NETWORK MANAGEMENT

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

Oleh :

Anggy Tias Kurniawan

09011181520024

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.

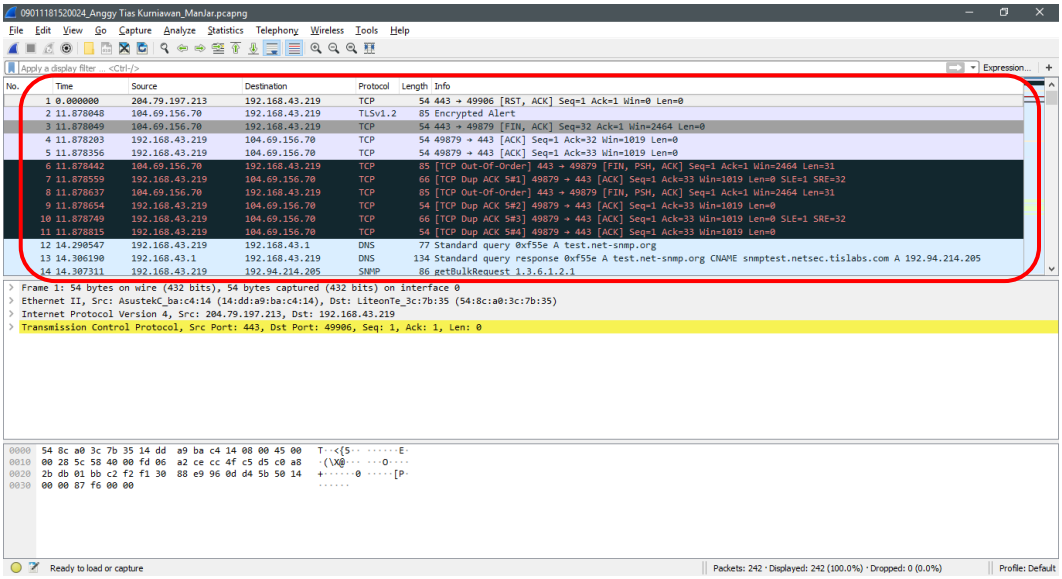
Sebelum melanjutkan ada baiknya kita mengetahui apa itu Manager, MIB, dan Agent, berikut penjelasannya :

- 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.

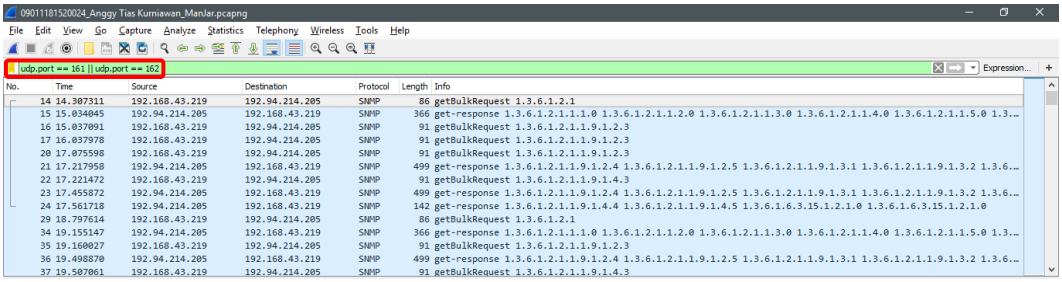
- Agent, yaitu suatu elemen jaringan yang dimonitoring atau dikontrol oleh manager. Pada umumnya perangkat jaringan seperti router dan server difungsikan sebagai agen dalam sistem manajemen jaringan. Hal ini disebabkan lalu lintas trafik data dengan jumlah yang besar melalui atau bermuara pada kedua 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

Pada gambar 1.1 , Dapat kita lihat kumpulan dari tampilan data-data yang telah di capture sebelumnya menggunakan wireshark. Terdapat begitu banyak data yang di capture. Untuk mempermudah kita dalam mencari paket data SNMP, kita dapat menggunakan filter yang akan menyaring data yang ditampilkan sesuai dengan filter yang kita kehendaki. Dengan mengetikkan "*udp.port == 161 || udp.port == 162*" pada kolom filter, maka data-data yang ditampilkan hanya merupakan protocol SNMP saja seperti yang dapat kita lihat pada gambar 1.2.

