Wireshark

Nama Penulis
inungf@ymail.com
http://inungandthenotes.blogspot.com

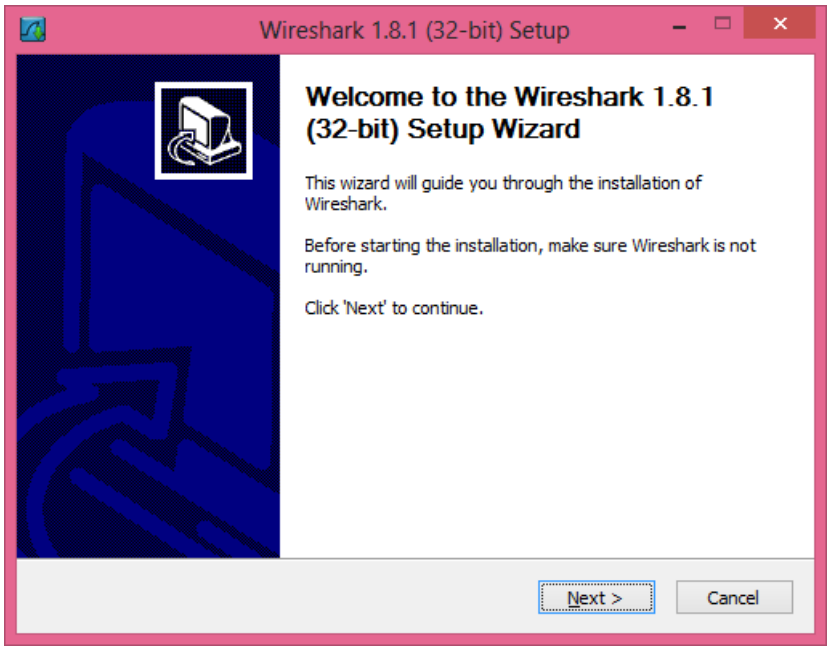
Browsing internet merupakan salah satu kegiatan utama yang kita lakukan di era globalisasi saat ini. Mulai dari melakukan browsing gambar, video,e-mail, dll. Ketika kita melakukan akses apapun, sebenarnya ada *packet* data yang dikirim dan diterima oleh sebuah perangkat komputer dengan internet sehingga apa yang kita browsing dapat kita dapati. Selama kita melakukan koneksi internet disertai dengan browsing data apapun protokol yang dikirim lewat paket data adalah protokol TCP/IP. Contoh lainnya adalah SMTP yang merupakan protokol yang digunakan untuk melakukan komunikasi melalui e-mail. Untuk mengetahui protokol yang lalu lalang di internet, banyak aplikasi yang mampu melakukan analisis paket-paket itu, ada commview, netcat, nethogs, wireshark, dll. Tapi kali ini saya akan membahas tentang wireshark.

WireShark adalah sebuah Network Packet Analyzer. Network Packet Analyzer akan mencoba menangkap" paket-paket jaringan dan berusaha untuk menampilkan semua informasi di paket tersebut sedatail mungkin. Kita bisa mengumpamakan sebuah Network Packet Analyzer sebagai alat untuk memeriksa apa yang sebenarnya sedang terjadi di dalam kabel jaringan, seperti halnya voltmeter atau tespen yang digunakan untuk memeriksa apa yang sebenarnya sedang terjadi di dalam sebuah kabel listrik.

