Cara sniffing password menggunakan wireshark

Keterangan:

Sniffing adalah salah satu teknik untuk mengetahui suatu password dalam suatu jaringan. Sehingga kita bisa mengetahui password suatu account.

Sedangkan aplikasi WireShark disebut juga Network Paket Analyzer. Aplikasi ini berkemampuan untuk menangkap paket-paket jaringan dan berusaha untuk menampilkannya dengan informasi serinci mungkin. Nah, aplikasi inilah yang bisa digunakan untuk melihat password dalam suatu jaringan. Password apapun itu, seperti facebook, google, website dan semacamnya.

Saya akan melakukan praktek untuk melihat password suatu website www.Ilmu-Programmer.com.

1. Instal WireShark terlebih dahulu

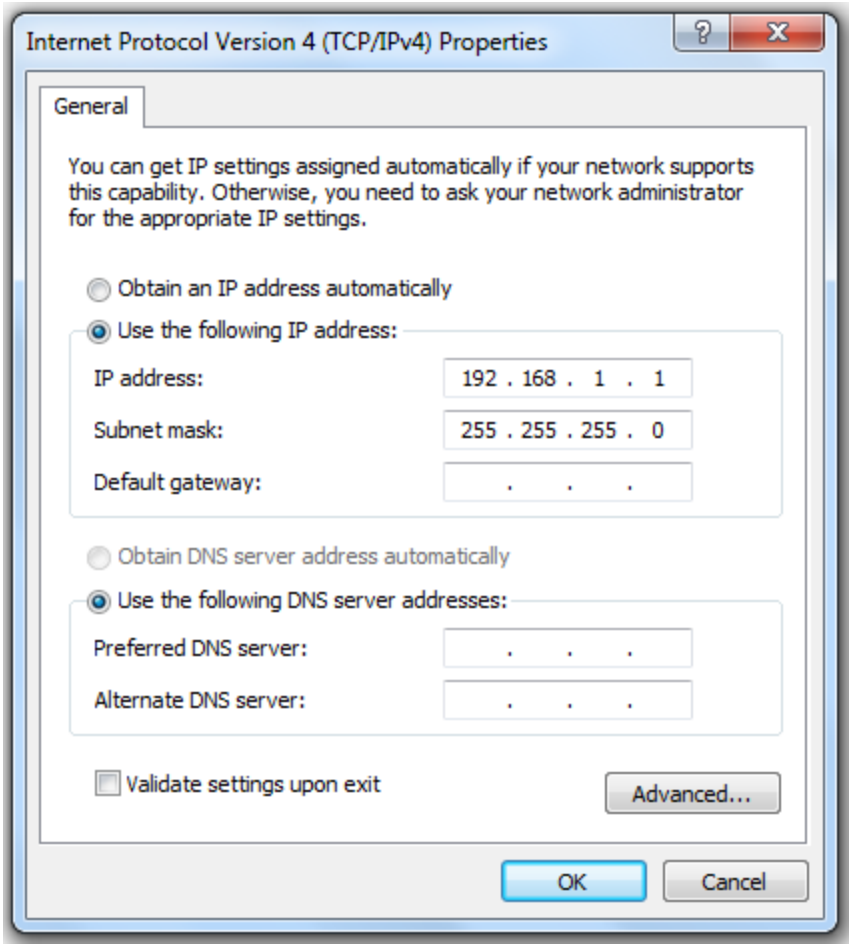
2. Setelah WireShark terinstal, silahkan hubungkan laptop kita dengan jaringan. Saya menggunakan laptop yang terhubung dengan laptop lainnya menggunakan kabel LAN bertipe Cross. Jadi, koneksi yang digunakan adalah koneksi laptop yang lainnya yang di sharing. Caranya sebagai berikut :

- Hubungkan 2 komputer dengan kabel LAN bertipe Cross. Kemudian lakukan setting sebagai berikut :

