pelaksana dan manajemen jaringan. Pada kenyataannya manager ini merupakan komputer biasa yang ada pada jaringan yang mengoperasikan perangkat lunak untuk manajemen jaringan. Manajer 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. Struktur ini bersifat hierarki dan memiliki aturan sedemikian rupa sehingga informasi setiap variabel dapat dikelola atau ditetapkan dengan mudah.
- c. 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. 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.

## Analisa Paket data menggunakan Wireshark

The image shows a Wireshark packet capture of an SNMP session. The top pane displays a list of packets, with packet 138 selected. The middle pane shows the details of packet 138, which is an SNMP GET request. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
138	94.236072	10.100.227.62	192.94.214.205	SNMP	86	getBulkRequest 1.3.6.1.2.1
139	94.814234	192.94.214.205	10.100.227.62	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 1.3.6.1.2.1.1.6.0 1.3.6.1.2.1.1.7.0 1.3.6.1.2.1.1.8.0 1.3.6.1.2.1.1.9.0 1.3.6.1.2.1.1.10.0 1.3.6.1.2.1.1.11.0 1.3.6.1.2.1.1.12.0 1.3.6.1.2.1.1.13.0 1.3.6.1.2.1.1.14.0 1.3.6.1.2.1.1.15.0 1.3.6.1.2.1.1.16.0 1.3.6.1.2.1.1.17.0 1.3.6.1.2.1.1.18.0 1.3.6.1.2.1.1.19.0 1.3.6.1.2.1.1.20.0 1.3.6.1.2.1.1.21.0 1.3.6.1.2.1.1.22.0 1.3.6.1.2.1.1.23.0 1.3.6.1.2.1.1.24.0 1.3.6.1.2.1.1.25.0 1.3.6.1.2.1.1.26.0 1.3.6.1.2.1.1.27.0 1.3.6.1.2.1.1.28.0 1.3.6.1.2.1.1.29.0 1.3.6.1.2.1.1.30.0 1.3.6.1.2.1.1.31.0 1.3.6.1.2.1.1.32.0 1.3.6.1.2.1.1.33.0 1.3.6.1.2.1.1.34.0 1.3.6.1.2.1.1.35.0 1.3.6.1.2.1.1.36.0 1.3.6.1.2.1.1.37.0 1.3.6.1.2.1.1.38.0 1.3.6.1.2.1.1.39.0 1.3.6.1.2.1.1.40.0 1.3.6.1.2.1.1.41.0 1.3.6.1.2.1.1.42.0 1.3.6.1.2.1.1.43.0 1.3.6.1.2.1.1.44.0 1.3.6.1.2.1.1.45.0 1.3.6.1.2.1.1.46.0 1.3.6.1.2.1.1.47.0 1.3.6.1.2.1.1.48.0 1.3.6.1.2.1.1.49.0 1.3.6.1.2.1.1.50.0 1.3.6.1.2.1.1.51.0 1.3.6.1.2.1.1.52.0 1.3.6.1.2.1.1.53.0 1.3.6.1.2.1.1.54.0 1.3.6.1.2.1.1.55.0 1.3.6.1.2.1.1.56.0 1.3.6.1.2.1.1.57.0 1.3.6.1.2.1.1.58.0 1.3.6.1.2.1.1.59.0 1.3.6.1.2.1.1.60.0 1.3.6.1.2.1.1.61.0 1.3.6.1.2.1.1.62.0 1.3.6.1.2.1.1.63.0 1.3.6.1.2.1.1.64.0 1.3.6.1.2.1.1.65.0 1.3.6.1.2.1.1.66.0 1.3.6.1.2.1.1.67.0 1.3.6.1.2.1.1.68.0 1.3.6.1.2.1.1.69.0 1.3.6.1.2.1.1.70.0 1.3.6.1.2.1.1.71.0 1.3.6.1.2.1.1.72.0 1.3.6.1.2.1.1.73.0 1.3.6.1.2.1.1.74.0 1.3.6.1.2.1.1.75.0 