


TIS13534P KOMUNIKASI DAN KEAMANAN DATA

Minggu 4 - Monitoring



Apa itu Monitoring?

- Sebuah kegiatan mengobservasi (terkadang merekam data yang diobservasi) lalu lintas data yang mengalir di dalam jaringan.
- Monitoring dilakukan untuk mengetahui lalu lintas apa saja yang sedang mengalir saat ini. Bahkan keadaan suatu perangkat jaringan yang terhubung ke jaringan.

Tujuan Monitoring

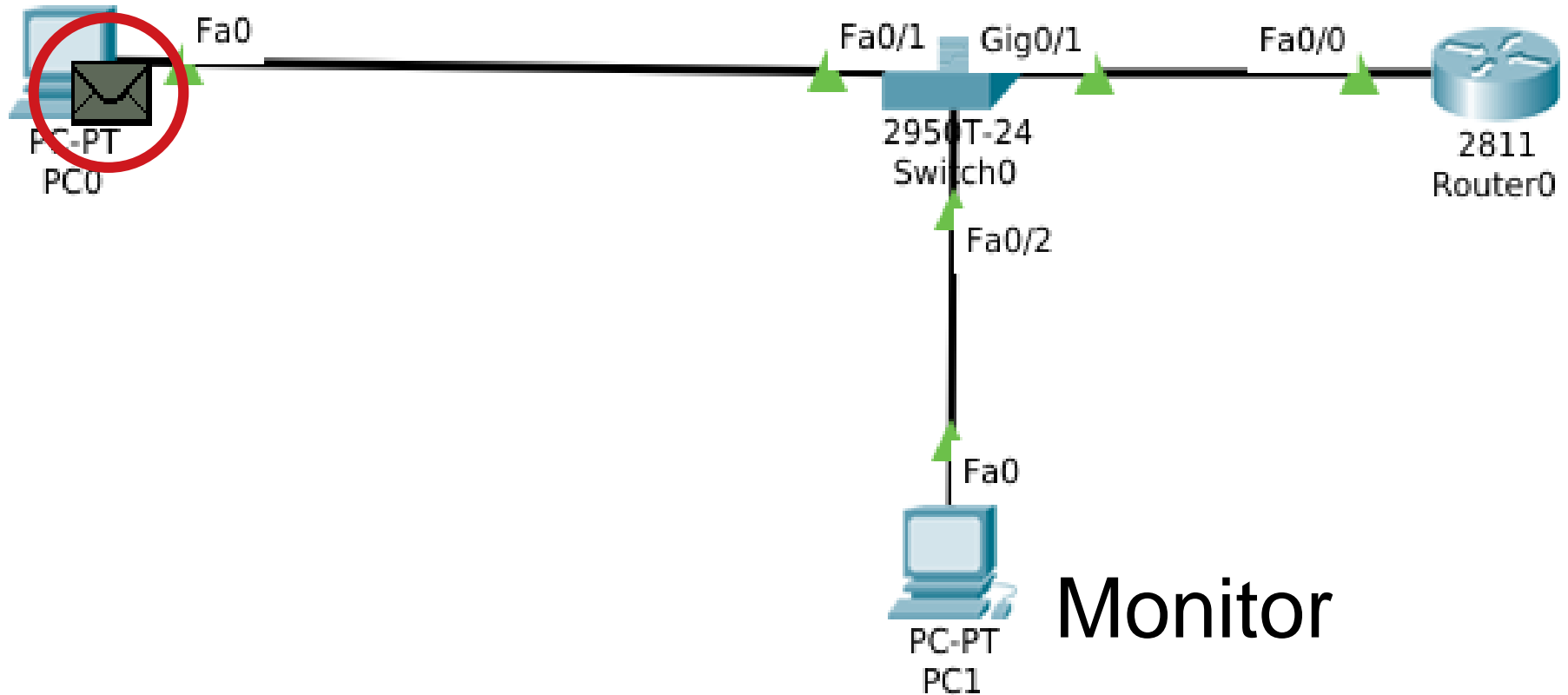
- Melihat keadaan perangkat jaringan
- Untuk analisa jika terjadi serangan
- Memonitor berapa bandwidth yang digunakan perangkat LAN komputer
- Melihat aliran lalu lintas data

Manfaat Monitoring

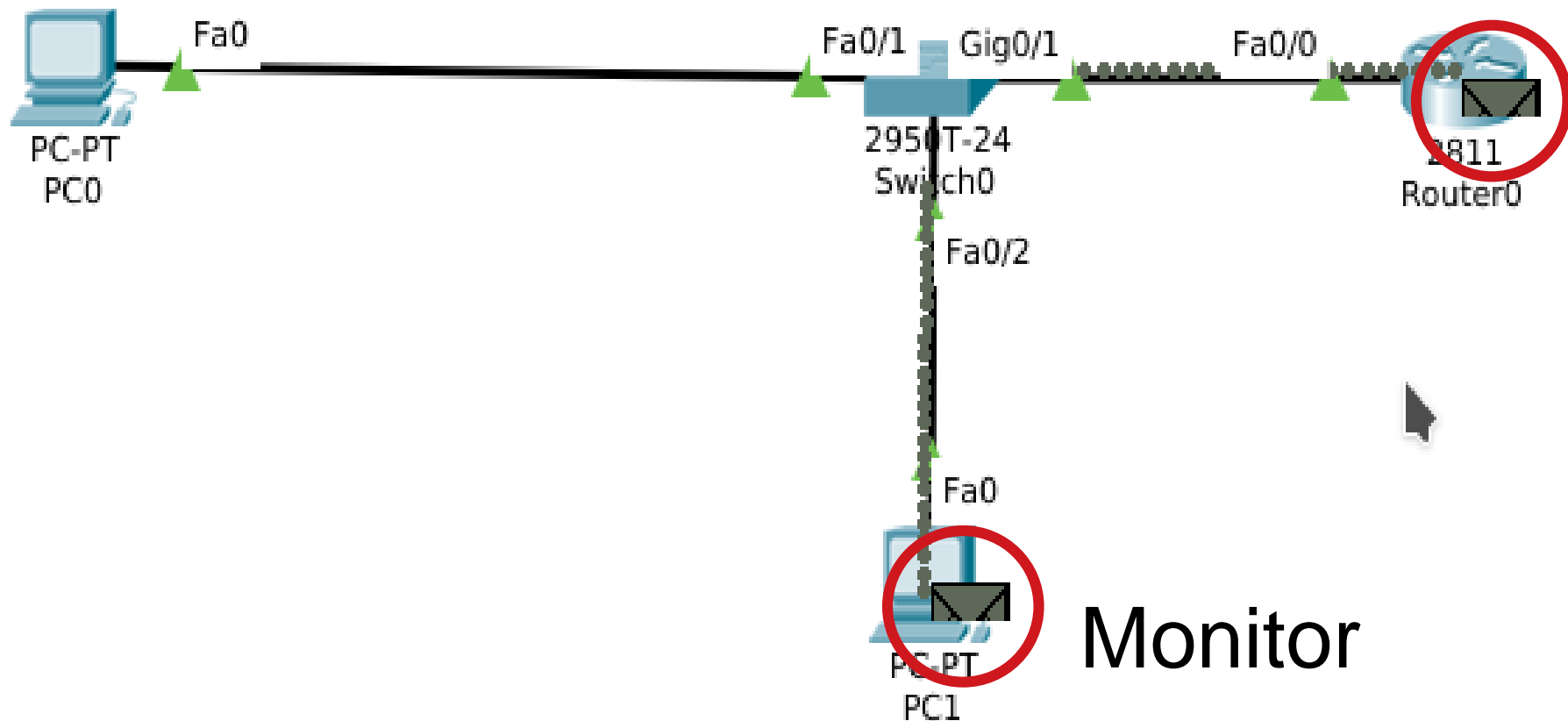
- Menghindari kerugian dari Sistem yang Gagal dan tidak terdeteksi
- Mudah menyelidiki permasalahan, dan bisa segera mengambil tindakan
- Lebih cepat mengetahui adanya *bottleneck* di dalam jaringan

