

ANALISA SNMP

Nama : Nanda Hasyim Marfianshar

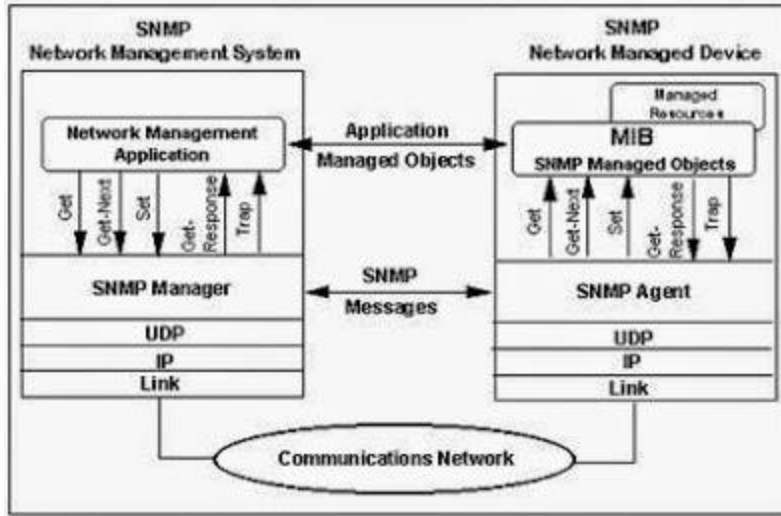
NIM : 09011281520096

Kelas : SK7C

Definisi SNMP

SNMP merupakan sebuah protocol jaringan yang didesain bagi pengguna khususnya administrator jaringan untuk memonitor aktifitas jaringan computer dan mengontrol sebuah computer atau server secara sistematis dari jarak jauh. SNMP bekerja mengumpulkan data informasi dari elemen-elemen jaringan dengan parameter dan variable tertentu dan menyimpannya dalam sebuah database. SNMP terdiri atas tiga elemen sebagai berikut:

- **Manager**, yaitu bertugas sebagai manajemen jaringan yang mengumpulkan data informasi dari elemen-elemen jaringan yang ingin dimonitoring dan atau dikontrol. Bentuk dari manager ini berupa perangkat lunak yang didesain sedemikian rupa sekaligus memiliki fungsi antarmuka yang baik bagi penggunaanya 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.
- **Agent**, yaitu suatu elemen jaringan yang dimonitoring atau dikontrol oleh manager. Pada umumnya perangkat jaringan seperti router dan server difungsikan sebagai agen dalam system manajemen.



Gambar 1. Skema Komunikasi pada SNMP

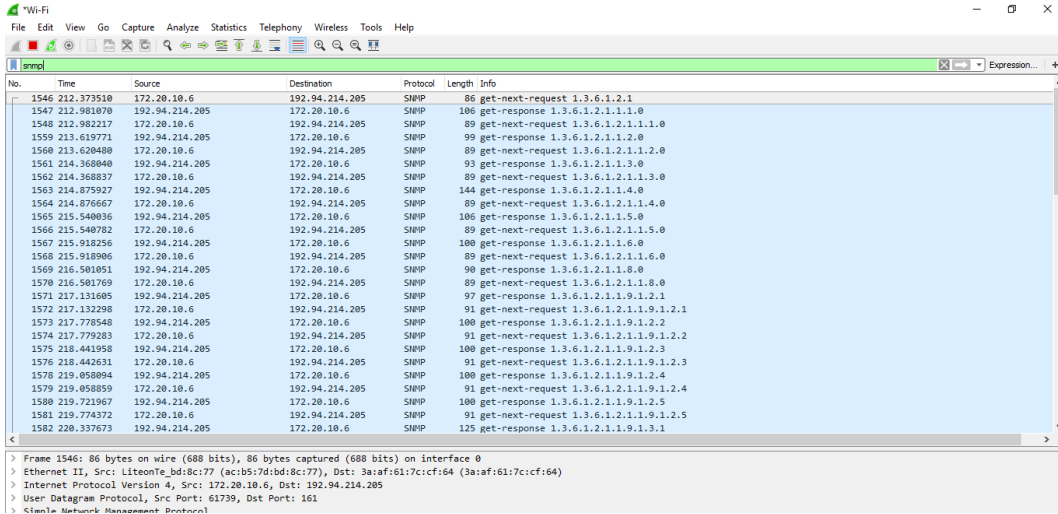
(sumber : blogs.itb.ac.id).

