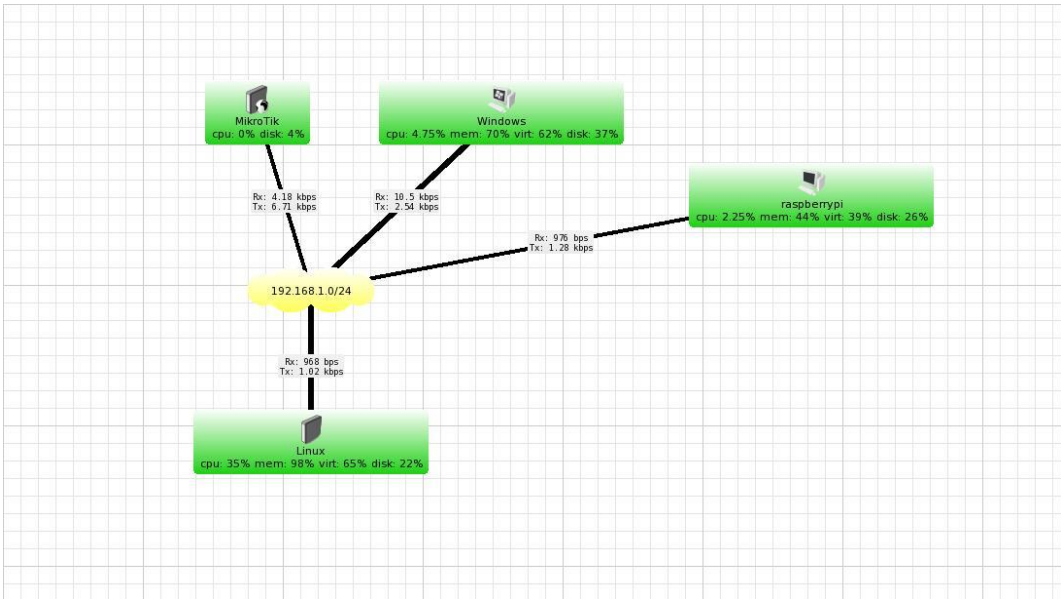
Nama : Maya Sari

Nim : 09011181320042

Mata Kuliah : Manajemen Jaringan

Analisa Pcap dari Monitoring Jaringan Dengan Menggunakan Aplikasi Open Source The Dude

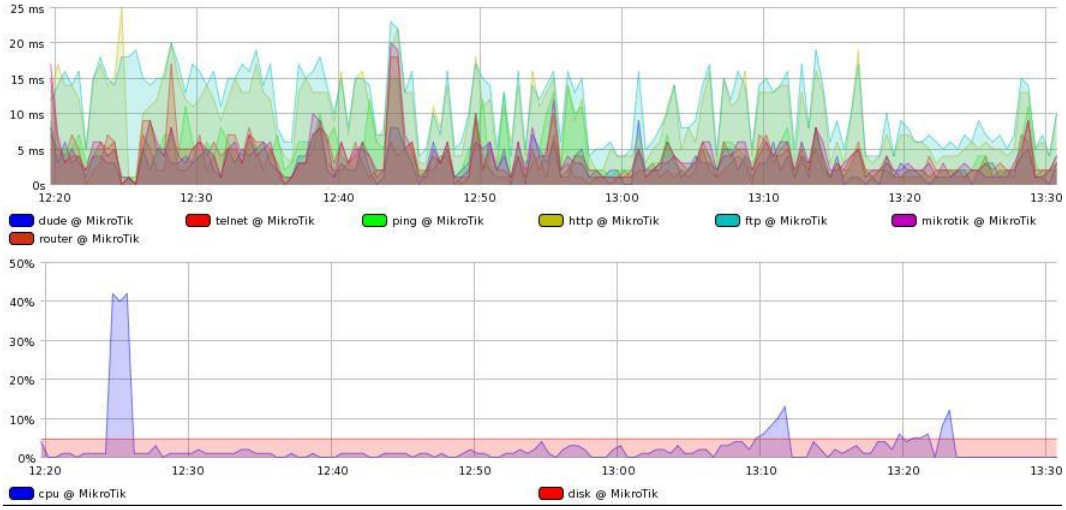


Dari gambar diatas merupakan topologi yang digunakan untuk monitoring jaringan dengan menggunakan aplikasi open source the dude, mikrotik menggunakan ip 192.168.1.1 , windows menggunakan ip 192.168.1.2, linux menggunakan ip 192.168.1.3, dan raspberry pi menggunakan ip 192.168.1.4.