<https://blog.paessler.com/interview-the-benefits-of-network-monitoring-part-1>

Ilustrasi – LAN Cable

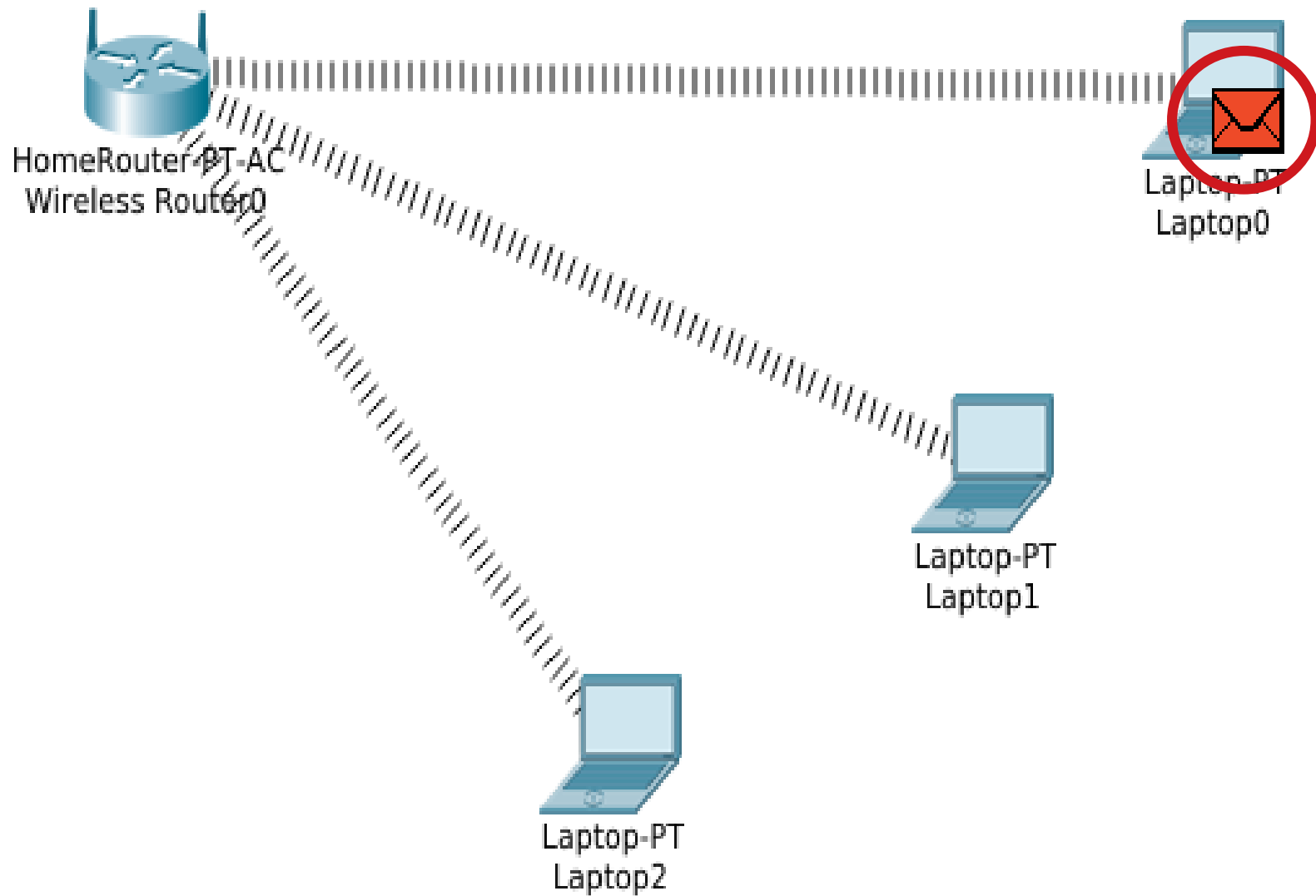


Ilustrasi – LAN Cable

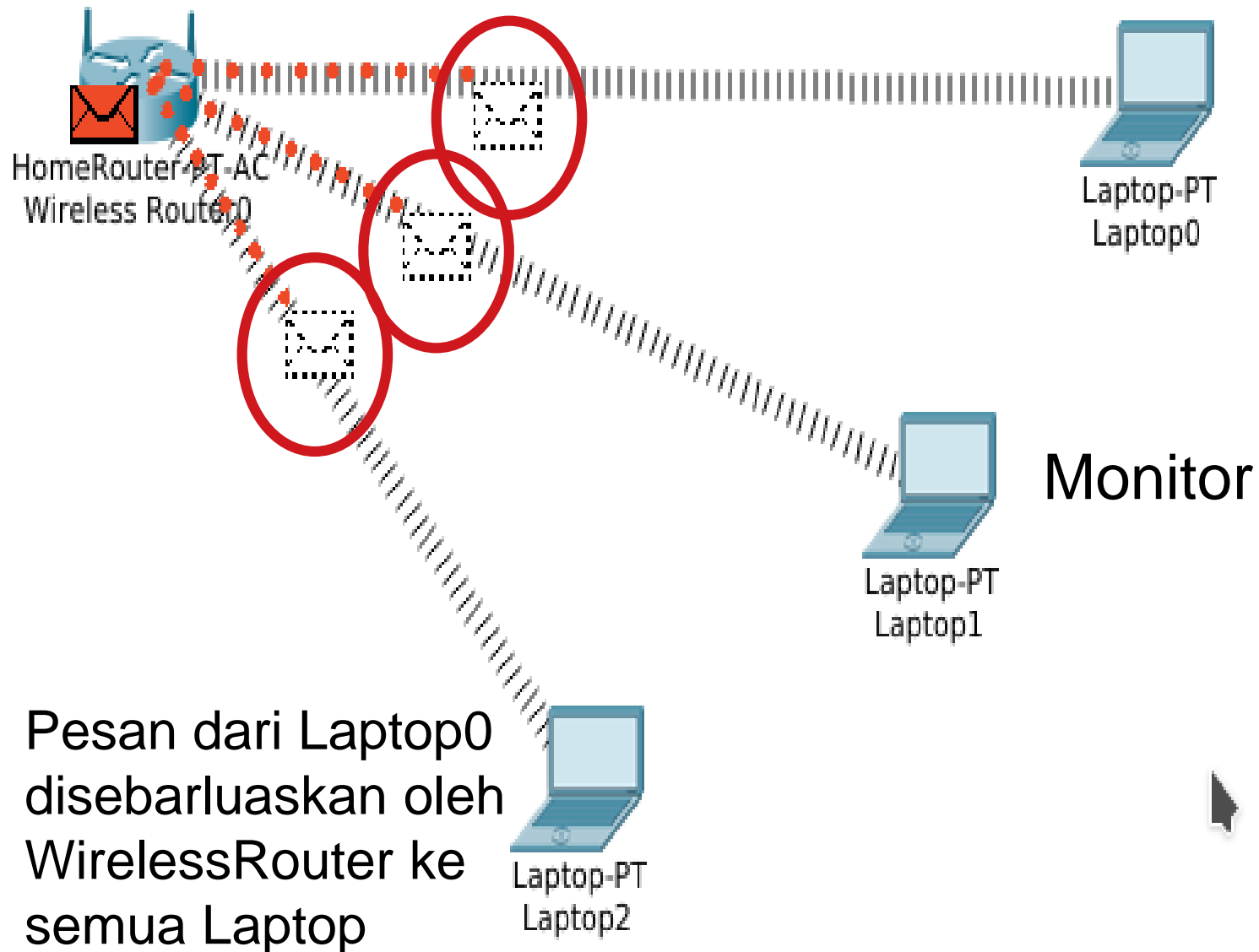


Paket dari PC0 terkirim ke PC1.
Khusus wired, dibutuhkan konfigurasi khusus untuk mirror traffic

Ilustrasi - Wireless



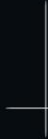
Ilustrasi - Wireless



Singkatnya

- Baik pengiriman maupun balasan pesan, semua akan terbaca oleh komputer orang lain (khususnya untuk wireless, untuk wired dibutuhkan konfigurasi khusus di switchnya).
 - Alat monitoring dapat menangkap dan membaca pesan-pesan tersebut meskipun salah alamat (bukan tujuan pesan tersebut).
-


Efek Buruk Monitoring

- Analisis data terbalik untuk mendapatkan password.
 - Mencari alamat untuk di DDoS karena orang memakai semua bandwidth
 - Untuk mengubah data yang orang kirim (tampering)
-
- 

Protokol Monitoring dan Alat Monitoring

SNMP (Simple Network Management Protocol)

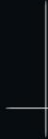
SNMP adalah sebuah protokol jaringan yang dibuat untuk monitoring, konfigurasi perangkat jaringan, dan menerima pemberitahuan jika terjadi sesuatu.