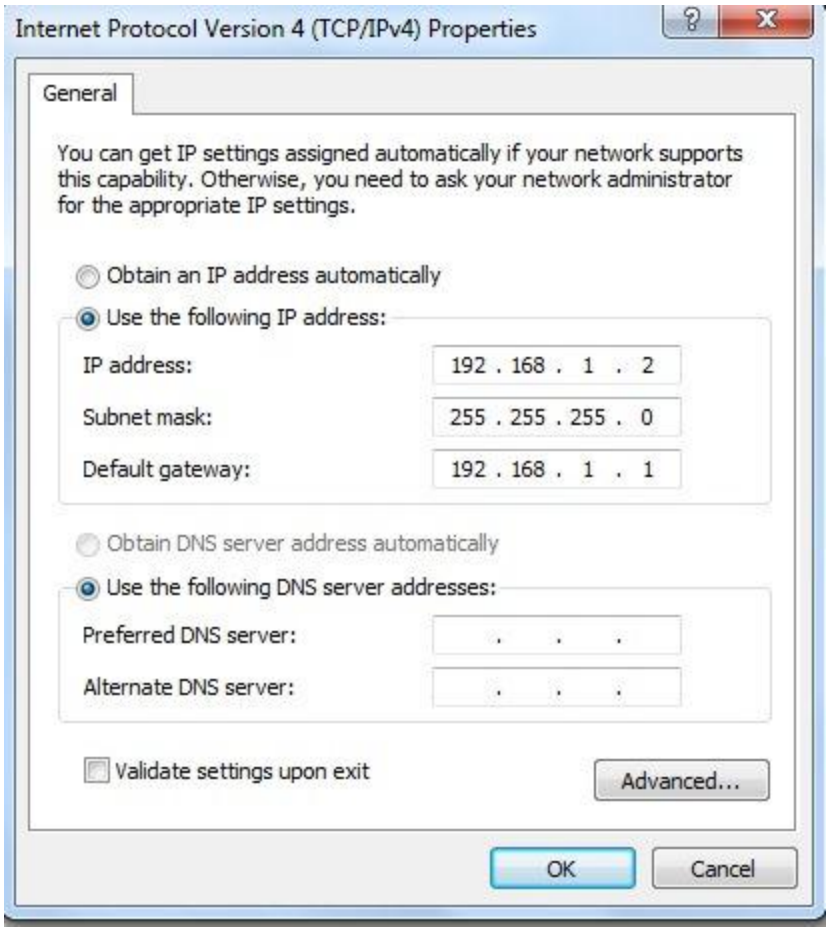
a. Klik Start –> Control Panel –> Network dan Internet –> Network and Sharing Center –> Change Adapter Setting.

b. Cari Local Area Connection dan klik 2x –> Pilih Tab Networking –> Klik 2x pada Internet Protocol Version 4 (TCP/IPv4) –> Pilih Use the Following IP Address dan lakukan setting IP Addressnya seperti berikut ini :

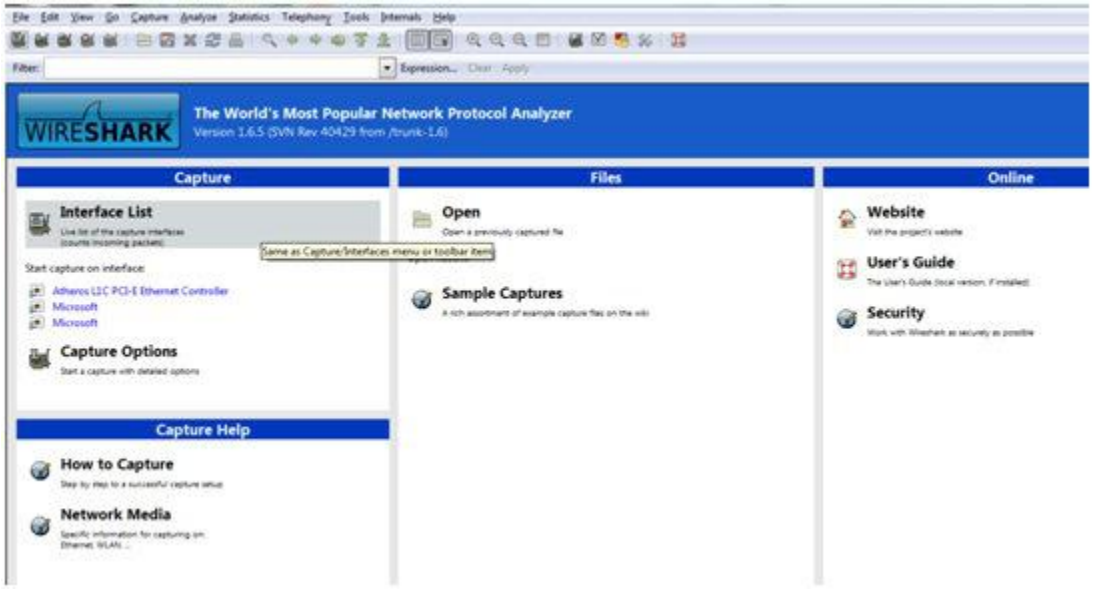
Pada Laptop yang Punya Koneksi sebagai Laptop Induk



