

## **Analysis protocol TCP, UDP, dan monitoring protocol SSL**

Dwi Nabella Hendra Apriawan

dnha03@gmail.com

<http://nabellahendra.blogspot.com>

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.

pada artikel kali ini saya akan sedikit mengupas tentang protocol TCP, UDP, dan SSL. Berikut analysis beberapa protocol tersebut.

TCP (Transmission Control Protocol) adalah salah satu protokol yang umum digunakan dalam dunia internet, karena TCP mempunyai kelebihan yaitu adanya koreksi kesalahan. Dengan menggunakan protokol TCP, maka proses pengiriman akan terjamin dengan adanya bagian untuk sebuah metode yang disebut flow control.

UDP (User Datagram Protocol) adalah protokol umum lainnya yang digunakan di dunia internet dan merupakan connectionless. UDP tidak pernah digunakan untuk mengirim data penting seperti halaman web, informasi database, dan sebagainya. Tetapi UDP biasanya digunakan untuk streaming audio dan video, karena UDP mempunyai kelebihan yaitu pada kecepatan transfer. UDP lebih cepat dari TCP karena pada protokol UDP tidak ada bentuk kontrol aliran dan koreksi kesalahan.

Analisa TCP dan UDP menggunakan Wireshark

TCP (Transmission Control Protocol)

berikut ini adalah gambar hasil capture protokol TCP dengan Wireshark



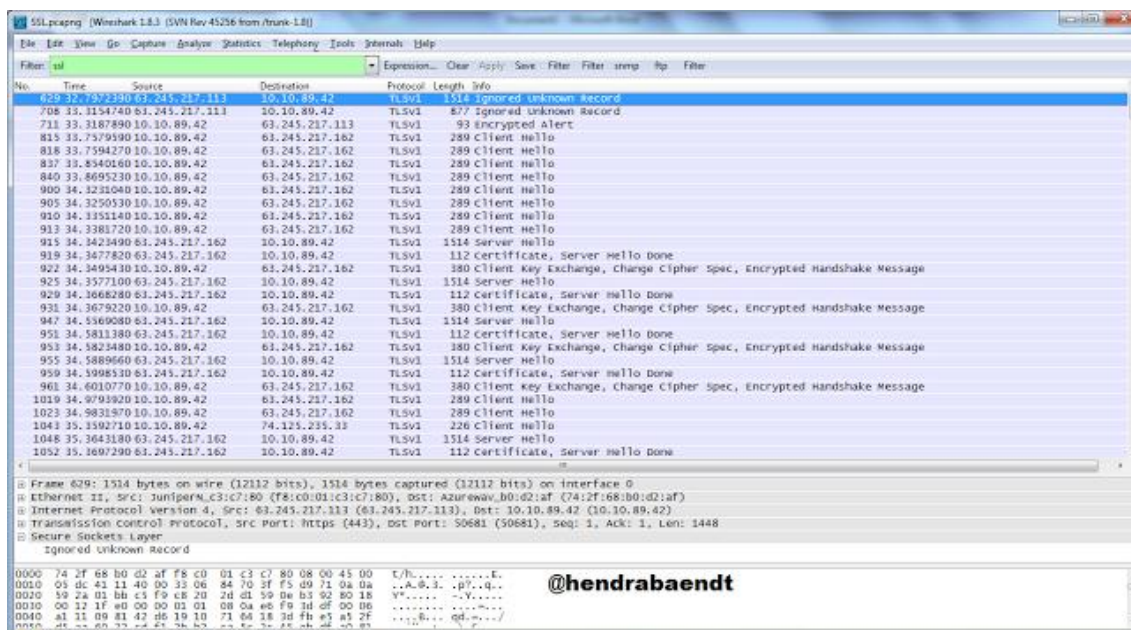
dari gambar diatas dapat dilihat protokol UDP yang tercapture wireshark diaman IP source 10.10.40.110 menggunakan port 54758 dimana pada sesi ini dia adalah pengirim data/ informasi berupa suara dan IP destination 10.10.40.21 port 14791 adalah yang akan menerima informasi suara dan gambar dari source. Pada UDP tidak ada proses koreksi kesalahan/flow control.