Kelebihan SNMP

- Bisa memonitor berbagai perangkat yang dibuat oleh pabrik yang berbeda, dan dipasang di jaringan secara fisik.
- Digunakan di jaringan internet yang heterogen, yang berisi topologi LAN dan WAN oleh router yang berbeda-beda.
- Mengirimkan pesan notifikasi jika terjadi error atau kegagalan sistem di salah satu perangkat

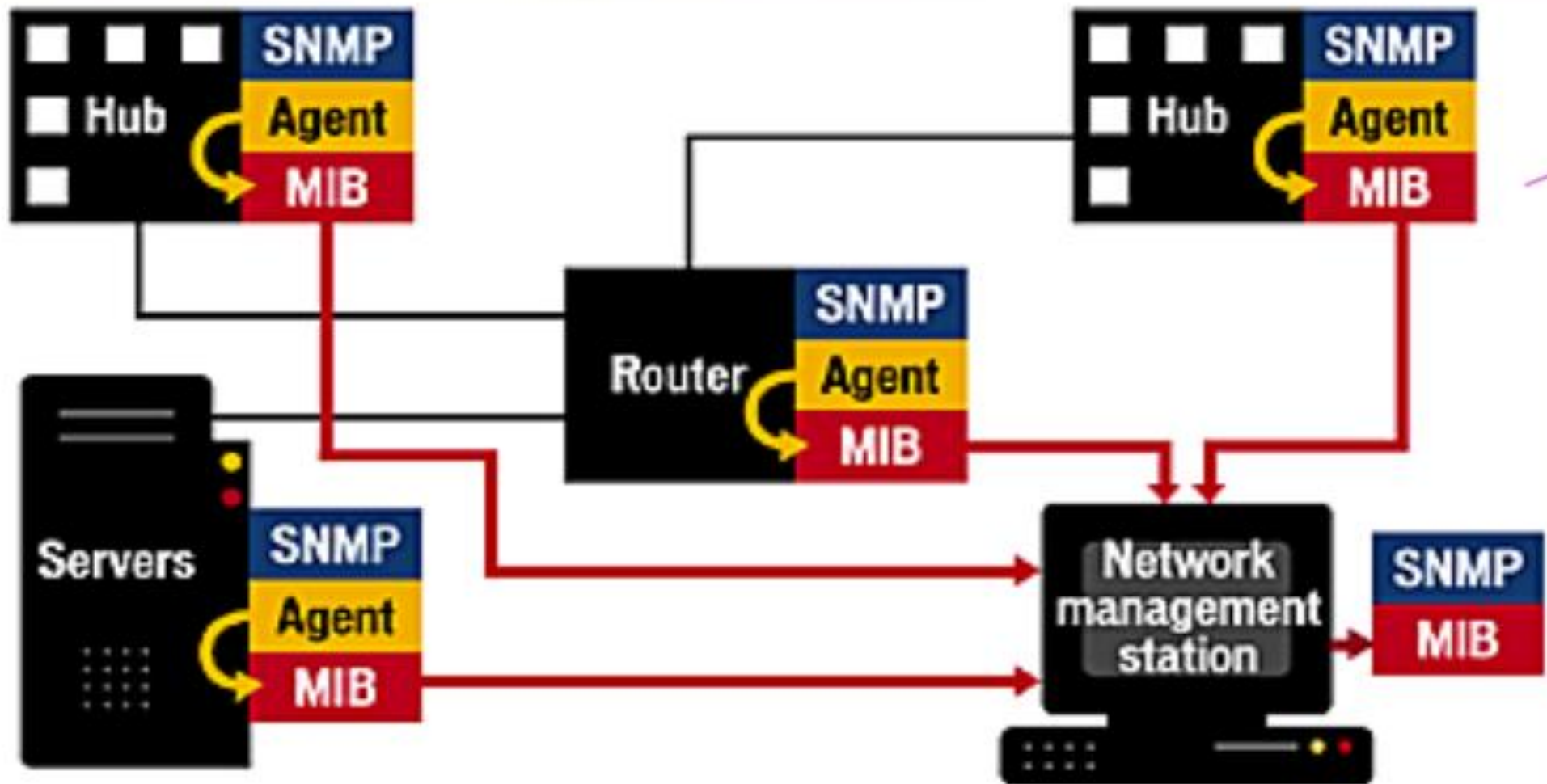
Bagaimana SNMP bekerja?

- Setiap perangkat jaringan akan memiliki yang namanya:
 - SNMP
 - Agent
 - MIB (Management Information Base)
-
- 

Bagaimana SNMP bekerja?

- Agent di dalam perangkat akan menyiapkan Packet Data Unit yang berisi data-data mengenai perangkat, dan disimpan di MIB
 - MIB akan meneruskan data itu ke Komputer Monitor
-
- 

Ilustrasi



- Black lines are normal network connections.
- Gold lines are SNMP agents getting PDUs and storing them in the MIB.
- Red lines are SNMP agents forwarding MIB data to the network management station, which stores them in its own composite MIB.