- Capture dengan I/O Grafik Wireshark dan Visualisasi Rapidminer

- Capture semua protocol dengan menggunakan wireshark

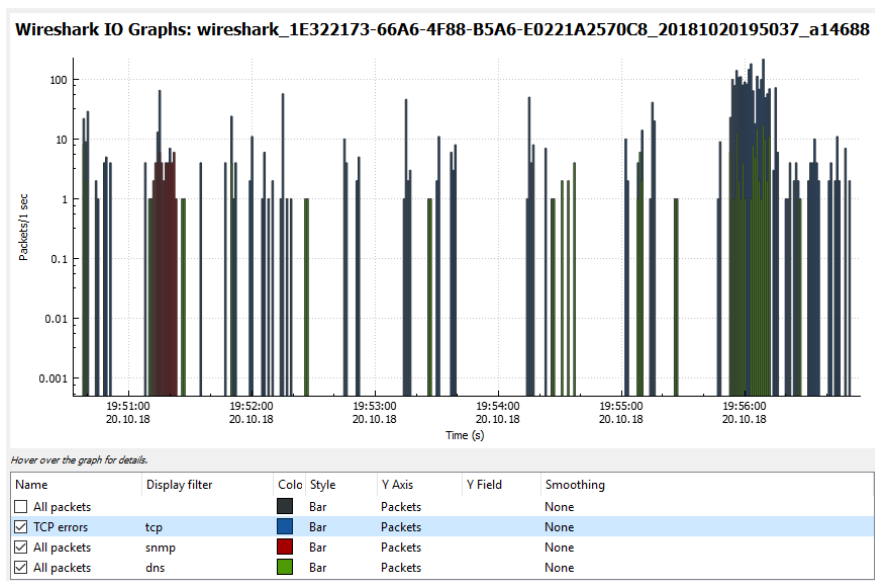
No.	Time	Source	Destination	Protocol	Length	Info
1520	205.100543	172.20.10.6	52.109.124.22	TCP	54	51197 → 443 [ACK] Seq=191 Ack=5601 Win=65792 Len=0
1521	205.113609	52.109.124.22	172.20.10.6	TLSv1.2	125	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
1522	205.119398	172.20.10.6	52.109.124.22	TLSv1.2	268	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1523	205.175619	52.109.124.22	172.20.10.6	TCP	54	443 → 51197 [ACK] Seq=5672 Ack=405 Win=4604 Len=0
1524	205.192844	52.109.124.22	172.20.10.6	TLSv1.2	161	Change Cipher Spec, Encrypted Handshake Message
1525	205.192875	172.20.10.6	52.109.124.22	TLSv1.2	459	Application Data
1526	205.193117	172.20.10.6	52.109.124.22	TCP	1454	51197 → 443 [ACK] Seq=810 Ack=5779 Win=65536 Len=1400 [TCP segment of a reassembled PDU]
1527	205.193125	172.20.10.6	52.109.124.22	TCP	1454	51197 → 443 [ACK] Seq=2210 Ack=5779 Win=65536 Len=1400 [TCP segment of a reassembled PDU]
1528	205.193132	172.20.10.6	52.109.124.22	TLSv1.2	459	Application Data
1529	205.242303	52.109.124.22	172.20.10.6	TCP	54	443 → 51197 [ACK] Seq=5779 Ack=810 Win=5008 Len=0
1530	205.251823	52.109.124.22	172.20.10.6	TCP	54	443 → 51197 [ACK] Seq=5779 Ack=2210 Win=6408 Len=0
1531	205.253025	52.109.124.22	172.20.10.6	TCP	54	443 → 51197 [ACK] Seq=5779 Ack=3610 Win=7808 Len=0
1532	205.253256	52.109.124.22	172.20.10.6	TCP	54	443 → 51197 [ACK] Seq=5779 Ack=4015 Win=8212 Len=0
1533	207.043865	172.20.10.6	104.199.241.234	SSL	65	Continuation Data
1534	207.250759	52.109.124.22	172.20.10.6	TLSv1.2	779	Application Data
1535	207.250760	104.199.241.234	172.20.10.6	TCP	54	443 → 49439 [ACK] Seq=966 Ack=3525 Win=30052 Len=0
1536	207.254303	104.199.241.234	172.20.10.6	SSL	65	Continuation Data
1537	207.254374	172.20.10.6	104.199.241.234	TCP	60	[TCP Retransmission] 51197 → 1688 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1538	207.294179	172.20.10.6	104.199.241.234	TCP	54	49439 → 443 [ACK] Seq=3525 Ack=977 Win=252 Len=0
1539	207.294278	172.20.10.6	52.109.124.22	TCP	54	51197 → 443 [ACK] Seq=4015 Ack=6504 Win=64768 Len=0
1540	209.184024	172.20.10.6	104.199.241.234	TCP	54	49439 → 443 [FIN, ACK] Seq=3525 Ack=977 Win=252 Len=0
1541	209.372387	104.199.241.234	172.20.10.6	TCP	54	443 → 49439 [ACK] Seq=977 Ack=3526 Win=30052 Len=0
1542	209.414439	104.199.241.234	172.20.10.6	TCP	54	443 → 49439 [FIN, ACK] Seq=977 Ack=3526 Win=30052 Len=0
1543	209.414478	172.20.10.6	104.199.241.234	TCP	54	49439 → 443 [ACK] Seq=3526 Ack=978 Win=252 Len=0
1544	209.804482	172.20.10.6	172.20.10.1	DNS	77	Standard query 0xe1a9 A test.net-snmpp.org
1545	212.262510	172.20.10.1	172.20.10.6	DNS	134	Standard query response 0xe1a9 A test.net-snmpp.org CNAME snmptest.netsec.tislabs.com A 192.94.214.205