SSL (secure socket layer) adalah protokol keamanan yang digunakan oleh hampir semua transaksi yang sensitif yang membutuhkan keamanan lebih seperti Paypal, Internet Banking, dan lain-lain. Keamanan dijamin dengan menggunakan kombinasi dari kriptografi kunci publik dan kriptografi kunci simetri bersamaan dengan sebuah infrastruktur sertifikat. Sebuah sertifikat adalah sebuah kumpulan data identifikasi dalam format yang telah distandardisasi. Data tersebut digunakan dalam proses verifikasi identitas dari sebuah entitas (contohnya sebuah web server) pada internet.

Berikut ini adalah capture protocol SSL dengan menggunakan wireshark

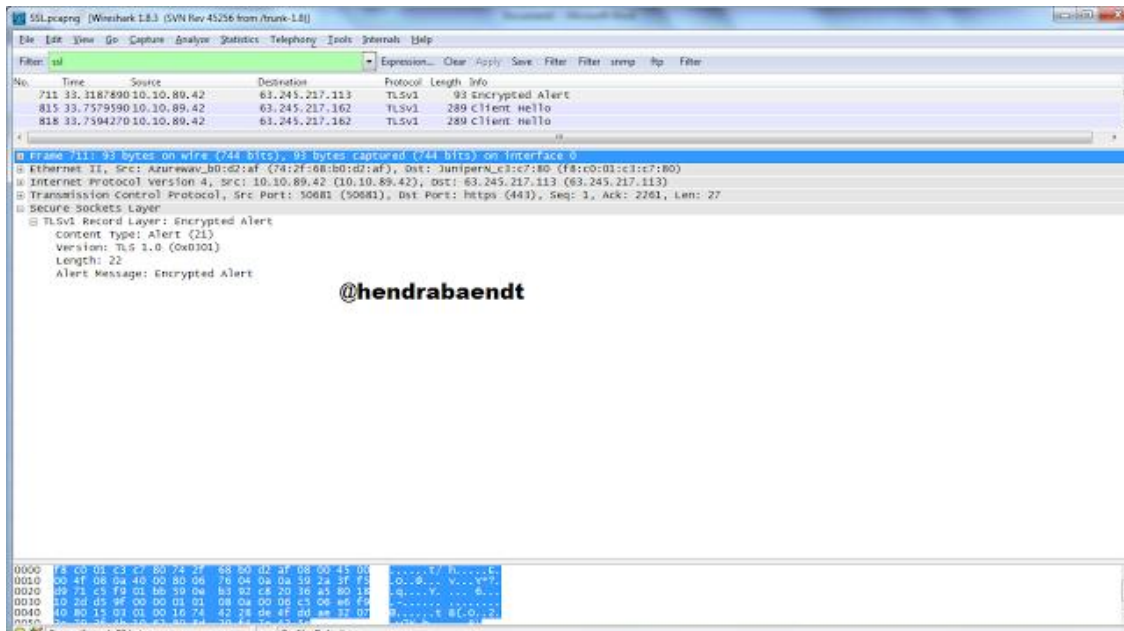
1. Bukalah wireshark kemudian mulailah proses capture
2. Buka browser anda bukalah alamat dengan menggunakan https (misal: <https://www.youtube.com>)
3. Setelah itu stop capture pada wireshark

