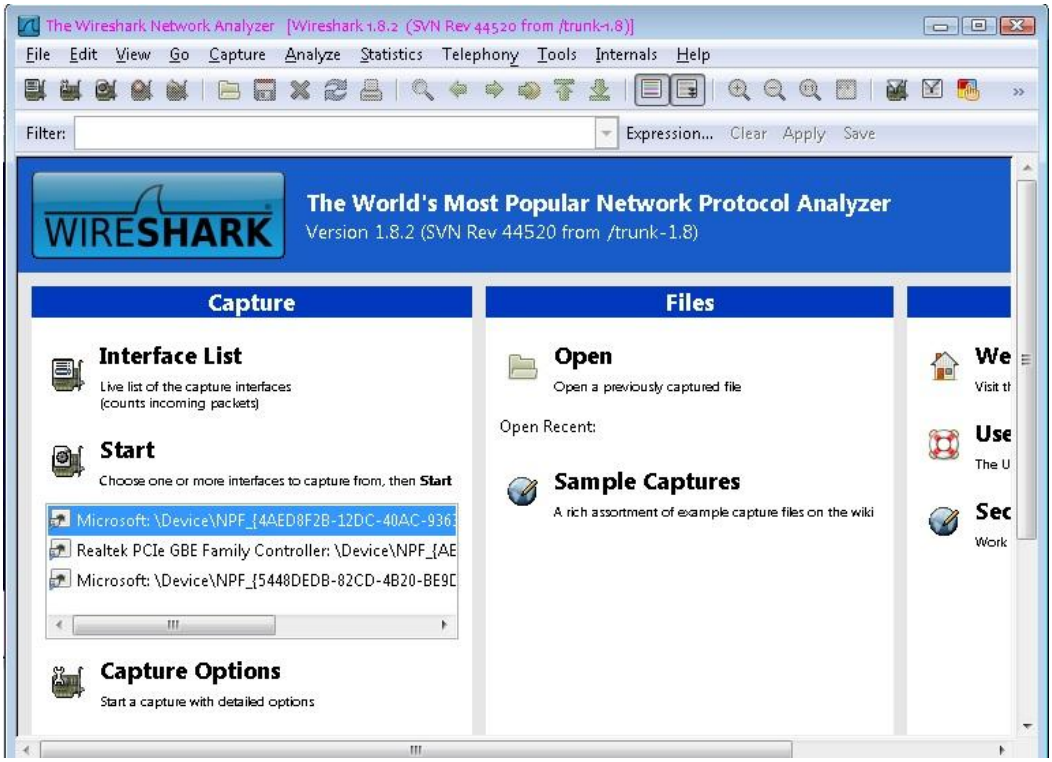
Mengintip Proses Request Data dengan Wireshark

Sekar Langit
Sekarlangit9312@gmail.com
http://theflowerofsky.blogspot.com

Dalam kehidupan sehari-hari anak muda jaman sekarang tentunya lekat sekali dengan teknologi yang bernama internet. Apapun yang kita cari dari mulai bahan kuliah, game-game terbaru, film-film box office, lagu yang sedang populer, resep masakan, sampai denah lokasi bisa kita temukan dengan mudah disana. Maka tidak heran kalau cara mengumpulkan informasi dengan mencari referensi di perpustakaan konvensional sudah mulai agak terlupakan dan digantikan dengan browsing di internet.

Tapi apakah kita pernah berpikir proses apa saja yang terjadi dalam “cloud” saat kita mencoba mengakses sebuah website di internet ??
Nah kali ini saya akan mengupas perjalanan data dari proses requesting sampai data tersebut muncul di layar komputer kita. Software yang saya gunakan adalah wireshark.