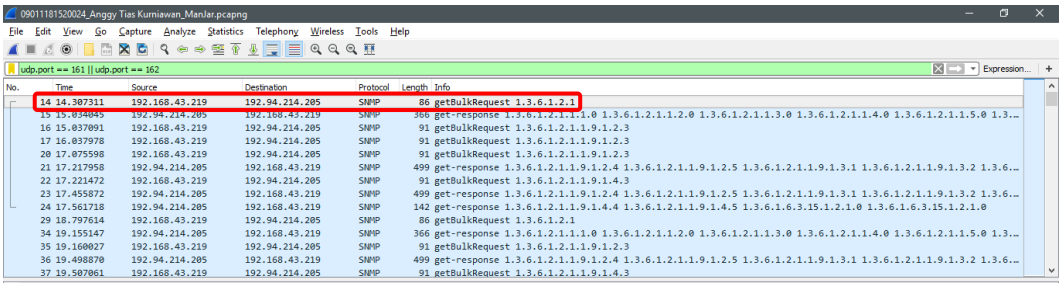


Gambar 1.1 Hasil Pcaps Wireshark



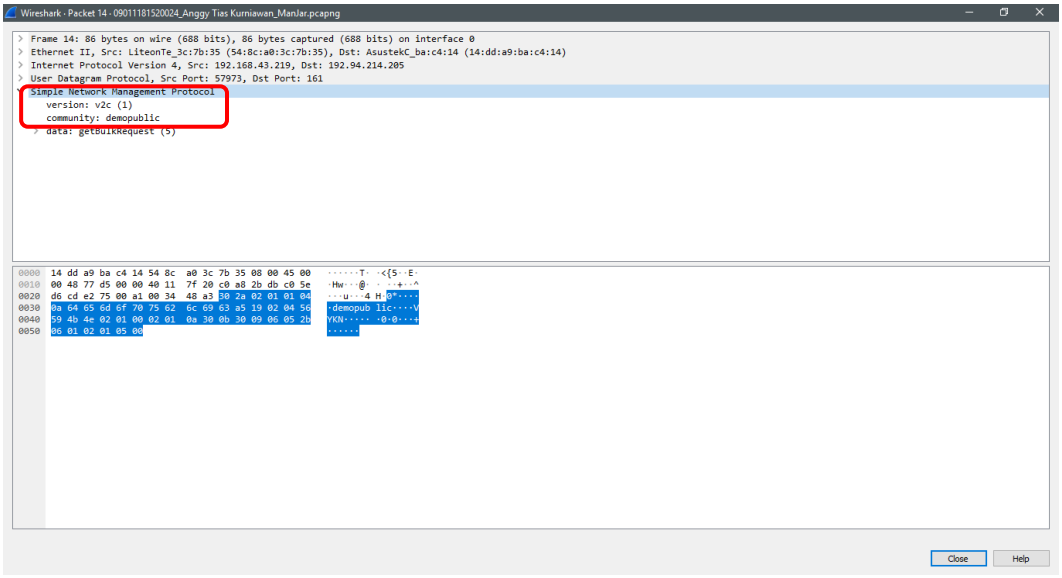
Gambar 1.2 Hasil Pcaps setelah di filter

Pada gambar 1.3 dapat kita lihat bahwa sebuah komputer source dengan IP address 192.168.43.219 memiliki destination ke IP address 192.94.214.205 dan memiliki info "*getBulkRequest*". getBulkRequest merupakan operasi yang biasanya digunakan untuk mengambil sejumlah data yang besar, terutama data dari tabel-tabel yang besar. Sebuah Request dari getBulk dibuat dengan memberikan list OID bersamaan dengan Max-Repetitions value dan Nonrepeaters value nya.