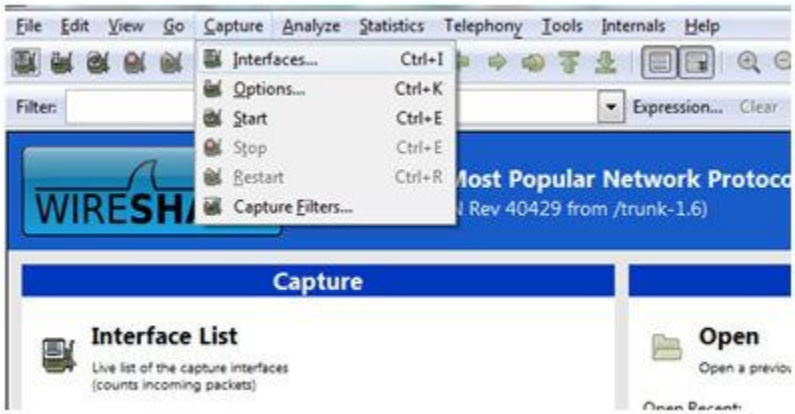
Pada Laptop yang Kedua yang menerima koneksi dari laptop induk



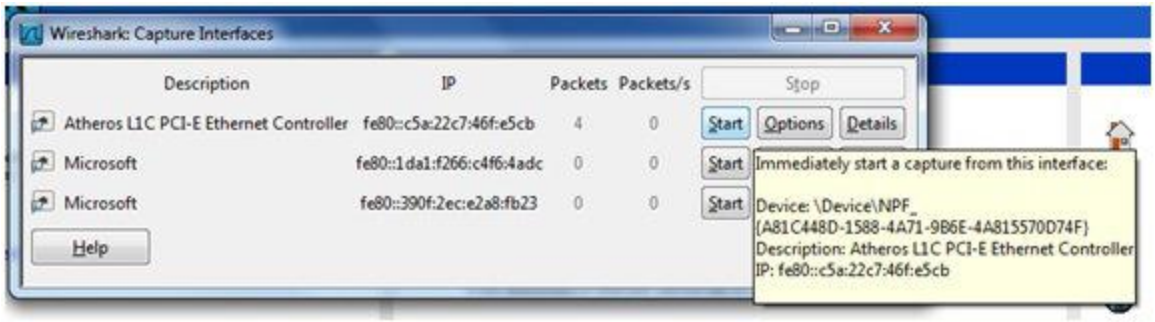
3. Apabila komputer yang kedua sudah mendapat koneksi (dalam hal ini komputer kita adalah komputer yang kedua), silahkan buka aplikasi WireSharknya. Tampilannya seperti ini :