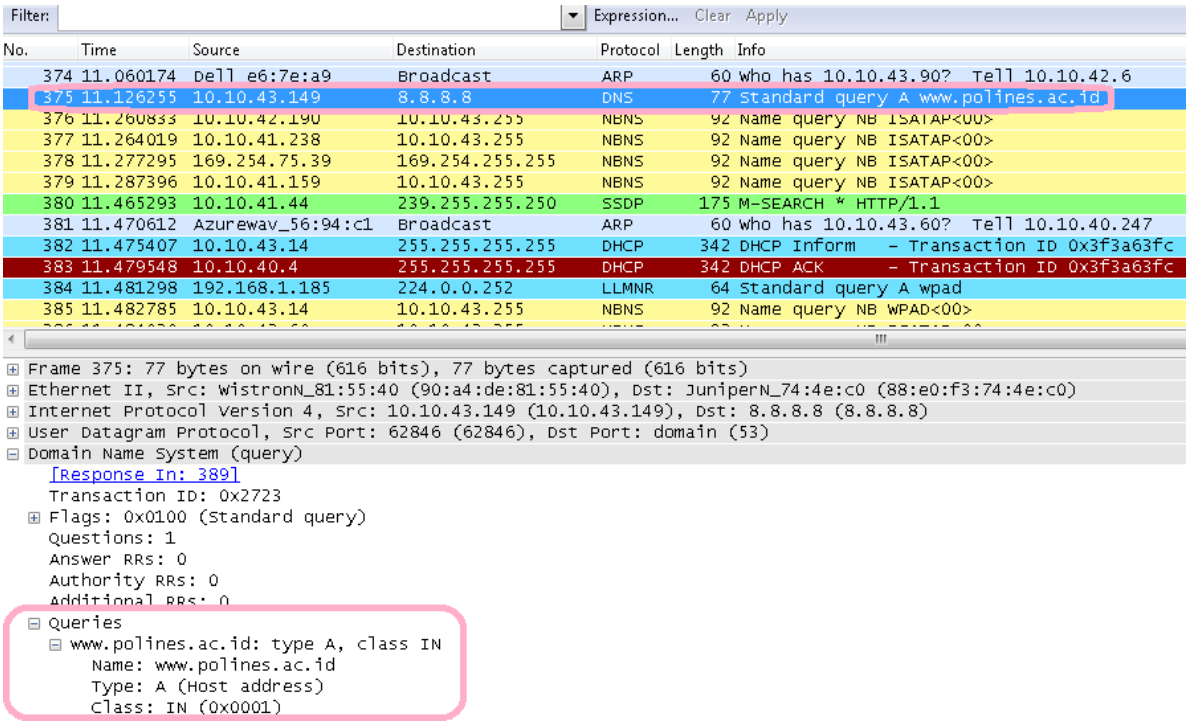
1. Jalankan aplikasi wireshark di komputer kita.



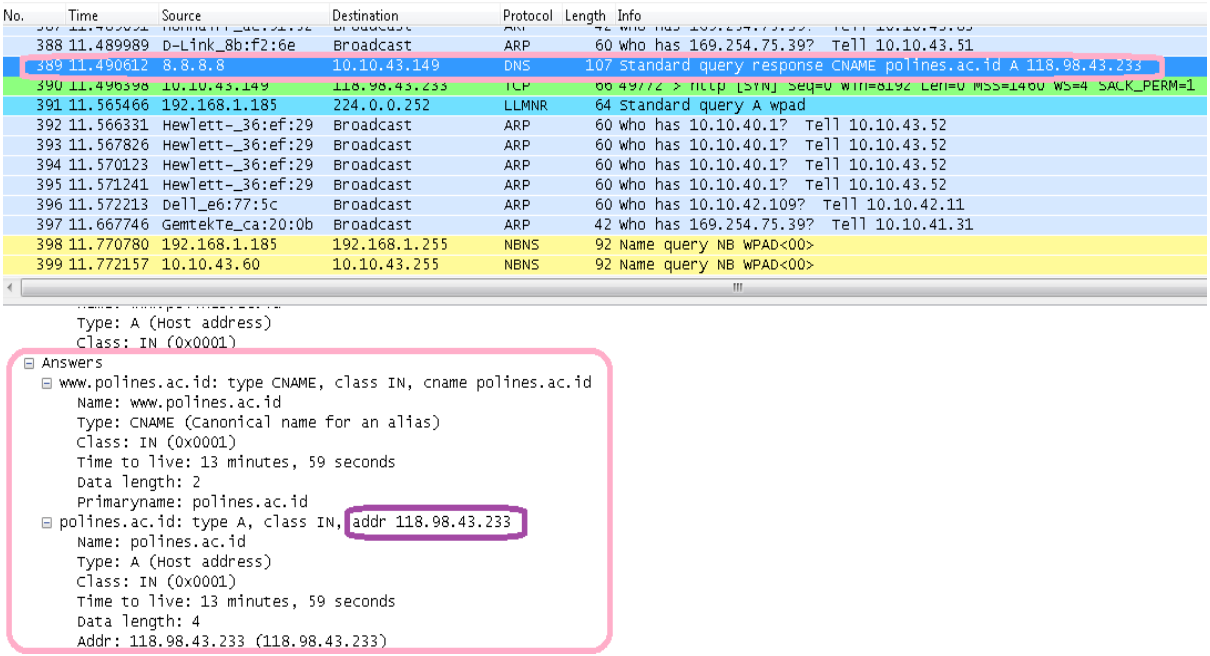
2. Klik ‘interface list’ lalu pilih interface yang aktif (bisa dilihat dari angka yang muncul di sebelah nama interface, jika 0 berarti tidak aktif.)