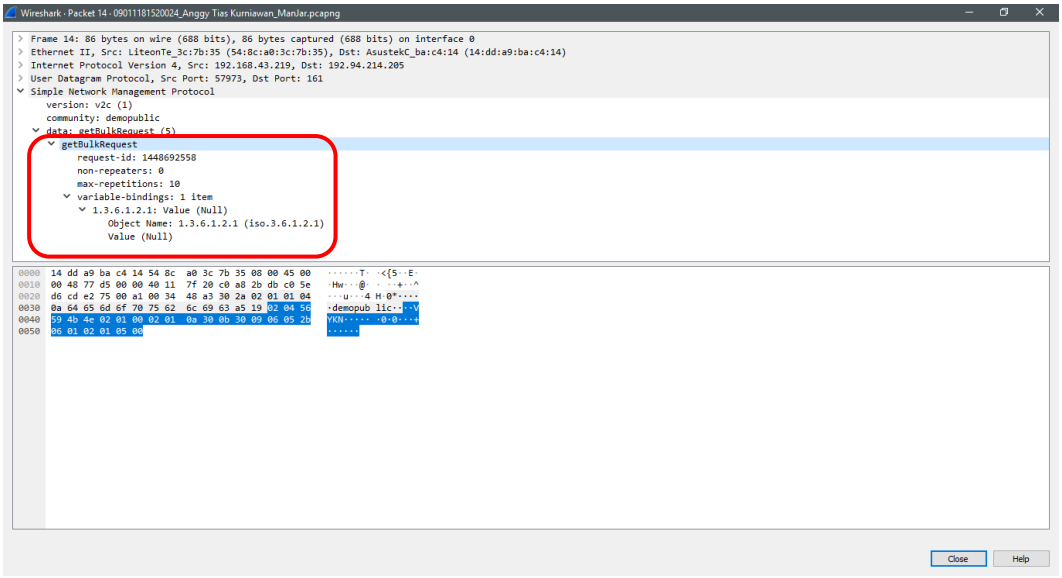
Gambar 1.3 IP Request

Gambar 1.4 merupakan informasi-informasi yang terkandung didalam data yang terkait pada gambar 1.3. Pada gambar 1.4 dapat kita lihat informasi dari Version yang digunakan yaitu versi v2c dan Community yang digunakan yaitu demopublic.



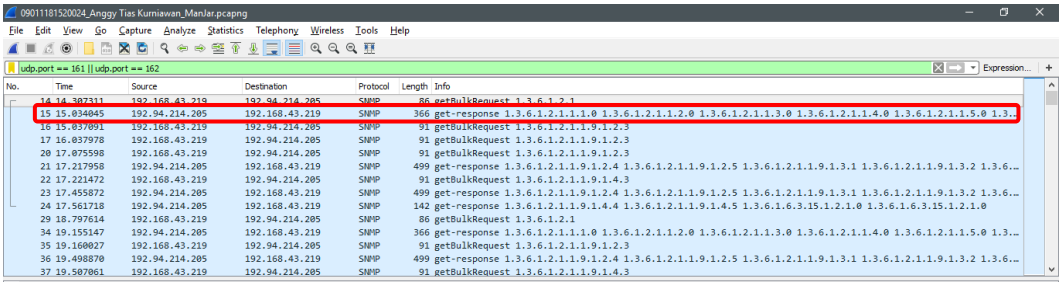
Gambar 1.4 Informasi packet IP Request

Sedangkan pada gambar 1.5 dapat kita lihat informasi seperti "*data : getBulkRequest*" yang merupakan operasi yang biasanya digunakan untuk mengambil sejumlah data yang besar, Terdapat juga "*request-id, non-repeaters*, dan *max-repetition* nya". Pada bagian "*variable –bindings : 1 item*" dapat kita lihat OID nya. OID adalah Objek ID dari sistem yang ingin kita tampilkan dan sudah ditentukan oleh MIB. Dari capturan pada gambar 1.5 dibawah, IP source 192.168.43.219 dan IP destination 192.94.214.205 dan menggunakan protocol SNMP dengan request-id: 1448692558 pada variable binding terdapat 1 items dengan 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 .