1.3.6.1.2.1.1.76.0 1.3.6.1.2.1.1.77.0 1.3.6.1.2.1.1.78.0 1.3.6.1.2.1.1.79.0 1.3.6.1.2.1.1.80.0 1.3.6.1.2.1.1.81.0 1.3.6.1.2.1.1.82.0 1.3.6.1.2.1.1.83.0 1.3.6.1.2.1.1.84.0 1.3.6.1.2.1.1.85.0 1.3.6.1.2.1.1.86.0 1.3.6.1.2.1.1.87.0 1.3.6.1.2.1.1.88.0 1.3.6.1.2.1.1.89.0 1.3.6.1.2.1.1.90.0 1.3.6.1.2.1.1.91.0 1.3.6.1.2.1.1.92.0 1.3.6.1.2.1.1.93.0 1.3.6.1.2.1.1.94.0 1.3.6.1.2.1.1.95.0 1.3.6.1.2.1.1.96.0 1.3.6.1.2.1.1.97.0 1.3.6.1.2.1.1.98.0 1.3.6.1.2.1.1.99.0 1.3.6.1.2.1.1.100.0 1.3.6.1.2.1.1.101.0 1.3.6.1.2.1.1.102.0 1.3.6.1.2.1.1.103.0 1.3.6.1.2.1.1.104.0 1.3.6.1.2.1.1.105.0 1.3.6.1.2.1.1.106.0 1.3.6.1.2.1.1.107.0 1.3.6.1.2.1.1.108.0 1.3.6.1.2.1.1.109.0 1.3.6.1.2.1.1.110.0 1.3.6.1.2.1.1.111.0 1.3.6.1.2.1.1.112.0 1.3.6.1.2.1.1.113.0 1.3.6.1.2.1.1.114.0 1.3.6.1.2.1.1.115.0 1.3.6.1.2.1.1.116.0 1.3.6.1.2.1.1.117.0 1.3.6.1.2.1.1.118.0 1.3.6.1.2.1.1.119.0 1.3.6.1.2.1.1.120.0 1.3.6.1.2.1.1.121.0 1.3.6.1.2.1.1.122.0 1.3.6.1.2.1.1.123.0 1.3.6.1.2.1.1.124.0 1.3.6.1.2.1.1.125.0 1.3.6.1.2.1.1.126.0 1.3.6.1.2.1.1.127.0 1.3.6.1.2.1.1.128.0 1.3.6.1.2.1.1.129.0 1.3.6.1.2.1.1.130.0 1.3.6.1.2.1.1.131.0 1.3.6.1.2.1.1.132.0 1.3.6.1.2.1.1.133.0 1.3.6.1.2.1.1.134.0 1.3.6.1.2.1.1.135.0 1.3.6.1.2.1.1.136.0 1.3.6.1.2.1.1.137.0 1.3.6.1.2.1.1.138.0 1.3.6.1.2.1.1.139.0 1.3.6.1.2.1.1.140.0 1.3.6.1.2.1.1.141.0 1.3.6.1.2.1.1.142.0 1.3.6.1.2.1.1.143.0 1.3.6.1.2.1.1.144.0 1.3.6.1.2.1.1.145.0 1.3.6.1.2.1.1.146.0 1.3.6.1.2.1.1.147.0 1.3.6.1.2.1.1.148.0 1.3.6.1.2.1.1.149.0 1.3.6.1.2.1.1.150.0 1.3.6.1.2.1.1.151.0 1.3.6.1.2.1.1.152.0 1.3.6.1.2.1.1.153.0 1.3.6.1.2.1.1.154.0 1.3.6.1.2.1.1.155.0 1.3.6.1.2.1.1.156.0 1.3.6.1.2.1.1.157.0 1.3.6.1.2.1.1.158.0 1.3.6.1.2.1.1.159.0 1.3.6.1.2.1.1.160.0 1.3.6.1.2.1.1.161.0 1.3.6.1.2.1.1.162.0 1.3.6.1.2.1.1.163.0 1.3.6.1.2.1.1.164.0 1.3.6.1.2.1.1.165.0 1.3.6.1.2.1.1.166.0 1.3.6.1.2.1.1.167.0 1.3.6.1.2.1.1.168.0 1.3.6.1.2.1.1.169.0 1.3.6.1.2.1.1.170.0 1.3.6.1.2.1.1.171.0 1.3.6.1.2.1.1.172.0 1.3.6.1.2.1.1.173.0 1.3.6.1.2.1.1.174.0 1.3.6.1.2.1.1.175.0 1.3.6.1.2.1.1.176.0 1.3.6.1.2.1.1.177.0 1.3.6.1.2.1.1.178.0 1.3.6.1.2.1.1.179.0 1.3.6.1.2.1.1.180.0 1.3.6.1.2.1.1.181.0 1.3.6.1.2.1.1.182.0 1.3.6.1.2.1.1.183.0 1.3.6.1.2.1.1.184.0 1.3.6.1.2.1.1.185.0 1.3.6.1.2.1.1.186.0 1.3.6.1.2.1.1.187.0 1.3.6.1.2.1.1.188.0 1.3.6.1.2.1.1.189.0 1.3.6.1.2.1.1.190.0 1.3.6.1.2.1.1.191.0

