# TUTORIAL DASAR WIRESHARK


## Apa itu 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.

Dulunya, tool-tool semacam ini sangatlah mahal harganya, dan biasanya dengan embel-embel hak cipta. Namun dengan adanya WireShark, kita akan sangat dimudahkan. Makanya tidak sedikit yang bilang bahwa WireShark adalah salah satu tool gratis (dan bahkan open source) terbaik untuk menganalisa paket jaringan

## Kenapa kita perlu menganalisa paket-paket jaringan?

Ada beberapa contoh penggunaan WireShark:

- Admin sebuah jaringan menggunakannya untuk troubleshooting masalah-masalah di jaringannya
- Teknisi keamanan jaringan menggunakannya untuk memeriksa keamanan jaringan
- Pengembang software bisa menggunakannya untuk men-debug implementasi protokol jaringan dalam software mereka
- Banyak orang memakainya untuk mempelajari protokol jaringan secara detail
- Banyak juga orang usil yang menggunakannya sebagai sniffer atau “pengendus” data-data privasi di jaringan.

Masih ada banyak fitur dan kelebihan WireShark ini, diantaranya:

- Tersedia buat Linux dan Windows
- “Menangkap” / Capture paket data secara langsung dari sebuah network interface
- Mampu menampilkan informasi yang sangat detail mengenai hasil capture tersebut
- Bisa Import dan Export hasil capture dari atau ke komputer lain
- Pencarian paket dengan berbagai macam kriteria filter.
- Bisa membuat berbagai macam tampilan statistika, dan masih banyak lagi.

## Di mana kita bisa mendapatkan WireShark?

Untuk mendapatkan versi terbaru dari WireShark ini, kita bisa memeriksa di www.WireShark.org/download.html. di sini nantinya akan ada banyak mirror yang menyeidiakan download link buat WireShark ini. Pastikan untuk mendapatkan versi paling baru.

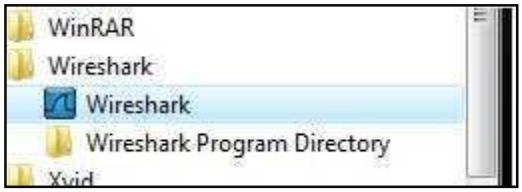
## Instalasi WireShark

Untuk instalasi WireShark sepertinya tidak memerlukan perlakuan tambahan apa-apa, apabila kita tidak yakin dengan setingan manual, coba saja instal dengan setingan default installer.

Pada saat instalas WireShark, kita juga akan diminta penginstall WinPcap, apabila tidak mempunyai WinPcap, nanti kita tidak akan bisa meng-capture menggunakan WireShark, namun masih bisa membuka hasil capture-an, oleh karena itu install saja WinPcap.

## Menjalankan WireShark

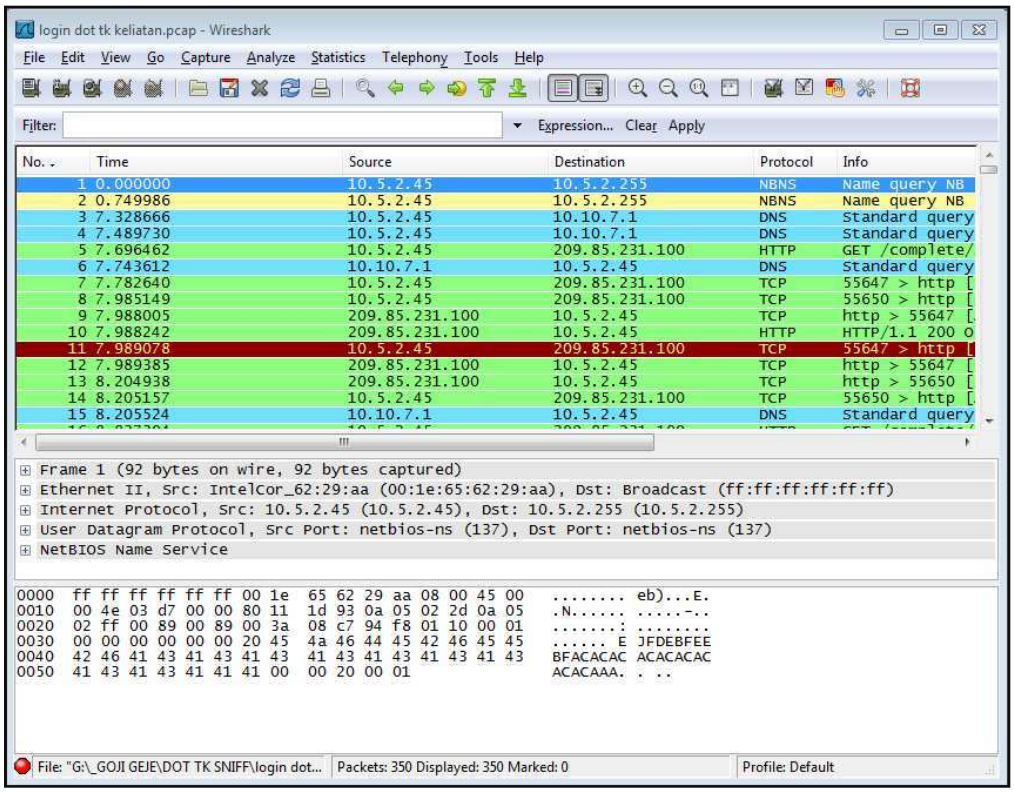
Setelah menginstall WireShark, mari kita mulai menjalankan WireShark. Jalankan saja lewat shortcut yang ada di start menu seperti ini:




Setelah itu akan muncul Splash Screen dari WireShark yang sedang me-load komponen-komponen yang diperlukan


Berikut ini adalah contoh tampilan WireShark yang sedang meng-capture paket-paket jaringan:

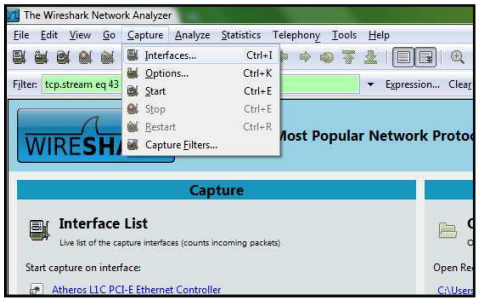
WireShark ketika sedang ‘beraksi’ ☺



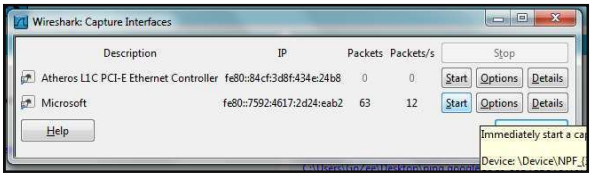

## Meng-Capture Paket dengan WireShark

Kita bisa memulai capture dengan langkah-langkah berikut ini:

Pada menu **Capture → Interfaces**

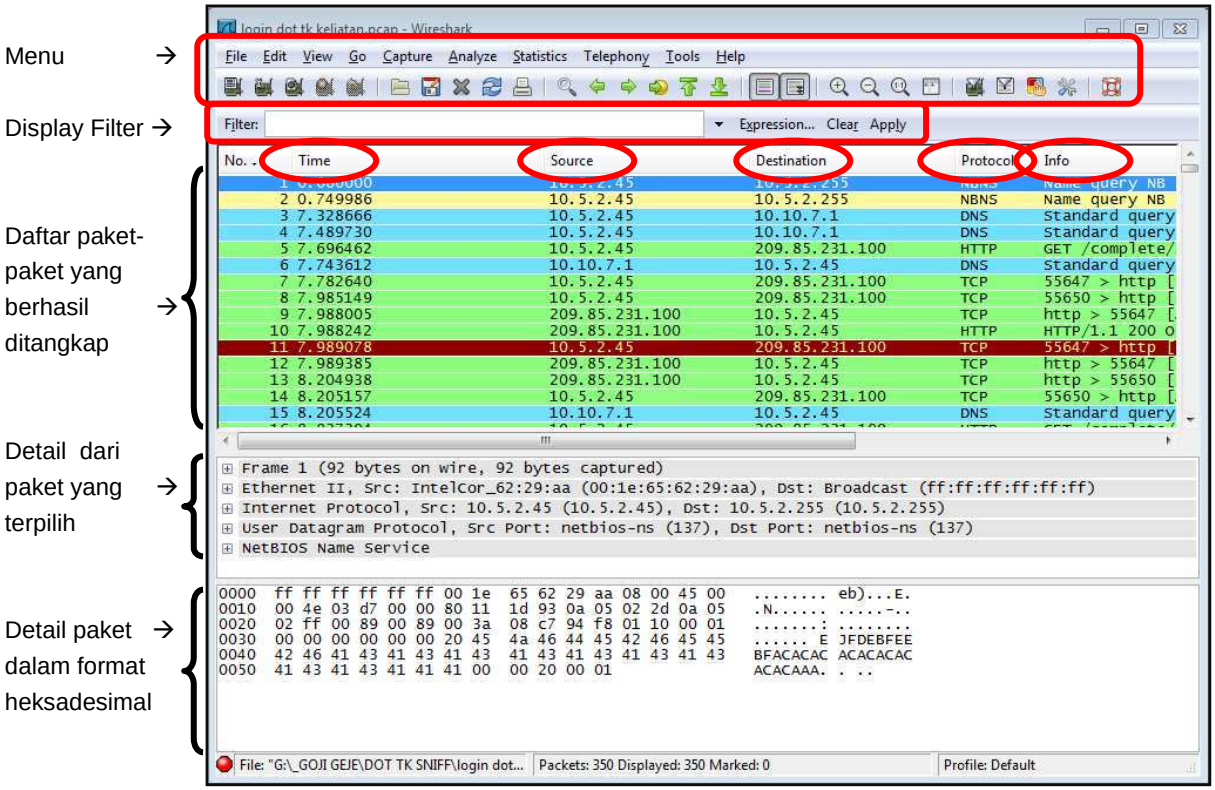



Kemudian kita akan dihadapkan dengan tampilan untuk memilih interface yang akan kita capture nantinya, seperti ini:




Pilih interface yang akan kita capture, di tutorial ini saya contohkan untuk meng-capture Inteface “**Microsoft**”, klik tombol “**Start**” pada bagian kanan interface tersebut.

Setelah itu, WireShark akan segera meng-capture paket-paket di dalam jaringan dan menampilkannya dengan segera. Berikut ini adalah tampilan utama WireShark saat bekerja meng-capture paket-paket data jaringan.




**Menu** → Di sini kita bisa bernavigasi antar menu-menu yang tersedia di WireShark.

**Display Filter** → Sebenarnya adalah sebuah kolom, kita akan mengisinya dengan sintaks-sintaks untuk memfilter (membatasi) paket-paket apa saja yang bakalan ditampilkan pada list paket.

**Daftar Paket** → Di sini akan ditampilkan paket-paket yang berhasil ditangkap oleh WireShark, berurutan mulai dari paket pertama yang ditangkap, dan seterusnya.

**Detail Paket** → Sebuah paket tentunya membawa informasi tertentu yang bisa berbeda-beda antar paketnya, di sini akan ditampilkan dari detail paket yang terpilih pada Daftar paket di atasnya.

**Detail Heksa** → Detail paket yang terpilih akan ditampilkan dalam bentuk heksa, terkadang akan lebih mudah bagi kita mendapatkan informasi dari bagian ini.

Pada daftar bagian Daftar Paket, terdapat kolom-kolom seperti berikut ini:

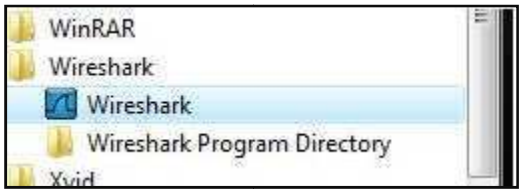
- Time : Menampilkan waktu saat paket tersebut tertangkap
- Source : Menampilkan ip sumber dari paket data tersebut
- Destination : Menampilkan ip tujuan dari paket data tersebut
- Protocol : Menampilkan protokol apa yang dipakai sebuah paket data
- Info : Menampilkan informasi mendetail tentang paket data tersebut.

## Mencoba Meng-Capture Paket Data Protokol HTTP

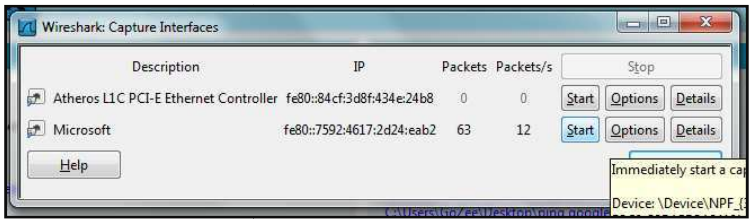
Berikutnya kita akan mencoba meng-capture paket data yang ditransmisikan ketika kita sedang membuka sebuah halaman web atau paket data yang melewati protokol HTTP.

Ikuti langkah-langkah berikut ini:

- Jalankan WireShark



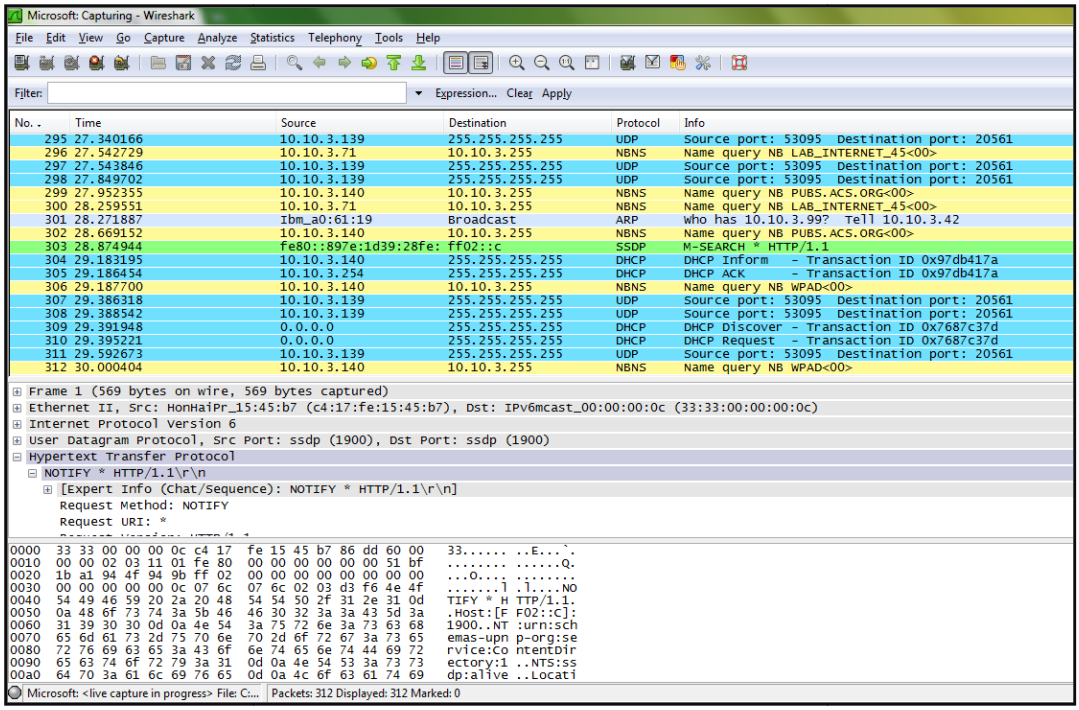

- Pilih interface jaringan yang akan kita gunakan untuk mengakses halaman web nanti, di sini saya memilih interface "**Microsoft**", yang mana interface ini adalah interface Wireless Network yang drivernya masih asli dari Windows (karena saya menggunakan Windows 7, yang sudah bisa langsung mengenali kartu jaringan saya ☺), Interface wireless ini bisa saja bernama lain di masing-masing komputer.




Klik button "**Start**" di sebelah interface "**Microsoft**" / Interface jaringan yang akan kita tangkap paket datanya.

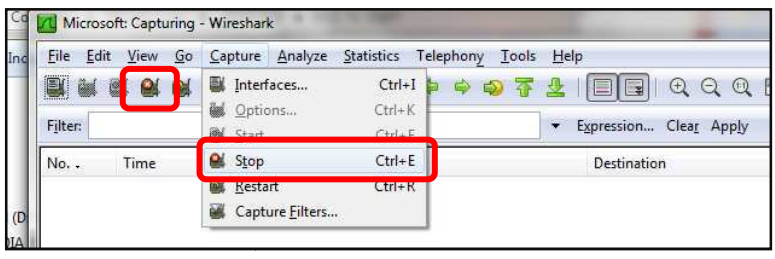
- Buka browser kita, lalu bukalah salah satu situs, terserah situs apa. Google boleh, Yahoo boleh, facebook juga boleh ☺
  Kebetulan saya akan login ke account dot.tk saya, saya buka http://www.my.dot.tk di browser saya

- Nah, selanjutanya begitu kita me-load halaman my.dot.tk ini, pada WireShark juga akan langsung tertampil paket-paket data yang tertangkap, seperti gambar di bawah ini

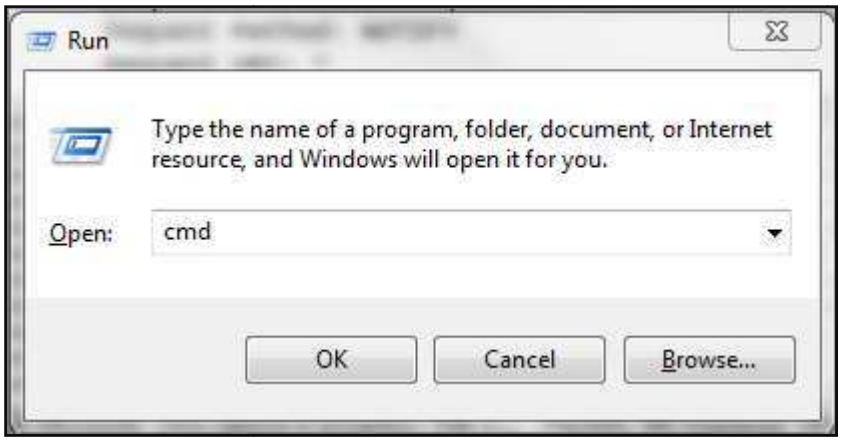



- Nah, mumpung sudah nyampe di dot.tk, maka sekalian saya login aah.. ☺ Saya masukin username saya, kemudian sekalian passwordnya, kita lihat, apakah si WireShark ini nantinya bisa nangkap username dan password saya ini ☺

