

**MANAGEMENT JARINGAN**

**(TRAFFIC SNMP)**



**NOVIT HARDIANTO**

**09011281520086**

**JURUSAN SISTEM KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**2018**

SNMP (Simple Network Management Protocol) sebuah protocol yang dirancang untuk memberikan kemampuan pengguna untuk mengatur dan memantau jaringan komputer secara sistematis sementara MIB atau manager information base dapat dikatakan sebagai struktur basis data variable dari elemen jaringan yang dikelola. Struktur ini bersifat hierarki dan memiliki aturan sedemikian rupa sehingga informasi setiap variable dapat dikelola atau ditetapkan dengan mudah MIB mempunyai beberapa struktur diantaranya:

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

Wireshark merupakan salah satu dari tool Network Analyzer yang biasa digunakan oleh Network Administrator pemecahan masalah jaringan, analisis, perangkat lunak dan pengembangan protokol komunikasi, dan pendidikan. Awalnya bernama Ethereal, dan pada Mei 2006 proyek ini berganti nama menjadi Wireshark karena masalah merek dagang. Bahasa Pemrograman yang digunakan adalah bahasa C dengan lisensi public umum GNU. Wireshark banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis. Seperti namanya, Wireshark mampu menangkap paket-paket data/informasi yang bertebaran dalam jaringan yang kita “intip”. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tidak jarang tool ini juga dapat dipakai untuk sniffing (memperoleh informasi penting spt password email atau account lain) dengan menangkap paket-paket yang berseliweran di dalam jaringan dan menganalisisnya. Untuk menggunakan tool ini pun cukup mudah. Kita cukup memasukkan perintah untuk mendapatkan informasi yang ingin kita capture (yang ingin diperoleh) dari jaringan kita.

## Taping data respons

No.	Time	Source	Destination	Protocol	Length	Info
97	11.280562	10.94.16.173	192.94.214.205	SNMP	86	getBulkRequest 1.3.6.1.2.1
103	11.554579	192.94.214.205	10.94.16.173	SNMP	366	get-response 1.3.6.1.2.1.1.0 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...
104	11.559959	10.94.16.173	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.2.3
109	11.834764	192.94.214.205	10.94.16.173	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...
110	11.841333	10.94.16.173	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.4.3
117	12.841920	10.94.16.173	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.4.3
122	13.126384	192.94.214.205	10.94.16.173	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

> Frame 103: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits) on interface 0  
> Ethernet II, Src: Routerbo\_44:6b:88 (d4:ca:6d:44:6b:88), Dst: AsustekC\_1c:70:e7 (88:d7:f6:1c:70:e7)  
> Internet Protocol Version 4, Src: 192.94.214.205, Dst: 10.94.16.173  
> User Datagram Protocol, Src Port: 161, Dst Port: 60246  
▼ Simple Network Management Protocol  
  version: v2c (1)  
  community: demopublic  
  data: get-response (2)  
    get-response  
      request-id: 1087550717  
      error-status: noError (0)  
      error-index: 0  
      variable-bindings: 10 items  
        1.3.6.1.2.1.1.1.0: 746573742e6e5742d736e6d702e6f7267

```
0000 88 d7 f6 1c 70 e7 d4 ca 6d 44 6b 88 08 00 45 00  ...mDk...E
0010 01 60 00 00 40 00 30 11 97 56 c0 5e d6 cd 0a 5e  ...@0...V...^
0020 10 ad 00 a3 eb 56 01 4c 02 eb 30 02 01 40 02 01  ...V...@
0030 01 04 0a 64 65 6d 6f 70 75 62 6c 69 63 a2 82 01  ...demopublic...
0040 2d 02 04 40 d2 b4 fd 02 01 00 02 01 00 30 82 01  ...@...0...
0050 1d 30 1d 06 08 2b 06 01 02 01 01 01 00 04 11 74  ...0...+...t
0060 65 73 74 2e 6e 65 74 2d 73 6e 6d 70 2e 6f 72 67  est.net-snmp.org
0070 30 16 06 08 2b 06 01 02 01 01 02 00 06 0a 2b 06  0...+...+
0080 01 04 01 bf 08 03 02 0a 30 10 06 08 2b 06 01 02  ...+...+
0090 01 01 03 00 43 04 03 eb 9e d0 30 43 06 00 2b 06  ...C...@...+
00a0 01 02 01 01 04 00 04 37 4e 65 74 2d 53 4e 4d 50  ...7 Net-SNMP
00b0 20 43 6f 64 65 72 73 20 3c 6e 65 74 2d 73 6e 6d  Coders <net-smn
00c0 70 2d 63 6f 64 65 72 73 40 6c 69 73 74 73 2e 73  p-coders @lists.s
00d0 6f 75 72 63 65 66 6f 72 67 65 2e 6e 65 74 3e 30  ourcefor ge.net>0
```