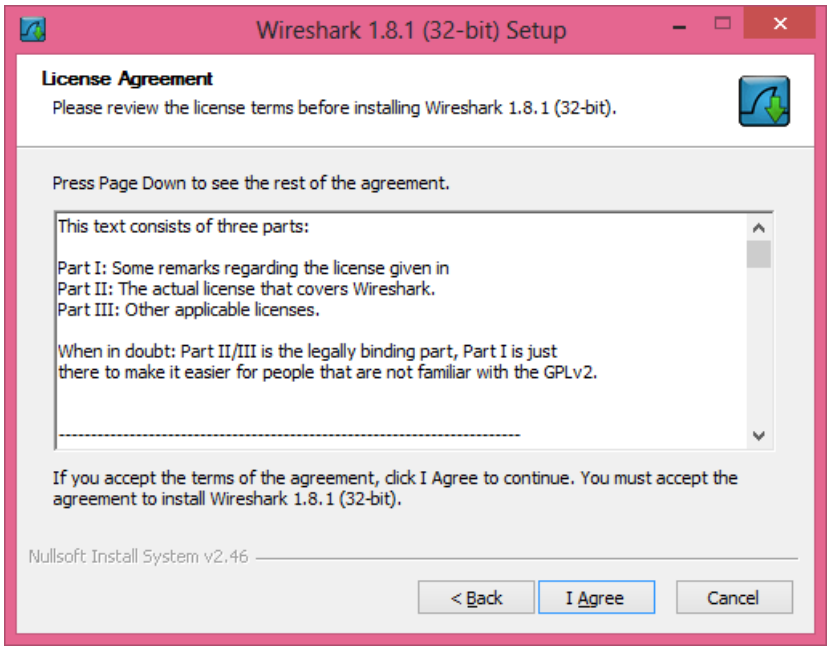
Wireshark banyak digunakan admin jaringan memecahkan troubleshooting di jaringannya, memeriksa keamanan jaringan, men-debug implementasi protokol jaringan dalam software mereka, mempelajari protokol jaringan secara detail banyak juga orang usil yang menggunakannya sebagai sniffer atau "pengendus" data-data privasi di jaringan.

Langkah-langkah instalasinya pun cukup mudah, seperti aplikasi kebanyakan kita tinggal klik "*Next*" dan "*Finish*".