Gambar 1.1

Berdasarkan dari gambar 1.1 dapat kita lihat pada Info bahwa setiap pesan SNMP terdapat Request dan Response.

Arti dari Get-Request dan Get-Response :

1. Get-Request : dikirim oleh SNMP manager untuk mengambil satu atau lebih variabel MIB yang diminta.
2. Get-Response : dikirim oleh SNMP agent dalam menanggapi Get-Request, Get-Next-Request atau Set-Request.

**Keterangan :**

No.	Time	Source	Destination	Protocol	Length	Info
138	94.236072	10.100.227.62	192.94.214.205	SNMP	86	getBulkRequest 1.3.6.1.2.1
139	94.814234	192.94.214.205	10.100.227.62	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 1.3.6.1.2.1.1.6.0 1.3.6.1.2.1.1.7.0 1.3.6.1.2.1.1.8.0 1.3.6.1.2.1.1.9.0 1.3.6.1.2.1.1.10.0 1.3.6.1.2.1.1.11.0 1.3.6.1.2.1.1.12.0 1.3.6.1.2.1.1.13.0 1.3.6.1.2.1.1.14.0 1.3.6.1.2.1.1.15.0 1.3.6.1.2.1.1.16.0 1.3.6.1.2.1.1.17.0 1.3.6.1.2.1.1.18.0 1.3.6.1.2.1.1.19.0 1.3.6.1.2.1.1.20.0 1.3.6.1.2.1.1.21.0 1.3.6.1.2.1.1.22.0 1.3.6.1.2.1.1.23.0 1.3.6.1.2.1.1.24.0 1.3.6.1.2.1.1.25.0 1.3.6.1.2.1.1.26.0 1.3.6.1.2.1.1.27.0 1.3.6.1.2.1.1.28.0 1.3.6.1.2.1.1.29.0 1.3.6.1.2.1.1.30.0 1.3.6.1.2.1.1.31.0 1.3.6.1.2.1.1.32.0 1.3.6.1.2.1.1.33.0 1.3.6.1.2.1.1.34.0 1.3.6.1.2.1.1.35.0 1.3.6.1.2.1.1.36.0 1.3.6.1.2.1.1.37.0 1.3.6.1.2.1.1.38.0 1.3.6.1.2.1.1.39.0 1.3.6.1.2.1.1.40.0 1.3.6.1.2.1.1.41.0 1.3.6.1.2.1.1.42.0 1.3.6.1.2.1.1.43.0 1.3.6.1.2.1.1.44.0 1.3.6.1.2.1.1.45.0 1.3.6.1.2.1.1.46.0 1.3.6.1.2.1.1.47.0 1.3.6.1.2.1.1.48.0 1.3.6.1.2.1.1.49.0 1.3.6.1.2.1.1.50.0 1.3.6.1.2.1.1.51.0 1.3.6.1.2.1.1.52.0 1.3.6.1.2.1.1.53.0 1.3.6.1.2.1.1.54.0 1.3.6.1.2.1.1.55.0 1.3.6.1.2.1.1.56.0 1.3.6.1.2.1.1.57.0 1.3.6.1.2.1.1.58.0 1.3.6.1.2.1.1.59.0 1.3.6.1.2.1.1.60.0 1.3.6.1.2.1.1.61.0 1.3.6.1.2.1.1.62.0 1.3.6.1.2.1.1.63.0 1.3.6.1.2.1.1.64.0 1.3.6.1.2.1.1.65.0 1.3.6.1.2.1.1.66.0 1.3.6.1.2.1.1.67.0 1.3.6.1.2.1.1.68.0 1.3.6.1.2.1.1.69.0 1.3.6.1.2.1.1.70.0 1.3.6.1.2.1.1.71.0 1.3.6.1.2.1.1.72.0 1.3.6.1.2.1.1.73.0 1.3.6.1.2.1.1.74.0 1.3.6.1.2.1.1.75.0 1.3.6.1.2.1.1.76.0 1.3.6.1.2.1.1.77.0 1.3.6.1.2.1.1.78.0 1.3.6.1.2.1.1.79.0 1.3.6.1.2.1.1.80.0 1.3.6.1.2.1.1.81.0 1.3.6.1.2.1.1.82.0 1.3.6.1.2.1.1.83.0 1.3.6.1.2.1.1.84.0 1.3.6.1.2.1.1.85.0 1.3.6.1.2.1.1.86.0 1.3.6.1.2.1.1.87.0 1.3.6.1.2.1.1.88.0 