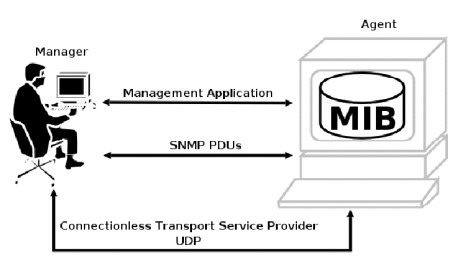
**Classification of SNMP in Traffic Data Using Wireshark and Visualisation with ORANGE**

**Meidi Dwi Hafiz - 09011281520097 | Manajemen Jaringan |Dosen Pengajar : Deris Stiawan**

SNMP merupakan protokol untuk menajemen peralatan yang terhubung dalam jaringan IP (Internet Protocol).  Peralatan-peralatan itu antara lain switch, router, modem, komputer, server dan lain-lain. SNMP menggunakan data-data yang didapatkan dari komunikasi UDP dengan device/peralatan yang masuk dalam jaringan tersebut. SNMP dapat meminta data ataupun melakukan setting kepada peralatan yang bersangkutan.



Gambar 1. Struktur SNMP

* **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,

2. Kemudian Connect ke salah satu Wi-Fi publik dalam hal ini penulis menggunakan jaringan Wi-Fi Fasilkom Unsri Indralaya,

3. Capturing data pada jaringan Wi-Fi tersebut menggunakan software wireshark,

4. Kemudian 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*

5. Jika *snmpbulkwalk* command tidak muncul atau valid, maka install terlebih dahulu snmp pada terminal,

6. Kemudian, stop capturing dan simpan data.

Berikut hasil:

  
Gambar 2. Hasil tapping data snmp pada wireshark

Pada gambar diatas terdapat info Getbulk req dan Res :

**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*.

Dan pada gambar tersebut terjadi three way handshake :



Gambar 3. Three Way Handshake

* **Visualisasi menggunakan Orange**



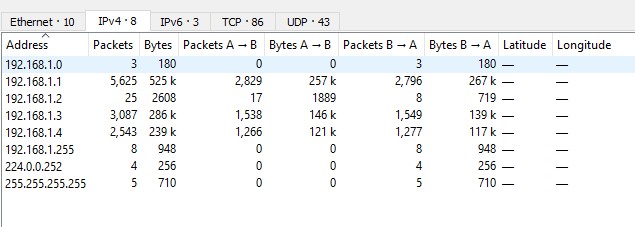
Gambar 4. Visual Scatter Plot



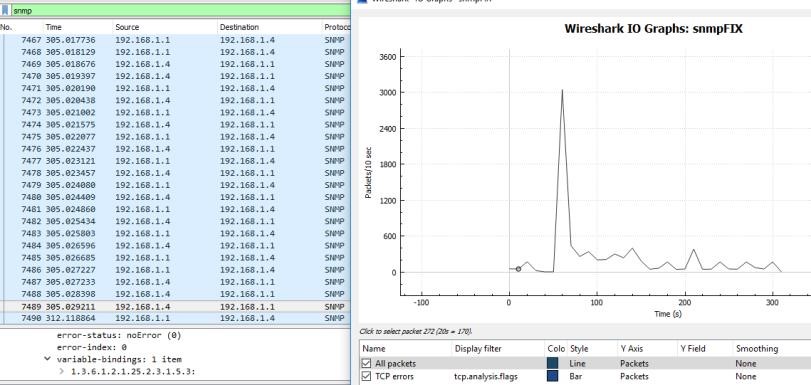
Gambar 5. Distribusi Visual

Kesimpulan :

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.



Gambar 7. Endpoint packet



Gambar 8. Trafic dari server ke raspberry dan sebaliknya

Kesimpulannya adalah dengan monitoring dengan menggunakan The Dude pada SNMP agent dapat mengetahui beban trafik yang terjadi pada setiap device, kemuadian trafik tertinggi terjadi pada 12.40-13.00 dengan packet yang dikirimkan server mencapai 525 kb. Dengan demikian SNMP sangat mempermudah dalam memonitoring semua perangkat hanya dengan satu komputer administrator.

DAFTAR PUSTAKA

1. Sidnie Feit, “*A Guide to Network Management SNMP*” McGraw-Hill, USA, 1995
2. Muhammad Zen Samsono Hadi, ST. Msc. “SNMP (Simple Network Management Protocol)