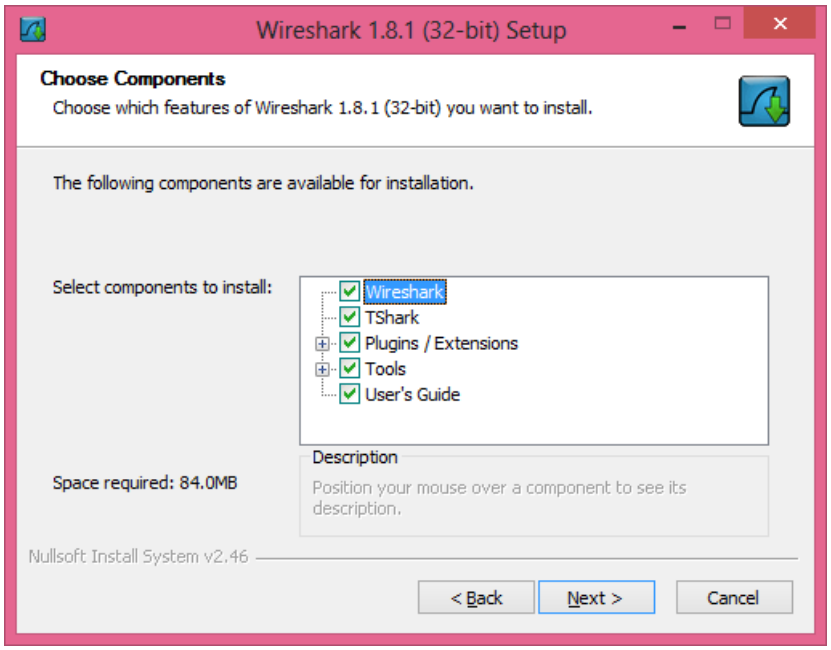
Klik Next,



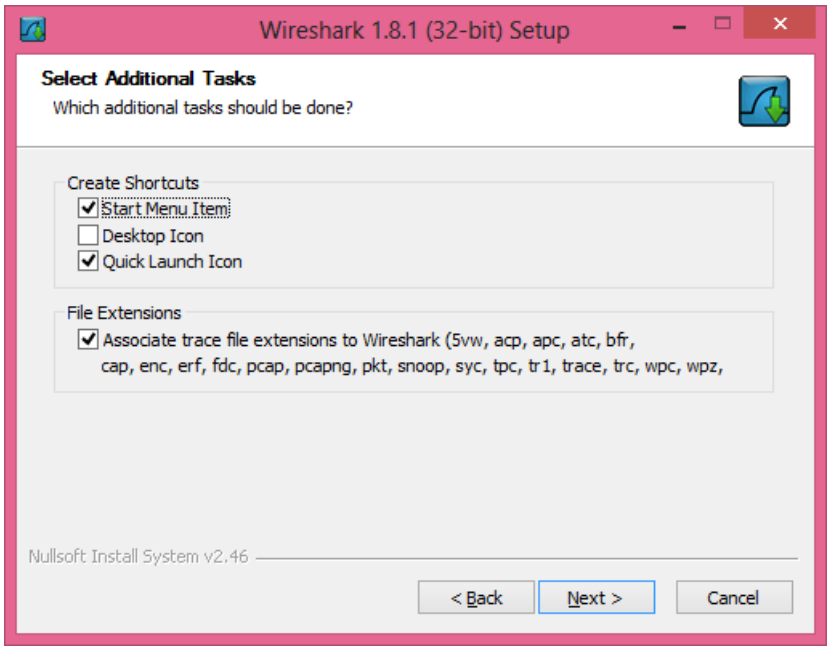
Klik I Agree,



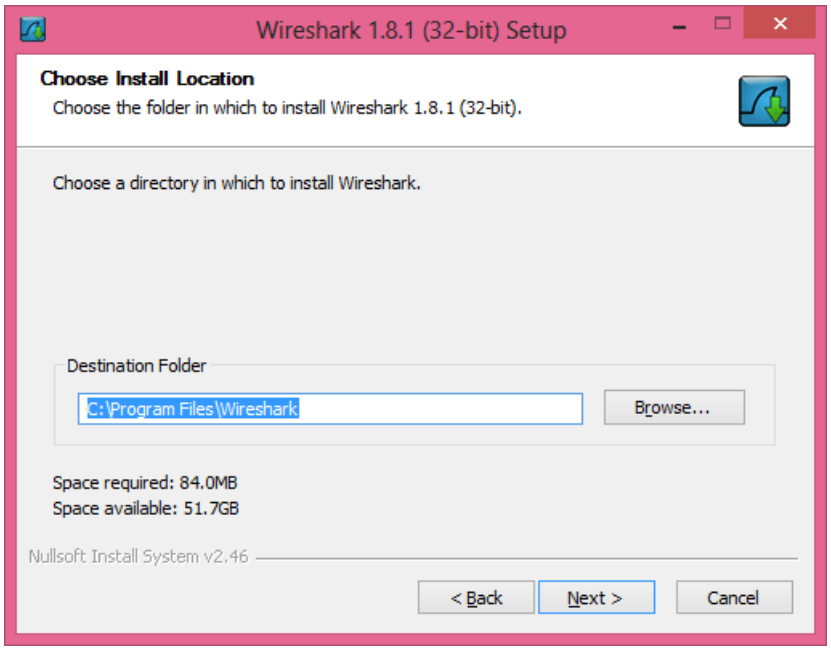
Klik *Next* lagi,



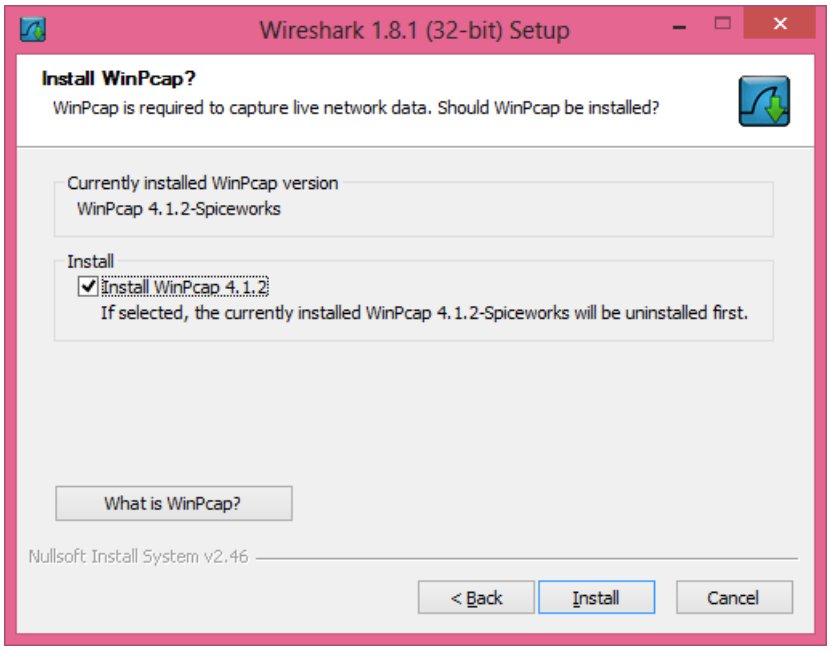
And Next,

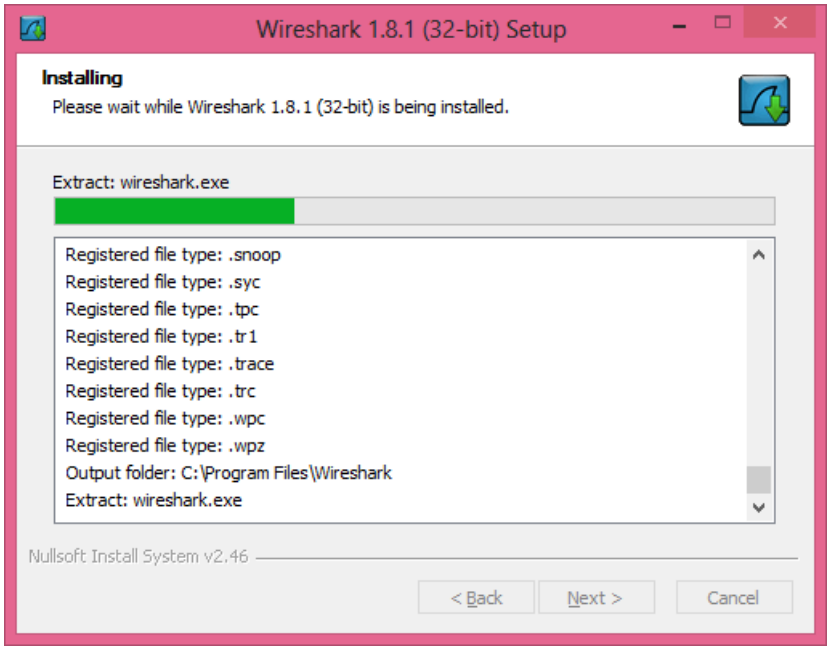