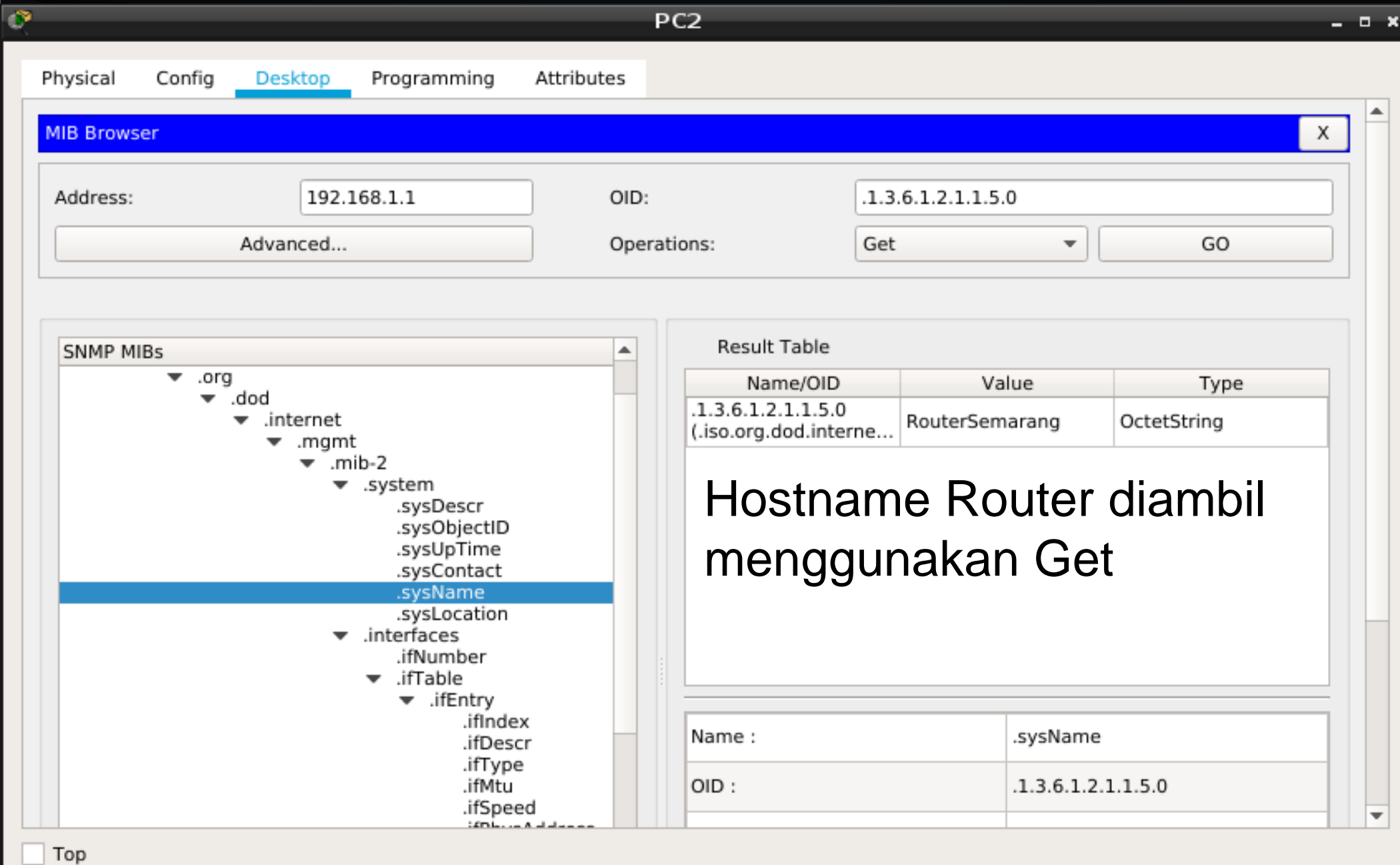
Jenis Pesan SNMP

- Pesan ini dimaksudkan bagaimana SNMP klien meminta data ke SNMP server.
- Ada beberapa jenis pesan sesuai dengan fungsinya.

Jenis Pesan SNMP

Jenis	Fungsi
Get (GetRequest)	Meminta data yang tersimpan di dalam MIB, hanya satu set data saja yang diberikan
GetNext	Meminta data berikutnya sesuai urutan leksikal yang tersimpan di dalam MIB
GetBulk	Meminta beberapa set data secara efisien kepada server
GetResponse	Dari agen/klien ke manager
Set (SetRequest)	Mengganti nilai variabel di MIB
Trap	Pesan notifikasi dari agent ke manager (manager tidak meminta pesan notifikasi) yang berupa error atau kegagalan

Contoh

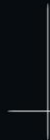


Klien SNMP

- PRTG : untuk analisa dan monitor penggunaan bandwidth (gratis untuk 100 sensor)
- PowerSNMP (ditulis dengan bahasa .NET)
- Net-SNMP crossplatform klien SNMP

Multi Router Traffic Grapher

- Sebuah software gratis yang dapat digunakan untuk memonitor penggunaan bandwidth dalam waktu tertentu secara grafis
- MRTG menggunakan SNMP untuk mendapatkan informasi yang dibutuhkan, lalu disimpan dalam bentuk gambar



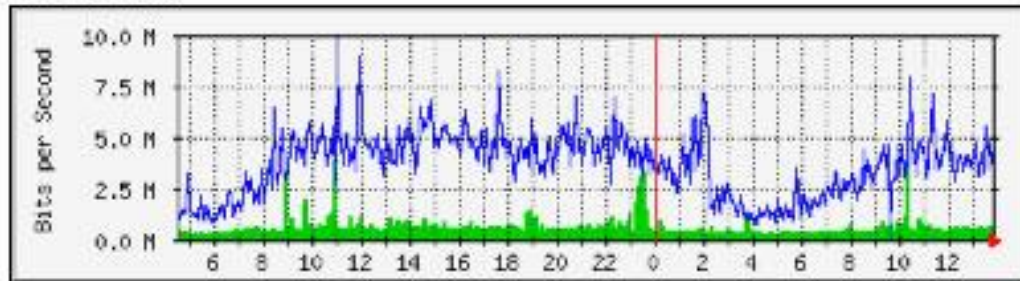
Fitur dari MRTG

- Mengukur Input dan Output muatan lalu lintas data per target
- Mengambil data setiap 5 menit (bisa diatur)
- Membuat sebuah halaman HTML per target untuk mempermudah pembacaan
- Menampilkan Maksimum, Rata-rata, dan Nilai saat ini untuk Input dan Output
- Bisa mengirimkan email peringatan jika target mencapai titik tertentu