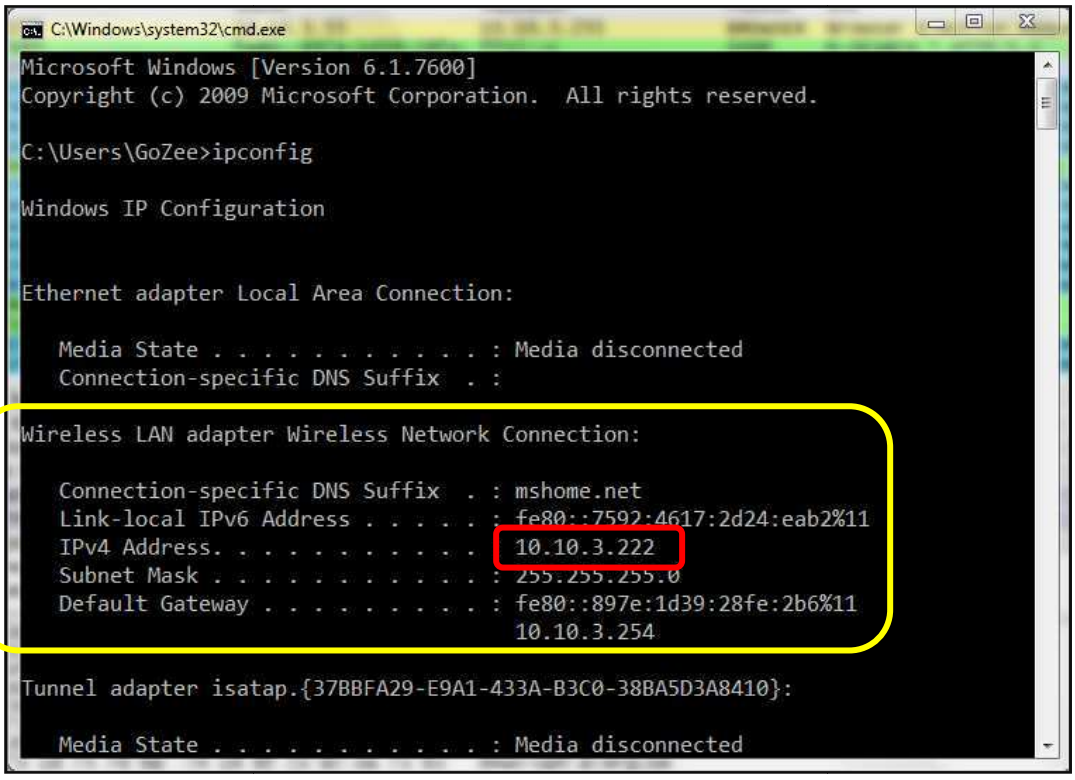

- Kemudian setelah berhasil login dan masuk, kita hentikan capture kita, lewat menu **Capture → Stop**, atau dengan button **Stop Capture**



- Kemudian kita lihat alamat IP komputer kita untuk memastikan. Buka Command Prompt, Caranya, tekan tombol **Windows + R**, kemudian akan mucul kotak dialog seperti ini:
  Ketikkan **cmd** kemudian tekan tombol **OK**.




- Akan muncul jendela console Command Prompt, di console, ketikkan **ipconfig** lalu tekan tombol **Enter**, akan keluar hasi seperti ini:




  Terlihat konfigurasi Adapter Wireless LAN kita, di mana IPv4 kita ditunjukkan dengan kotak merah, yaitu **10.10.3.222**
  Catat, kalau perlu hafalkan ☺

- Selanjutnya, kita lihat IP dot.tk, caranya sama, di console Command Prompt kita masukkan perintah Ping

Ketikkan → **ping**[spasi]**my.dot.tk**
Akan mucul hasil seperti berikut ini:

```
C:\Users\GoZee>ping my.dot.tk

Pinging webapp.dot.tk [217.115.151.99] with 32 bytes of data:
Request timed out.
Request timed out.
```

(Meskipun timeout, tapi paling nggak kita sudah bisa mengetahui alamat IP my.dot.tk → **217.115.151.99** ☺)