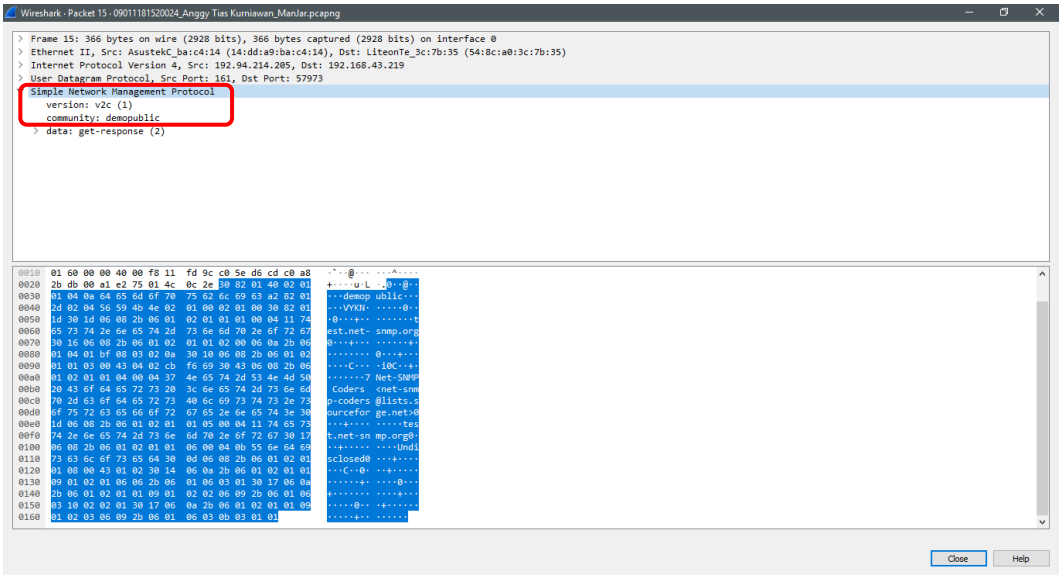
Gambar 1.5 Informasi packet IP Request

Selanjutnya kita beralih ke IP Response. Pada gambar 1.5 dapat kita lihat bahwa sebuah komputer source dengan IP address 192.94.214.205 memiliki destination ke IP address.168.43.219 dan memiliki info "*get-response*". Jika kita perhatikan, IP source dan IP destination pada gambar 1.6 ini merupakan kebalikan dari gambar 1.3. Pada gambar 1.6 menunjukkan respon dari request sebelumnya.



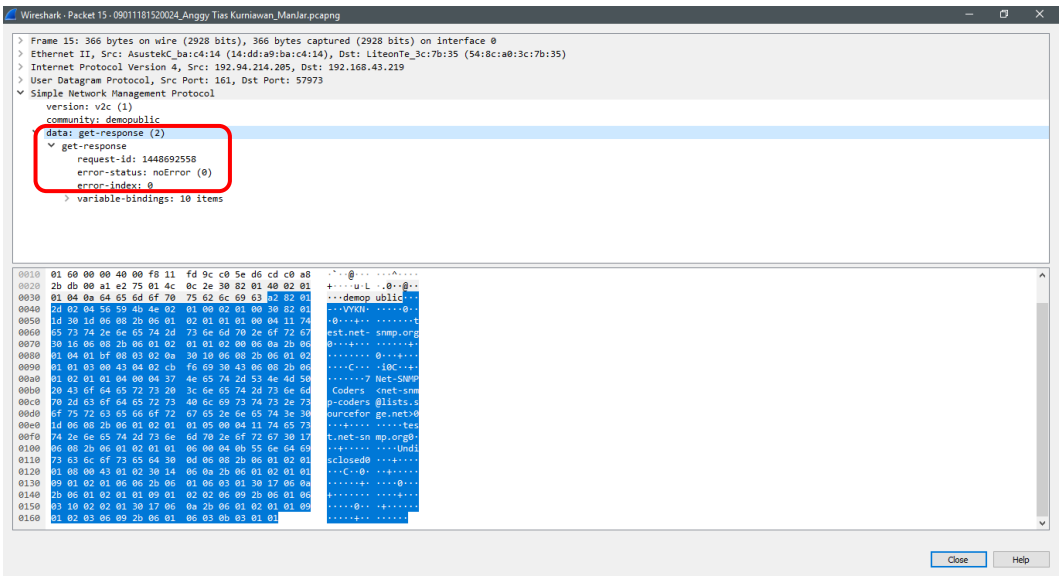
Gambar 1.6 IP Response

Seperti yang telah kita lihat sebelumnya Pada gambar 1.4, pada gambar 1.7 dapat kita lihat informasi dari Version yang digunakan yaitu versi v2c dan Community yang digunakan yaitu demopublic.