Sebelum menganalisis pcap maka akan dijelaskan bahwa monitoring jaringan adalah salah satu dari fungsi manajemen yang berguna untuk menganalisa apakah dari suatu jaringan masih cukup layak untuk digunakan atau perlu tambahan kapasitas. Hasil monitoring juga dapat membantu jika admin perlu mendesin ulang jaringan yang telah ada. Banyak aplikasi untuk memonitoring jaringan baik open source maupun juga yang tidak. Namun pada

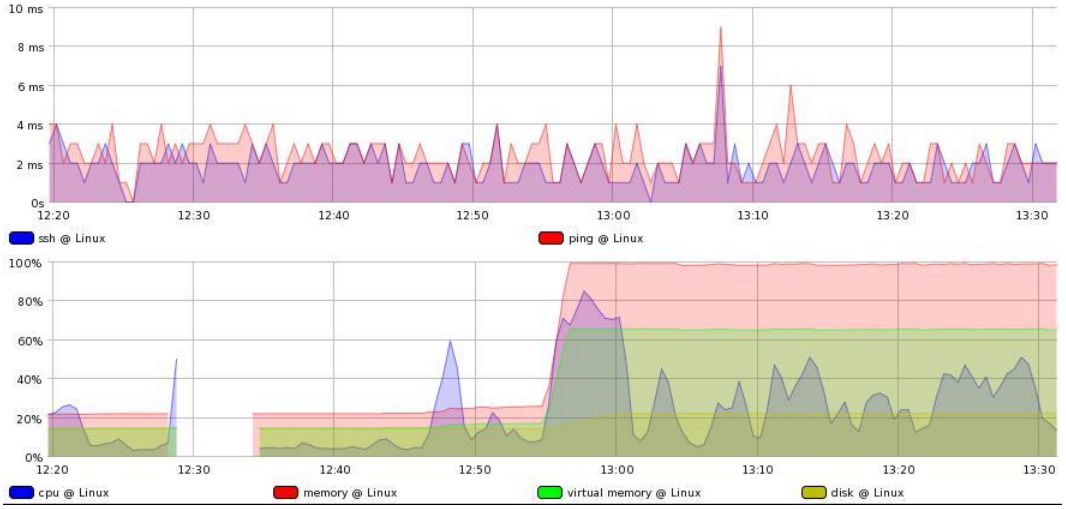
analisis yang digunakan saat ini menggunakan aplikasi open source The Dude sebagai aplikasi monitoring yang digunakan. Dengan menggunakan SNMP (Simple Network Management Protocol) yang merupakan protokol yang dapat digunakan untuk melakukan manajemen jaringan. Melalui protokol ini, kita akan mendapat informasi tentang status dari suatu jaringan. Hal ini juga menampilkan traffic jaringan agar mengetahui beban jaringan pada tiap link tersebut.