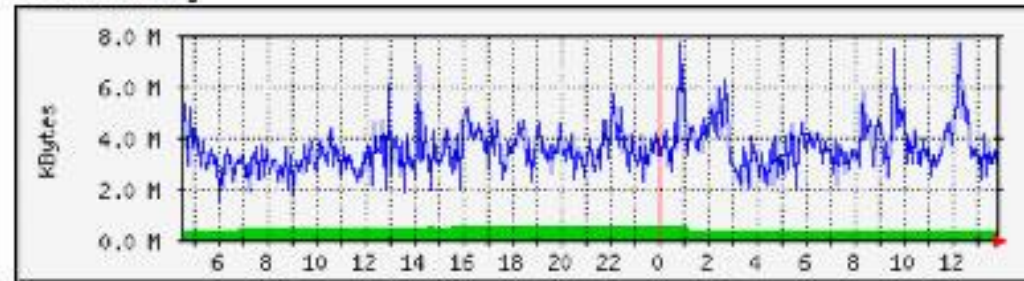
Grafik MRTG

MRTG Index Page

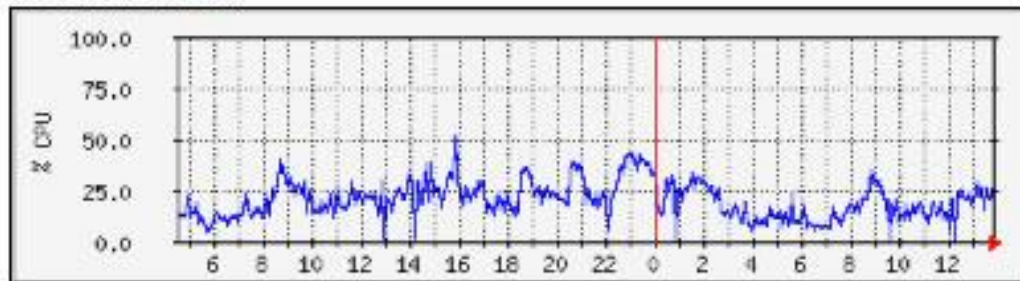
Traffic Load



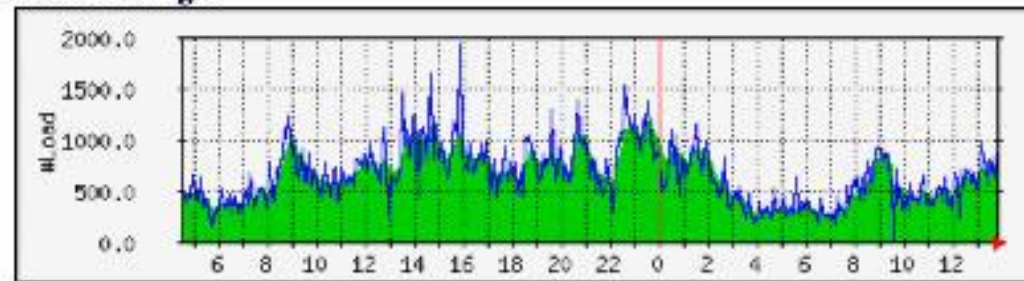
Free Memory



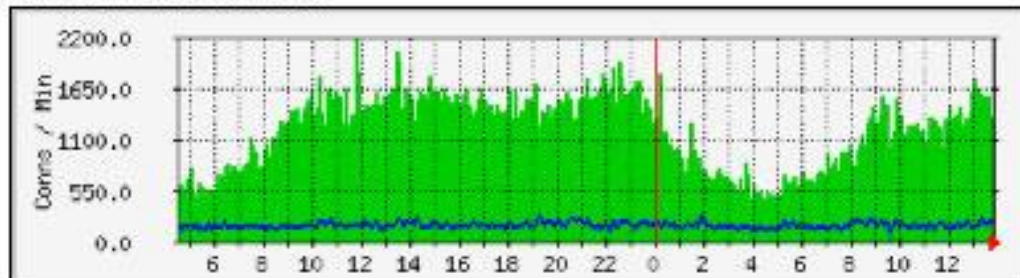
CPU Utilization



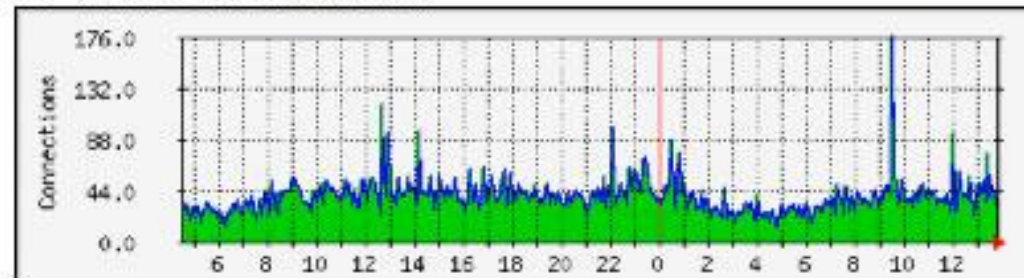
Load Average




New TCP Connections



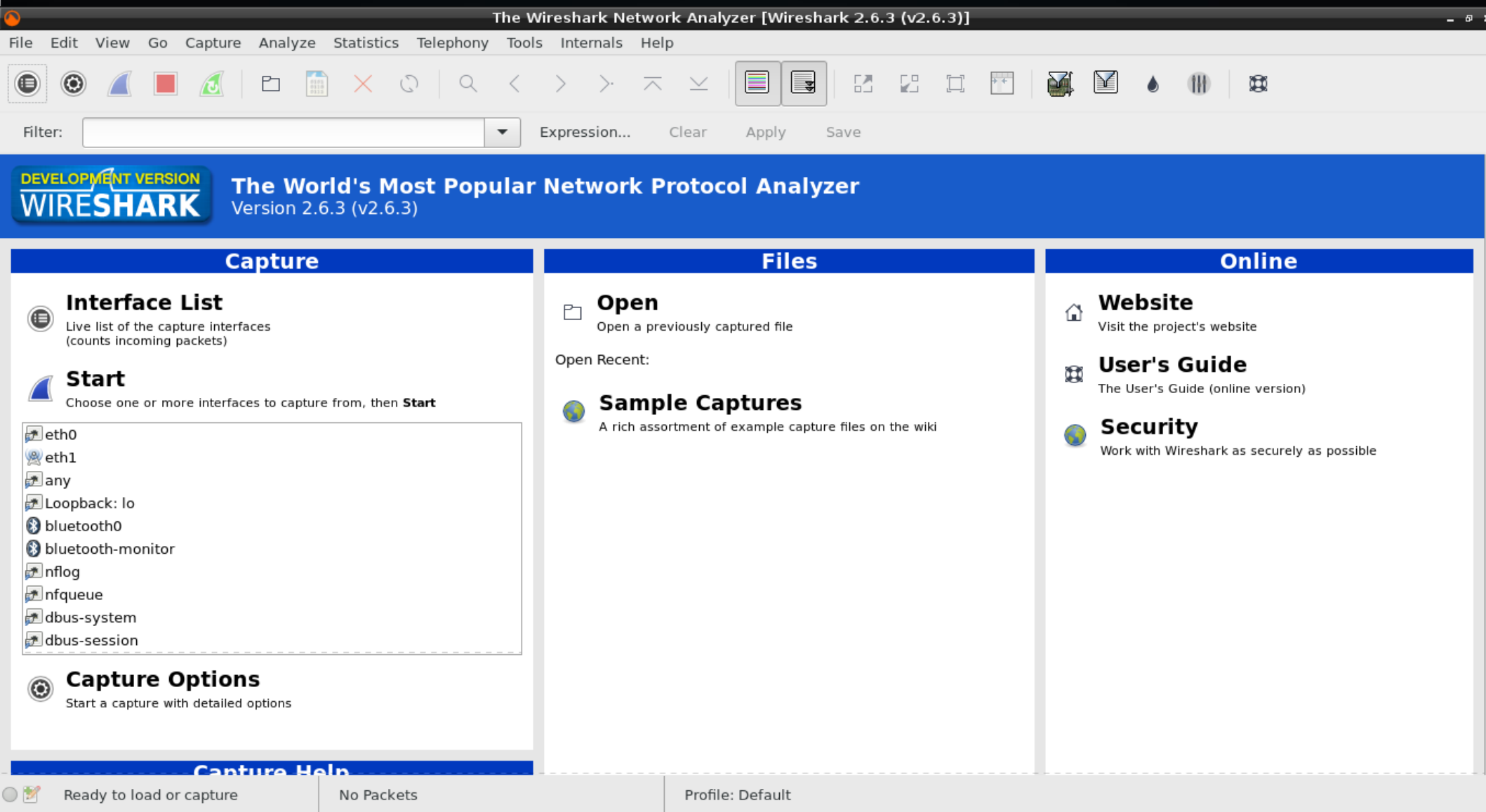
Established TCP Connections




Wireshark

- Sebuah software crossplatform yang berguna untuk menganalisa paket-paket data yang mengalir di jaringan
 - Bisa digunakan untuk memonitor paket di Kabel, Wireless, bahkan Bluetooth (versi terbaru)
-
- 


Tampilan Wireshark



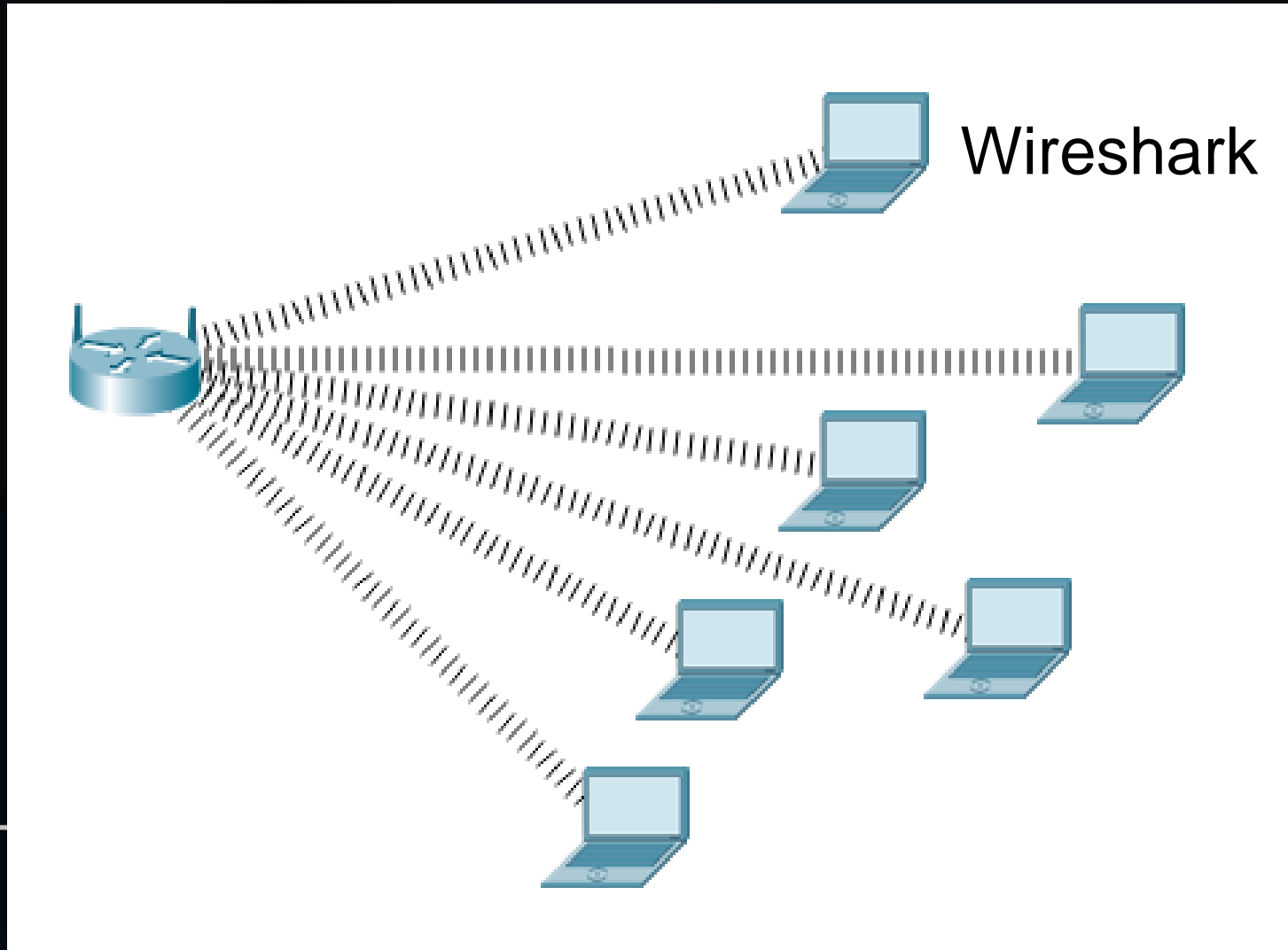
Wireshark:

- Wireshark memerlukan jaringan aktif (minimal LAN atau PAN) yang terhubung baik via kabel LAN, Wireless, atau Bluetooth
 - Wireshark bisa dimulai dengan meng-klik Interface/Perangkat Jaringan yang ada
-
- 

Wireshark:

- Memiliki Mode : Promiscuous Mode di mana aliran data dari NIC dialirkan menuju CPU untuk dianalisa isinya.
 - Bisa membaca semua aliran data tanpa konfigurasi khusus (hanya di wireless)
 - Memerlukan konfigurasi khusus di switch agar Wireshark bisa membaca semua aliran jika terhubung dengan kabel
-
- 

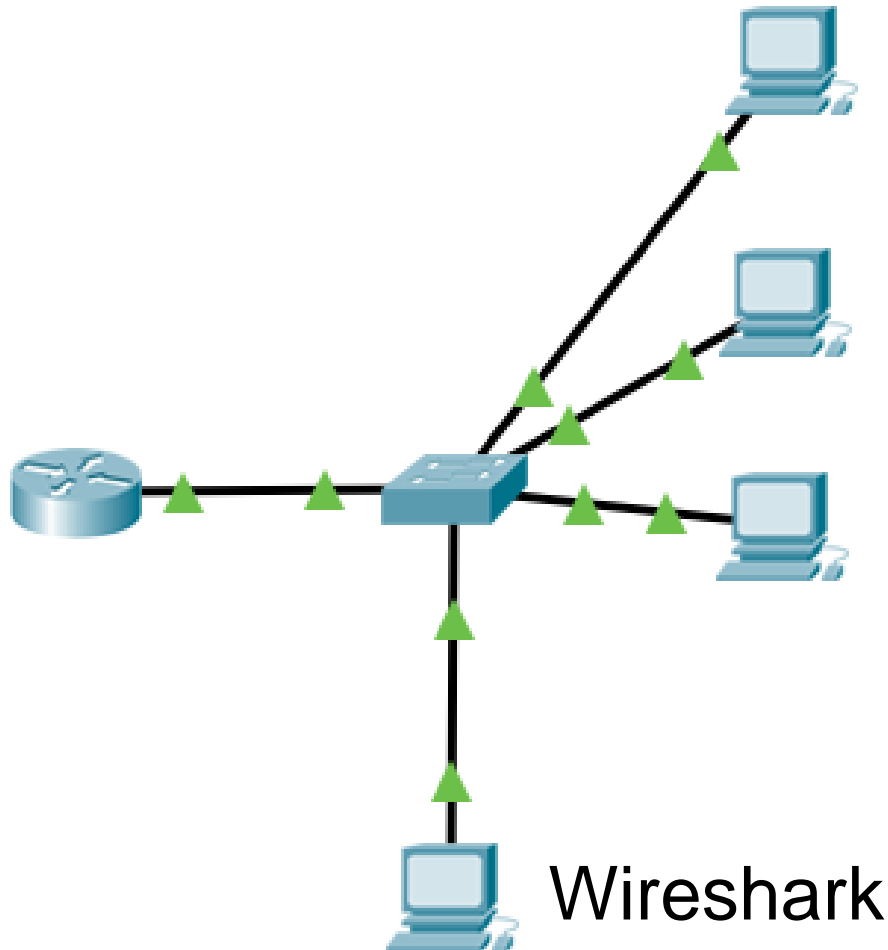
Ilustrasi: Wireshark - Wireless



Wireshark bisa mengintip data orang lain tanpa harus konfigurasi di router access pointnya.

Sehingga wireless dianggap rawan pencurian data

Ilustrasi: Wireshark - Wired



Jika switch tidak dikonfigurasi, Wireshark hanya bisa membaca aliran data dari dan ke dirinya saja.











Tidak bisa mengintip aliran data orang lain

Wireshark:



Start

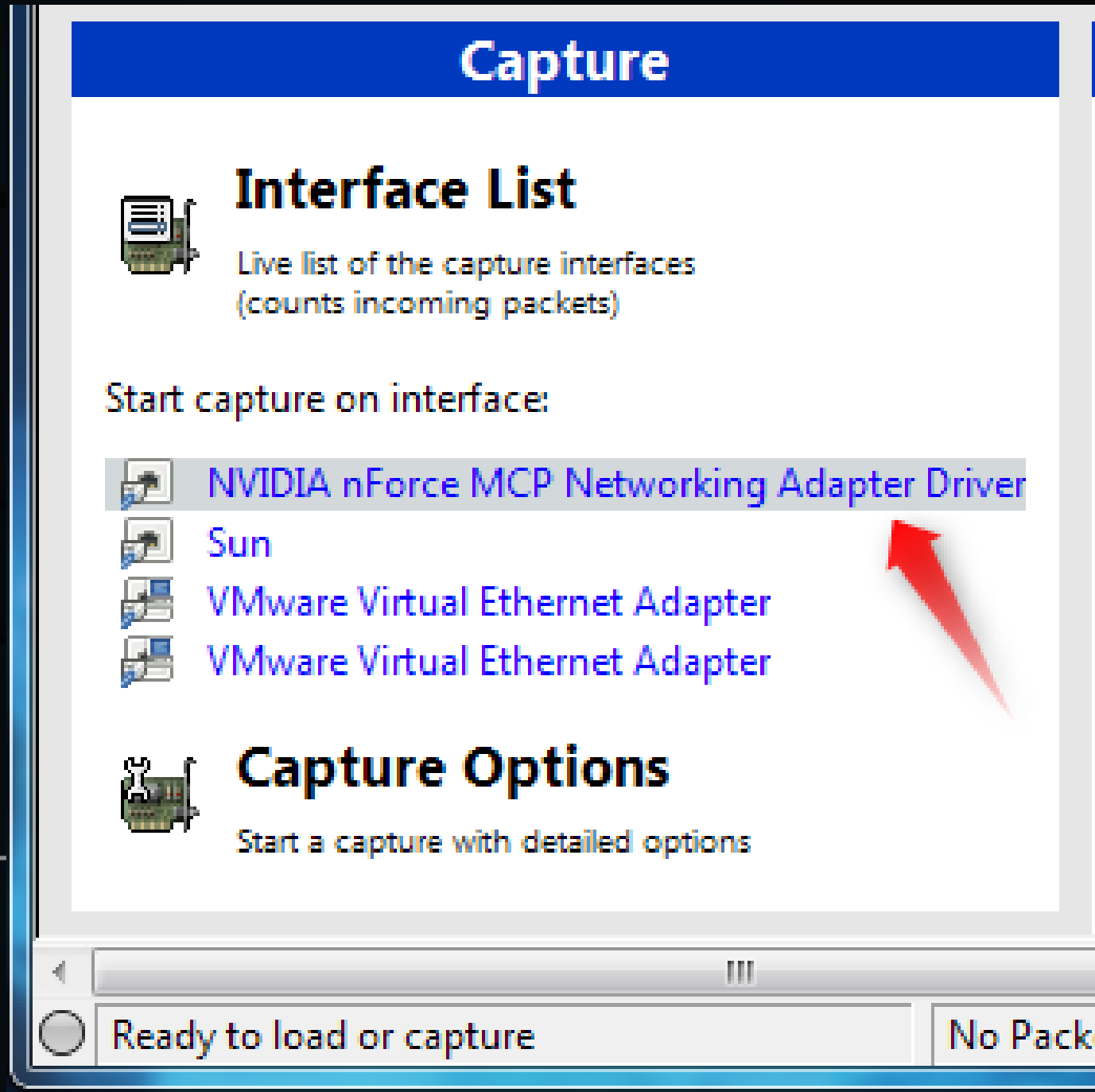
Choose one or more interfaces to capture from, then **Start**