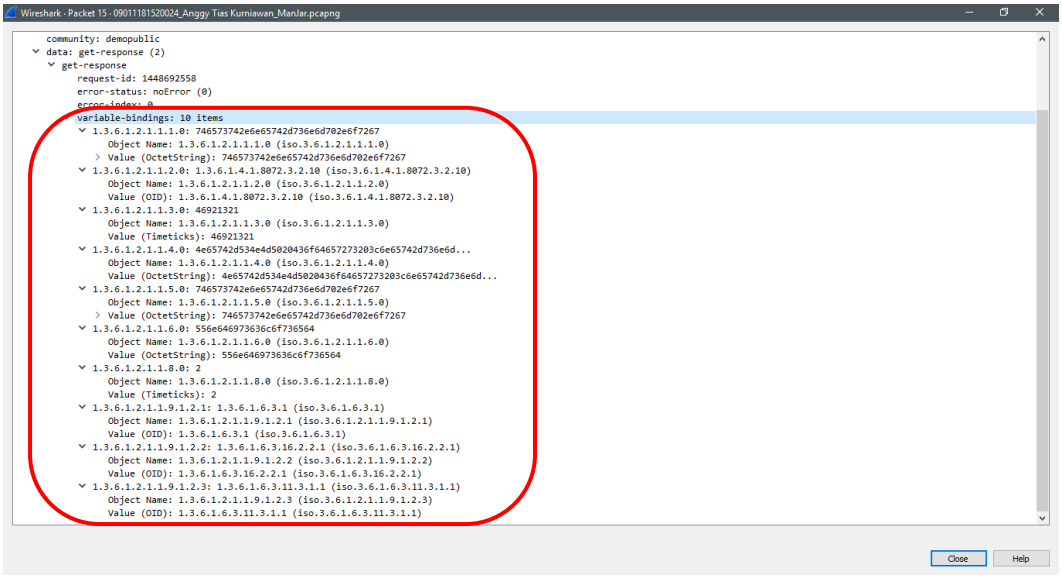


Gambar 1.7 Informasi packet IP Response

Pada gambar 1.8 terdapat informasi pada "*get-response"* yang mengandung "*request-id*" yang memiliki kesamaan ID dengan ID pada IP Request sebelumnya, "*error-status*" dan "*error-index*".

