

Monitoring Jaringan Komputer dengan *Network Protocol Analyzer*

Didha Dewannanta

didhadewannanta@gmail.com

http://jarkomindonesia.tk

Lisensi Dokumen:

Copyright © 2003-2007 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

SoftPerfect Network Protocol Analyzer adalah alat profesional gratis untuk menganalisis, debugging, pemeliharaan dan pemantauan jaringan lokal dan koneksi internet. *Tools* ini menangkap data melewati koneksi *dial-up* atau kartu jaringan *Ethernet*, menganalisis data paket dan kemudian mengubah dalam bentuk yang mudah dibaca. *SoftPerfect Network Protocol Analyzer* adalah alat yang berguna bagi administrator jaringan, spesialis keamanan, pengembang aplikasi jaringan dan siapa pun yang membutuhkan gambaran yang komprehensif tentang lalu lintas yang melewati koneksi jaringan atau segmen jaringan area lokal.

SoftPerfect Network Protocol Analyzer menyajikan hasil analisis jaringan dalam format yang mudah digunakan dan mudah dimengerti. Hal ini juga memungkinkan anda untuk defragment dan mengumpulkan kembali paket data ke jaringan. Program ini dapat dengan mudah menganalisa lalu lintas jaringan berdasarkan sejumlah protokol internet yang berbeda seperti yang tercantum di bawah ini.

SoftPerfect Network Protocol Analyzer mendukung fitur protokol jaringan pada *layer* bawah OSI layer sebagai berikut: AH, ARP, ESP, ICMP, ICMPv6, IGMP, IP, IPv6, IPX, LLC, MSG, REVARP, RIP, SAP, SER, SNAP, SPX, TCP dan UDP. Dan juga mendukung protokol *layer* atas OSI *layer* seperti HTTP, SMTP, POP, IMAP, FTP, TELNET dan lain-lain.

Sistemnya fleksibel bisa diatur, filter dan dapat digunakan untuk membuang semua lalu lintas jaringan kecuali pola lalu lintas tertentu yang anda inginkan untuk dianalisis. *SoftPerfect Network Protocol Analyzer* juga dilengkapi pembangun paket. Alat ini memungkinkan anda untuk membangun paket jaringan anda sendiri dan mengirim paket tersebut ke jaringan. Anda bisa menggunakan fitur pembangun paket untuk memeriksa jaringan anda, untuk perlindungan terhadap serangan dan penyusup.

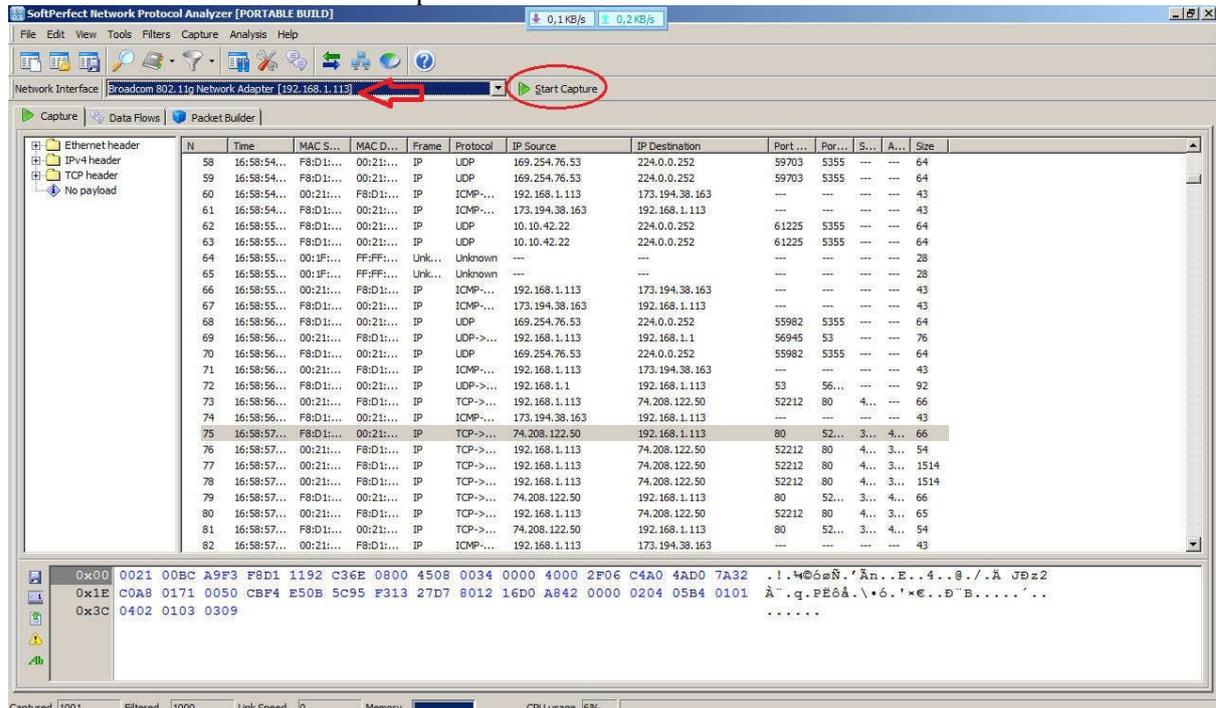
Perangkat lunak ini memerlukan Windows 2000/XP/2003/Vista/2008/Seven. Kedua sistem 32-bit dan 64-bit yang didukung. Hal ini juga memerlukan sambungan jaringan, yang bisa berasal dari koneksi nirkabel, atau modem yang sesuai dengan standar NDIS.