Activate Windows  
Go to Settings to activate Windows.

Dari taping data dia atas dapat kita simpulkan bahwa saya menggunakan aplikasi whireshark dimana pada gambar tersebut menjelaskan tentang bagaimana IP melakukan response. Dari capturan diatas IP source 192.94.214.205 dan IP destination 10.94.16.173 dan menggunakan protocol SNMP. Cara perhittungan variable sama dengan saat IP melakukan request

### Taping data request

No.	Time	Source	Destination	Protocol	Length	Info
520	17.200354	10.94.16.173	192.94.214.205	SNMP	85	get-next-request 1.3.6.1.2.1
523	17.459573	192.94.214.205	10.94.16.173	SNMP	105	get-response 1.3.6.1.2.1.1.1.0
524	17.461048	10.94.16.173	192.94.214.205	SNMP	88	get-next-request 1.3.6.1.2.1.1.1.0
525	17.724247	192.94.214.205	10.94.16.173	SNMP	98	get-response 1.3.6.1.2.1.1.2.0
526	17.726044	10.94.16.173	192.94.214.205	SNMP	88	get-next-request 1.3.6.1.2.1.1.2.0
530	17.985023	192.94.214.205	10.94.16.173	SNMP	92	get-response 1.3.6.1.2.1.1.3.0
531	17.986810	10.94.16.173	192.94.214.205	SNMP	88	get-next-request 1.3.6.1.2.1.1.3.0

```

> Frame 520: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
> Ethernet II, Src: AsustekC_1c:70:e7 (88:d7:f6:1c:70:e7), Dst: Routerbo_44:6b:88 (d4:ca:6d:44:6b:88)
> Internet Protocol Version 4, Src: 10.94.16.173, Dst: 192.94.214.205
> User Datagram Protocol, Src Port: 64580, Dst Port: 161
▼ Simple Network Management Protocol
  version: v2c (1)
  community: demopublic
  ▼ data: get-next-request (1)
    ▼ get-next-request
      request-id: 404667
      error-status: noError (0)
      error-index: 0
      ▼ variable-bindings: 1 item
        ▼ 1.3.6.1.2.1: Value (Null)
  