3. Setelah itu buka web browser dan coba mengakses sebuah situs. Sebagai contoh saya akan mencoba mengakses situs kampus saya yaitu www.polines.ac.id

4. Lihat paket yang tercapture di wireshark, disitu terlihat bahwa komputer saya dengan IP address 10.10.43.149 merequest alamat www.polines.ac.id. Karena komputer saya belum mengetahui alamat IP dari DNS tersebut maka terlebih dahulu request akan dikirimkan ke DNS server untuk mengetahui alamat IP dari website www.polines.ac.id.



5. DNS server akan mengirimkan jawaban berupa IP address dari website www.polines.ac.id, yaitu 118.98.43.233

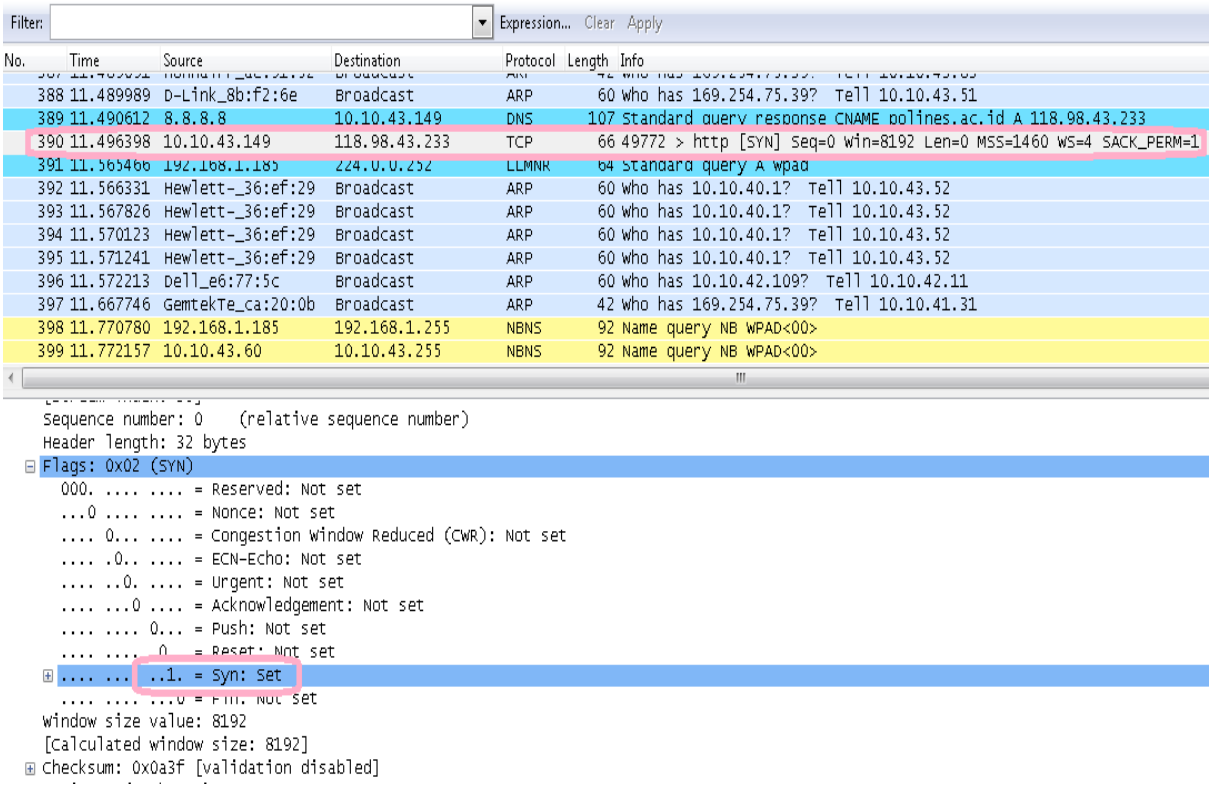


6. Setelah mengetahui IP address dari www.polines.ac.id, maka barulah komputer saya dengan alamat IP 10.10.43.149 akan merequest ke alamat IP website yaitu 118.98.43.233 dengan menggunakan protokol TCP.