Fitur Utama

- Mampu menangkap semua paket jaringan.
- Mengubah paket dan menampilkannya dalam format yang mudah dibaca.
- Memungkinkan Anda membangun paket *custom* dan mengirim mereka ke jaringan.
- Menawarkan sistem lalu lintas yang fleksibel dalam penyaringan. Filter apapun dapat menjadi inklusif atau eksklusif.
- Merekonstruksi paket ke jaringan sehingga Anda dapat dengan mudah melihat pertukaran data lengkap Telnet, POP3, SMTP, IMAP, FTP, HTTP dan protokol lainnya.
- Memungkinkan Anda memonitor koneksi loopback dalam sistem.

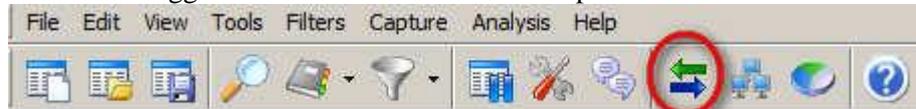
Tutorial

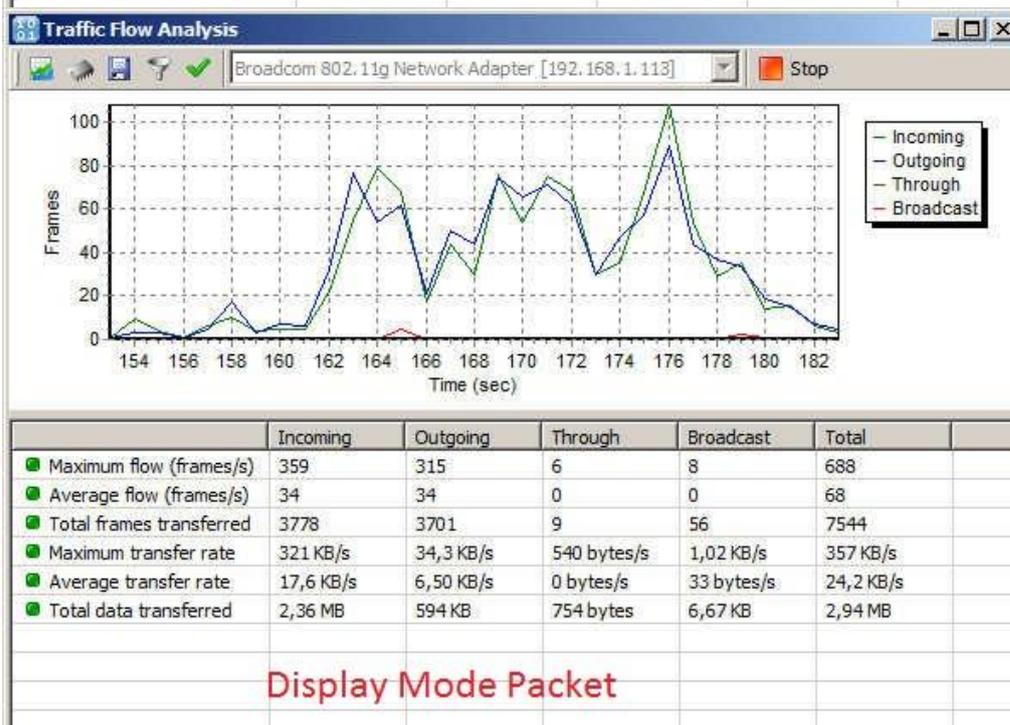
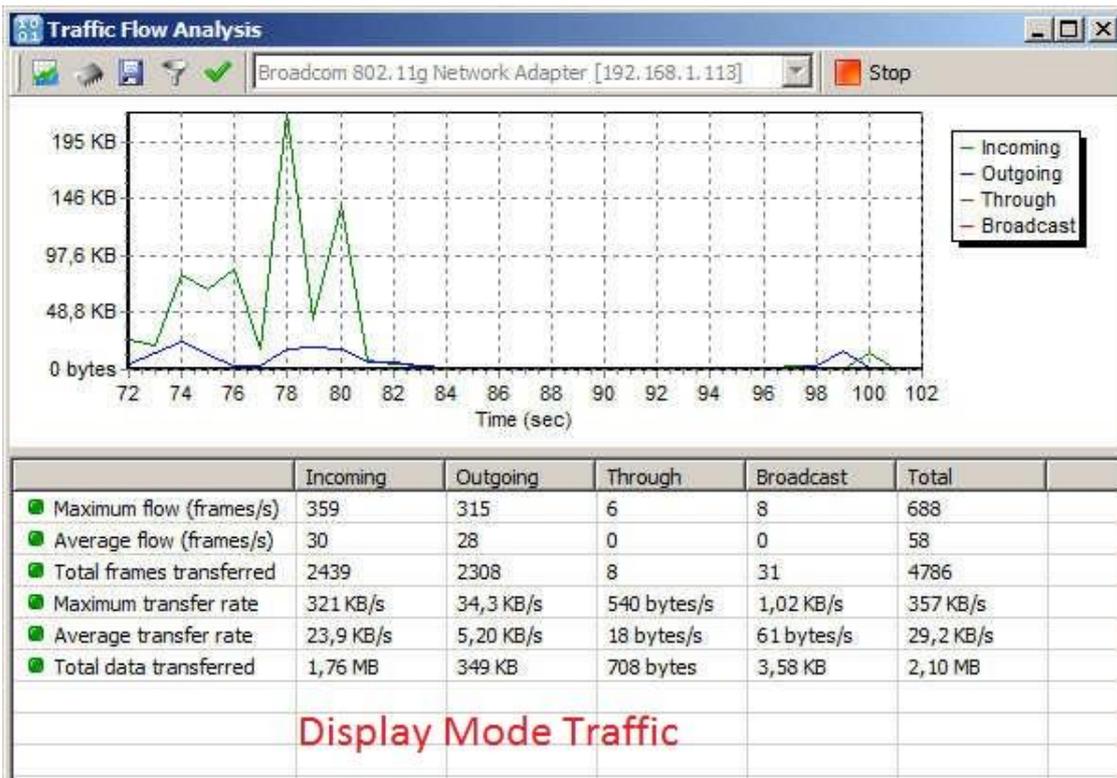
1. Cara penggunaannya sama dengan tools Monitoring lain, dengan cara memilih interface dan kemudian klik start capture.



akan muncul paket – paket data yang lewat, ada MAC, Frame, Protocol, IP source dan destination, dll.

2. Keunggulan dari tools ini adalah kita dapat memonitor traffic flow analysis.





3. Kita juga melihat aktivitas yang sedang dilakukan oleh host

The screenshot shows the Host Activity Monitor window in Wireshark. The network interface is 'Broadcom 802.11g Network Adapter [192.168.1.113]'. The active senders list shows 192.168.1.113 as the primary host. A pie chart shows traffic distribution to 198.15.64.10, 224.0.0.252, and 192.168.1.113.