```

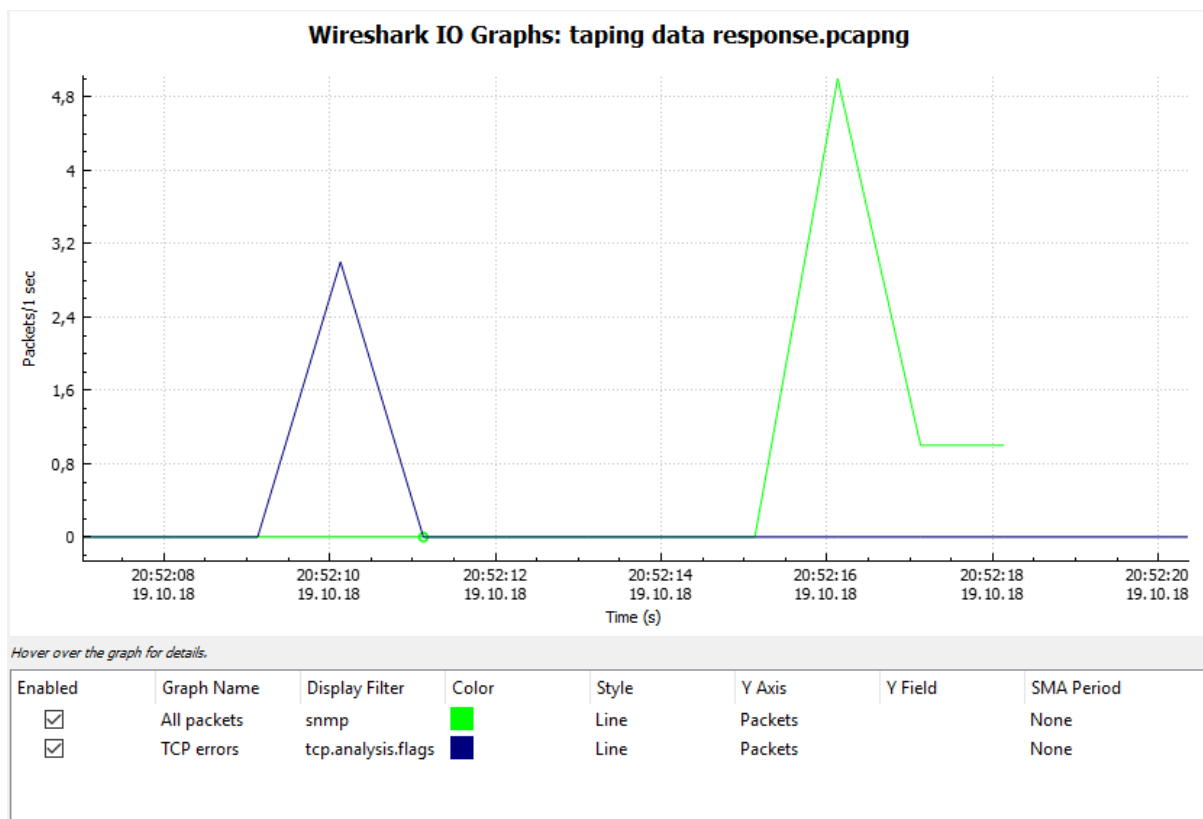
  

```

0000 d4 ca 6d 44 6b 88 88 d7 f6 1c 70 e7 08 00 45 00  ..mDk... ..p...E.
0010 00 47 66 aa 00 00 80 11 21 c5 0a 5e 10 ad c0 5e  .Gf.... !...^..^
0020 d6 cd fc 44 00 a1 00 33 1a a1 30 29 02 01 01 04  ...D...3 ..0)....
0030 0a 64 65 6d 6f 70 75 62 6c 69 63 a1 18 02 03 06  .demopub lic.....
0040 2c bb 02 01 00 02 01 00 30 0b 30 09 06 05 2b 06  ,.....0-0-...+
0050 01 02 01 05 00  ....
  