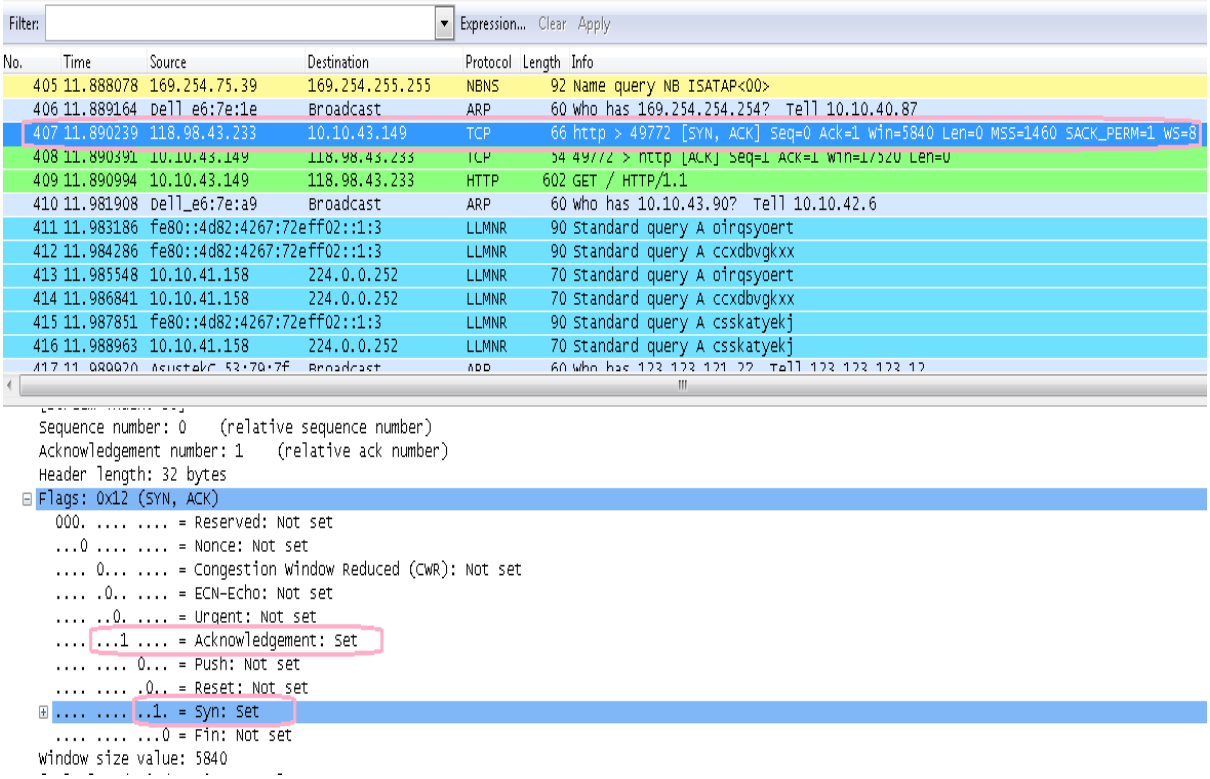
Protocol TCP ini adalah protocol yang terletak pada lapisan transport yang digunakan untuk melakukan browsing. Tapi sebelumnya saya akan sedikit menjelaskan tentang flag-flag pada TCP serta fungsi dari flag-flag yang ada pada program Wireshark.