Pilih direktori, lalu *Next*,



Klik Install,

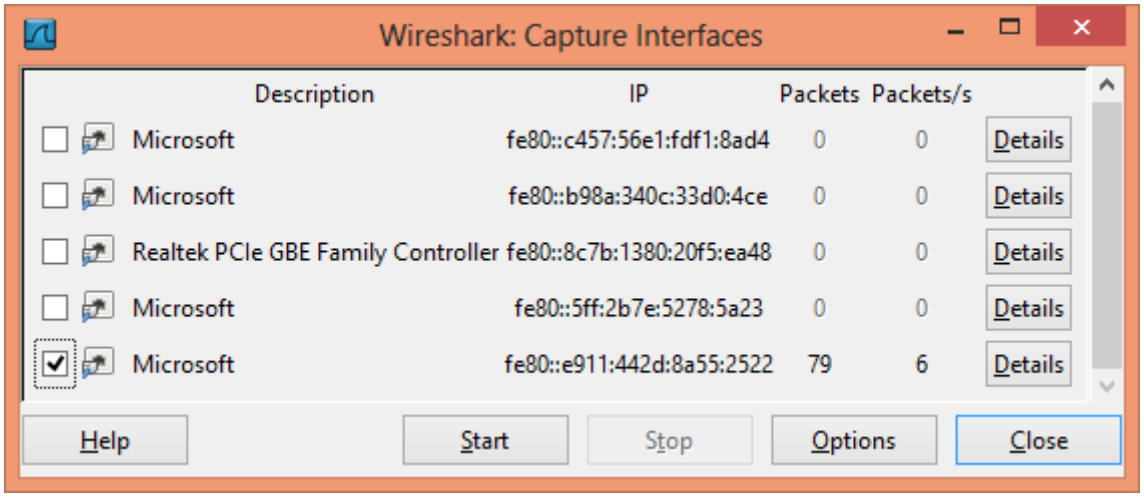


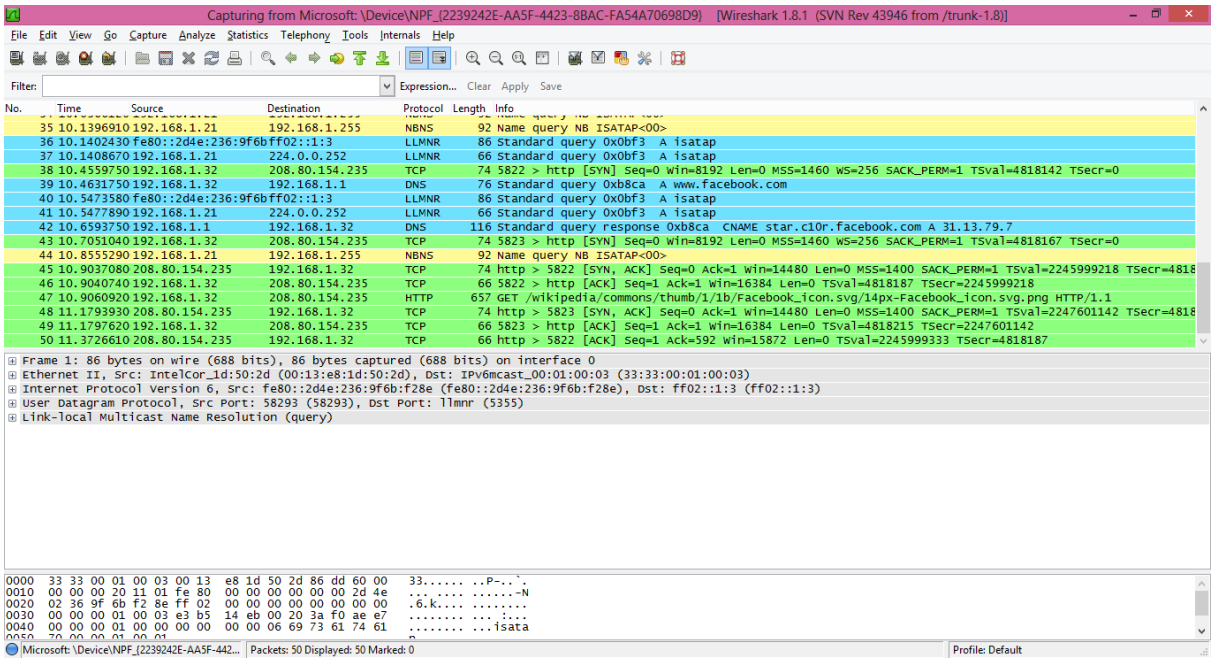


Lakukan kegiatan *Next* lagi dan lagi, jika ada permintaan instal WinPcap, ceklist lalu klik *Instal*. Tunggu proses instalasi selesai dan klik *Finish.*

Setelah instalasi selesai mari kita lihat tampilan dari Wireshark itu seperti gambar di bawah.

Untuk melakukan capture klik icon yang diberi warna merah, lalu pilih adapter yang digunakan untuk koneksi internet.



