**SNMP (Simple Network Management Protocol)**

SNMP adalah kependekan dari Simple Network Management Protocol. Dari kepanjangan tersebut kita dapat menebak bahwa SNMP digunakan untuk manajemen network.

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

**Arsitektur SNMP**
Framework dari SNMP terdiri dari :

**Master Agent**
Master agent merupakan perangkat lunak yang berjalan pada perangkat yang mendukung SNMP, dimana bertujuan untuk merespon permintaan dari SNMP dari management station. Master agent kemudian meneruskan kepada subagent untuk memberikan informasi tentang manajemen dengan fungsi tertentu.

**Subagent**
ubagent merupakan perangkat lunak yang berjalan pada perangkat yang mendukung SNMP dan mengimplementasikan MIB. Subagent memiliki kemampuan :

* Mengumpulkan informasi dari objek yang dimanaj
* Mengkonfigurasi informasi dari objek yang dimanaj
* Merespon terhadap permintaan manajer
* Membangkitkan alarm atau trap

**Management Station**
Management station merupakan client dan melakukan permintaan dan mendapakan trap dari SNMP server.

3. **Protokol SNMP**
PDU dari SNMP (versi 1) antara lain :

1. GET REQUEST – digunakan untuk mendapatkan informasi manajemen
2. GETNEXT REQUEST – digunakan secara iteratif untuk mendapatkan sekuen dari informasi manajemen
3. GET RESPONSE
4. SET – digunakan untuk melakukan perubahan terhadap subsistem
5. TRAP – digunakan untuk melakukan pelaporan terhadap subsistem manajemen

Untuk versi berikutnya ditambahkan PDU :

1. GETBULK REQUEST – iterasi yang lebih cepat untuk mendapatkan informasi
2. INFORM – acknowledge terhadap TRAP

SNMP menggunakan UDP pada port 161 untuk agent dan 162 untuk manager. Manager mengirimkan permintaan terhadap agent pada port 161 dan diterima pada manager pada port 162.

Berikut merupakan hasil Capture data yg di dapat dari WireShark ketika terkoneksi dengan jaringan public di Fasilkom Unsri



Dari gambar di atas dapat dilihat bahwa data yg di tampilkan merupakan data “Request” & “Response” dari IP source & IP destination

Setelah data di atas di dapat kan, kemudian data itu di ekport dalam format “.pcap” kemudian file tersebut di load pada aplikasi “Rumint” dan menampil kan hasil sebagai berikut



Dari Visualisasi di atas hanya beberapa point yg dapat saya analisis di antara nya adalah “Detail View” pada bagian ini berisikan data atau isi dari pada paket SNMP dan berisi nilai hexa dari data tersebut yg di kirim atau pun yg di terima, pada bagian “Text Rainfall” berisikan data yg berkeliaran & berhasil di tangkap dan di tampilkan dalam bentuk text namun bukan pada bentuk plaintext