 eth0
 eth1
 any
 Loopback: lo
 bluetooth0
 bluetooth-monitor
 nflog
 nfqueue
 dbus-system
 dbus-session

Interface yang muncul disesuaikan dengan Sistem Operasi yang dijalankan. Gambar ini merupakan salah satu contoh Interface dari Linux

Wireshark:

Biasanya kalo Windows, yang akan ditampilkan adalah nama adapter yang terpasang



Kelebihan Wireshark:

1. Status paket (terkirim, gagal terkirim) bisa dilihat dengan jelas
2. Grafik Input/Output
3. Analisis per paket yang dikirim
4. Filter yang bisa digunakan untuk memilah rekaman yang sangat banyak

Wireshark: Scanning Ping

*eth0 [Wireshark 2.6.3 (v2.6.3)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.addr==192.168.100.7` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
10	1.003937023	192.168.100.7	192.168.100.2	ICMP	98	Echo (ping) reply id=0x6b23, seq=6/1536, ttl=64 (request in 9)
20	2.004030471	192.168.100.2	192.168.100.7	ICMP	98	Echo (ping) request id=0x6b23, seq=7/1792, ttl=64 (reply in 22)
22	2.008724433	192.168.100.7	192.168.100.2	ICMP	98	Echo (ping) reply id=0x6b23, seq=7/1792, ttl=64 (request in 20)
34	3.005007201	192.168.100.2	192.168.100.7	ICMP	98	Echo (ping) request id=0x6b23, seq=8/2048, ttl=64 (reply in 35)
35	3.009776523	192.168.100.7	192.168.100.2	ICMP	98	Echo (ping) reply id=0x6b23, seq=8/2048, ttl=64 (request in 34)
43	4.006023042	192.168.100.2	192.168.100.7	ICMP	98	Echo (ping) request id=0x6b23, seq=9/2304, ttl=64 (reply in 44)
44	4.010653380	192.168.100.7	192.168.100.2	ICMP	98	Echo (ping) reply id=0x6b23, seq=9/2304, ttl=64 (request in 43)
45	5.007032179	192.168.100.2	192.168.100.7	ICMP	98	Echo (ping) request id=0x6b23, seq=10/2560, ttl=64 (reply in 46)
46	5.013272638	192.168.100.7	192.168.100.2	ICMP	98	Echo (ping) reply id=0x6b23, seq=10/2560, ttl=64 (request in 45)
49	6.008004230	192.168.100.2	192.168.100.7	ICMP	98	Echo (ping) request id=0x6b23, seq=11/2816, ttl=64 (reply in 50)
50	6.072691227	192.168.100.7	192.168.100.2	ICMP	98	Echo (ping) reply id=0x6b23, seq=11/2816, ttl=64 (request in 49)
51	7.009008618	192.168.100.2	192.168.100.7	ICMP	98	Echo (ping) request id=0x6b23, seq=12/3072, ttl=64 (reply in 52)
52	7.014376758	192.168.100.7	192.168.100.2	ICMP	98	Echo (ping) reply id=0x6b23, seq=12/3072, ttl=64 (request in 51)
67	8.010461596	192.168.100.2	192.168.100.7	ICMP	98	Echo (ping) request id=0x6b23, seq=13/3328, ttl=64 (reply in 68)
68	8.015055267	192.168.100.7	192.168.100.2	ICMP	98	Echo (ping) reply id=0x6b23, seq=13/3328, ttl=64 (request in 67)
100	9.012022199	192.168.100.2	192.168.100.7	ICMP	98	Echo (ping) request id=0x6b23, seq=14/3584, ttl=64 (reply in 101)
101	9.018162994	192.168.100.7	192.168.100.2	ICMP	98	Echo (ping) reply id=0x6b23, seq=14/3584, ttl=64 (request in 100)
120	10.01329289	192.168.100.2	192.168.100.7	ICMP	98	Echo (ping) request id=0x6b23, seq=15/3840, ttl=64 (reply in 121)
121	10.01802128	192.168.100.7	192.168.100.2	ICMP	98	Echo (ping) reply id=0x6b23, seq=15/3840, ttl=64 (request in 120)

► Ethernet II, Src: Raspberr_3e:1e:a9 (b8:27:eb:3e:1e:a9), Dst: Dell_0d:aa:af (00:26:b9:0d:aa:af)

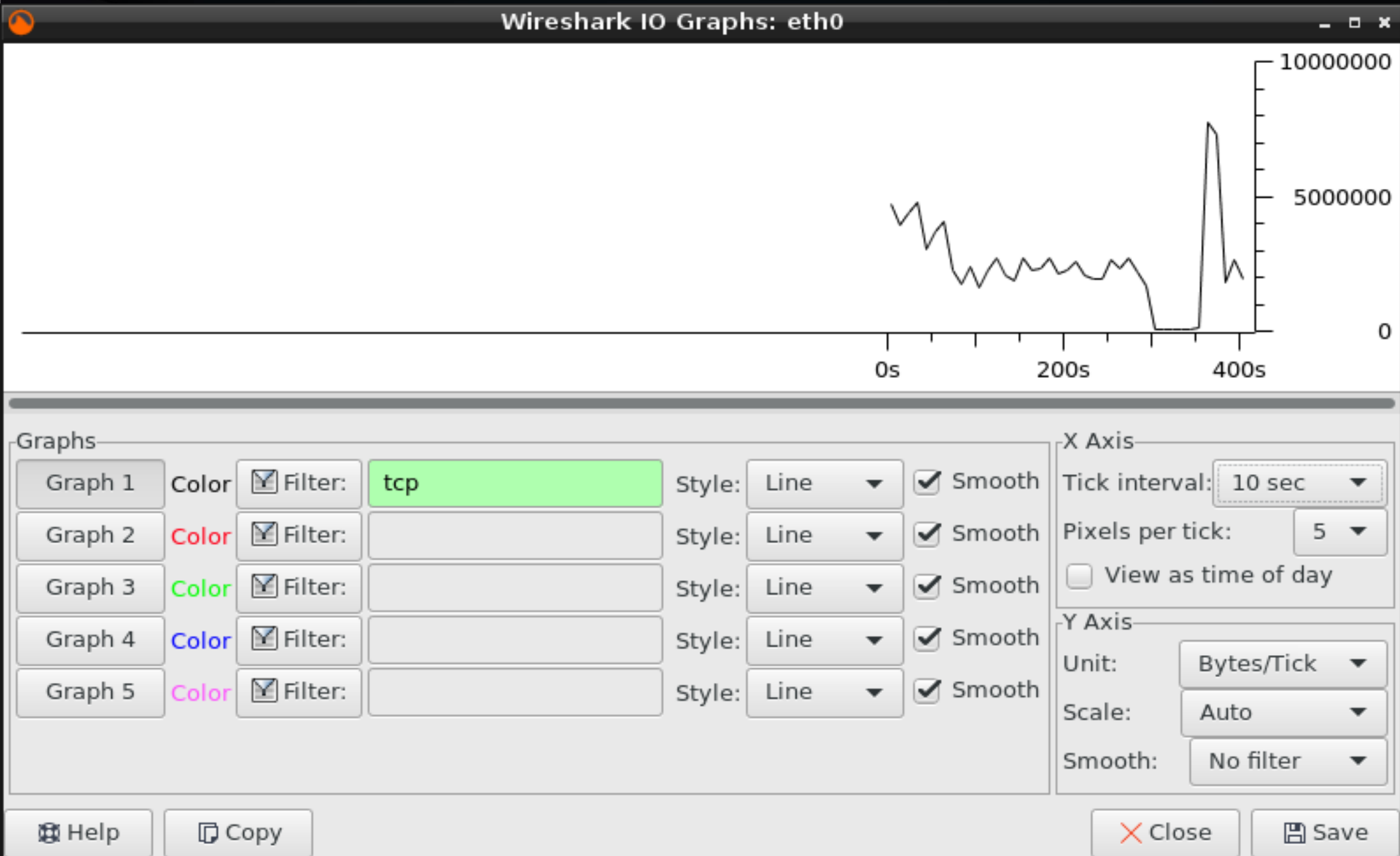
► Internet Protocol Version 4, Src: 192.168.100.7, Dst: 192.168.100.2