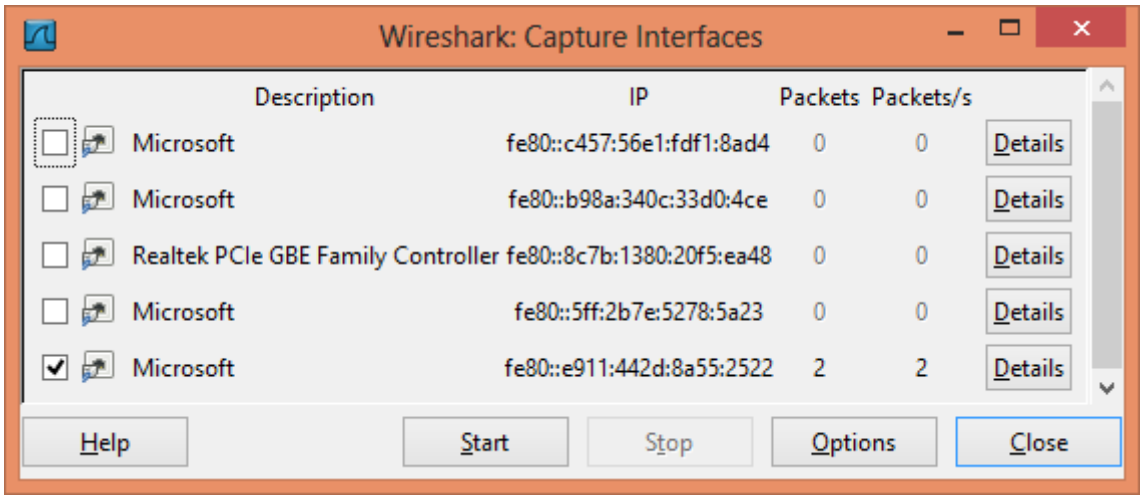


Klik *Start* lalu akan muncul paket-paket data yang berisi protokol-protokol jaringan yang sedang lalu-lalang antara laptop dan internet.

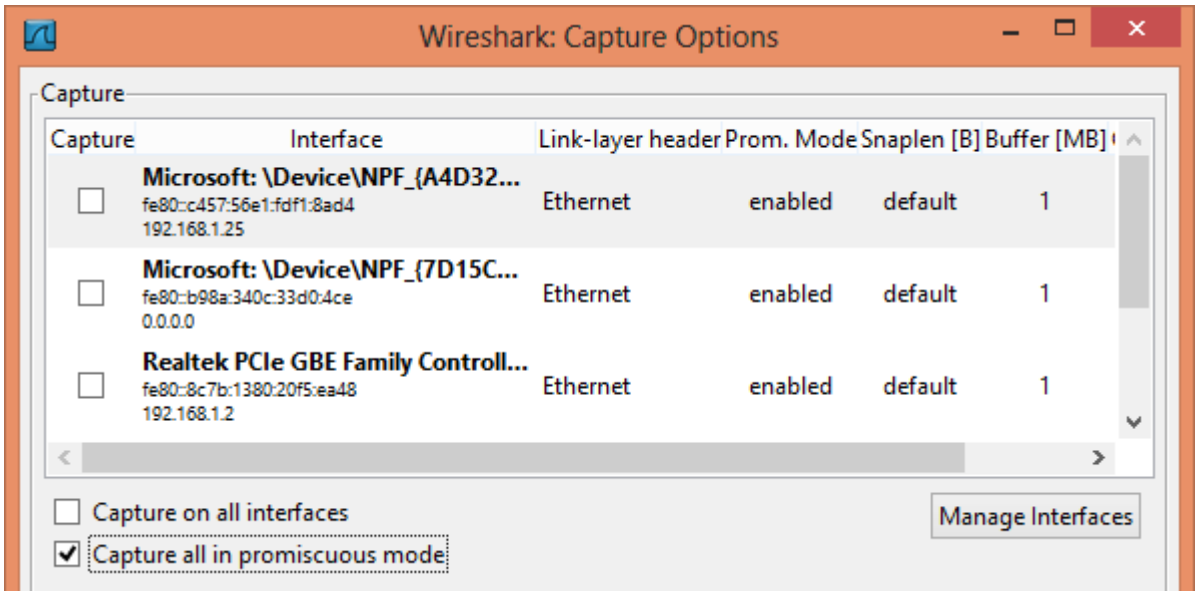
SNIFFING

Salah satu fungsi dari wireshark adalah *sniffing* atau lebih dikenal dengan proses penyadapan. Tentu saja yang disadap adalah *password* dari seorang *user,* namun dengan syarat si *user* ini harus terkoneksi dengan satu jaringan dengan si *sniffer* ini. Wireshark merupakan salah satu aplikasi yang mampu menyadap *user* dan *password* dengan baik pada LAN card, namun kali ini akan dicoba diterapkan dengan WLAN. Langkah-langkahnya seperti berikut.