1.3.6.1.2.1.1.89.0 1.3.6.1.2.1.1.90.0 1.3.6.1.2.1.1.91.0 1.3.6.1.2.1.1.92.0 1.3.6.1.2.1.1.93.0 1.3.6.1.2.1.1.94.0 1.3.6.1.2.1.1.95.0 1.3.6.1.2.1.1.96.0 1.3.6.1.2.1.1.97.0 1.3.6.1.2.1.1.98.0 1.3.6.1.2.1.1.99.0 1.3.6.1.2.1.1.100.0 1.3.6.1.2.1.1.101.0 1.3.6.1.2.1.1.102.0 1.3.6.1.2.1.1.103.0 1.3.6.1.2.1.1.104.0 1.3.6.1.2.1.1.105.0 1.3.6.1.2.1.1.106.0 1.3.6.1.2.1.1.107.0 1.3.6.1.2.1.1.108.0 1.3.6.1.2.1.1.109.0 1.3.6.1.2.1.1.110.0 1.3.6.1.2.1.1.111.0 1.3.6.1.2.1.1.112.0 1.3.6.1.2.1.1.113.0 1.3.6.1.2.1.1.114.0 1.3.6.1.2.1.1.115.0 1.3.6.1.2.1.1.116.0 1.3.6.1.2.1.1.117.0 1.3.6.1.2.1.1.118.0 1.3.6.1.2.1.1.119.0 1.3.6.1.2.1.1.120.0 1.3.6.1.2.1.1.121.0 1.3.6.1.2.1.1.122.0 1.3.6.1.2.1.1.123.0 1.3.6.1.2.1.1.124.0 1.3.6.1.2.1.1.125.0 1.3.6.1.2.1.1.126.0 1.3.6.1.2.1.1.127.0 1.3.6.1.2.1.1.128.0 1.3.6.1.2.1.1.129.0 1.3.6.1.2.1.1.130.0 1.3.6.1.2.1.1.131.0 1.3.6.1.2.1.1.132.0 1.3.6.1.2.1.1.133.0 1.3.6.1.2.1.1.134.0 1.3.6.1.2.1.1.135.0 1.3.6.1.2.1.1.136.0 1.3.6.1.2.1.1.137.0 1.3.6.1.2.1.1.138.0 1.3.6.1.2.1.1.139.0 1.3.6.1.2.1.1.140.0 1.3.6.1.2.1.1.141.0 1.3.6.1.2.1.1.142.0 1.3.6.1.2.1.1.143.0 1.3.6.1.2.1.1.144.0 1.3.6.1.2.1.1.145.0 1.3.6.1.2.1.1.146.0 1.3.6.1.2.1.1.147.0 1.3.6.1.2.1.1.148.0 1.3.6.1.2.1.1.149.0 1.3.6.1.2.1.1.150.0 1.3.6.1.2.1.1.151.0 1.3.6.1.2.1.1.152.0 1.3.6.1.2.1.1.153.0 1.3.6.1.2.1.1.154.0 1.3.6.1.2.1.1.155.0 1.3.6.1.2.1.1.156.0 1.3.6.1.2.1.1.157.0 1.3.6.1.2.1.1.158.0 1.3.6.1.2.1.1.159.0 1.3.6.1.2.1.1.160.0 1.3.6.1.2.1.1.161.0 1.3.6.1.2.1.1.162.0 1.3.6.1.2.1.1.163.0 1.3.6.1.2.1.1.164.0 1.3.6.1.2.1.1.165.0 1.3.6.1.2.1.1.166.0 1.3.6.1.2.1.1.167.0 1.3.6.1.2.1.1.168.0 1.3.6.1.2.1.1.169.0 1.3.6.1.2.1.1.170.0 1.3.6.1.2.1.1.171.0 1.3.6.1.2.1.1.172.0 1.3.6.1.2.1.1.173.0 1.3.6.1.2.1.1.174.0 1.3.6.1.2.1.1.175.0 1.3.6.1.2.1.1.176.0 1.3.6.1.2.1.1.177.0 1.3.6.1.2.1.1.178.0 1.3.6.1.2.1.1.179.0 1.3.6.1.2.1.1.180.0 1.3.6.1.2.1.1.181.0 1.3.6.1.2.1.1.182.0 1.3.6.1.2.1.1.183.0 1.3.6.1.2.1.1.184.0 1.3.6.1.2.1.1.185.0 1.3.6.1.2.1.1.186.0 1.3.6.1.2.1.1.187.0 1.3.6.1.2.1.1.188.0 1.3.6.1.2.1.1.189.0 1.3.6.1.2.1.1.190.0 1.3.6.1.2.1.1.191.0 1.3.6.1.2.1.1.192.0 1.3.6.1.2.1.1.193.0 1.3.6.1.2.1.1.194.0 1.3.6.1.2.1.1.195.0 1.3.6.1.2.1.1.196.0 1.3.6.1.2.1.1.197.0 1.3.6.1.2.1.1.198.0