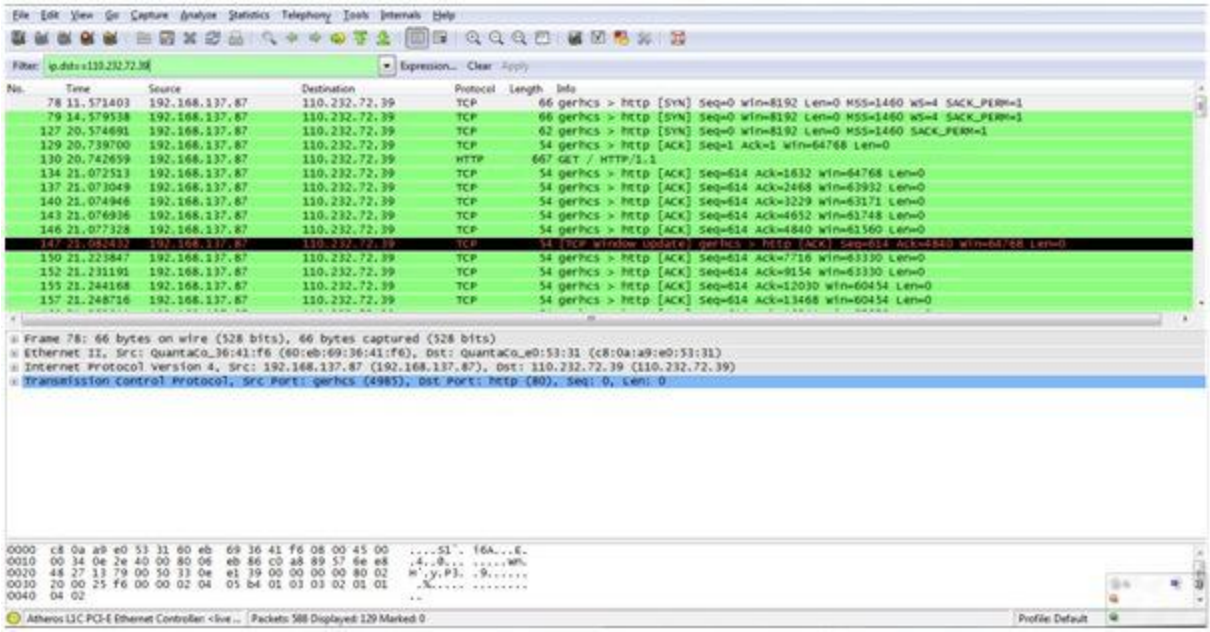
4. Setelah terbuka perhatikan bagian menu atasnya, pilih Menu Capture dan kemudian pilih submenu Interfaces. Tampilannya seperti dibawah ini :



5. Interfaces akan menampilkan semua NIC (kartu jaringan) yang ada koneksi. Kebetulan NIC saya bermerek Atheros. Lalu, pada kotak dialog yang ditampilkan pilih Start untuk memulai memonitor jaringan dari NIC tersebut. Gambarnya seperti dibawah ini :



Maka WireShark akan menampilkan paket-paket yang dikirim/diterima melalui NIC Atheros kita tadi. Berikut ini tampilannya :



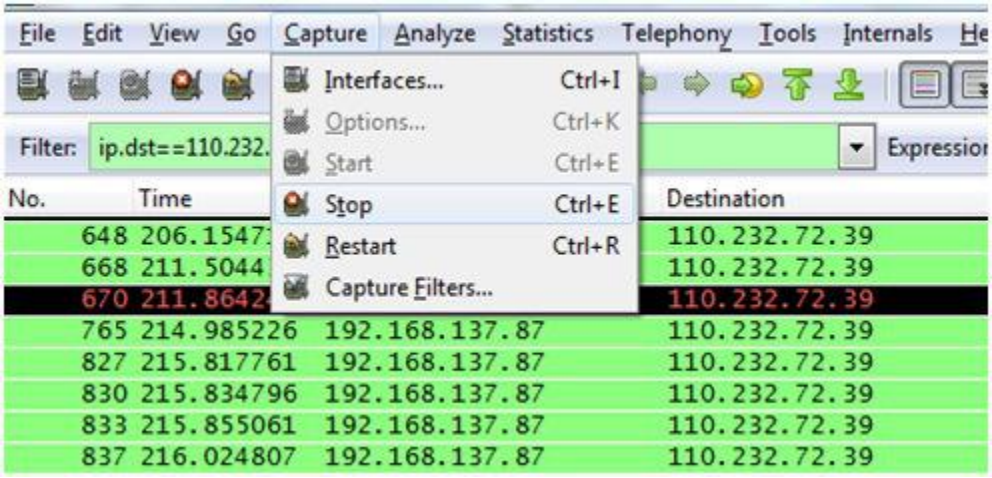
6. Sekarang kita akan mencoba Login ke akun saya di www.Ilmu-Programmer.com untuk menangkap paket ketika login. Tampilannya seperti ini :