Pertama-tama buka aplikasi Wireshark, lalu pilih Capture dan pilih interface yang terkoneksi dengan jaringan.

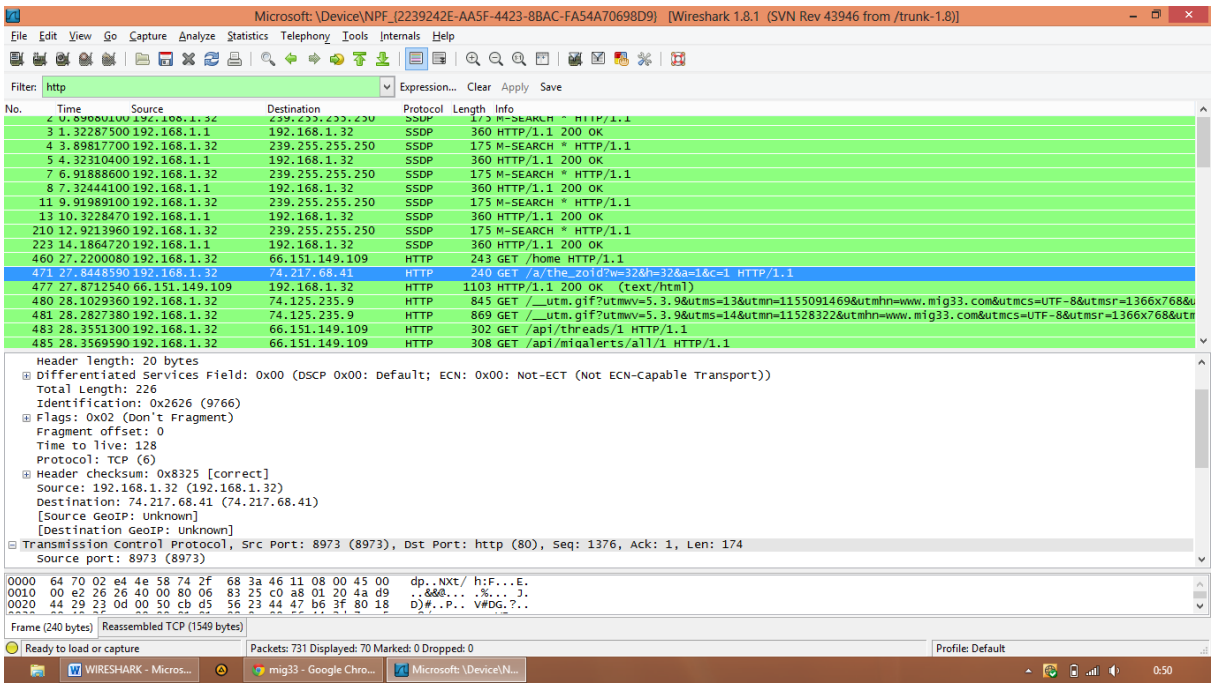


Lalu setelah pilih Option dan pastikan Capture packet in promecious dalam status ON.