- ✓ Flag URG (urgent) berfungsi untuk mengidentifikasi bahwa bagian dari TCP mengandung data yang sangat penting.
- ✓ Flag ACK (acknowledgment) berfungsi untuk mengetahui apakah data yang dikirimkan sudah diterima atau belum di komputer client.
- ✓ Flag PSH (push) berfungsi untuk mengindikasi isi dari TCP yang diterima dikomputer client. Jika PSH bernilai 1 maka data tidak boleh satu byte pun hilang, jika hilang maka data akan dikirim ulang.
- ✓ Flag RST (reset) berfungsi untuk mengidentifikasi jika koneksi yang dibuat gagal. Untuk sebuah koneksi TCP yang sedang berjalan (aktif), sebuah segmen dengan flag RST diset ke nilai 1 akan dikirimkan sebagai respons terhadap sebuah segmen TCP yang diterima yang ternyata segmen tersebut bukan yang diminta, sehingga koneksi pun menjadi gagal.
- ✓ Flag SYN berfungsi untuk mengindikasi bahwa segmen TCP yang bersangkutan mengandung Initial Sequence Number (ISN). Selama proses pembuatan sesi koneksi TCP, jika melakukan request maka akan memberikan nilai SYN bernilai 1.
- ✓ Flag FIN (Finish) berfungsi untuk menandakan bahwa pengirim segmen TCP telah selesai dalam mengirimkan data dalam sebuah koneksi TCP. Ketika sebuah koneksi TCP akhirnya dihentikan (akibat sudah tidak ada data yang dikirimkan lagi), setiap host TCP akan mengirimkan sebuah segmen TCP dengan flag FIN diset ke nilai 1.

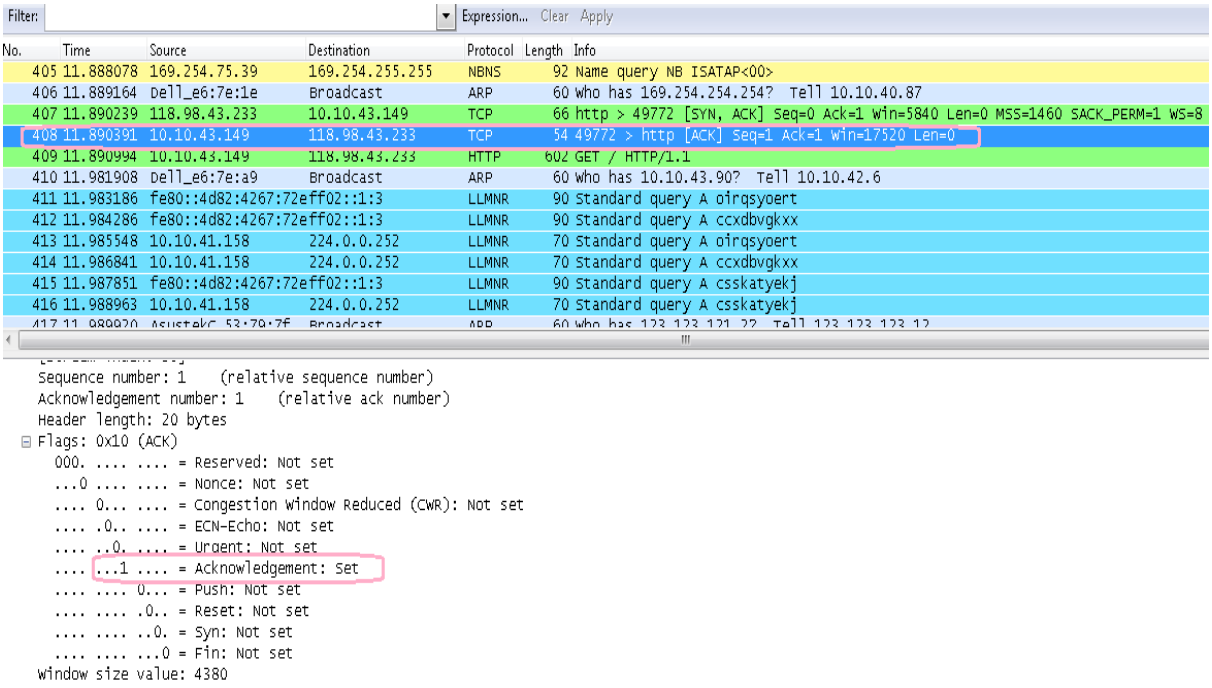
7. Sekarang saya akan menjelaskan proses ‘three way handshake’. Pada bagian ini komputer saya dengan alamat IP 10.10.43.149 mengirimkan request ke website polines dengan alamat IP 118.98.43.233 yang ditunjukkan dengan nilai ‘1’ pada flag SYN.