Host	Packets	Traffic
192.168.1.113 (ip host)	33978	46,5 MB
198.15.64.10	18458	1,03 MB
224.0.0.252	402	25,6 KB
74.125.135.103	312	56,6 KB
173.194.38.163	306	12,8 KB
58.26.1.33	238	34,8 KB
202.158.17.148	208	23,0 KB
74.125.135.191	193	27,2 KB
74.125.128.121	132	12,8 KB
74.125.135.102	130	13,4 KB
74.125.128.112	127	15,4 KB

The second screenshot shows the Host Activity Monitor window with the network interface still 'Broadcom 802.11g Network Adapter [192.168.1.113]'. The active senders list shows 198.15.64.10 as the primary host. A pie chart shows traffic distribution to 198.15.64.10, 74.125.135.103, 202.158.17.148, and 192.168.1.113.

Host	Packets	Traffic
192.168.1.113	8044	768 KB
198.15.64.10 (ip server)	7221	10,3 MB
74.125.135.103	404	499 KB
58.26.1.33	297	356 KB
202.158.17.148	259	295 KB
173.194.38.163	238	9,99 KB


```

C:\Users\dewan>ping datafilehost.com
Pinging datafilehost.com [198.15.64.10] with 32 bytes of data:
Reply from 198.15.64.10: bytes=32 time=259ms TTL=50
Reply from 198.15.64.10: bytes=32 time=266ms TTL=50
Reply from 198.15.64.10: bytes=32 time=263ms TTL=50
Reply from 198.15.64.10: bytes=32 time=257ms TTL=50

Ping statistics for 198.15.64.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 257ms, Maximum = 266ms, Average = 261ms
    
```

Host Activity Monitor - Screenshot 1

Network Interface: Broadcom 802.11g Network Adapter [192.168.1.113] Stop

Active Senders (MAC) | Active Receivers (MAC) | Active Senders (IP) | Active Receivers (IP)

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Broadcom 802.11g Network Adapter
Physical Address	00-21-00-BC-A9-F3
DHCP Enabled	Yes
IPv4 Address	192.168.1.113
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	22 Oktober 2012 16:53:15
Lease Expires	22 Oktober 2012 18:53:15
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1
IPv4 DNS Server	192.168.1.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80:fc0d:26dd:fb6b:ff64%10
IPv6 Default Gateway	
IPv6 DNS Server	

Host	Packets	Traffic
00:21:00:BC:A9:F3	50037	68,9 MB
F8:D1:11:92:C3:6E	31727	2,06 MB
FF:FF:FF:FF:FF:FF	105	13,0 KB
33:33:00:01:00:02	7	1,02 KB
01:00:5E:00:00:01	3	138 bytes
33:33:00:01:00:03	2	168 bytes
D8:75:33:72:30:1E	0	0 bytes
9C:B7:0D:8B:2A:B4	0	0 bytes
44:87:FC:CC:57:6B	0	0 bytes
00:21:00:BC:A9:F3	0	0 bytes
C0:18:85:9A:9E:60	0	0 bytes