Nah, karena WireShark menangkap semua paket tanpa ada penyaringan, sedangkan kita hanya akan melihat paket yang berasal dariwww.Ilmu-Programmer.com saja, maka kita harus melakukan penyaringan dahulu dari paket yang telah ditangkap. Terlebih dahulu kita harus mengetahui berapa IP Address www.Ilmu-Programmer.com karena WireShark menampilkan berdasarkan IP Address. Untuk mengetahui IP Address www.Ilmu-Programmer.com cara yang paling mudah adalah menggunakan Command Prompt pada Windows. Yaitu klik Start, pada kotak Search ketikkan **cmd** dan tekan enter. Setelah tampil kita ketikkan **ping ilmu-**

programmer.com. Maka akan langsung diketahui alamat IP Address www.Ilmu-Programmer.com. (Ping secara umum adalah perintah untuk mengecek jaringan apakah berfungsi dengan baik atau tidak, untuk mengetahui IP Address bisa menggunakan perintah nslookup dan sebagainya, lain waktu akan kita bahas mengenai topik ini). Setelah mengetahui IP Addresnya silahkan dicatat terlebih dahulu. Tampilannya seperti berikut ini :

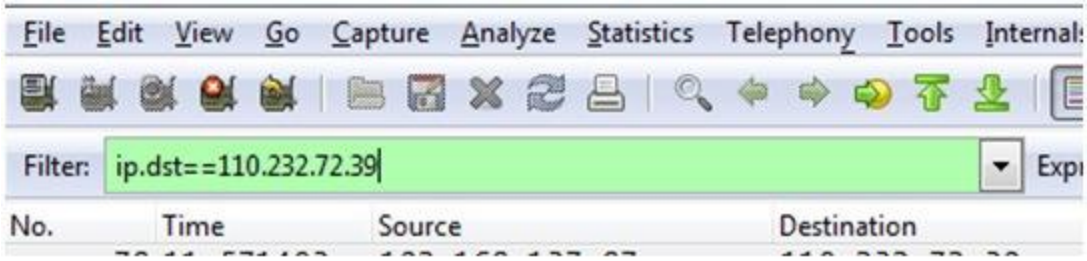
```
C:\Users\fernando>ping ilmu-programmer.com

Pinging ilmu-programmer.com [110.232.72.39] with 32 bytes of data:
Reply from 110.232.72.39: bytes=32 time=99ms TTL=56
Reply from 110.232.72.39: bytes=32 time=97ms TTL=56
Reply from 110.232.72.39: bytes=32 time=94ms TTL=56
Reply from 110.232.72.39: bytes=32 time=91ms TTL=56

Ping statistics for 110.232.72.39:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 91ms, Maximum = 99ms, Average = 95ms
```

7. Langkah selanjutnya adalah kita menghentikan proses Capture dengan cara pilih menu Capture kemudian pilih Stop. Karena jika kita berhasil login sebagai Admin di www.Ilmu-Programmer.com sebelumnya, maka bisa dipastikan password yang digunakan untuk login tadi sudah ditangkap oleh Wireshark.