Traffic dari mikrotik



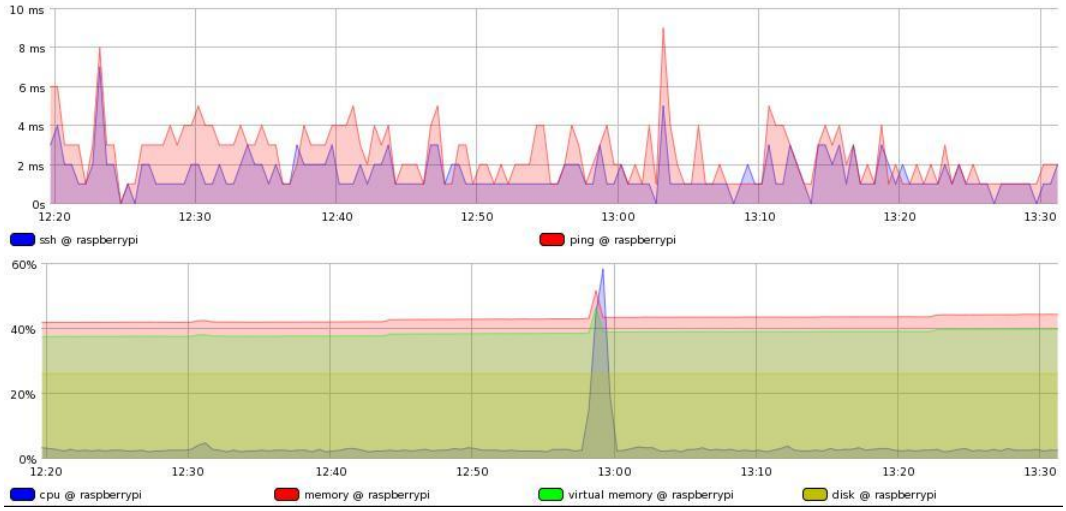
Dari gambar traffic tersebut cpu : 0% , disk : 4%

Traffic dari linux



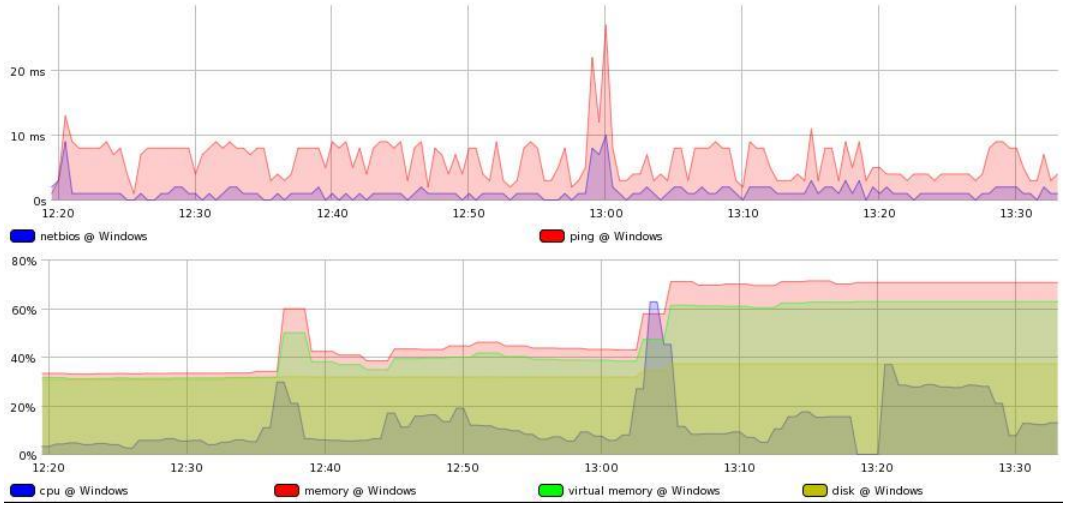
Dari gambar traffic tersebut cpu : 35% , virt : 65% , disk : 22%