```

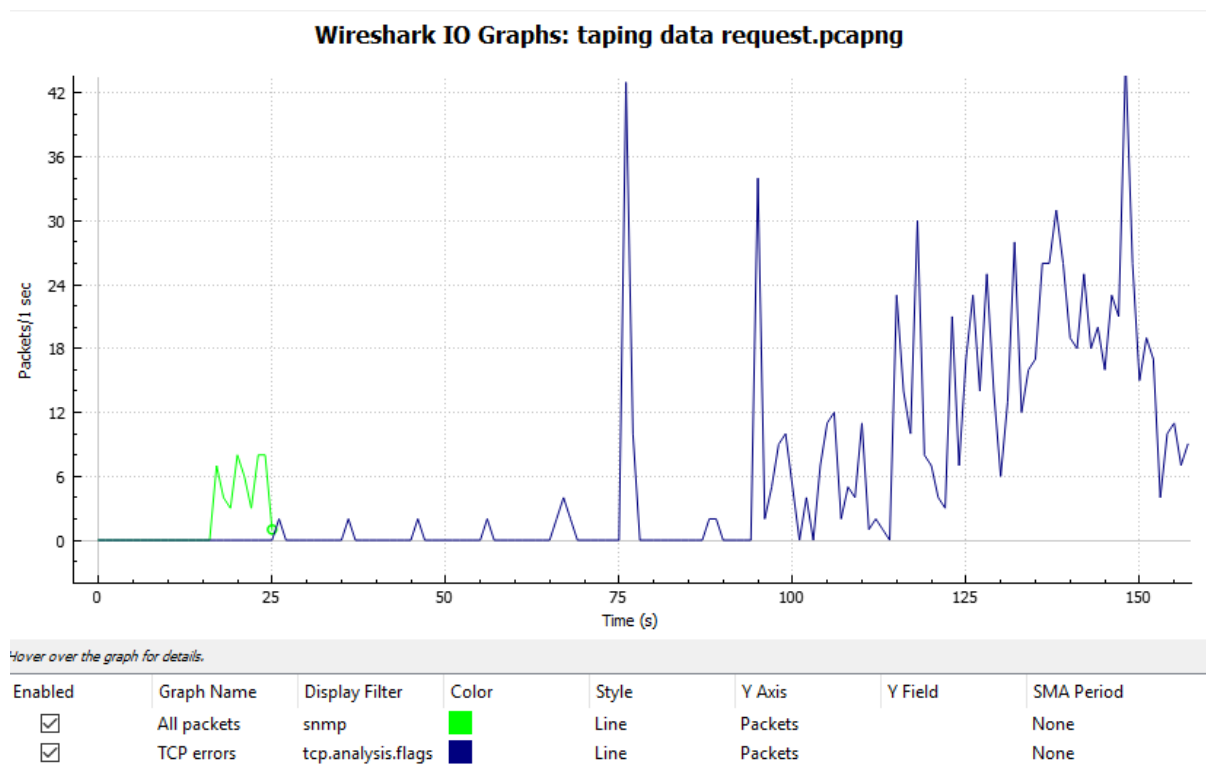
Dari gambar di atas merupakan sebuah capturan dari pcaps menggunakan aplikasi whireshark dimana pada gambar tersebut menjelaskan tentang bagaimana IP melakukan request. Dari capturan diatas IP source 10.94.16.173 dan IP destination 192.94.214.205 dan menggunakan protocol SNMP dengan request-id: 404667 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 , kemudian 1 lagi merupakan protocol SNMP dan 2 merupakan datagram dari SNMP, nah dari variable variable diatas terbentuklah satu kesatuan variable saat IP meminta request.