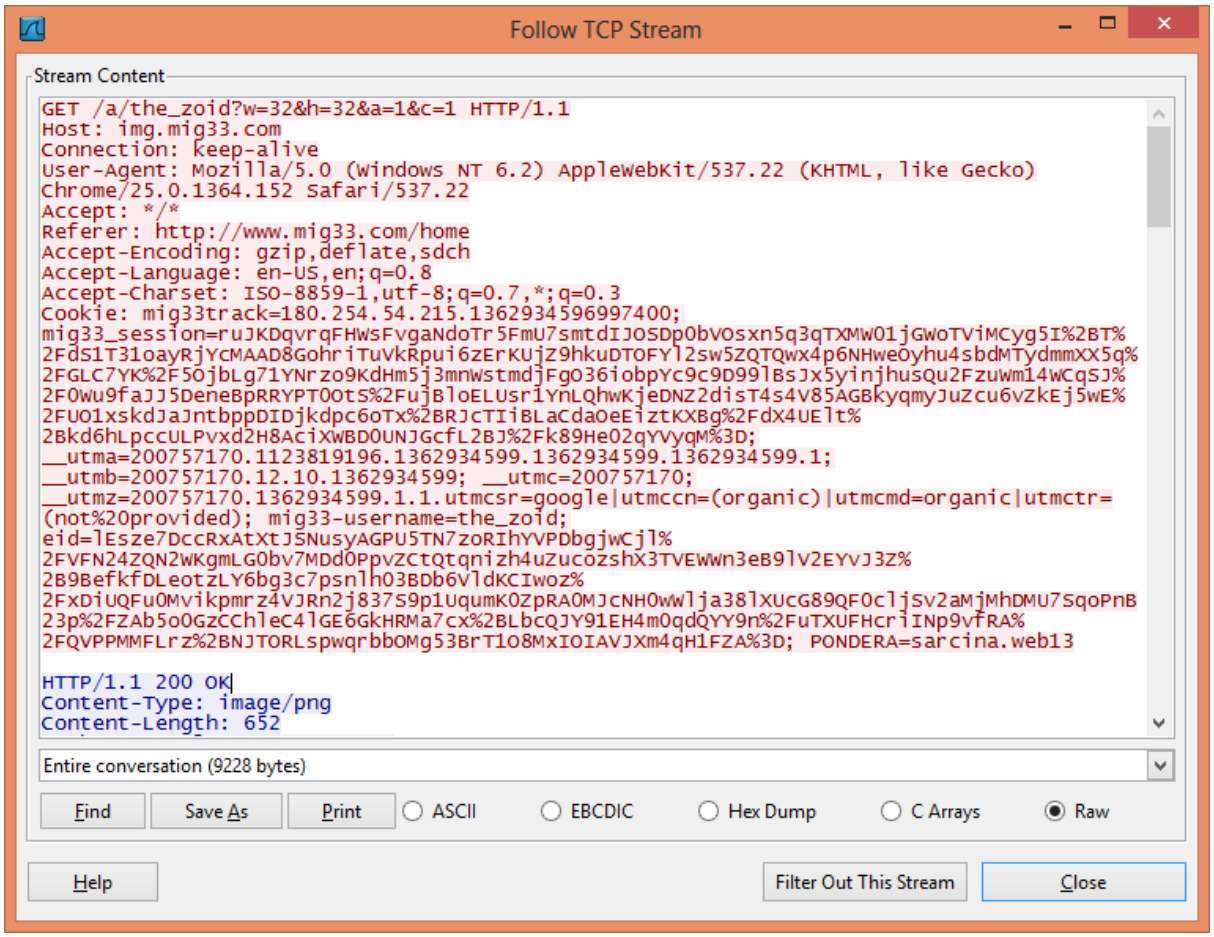
Pertama-tama buka website yang akan di-*sniffing*, di sini saya menggunakan contoh www.mig33.com. Isikan *user* dan *password*. Setelah itu LOGIN pada website tersebut.

Setelah LOGIN maka akan banyak paket yang masuk ke dalam wireshark, jika merasa sudah cukup banyak klik STOP capture (Alt + E). Untuk lebih meringkasnya pada kolom Filter ketikkan “http”.



Setelah itu pilih protokol “http” yang bergaris biru di atas maka akan didapat informasi

seperti di bawah. Yang menampilkan si *user* yang telah LOGIN tadi berada pada alamat website apa dan dengan nama *user* apa, namun *password* yang diharapkan tidak dapat dimunculkan di sini.



Selamat Mencoba. Terimakasih.

Biografi Penulis

Biografi Penulis

Ainul Fuad Farhan. Mahasiswa Politeknik Negeri Semarang Jurusan Teknik Elektro, Prodi D4 Telekomunkasi. Alumni SMA N 1 JUWANA tahun 2010.

Contact Person :

Blog : http://inungandthenotes.blogspot.com

Facebook : lukazkazx@yahoo.com

Twitter : @inungf