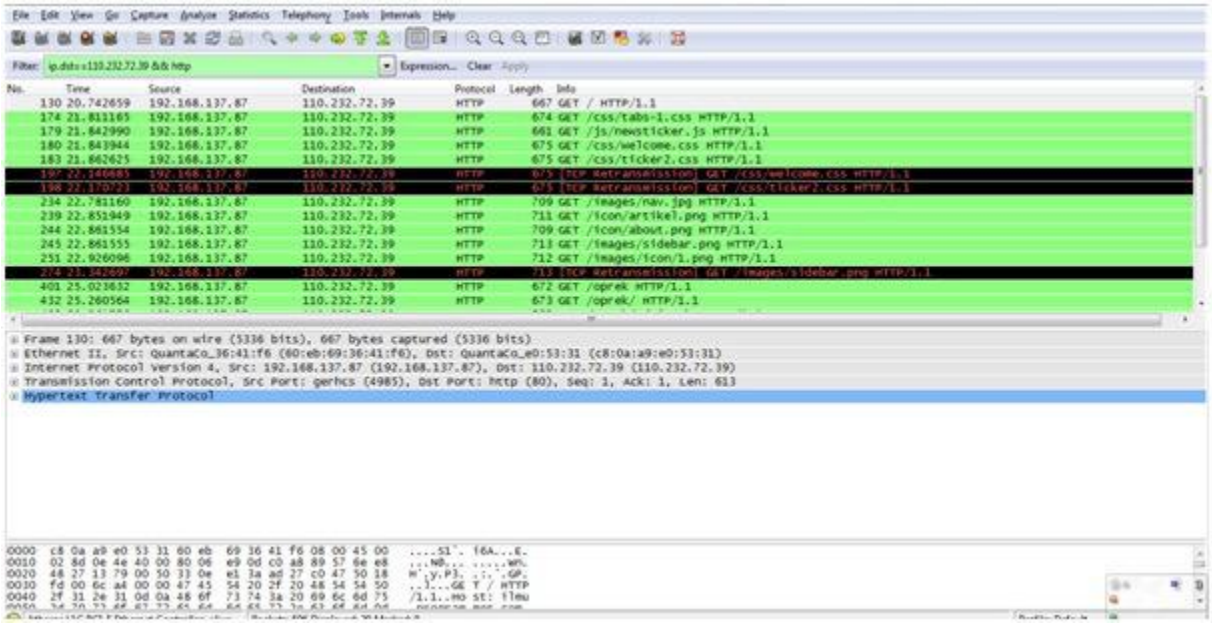


8. Sekarang kita akan melakukan filter (seleksi) paket seperti yang sudah saya jelaskan sebelumnya pada langkah 6. Caranya, pada address bar Filter yang ada dibawah kumpulan icon ketikkan perintah berikut ini : **ip.dst==110.232.72.39.** Silahkan ganti 110.232.72.39 dengan IP Address lainnya jika bereksperimen dengan situs yang berbeda. Maka, Wireshark akan menampilkan paket-paket yang memiliki IP Address seperti diatas.