Hasil capture protocol SSL

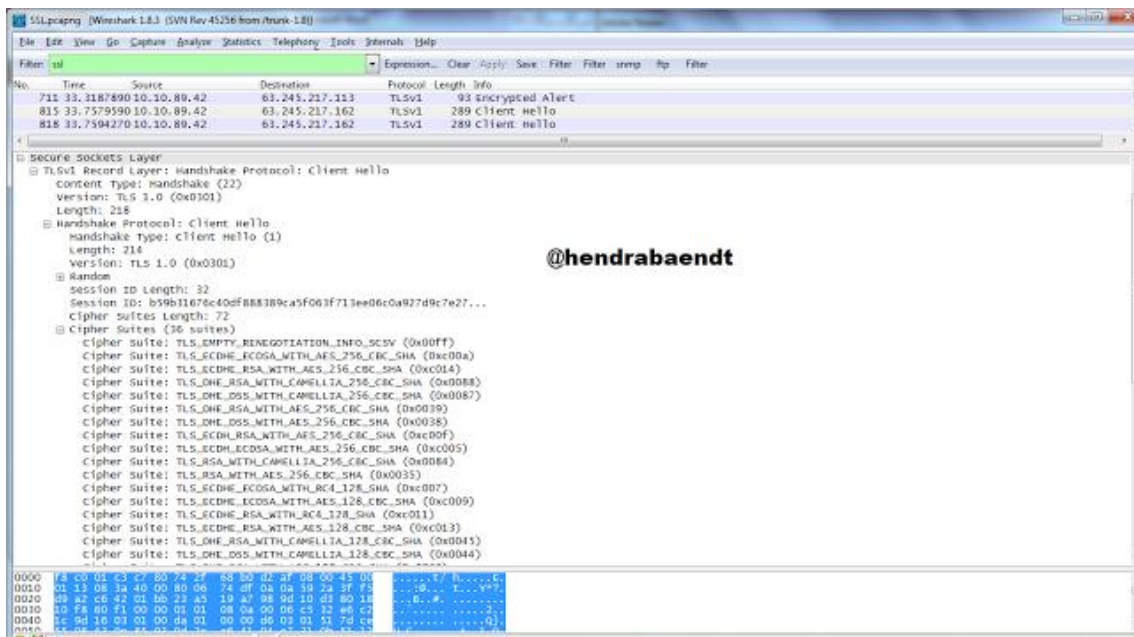


Dari gambar diatas dapat dilihat bahwa saat dilakukan filter protocol SSL yang muncul

adalah protocol TLSV1, protocol TLSV1 adalah protocol hasil pengembangan dari protocol SSL.

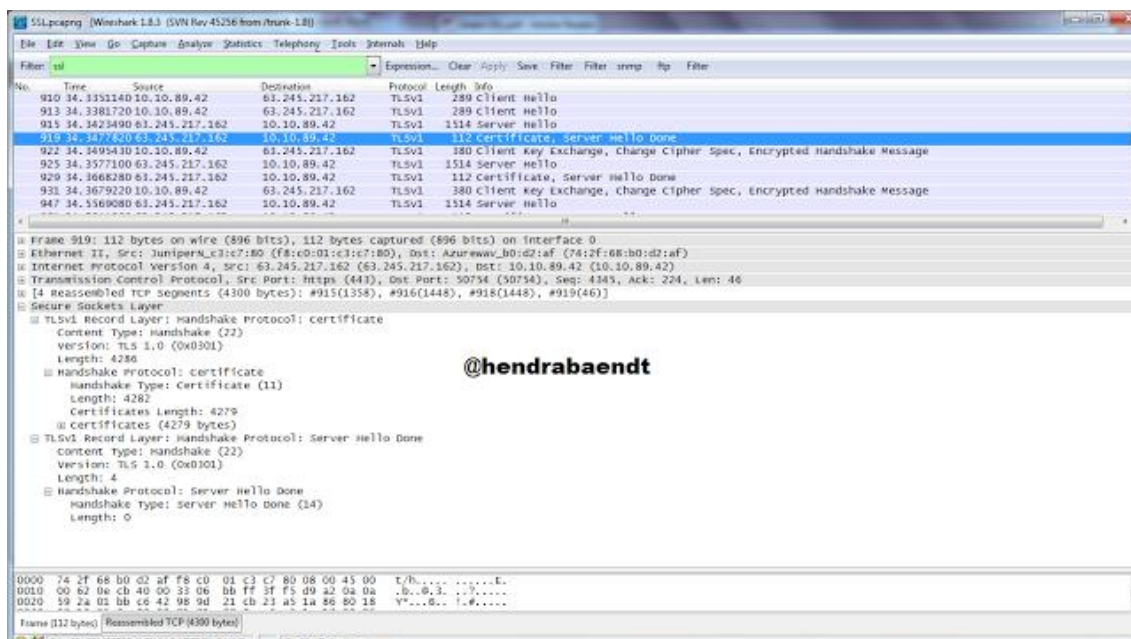


Pada gambar diatas protocol SSL yang tercapture adalah fase encrypted alert, dimana awal proses permintaan untuk enkripsi semua data yang akan dikirim ataupun diterima.