► Internet Control Message Protocol

```
0000  00 26 b9 0d aa af b8 27 eb 3e 1e a9 08 00 45 00  .&.....' .>....E.
0010  00 54 25 63 00 00 40 01 0b ec c0 a8 64 07 c0 a8  .T%C..@. ....d...
0020  64 02 00 00 d7 2e 6b 23 00 06 92 b2 bb 5b 00 00  d.....k# .....[...
0030  00 00 aa c6 06 00 00 00 00 00 10 11 12 13 14 15  .....
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..... .. !"#$$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,- ./012345
0060  36 37 67
```

Ready to load or capture Packets: 129 · Displayed: 26 (20.2%) · Dr... Profile: Default

Wireshark: Statistik Streaming YT



Wireshark: Summary YouTube

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	69679	69679	100.000%	0	0.000%
Between first and last packet	408.426 sec				
Avg. packets/sec	170.604				
Avg. packet size	1442 bytes				
Bytes	100464891	100464891	100.000%	0	0.000%
Avg. bytes/sec	245980.429				
Avg. MBit/sec	1.968				

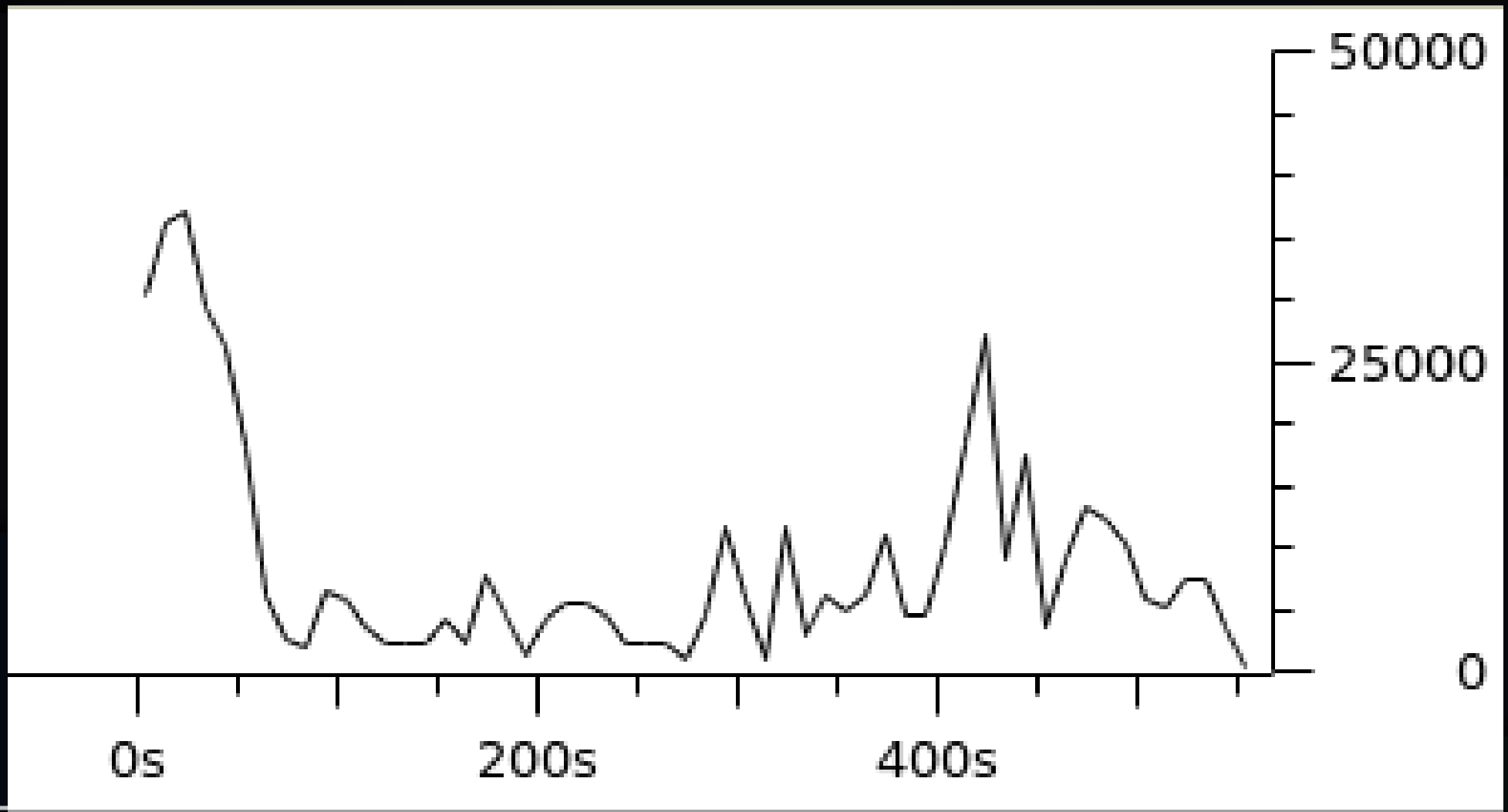
Nonton streaming YouTube kurang lebih 4 menit:

- Total Paket : 69.679 paket mengalir
- Rata-rata Paket : 170 paket/detik
- Rata-rata Ukuran Paket : 1442 bytes = 1,4KBytes
- Rata-rata bytes/detik : 245.980 bytes = 245KBytes

Tes Kirim Data via FTP

- File dikirim dari PC/Laptop ke HP via FTP Protocol dan di scan traffiknya menggunakan Wireshark.
- Scan dimulai sebelum file dikirim, dan di stop setelah pengiriman data selesai

Wireshark: Kirim File via FTP



Terjadi naik turun grafik data yang dikirim melalui FTP

Wireshark: Kirim File via FTP

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	722025	483965	67.029%	0	0.000%
Between first and last packet	553.178 sec	549.716 sec			
Avg. packets/sec	1305.231	880.391			
Avg. packet size	1064 bytes	1513 bytes			
Bytes	767945755	732456202	95.379%	0	0.000%
Avg. bytes/sec	1388244.075	1332426.547			
Avg. MBit/sec	11.106	10.659			

Terdapat:

- Total Paket FTP : 483.965 paket
- Rata-rata paket/detik : 880 paket/detik
- Rata-rata Ukuran Paket : 1513 bytes
- Rata-rata bytes/detik : 1.332.426 bytes/detik

= 1MBytes/detik

Bersabung ...