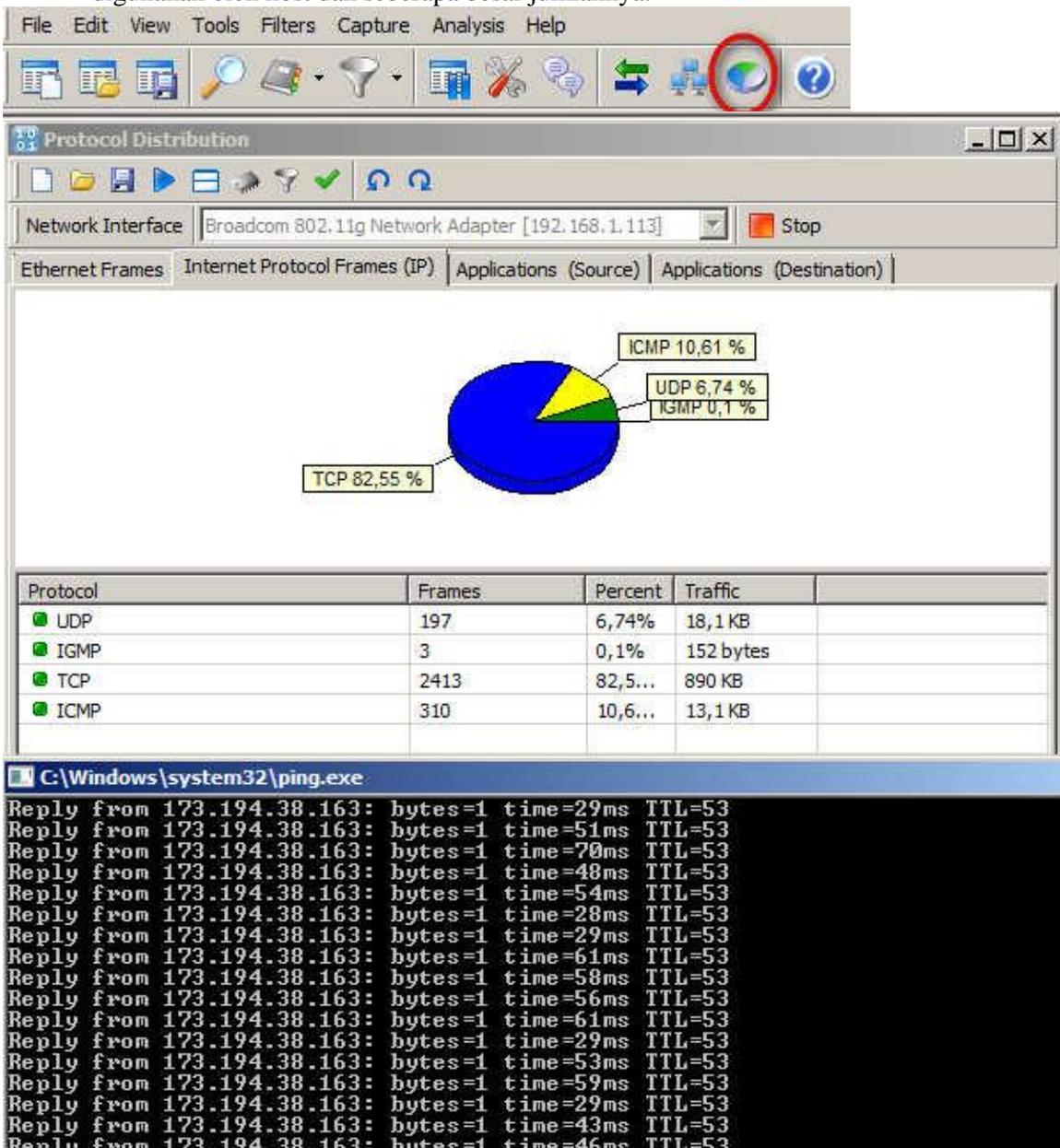
Host Activity Monitor - Screenshot 2

Network Interface: Broadcom 802.11g Network Adapter [192.168.1.113] Stop

Active Senders (MAC) | Active Receivers (MAC) | Active Senders (IP) | Active Receivers (IP)

Host	Packets	Traffic
F8:D1:11:92:C3:6E	64390	87,5 MB
00:21:00:BC:A9:F3	40703	2,64 MB
70:F3:95:81:74:AE	59	4,28 KB
C0:18:85:9A:9E:60	32	2,87 KB
9C:B7:0D:8B:2A:B4	19	1,47 KB
44:87:FC:CC:57:6B	10	783 bytes
D8:75:33:72:30:1E	6	824 bytes
01:00:5E:00:00:01	0	0 bytes
33:33:00:01:00:03	0	0 bytes
FF:FF:FF:FF:FF:FF	0	0 bytes
00:21:00:BC:A9:F3	0	0 bytes

4. Software ini juga memiliki kemampuan untuk melihat apa saja protokol yang digunakan oleh host dan seberapa besar jumlahnya.



ketika melakukan ping terlihat bahwa paket ICMP akan berubah.

Referensi

<http://www.softperfect.com/products/networksniffer>

Penutup

Sekian dulu sedikit penjelasan dan tutorial dalam melakukan monitoring jaringan komputer, mudah kan?? 😊

Pengen coba softwarena?? Silahkan [DOWNLOAD DISINI](#)

Biografi Penulis



Didha Dewannanta. Lahir di Semarang, 05 Mei 1992. Menyelesaikan di SMA Negeri 02 Semarang tahun 2009. Sedang melaksanakan kuliah jenjang sarjana di POLITEKNIK NEGERI SEMARANG angkatan 2009, Jurusan Teknik Elektro, Program Studi D4 Teknik Telekomunikasi, Konsentrasi Jaringan Radio dan Komputer. Telah melakukan sertifikasi MTCRE 1207RE011, CCNA CSCO12276731, JNCIA JPR169784

Contact Person :

didhadewannanta@gmail.com

YM didhadewannanta@yahoo.co.id