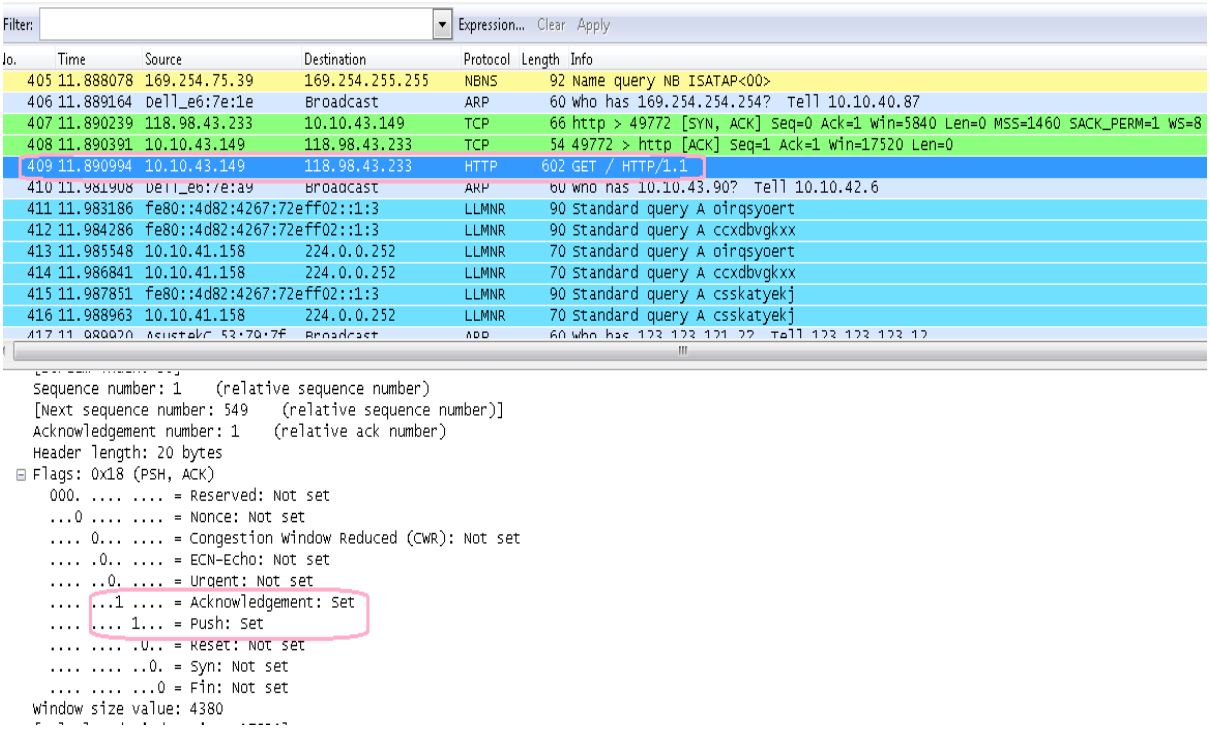
8. Setelah itu server dari 118.98.43.233 membalas request dengan mengirimkan flag ‘ACK’ bernilai ‘1’ yang artinya menyatakan persetujuan akses website dan mengkonfirmasi apakah tanda persetujuan telah sampai di komputer client. Terlihat pada gambar di bawah flag ‘ACK’ dan flag ‘SYN’ bernilai ‘1’.



9. Client yang disini berarti adalah komputer saya dengan alamat IP 10.10.43.149 membalas dengan mengirimkan flag 'ACK' bernilai '1' yang berarti memberitahukan bahwa data telah diterima di komputer client. Inilah akhir dari proses three way handshake yang menghasilkan output terbangunnya hubungan antara komputer saya dengan komputer server website polines.



10. Akhirnya barulah komputer server mengirimkan data melalui protokol HTTP. Seperti yang terlihat pada gambar di bawah, flag yang aktif adalah flag ACK dan flag PSH. Flag PSH berarti mengindikasi isi dari TCP yang diterima dikomputer client, jika PSH bernilai 1 maka data tidak boleh satu byte pun hilang, jika hilang maka data akan dikirim ulang.



Nah begitulah proses browsing yang biasa kita lakukan sehari-hari. Selama ini mungkin kita hanya duduk di depan komputer dan menunggu proses loading selesai tanpa tahu proses yang terjadi sebenarnya. Dan ternyata prosesnya tidak sesimple yang kita bayangkan.

Biografi Penulis

Sekar Langit. Menyelesaikan pendidikan Sekolah Dasar di SD Muktiharjo Kidul 02 Semarang, SMP di SMP PL Domenico Savio Semarang, dan SMA di SMAN 5 Semarang. Sekarang sedang menempuh pendidikan jenjang D4 di Politeknik Negeri Semarang jurusan Teknik Elektro dan prodi Teknik Telekomunikasi.