Gambar 1.2 Daftar Paket Data

```

> Frame 138: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
> Ethernet II, Src: LiteonTe_9e:bc:7f (cc:b0:da:9e:bc:7f), Dst: Routerbo_c2:57:3e (64:d1:54:c2:57:3e)
> Internet Protocol Version 4, Src: 10.100.227.62, Dst: 192.94.214.205
> User Datagram Protocol, Src Port: 64394, Dst Port: 161
> Simple Network Management Protocol

```

Gambar 1.3 Detail Paket Data

```

0000  64 d1 54 c2 57 3e cc b0 da 9e bc 7f 08 00 45 00  d·T·W>· ······E·
0010  00 48 53 5f 00 00 80 11 62 77 0a 64 e3 3e c0 5e  ·HS_···· bw·d·>·^
0020  d6 cd fb 8a 00 a1 00 34 88 9b 30 2a 02 01 01 04  ······4 ·0*····
0030  0a 64 65 6d 6f 70 75 62 6c 69 63 a5 19 02 04 7f  ·demopub lic····
0040  7f f5 cd 02 01 00 02 01 0a 30 0b 30 09 06 05 2b  ······ ·0·0···+
0050  06 01 02 01 05 00 ······

```

Gambar 1.4 Detail Paket Data Dalam Decimal

## Analisa Traffic data :

capture.snmp.pcapng

No.	Time	Source	Destination	Protocol	Length	Info
138	94.236072	10.100.227.62	192.94.214.205	SNMP	86	getBulkRequest 1.3.6.1.2.1
139	94.814234	192.94.214.205	10.100.227.62	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
140	94.901192	10.100.227.62	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.2.3
141	95.192564	192.94.214.205	10.100.227.62	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 1.3.6.1.2.1.1.9.1.4.1
142	95.501901	10.100.227.62	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.4.3
143	95.789524	192.94.214.205	10.100.227.62	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 1.3.6.1.6.3.15.1.2.1.1

Gambar 1.5

Pad gambar 1.5 menjelaskan tentang beberapa IP yang sedang melakukan traffic data dengan request dan response, dengan aplikasi ini lah kita dapat menganalisa IP mana yang sedang melakukan request dan melakukan response, yang dilengkapi dengan Time, Source dan Destination.