- Nah, kita telah mendapatkan alamat IP komputer kita dan alamat IP my.dot.tk
  IP kita → **10.10.3.222**
  IP my.dot.tk → **217.115.151.99**

- Kita lihat hasil capture di WireShark, terlihat daftar paket-paket yang sangat banyak, karena WireShark ini menangkap paket apapun yang terdeteksi di jaringan, karena itu, kita akan menyaring hanya paket-paket yang berkaitan dengan my.dot.tk saja yang akan kita tampilkan.
  Caranya adalah dengan menggunakan filter, seperti ini:

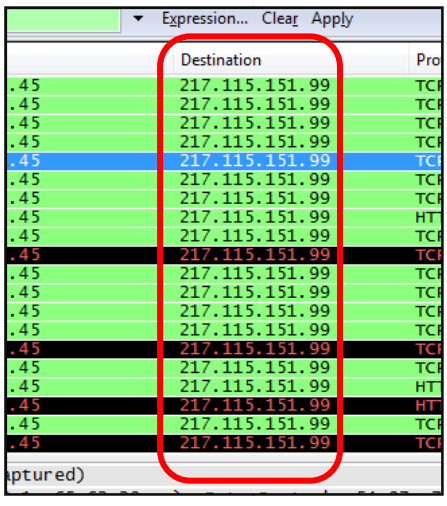
  Dalam kasus ini kita akan menganalisa paket-paket yang menuju ke my.dot.tk, berarti kita akan memfilter paket-paket yang menuju ke IP my.dot.tk

  Untuk menampilkan paket-paket dengan IP tujuan tertentu, kita masukkan sintaks ini ke filter:

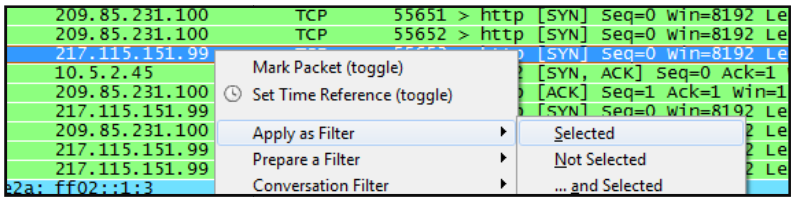
  **ip.dst==217.115.151.99** kemudian tekan Enter

  Keterangan: ip.dst → Destination IP / IP tujuan

  Maka di daftar paket hanya akan ditampilkan alamat-alamat IP dengan tujuan 217.115.151.99 saja, seperti ini:



Ada juga cara lain yang lebih mudah, dengan mouse, **klik kanan** IP 217.115.151.99 yang berada di **kolom Destination** (Ingat, harus di kolom Destination), kemudian pilih **Apply as Filter → Selected**, seperti ini