Traffic dari raspberry pi



Dari gambar traffic tersebut cpu : 2.25% ,mem 44% , disk : 26%

Traffic dari windows



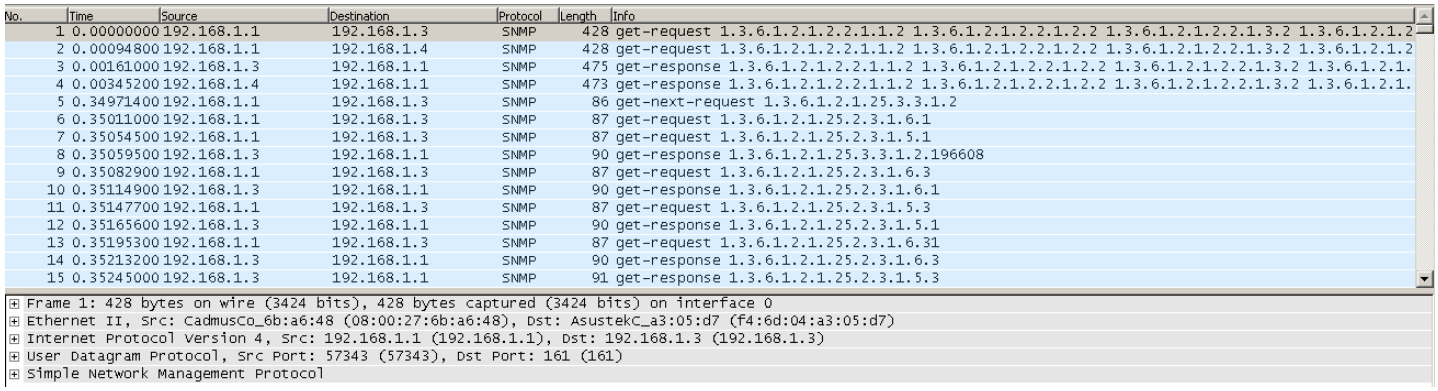
Dari gambar traffic tersebut cpu : 4.75% ,mem 70% virt : 62% , disk : 37%

Traffic diatas adalah Multi Router Traphic Grapher (MRTG) atau sebuah grafik yang merupakan perbandingan data bit keluar masuk. Meskipun tidak ada perbedaan yang begitu mencolok antara hasil grafik yang dihasilkan oleh The Dude dan MRTG hal ini didapat berdasarkan atas dokumentasi yang dipahami.

Jika dibahas persamaan nya maka akan mendapatkan banyak hal, seperti keharusan pengesetan SNMP.

Sehingga karena The Dude adalah software pemantau jaringan yang dibuat oleh mikrotik, maka bahasan tersebut terfokus bagaimana menampilkan grafik bit data keluar-masuk pada router berbasiskan mikrotik (route rboard). Agar dapat ditampilkan sebuah grafik bit data keluar-masuk pastikan untuk menggambar link pada topologi jaringan pantau yang telah dibuat seperti pada contoh gambar topologi yang ada diatas. Dari hasil dokumentasi yang ada telah menentukan target device ethernet yang ingin anda pantau menggunakan The Dude adalah koneksi lokal. Meskipun pada gambar yang telah diambil koneksinya sedang mati, terlihat bahwa jenis nya mengharuskan snmp. Untuk pengguna router mikrotik maka secara otomatis sebuah device ethernet akan muncul pada menu Interface. Terakhirnya untuk menambahkan agar setiap saat bisa mengetahui pergerakan grafik bit data keluar-masuk telah dilakukan dengan pengesetan Graph Bit Rate hal ini menjelaskan tentang grafik tersebut.