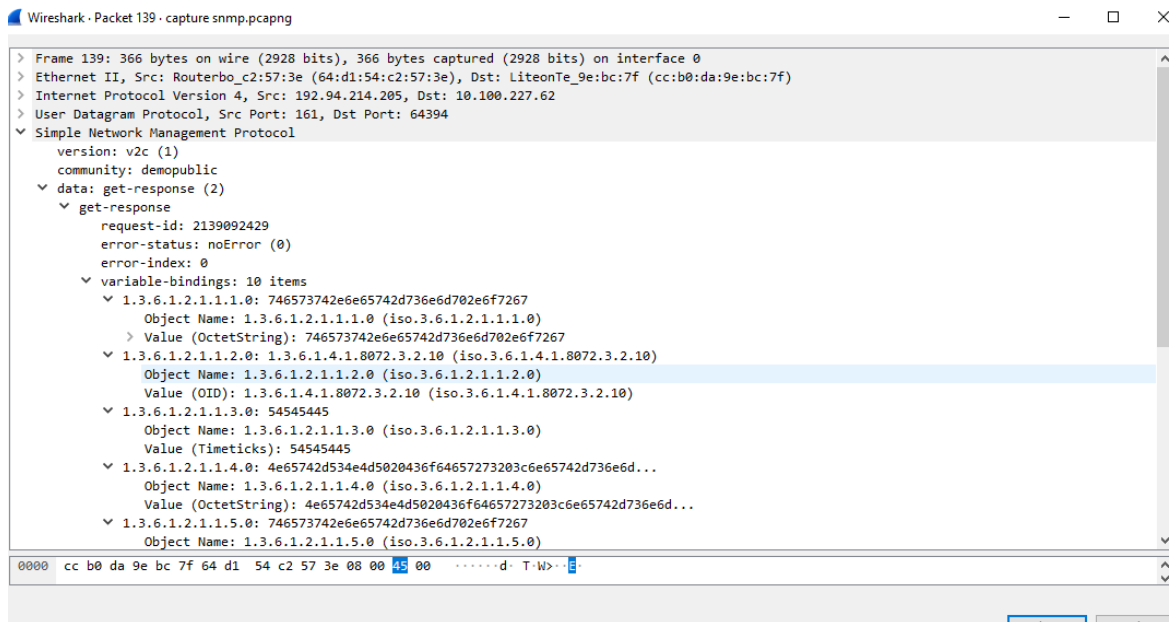
No.	Time	Source	Destination	Protocol	Length	Info
138	94.236072	10.100.227.62	192.94.214.205	SNMP	86	getBulkRequest 1.3.6.1.2.1
139	94.814234	192.94.214.205	10.100.227.62	SNMP	366	get-response 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.1.4.0
140	94.901192	10.100.227.62	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.2.3
141	95.192564	192.94.214.205	10.100.227.62	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 1.3.6.1.2.1.1.9.1.4.1
142	95.501901	10.100.227.62	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.4.3
143	95.789524	192.94.214.205	10.100.227.62	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 1.3.6.1.6.3.15.1.2.1.1.0

> Frame 138: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0  
 > Ethernet II, Src: LiteonTe\_9e:bc:7f (cc:b0:da:9e:bc:7f), Dst: Routerbo\_c2:57:3e (64:d1:54:c2:57:3e)  
 > Internet Protocol Version 4, Src: 10.100.227.62, Dst: 192.94.214.205  
 > User Datagram Protocol, Src Port: 64394, Dst Port: 161  
 > Simple Network Management Protocol  
   version: v2c (1)  
   community: demopublic  
   data: getBulkRequest (5)  
     getBulkRequest  
       request-id: 2139092429  
       non-repeaters: 0  
       max-repetitions: 10  
       variable-bindings: 1 item  
         1.3.6.1.2.1: Value (Null)  
           Object Name: 1.3.6.1.2.1 (iso.3.6.1.2.1)  
           Value (Null)