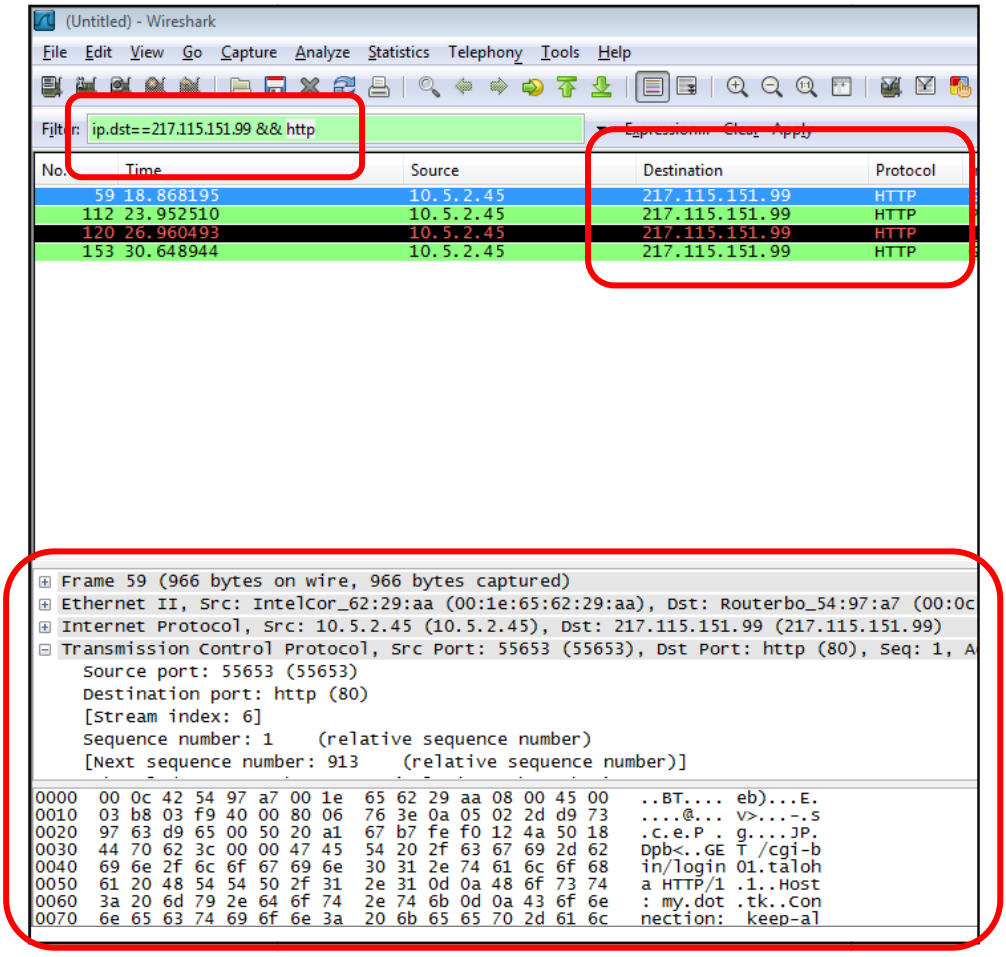

- Nah, kita sudah mendapatkan paket-paket yang menuju ke 217.115.151.99, namun kita lihat, ternyata masih sangat banyak ya ☹
  Ingat bahwa kita akan mencoba melihat paket yang melalui protokol HTTP, karena itu, kita akan coba filter sekali lagi.

  Kita akan filter alamat IP Tujuan 217.115.151.99 dan yang juga melalui protokol HTTP.

  Masukkan sintaks ini ke filter:

  **`ip.dst==217.115.151.99 && http`** kemudian tekan Enter

  akan kita dapat hasil seperti ini, dimana paket telah difokuskan lagi:



Kita juga bisa mendapatkan informasi mendetail dari paket tersebut di bagian bawah, bagian **Detail Paket** dan **Heksa**, kadang-kadang kita juga bisa membaca informasi string-string tertentu di bagian heksa ini.

## Sniffing Password Dengan WireShark ☺

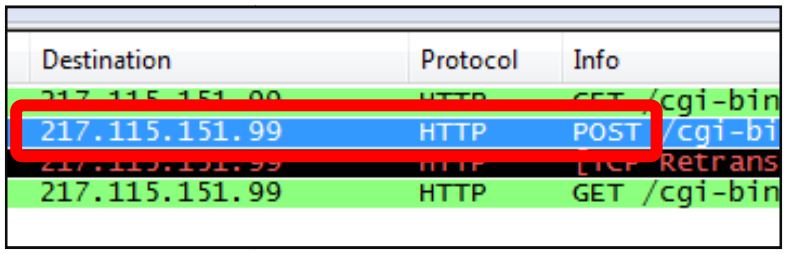
Apa itu sniffing password? Sniffing password adalah aktifitas 'mengendus' paket-paket yang berisi password di jaringan. WireShark bisa melakukan hal ini.

Kebetulan, sebelumnya saya telah melakukan login ke my.dot.tk, logikanya, data username dan password saya pastinya dikirimkan ke dot.tk melalui jaringan 'kan. Nah, kita akan coba melakukan sniffing password yang telah kita inputkan tadi.

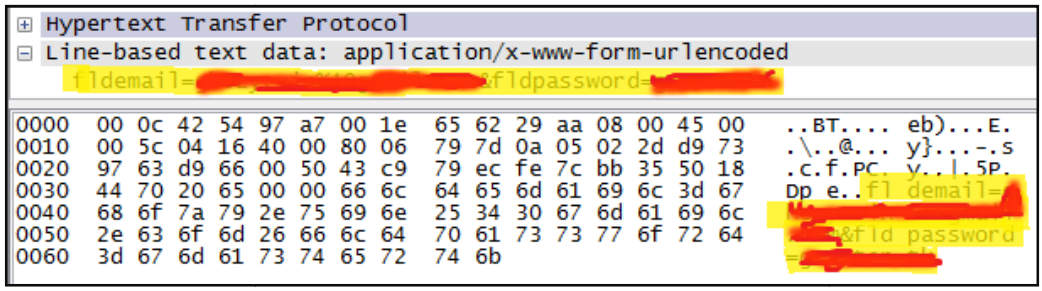
Dalam **HTML**, aktivitas mengirimkan sesuatu atau mengirimkan inputan ke server disebut dengan **POST**. Sedangkan kebalikannya, aktivitas mendapatkan sesuatu atau meminta data dari server disebut dengan **GET**.