Selanjutnya menjelaskan pcap dengan wireshark



No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.1.1	192.168.1.3	SNMP	428	get-request 1.3.6.1.2.1.2.2.1.1.2 1.3.6.1.2.1.2.2.1.2.2 1.3.6.1.2.1.2.2.1.3.2 1.3.6.1.2.1.2
2	0.00094800	192.168.1.1	192.168.1.4	SNMP	428	get-request 1.3.6.1.2.1.2.2.1.1.2 1.3.6.1.2.1.2.2.1.2.2 1.3.6.1.2.1.2.2.1.3.2 1.3.6.1.2.1.2
3	0.00161000	192.168.1.3	192.168.1.1	SNMP	475	get-response 1.3.6.1.2.1.2.2.1.1.2 1.3.6.1.2.1.2.2.1.2.2 1.3.6.1.2.1.2.2.1.3.2 1.3.6.1.2.1.
4	0.00345200	192.168.1.4	192.168.1.1	SNMP	473	get-response 1.3.6.1.2.1.2.2.1.1.2 1.3.6.1.2.1.2.2.1.2.2 1.3.6.1.2.1.2.2.1.3.2 1.3.6.1.2.1.
5	0.34971400	192.168.1.1	192.168.1.3	SNMP	86	get-next-request 1.3.6.1.2.1.25.3.3.1.2
6	0.35011000	192.168.1.1	192.168.1.3	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.6.1
7	0.35054500	192.168.1.1	192.168.1.3	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.5.1
8	0.35059500	192.168.1.3	192.168.1.1	SNMP	90	get-response 1.3.6.1.2.1.25.3.3.1.2.196608
9	0.35082900	192.168.1.1	192.168.1.3	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.6.3
10	0.35114900	192.168.1.3	192.168.1.1	SNMP	90	get-response 1.3.6.1.2.1.25.2.3.1.6.1
11	0.35147700	192.168.1.1	192.168.1.3	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.5.3
12	0.35165600	192.168.1.3	192.168.1.1	SNMP	90	get-response 1.3.6.1.2.1.25.2.3.1.5.1
13	0.35195300	192.168.1.1	192.168.1.3	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.6.31
14	0.35213200	192.168.1.3	192.168.1.1	SNMP	90	get-response 1.3.6.1.2.1.25.2.3.1.6.3
15	0.35245000	192.168.1.3	192.168.1.1	SNMP	91	get-response 1.3.6.1.2.1.25.2.3.1.5.3

– Untuk baris pertama perhatikan protokol SNMP merupakan protokol yang digunakan dari IP 192.168.1.1 ke IP 192.168.1.1 dengan panjang paket data 428 byte yang merupakan paket informasi, kemudian untuk angka-angka yang ada di info tersenut merupakan bagian dari MIB (Management Information Base) diamana dapat diartikan bahwa didalamnya terdapat SysContact, SysLocation, SysName.

- Untuk baris kedua perhatikan protokol SNMP merupakan protokol yang digunakan dari IP 192.168.1.1 ke IP 192.168.1.4 dengan panjang paket data 428 byte yang merupakan paket informasi, kemudian untuk angka-angka yang ada di info tersenut merupakan bagian dari MIB (Management Information Base) diamana dapat diartikan bahwa didalamnya terdapat SysContact, SysLocation, SysName.
- Untuk baris ketiga perhatikan protokol SNMP merupakan protokol yang digunakan dari IP 192.168.1.3 ke IP 192.168.1.1 dengan panjang paket data 475 byte yang merupakan paket informasi, kemudian untuk angka-angka yang ada di info tersenut merupakan bagian dari MIB (Management Information Base) diamana dapat diartikan bahwa didalamnya terdapat SysContact, SysLocation, SysName.
- Untuk baris keempat perhatikan protokol SNMP merupakan protokol yang digunakan dari IP 192.168.1.4 ke IP 192.168.1.1 dengan panjang paket data 86 byte yang merupakan paket informasi, kemudian untuk angka-angka yang ada di info tersenut merupakan bagian dari MIB (Management Information Base) diamana dapat diartikan bahwa didalamnya terdapat SysContact, SysLocation, SysName.

Dari penjelasan sebelumnya dengan memberikan 4 baris saja pada wireshark tersebut dapat dianalisa bahwa protokol yang digunakan adalah SNMP sebab dari data awal hingga akhir adalah SNMP untuk ip 192.168.1.1, 192.168.1.2, 192.168.1.3, 192.168.1.4, namun untuk panjang paket data yang diberikan berbeda dikarenakan ip awal ke ip tujuan berbeda-beda sehingga untuk angka-angka pada MIB juga berbeda, jadi dalam hal ini informasi data di dapat dari ip awal ke ip tujuan. Namun untuk angka-angka pada informasi terdapat SysContact, SysLocation, SysName jika pada protocol yang digunakan adalah SNMP.