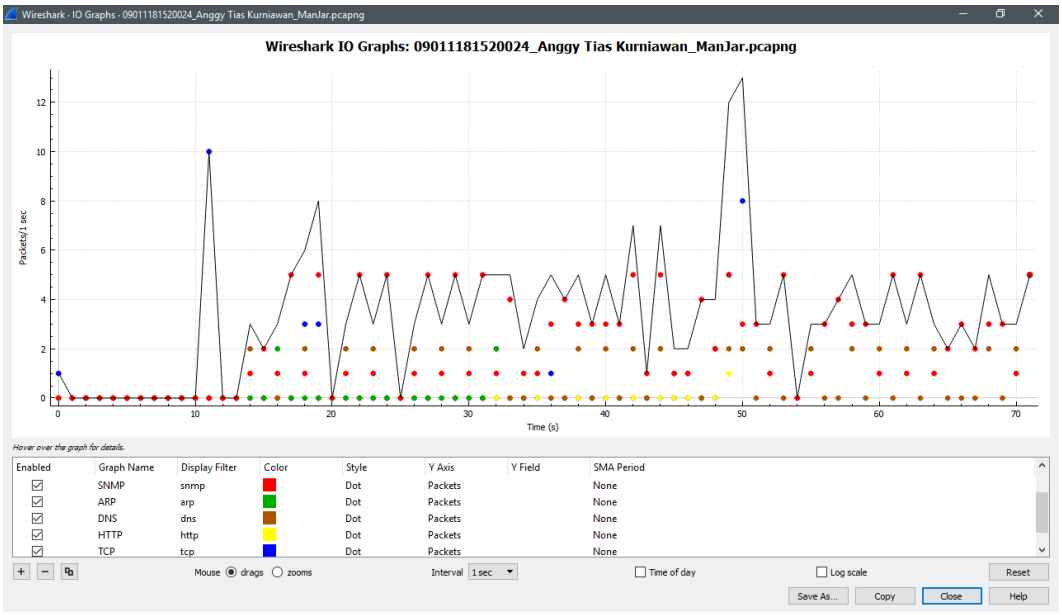


Gambar 1.8 Informasi packet IP Response



Gambar 1.9 Informasi packet IP Response

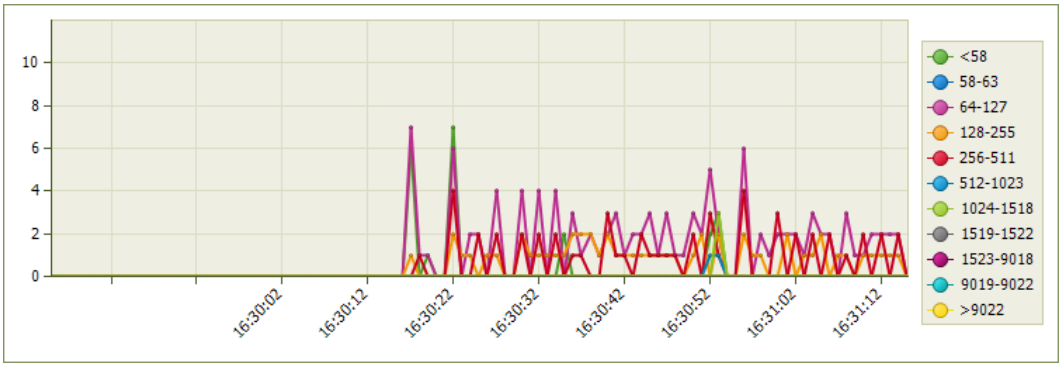
Pada gambar 1.10 dapat kita lihat sekumpulan traffic berbagai protocol dari data yang telah kita capture menggunakan wireshark mulai dari protocol SNMP yang ditandai dengan warna merah, ARP dengan warna hijau, DNS dengan warna coklat, HTTP dengan warna kuning, TCP dengan warna biru dan line hitam menunjukkan traffic dari seluruh paket data yang di capture.



Gambar 1.10 Traffic data menggunakan Wireshark

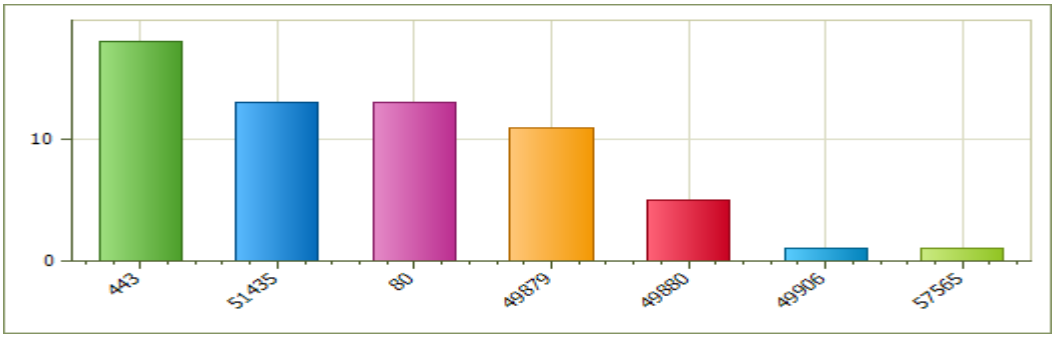
3. Visualisasi Traffic Menggunakan Colasoft

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.