Karenanya, kita akan mencoba 'mengintip' paket yang menuju ke dot.tk melewati protokol HTTP dan bertipe POST, barangkali ada data username dan password kita di sana ☺. Coba kita amati lagi paket dengan protokol HTTP.

Dan kebetulan, yang bertipe POST hanya ada satu, fokuskan ke paket ini:




Dan lagi-lagi kebetulan, tanpa perlu melihat data lebih mendalam lagi, data username dan pssword ini sudah menampakkan dirinya, coba klik paket data bertipe POST tadi, kemudian lihat di bagian detail bawahnya, naah, tuh, data privasi kita ternyata kelihatan ☺.



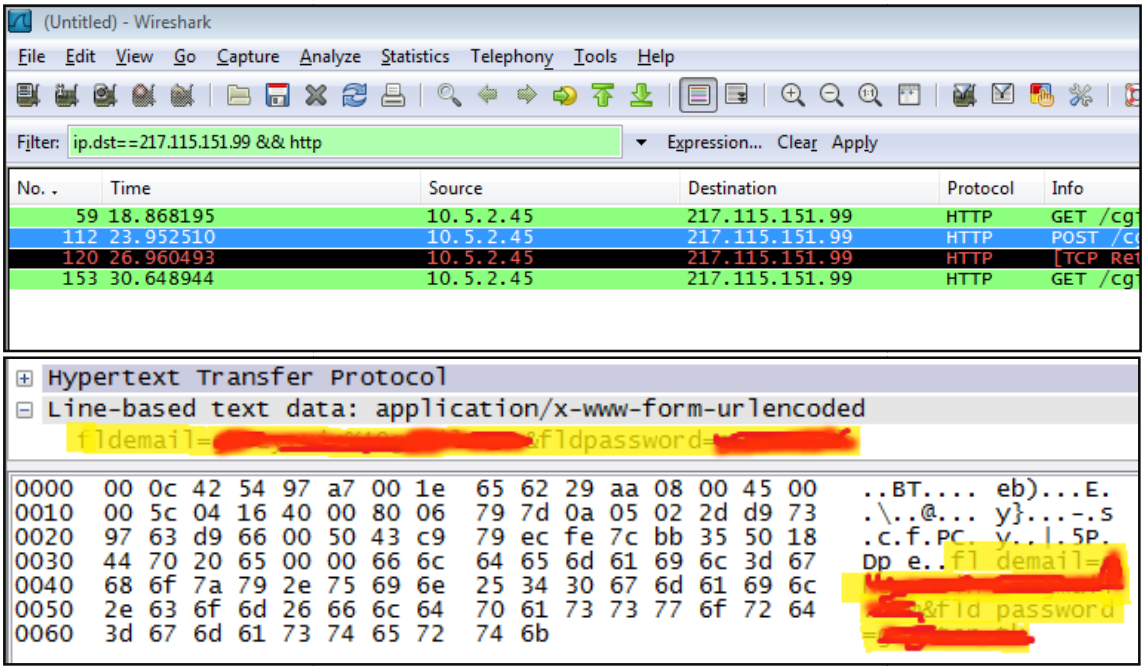
Nah, kalau ternyata WireShark dengan begitu mudahnya menunjukkan data privasi kita seperti itu, lalu bagaimana dengan data lain?? Data password facebook kita? Data akun blog kita, password email????

Tentu saja semuanya memiliki resiko yang sama besarnya untuk dibobol, tapi tentu saja pemilik website bersangkutan tidak akan membiarkan data privasi para penggunanya bisa diketahui dengan mudah oleh orang lain yang tidak berhak. Mereka tentunya akan melindunginya.

Salah satunya adalah dengan enkripsi, sehingga data aslinya hanya akan tertampil sebagai tulisan acak yang tidak berarti, cukup ampuh untuk menyulitkan langkah orang-orang usil. ☺

Namun bukan berarti juga enkripsi-enkripsi atau cara pengamanan itu tidak bisa ditembus, karena pada dasarnya sistem enkripsi atau pengaman tersebut adalah sistem yang juga buatan manusia, yang tak luput dari salah juga.

Jadi teringat sebuah kalimat yang patut direnungkan kembali: "*Tidak Ada yang 100% Aman di Internet*"




Alhamdulillah..

Kita sudah bisa menggunakan salah satu fungsi dari WireShark, tentunya masih banyak lagi fungsi-fungsi dari WireShark ini, yang masih menunggu kita untuk mencobanya ☺

*Belajar.. Berlatih... jangan pernah malas buat mencoba hal-hal baru..*

By Goji

ghozy.uin@gmail.com