Tampilan penyaringan paket

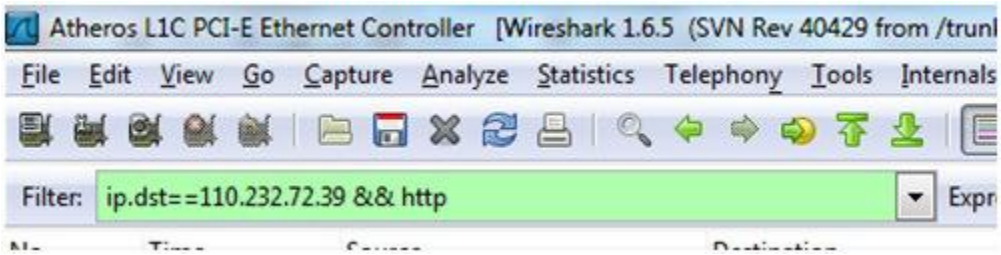


Paket setelah disaring

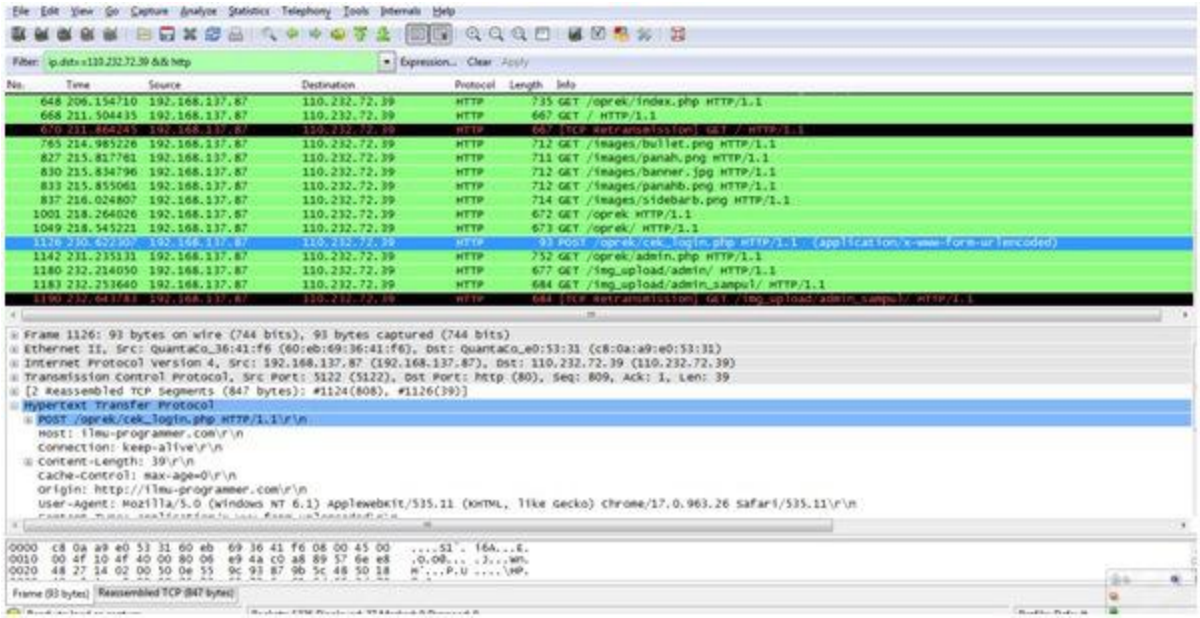


8. Nah, ternyata paket yang ditampilkan masih terlalu banyak dan kita akan melakukan penyaringan lagi. Paket yang ditampilkan ada yang HTTP, TCP dan lain-lain. Karena kita mengakses sebuah web, maka kita akan meyaring menggunakan kata kunci HTTP saja. Silahkan tambahkan kode berikut ini pada address bar Filter yang tadi : **&& http**. Maka WireShark hanya akan menampilkan paket yang bertipe HTTP saja.

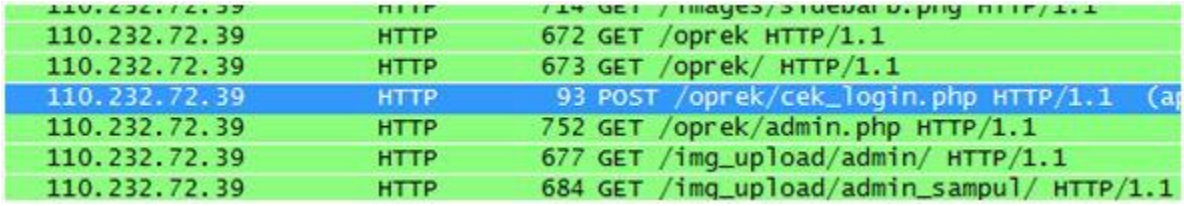
Filter untuk HTTP



Paket setelah disaring



9. Selanjutnya, perlu dipahami, dalam ilmu teknologi web, perintah GET berarti penerimaan paket terjadi dari web server ke komputer lokal, sedangkan POST berarti pengiriman paket terjadi dari komputer lokal ke web server. Karena secara logik ketika kita melakukan input password, artinya kita sedang melakukan POST password dari komputer lokal ke web server untuk dicek kebenaran password tersebut. Silahkan perhatikan pada paket yang sudah disaring tadi yang infonya POST. Tampilannya seperti dibawah ini :



Nah, kebetulan dari paket yang ada cuma ada 1 buah paket yang infonya POST. Silahkan klik 2x paket tersebut. Lihat pada baris paling bawah yang bertuliskan kalimat **"Line-based text data: application…"**. Kita akan menemukan username dan password yang kita gunakan tadi di www.Ilmu-Programmer.com.

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
Referer: http://ilmu-programmer.com/oprek/\r\n
Accept-Encoding: gzip,deflate,sdch\r\n
Accept-Language: en-US,en;q=0.8\r\n
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3\r\n
Cookie: HstCfa1995841=1348173632698; HstCmu1995841=1348173632698; ML
DNT: 1\r\n
\r\n
[Full request URI: http://ilmu-programmer.com/oprek/cek_login.php]
Line-based text data: application/x-www-form-urlencoded
username=[redacted]&password=[redacted]
```