- Capture protokol SNMP menggunakan wireshark

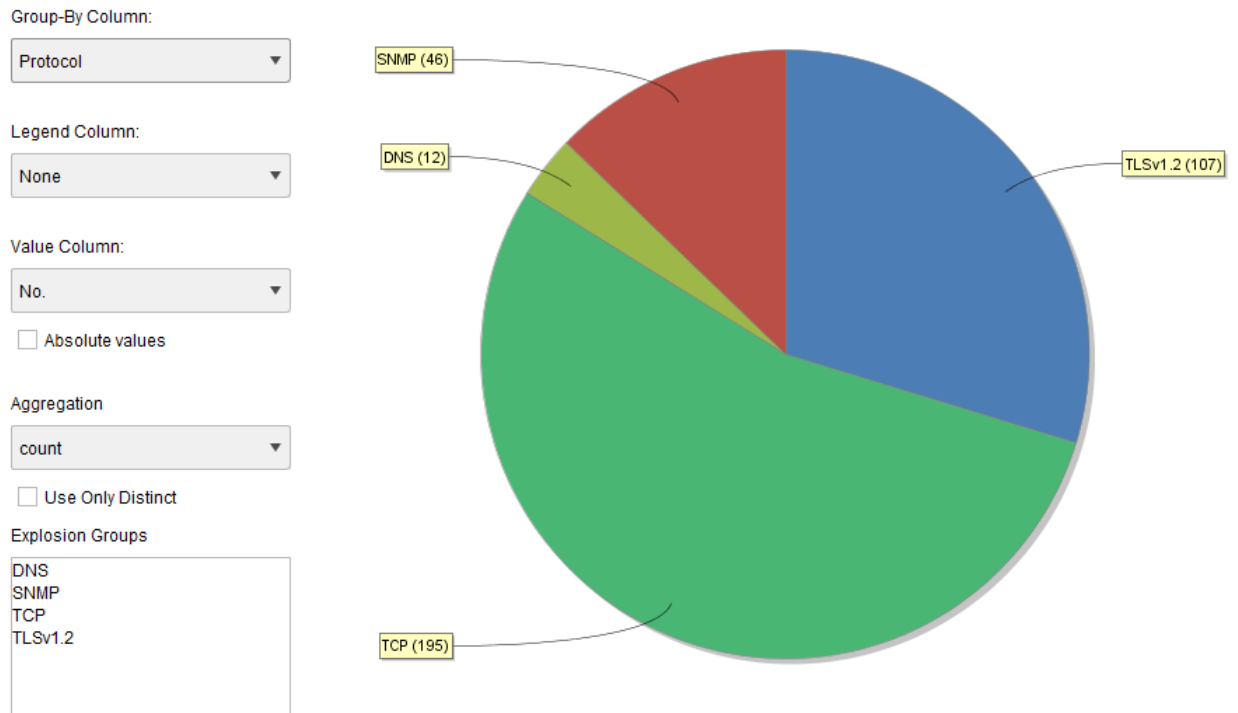


Setelah meng-capture semua protokol dan protocol SNMP kemudian file diexport menjadi file csv. Dan untuk melihat grafik I/O bisa dilihat di menu di bagian statistic. Untuk hasil dari capture wireshark di grafik I/O bisa dilihat pada gambar dibawah.

- Grafik I/O Wireshark



- Visualisasi Rapidminer



File yang telah dicapture kemudian di export menjadi file csv selanjutnya di import ke aplikasi Rapidminer. Dan hasil dari visualisasi terlihat pada gambar diatas.