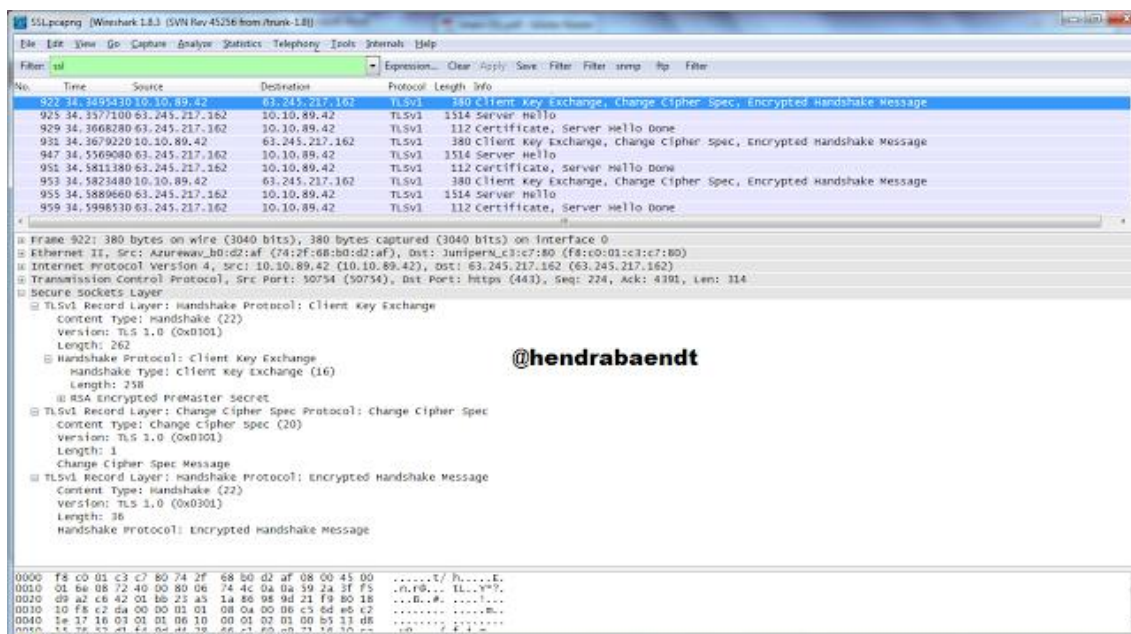
Client akan mengirimkan balasan berupa pesan client hello. Dapat dilihat dari isi pesan dalam protocol ini, berisi versi SSL dan Cipher suite.





@hendrabaendit

Kemudian server akan mengirimkan balasan berupa pesan server hello. Dapat dilihat dari isi pesan dalam protocol ini, berisi versi SSL dan certificate yang telah disepakati.



@hendrabaendit

Kemudian client akan memverifikasi pesan dari server menggunakan sertifikat kemudian mengekstraksi kunci public server melalui perintah key exchange. Setelah server menerima konfirmasi dari hasil verifikasi oleh klien selanjutnya proses dapat dilanjutkan dengan jalur yang aman karena data telah dienkripsi. Sampai disini artikel yang saya tulis tentang protocol TCP, UDP, dan SSL, semoga bermanfaat.

### Biografi Penulis



**Dwi Nabella Hendra Apriawan**, lahir tahun 1993 di kota Purbalingga Jawa Tengah. Menghabiskan waktu SD, SMP , dan SMA di Purbalingga, sekarang menjadi mahasiswa Politeknik Negeri Semarang jurusan Teknik Elektro program studi D4 Teknik Telekomunikasi. Tidak tertarik dengan hal yang tidak menarik.

Contact Person :

[dnha03@gmail.com](mailto:dnha03@gmail.com)

YM [dnha03@yahoo.com](mailto:dnha03@yahoo.com)

Twitter @hendrabaendt