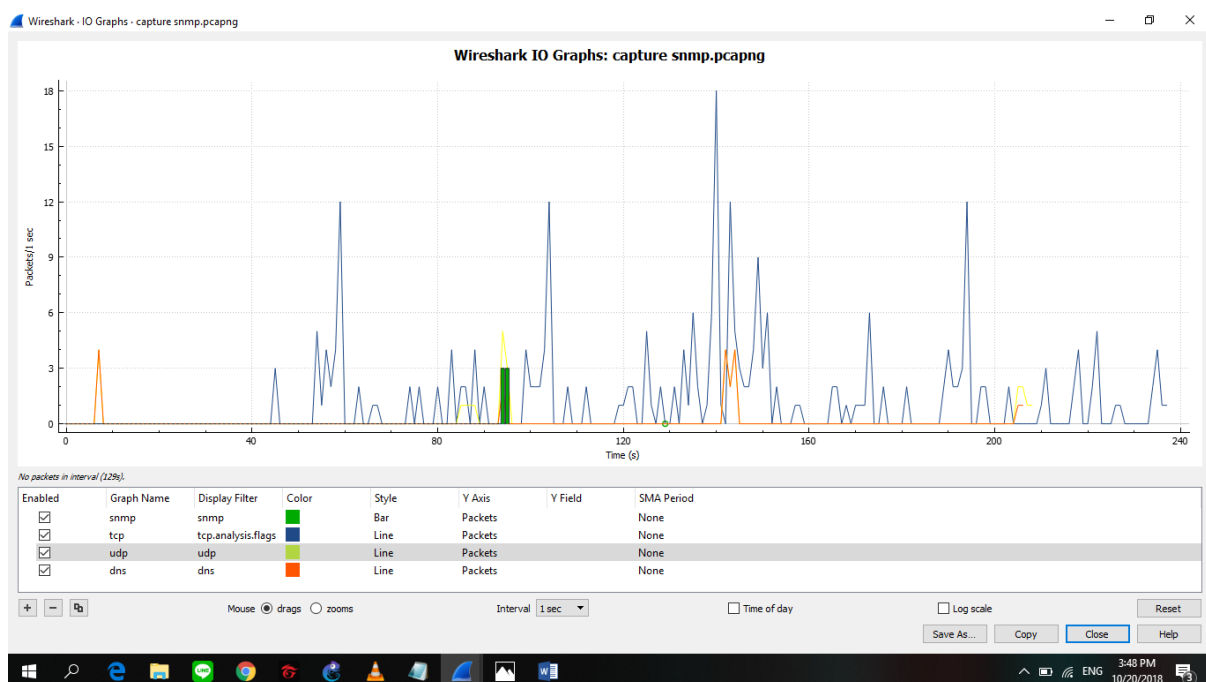
Gambar 1.6 Capture informasi paket Request

Pada gambar 1.6 merupakan sebuah capturan dari pcaps menggunakan aplikasi whireshark dimana pada gambar tersebut menjelaskan tentang bagaimana IP melakukan request. Dari capturan diatas IP source 10.100.227.62 dan IP destination 192.94.214..205 dan menggunakan protocol SNMP dengan request-id: 2139092429 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 nah dari variable variable diatas terbentuklah satu kesatuan variable saat IP meminta request.



Gambar 1.7 Capture informasi paket Response

Pada Gambar 1.7 merupakan sebuah capturan dari pcaps menggunakan aplikasi whireshark dimana pada gambar tersebut menjelaskan tentang bagaimana IP melakukan response. Dari capturan diatas IP source 192.92.214.205 dan IP destination 10.100.227.62 dan menggunakan protocol SNMP.



Gambar 1.8 Traffic Paket Data Menggunakan Wireshark

Pada gambar 1.8 dapat kita lihat sekumpulan traffic berbagai protocol dari data yang telah kita capture menggunakan wireshark mulai dari protocol SNMP yang ditandai dengan warna hijau, TCP dengan warna biru, UDP dengan warna kuning, DNS dengan warna Orange.