## Grafik data response



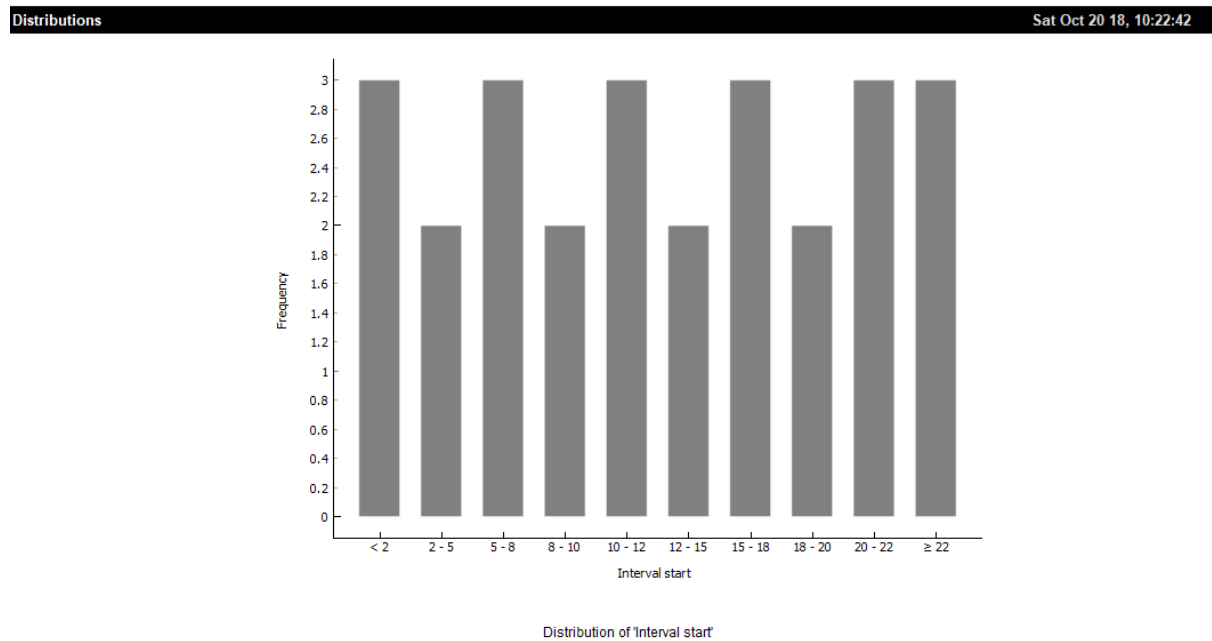
Dari grafik yang dapat di atas menggunakan wifi publik perpustakaan unsri disini dapat dilihat ada dua grafik yaitu (Grafik All packets) dan (Grafik TCP errors), dan All packets tersebut adalah data seluruh penggunaan menggunakan snmp pada wireshark dan dapat dilihat pada gambar di atas penggunaan data snmp banyaknya request dari pengguna jaringan dan banyak nya paket yang masuk sebanyak 48 pakets karena saat saya mencapture agak begitu lama . dan garis utuk warna biru melambangkan paket seluruh yang melintas yang ada pada wifi perpustakaan unsri tersebut.

## Grafik data request



Dari grafik yang dapat di atas menggunakan wifi publik perpustakaan unsri disini dapat dilihat ada dua grafik yaitu (Grafik All packets) dan (Grafik TCP errors), dan All packets tersebut adalah data seluruh penggunaan menggunakan snmp pada wireshark dan dapat dilihat pada gambar di atas penggunaan data snmp sedikitnya request dari pengguna jaringan dan garis utuk warna biru melambangkan paket seluruh yang melintas atau banyak nya request dari pengguna yang ada pada wifi perpustakaan unsri tersebut.

## Grafik distribution



Dapat di lihat pada grafik diatas menampilkan hasil dari PCAP pada wireshark yang telah di masukkan datanya di orange gambar diatas merupakan tingkat data protocol SNMP yang telah di dapat dari wifi perpustakaan Universitas Sriwijaya. dan hasil pengamatan yang telah dilakukan bahwa dalam protocol SNMP terjadi interaksi antara manager dan agent dengan saling berkirim pesan berupa permintaan manager yang meminta request kepada agent setelah agent menerima permintaan dari manager maka agent akan meresponse permintaan tersebut.

## Daftar pustaka

- [1] Asep, 2010 “<http://jaringankomputer.wordpress.com/2009/07/09/tentang-wireshark-dan-pemakaiannya>”
- [2] indyawan, farras ” wireshark adalah” <https://medium.com/@kitaadmin/wireshark-adalah-pengertian-dan-fungsi-256dc09c8292>
- [3] J. Schippers and A. Pras, “SNMP Traffic Analysis : Approaches , Tools, and FirstResult,”pp.323-332,2007.