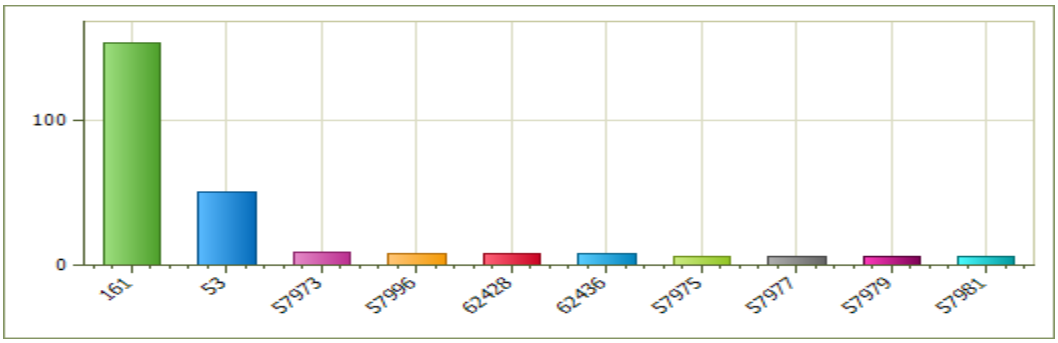


Gambar 2.1 Traffic data menggunakan Colasoft

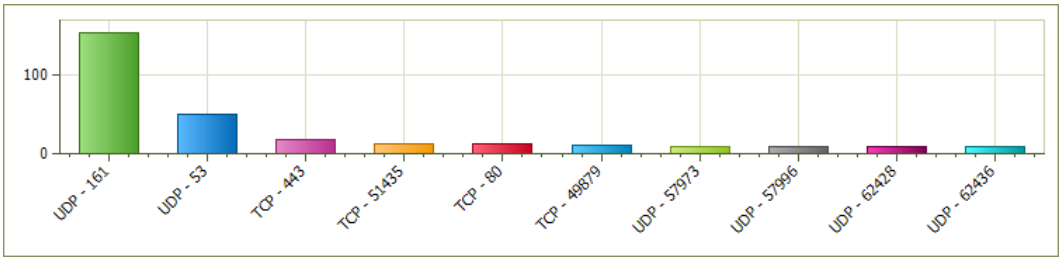
Pada gambar 2.2, 2.3 dan 2.4 menunjukkan penggunaan dari Port TCP, UDP dan keseluruhan Port terbanyak berdasarkan traffic nya.



Gambar 2.2 Top TCP port by total traffic



Gambar 2.3 Top UDP port by total traffic



Gambar 2.4 Top port by total traffic

Pada gambar 2.5 dapat kita lihat jumlah packet dan bytes untuk setiap protocol.

Name	Bytes	Packets	bps	pps	Bytes%	Packets%
Ethernet II	45.70 KB	242	1.136 Kbps	1	100.000%	100.000%
IP	45.53 KB	238	1.136 Kbps	1	99.641%	98.347%
UDP	38.40 KB	207	1.136 Kbps	1	84.034%	85.537%
SNMP	32.01 KB	153	1.136 Kbps	1	70.041%	63.223%
DNS	5.55 KB	50	1.688 Kbps	2	12.147%	20.661%
DNS Response	3.67 KB	25	1.072 Kbps	1	8.037%	10.331%
DNS Query	1.88 KB	25	616.000 bps	1	4.110%	10.331%
SSDP	864.00 B	4	1.728 Kbps	1	1.846%	1.653%
TCP	7.13 KB	31	43.880 Kbps	8	15.607%	12.810%
HTTP	5.55 KB	6	42.584 Kbps	5	12.136%	2.479%
SSL	442.00 B	4	1.496 Kbps	1	0.945%	1.653%
HTTPS	442.00 B	4	1.496 Kbps	1	0.945%	1.653%
ARP	168.00 B	4	672.000 bps	2	0.359%	1.653%
Request	84.00 B	2	336.000 bps	1	0.180%	0.826%
Response	84.00 B	2	336.000 bps	1	0.180%	0.826%

Gambar 2.5 Tabel Usage setiap protocol