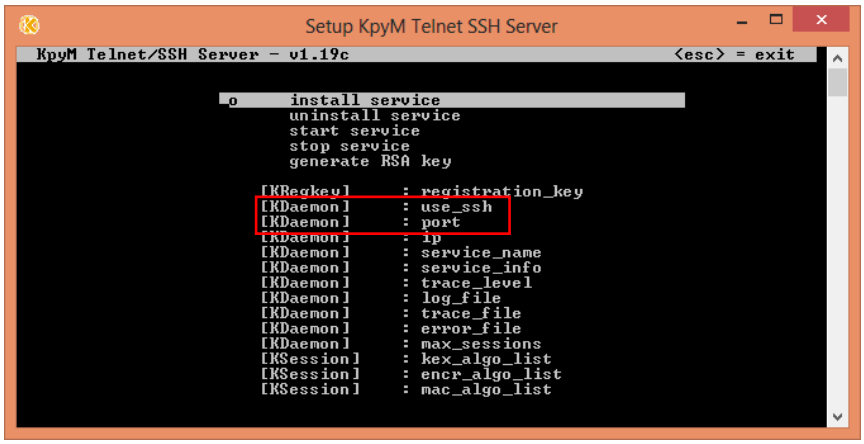
Monitoring Telnet

Ainul Fuad Farhan
inungf@ymail.com
http://inungandthenotes.blogspot.com

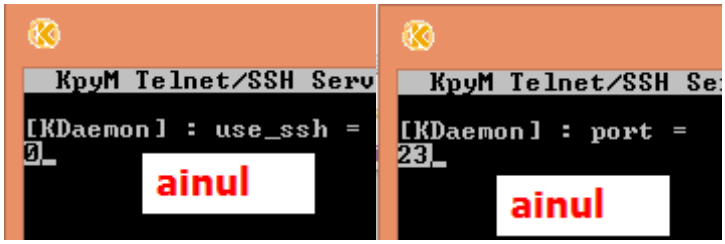
Telnet (Telecommunication network) adalah sebuah protokol jaringan yang digunakan pada Internet atau Local Area Network untuk menyediakan fasilitas komunikasi berbasis teks interaksi dua arah yang menggunakan koneksi virtual terminal. TELNET dikembangkan pada 1969 dan distandarisasi sebagai IETF STD 8, salah satu standar Internet pertama. TELNET memiliki beberapa keterbatasan yang dianggap sebagai risiko keamanan.

Telnet berisikan perintah user yang berdasarkan protokol TCP/IP untuk mengakses komputer dari jarak jauh (remote). Melalui Telnet, administrator atau user lain dapat mengakses komputer dari jarak jauh. Pada Web, kita dapat menggunakan protokol HTTP dan FTP untuk mengakses komputer jarak jauh, tetapi hanya login seperti user biasa sesuai dengan hak akses yang telah di set pada komputer yang dituju.

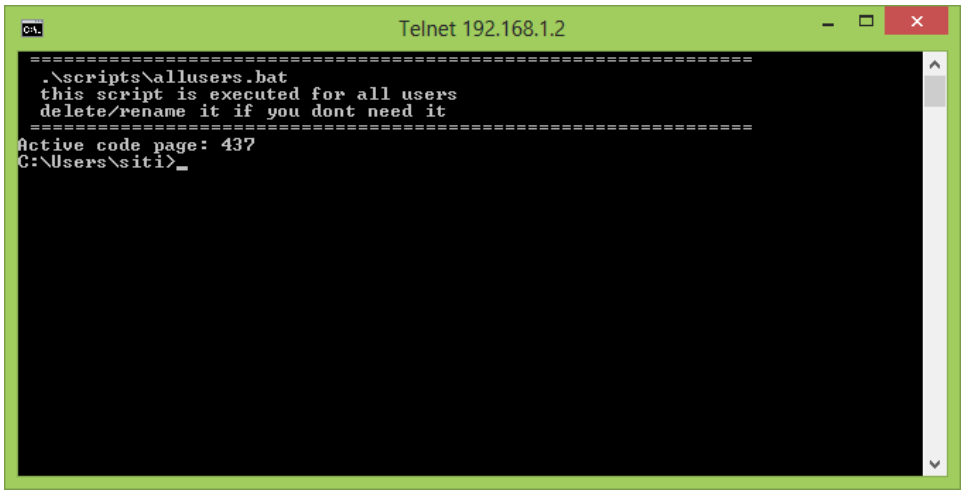
Dengan menggunakan telnet kita mampu melakukan *remote* ke *directory* komputer lain, tentunya dengan mengatahui *user* dan *password* dari komputer yang kita tuju tersebut. Namun pada perangkat seperti laptop dan komputer kita memerlukan bantuan dari aplikasi lain guna menjadikan port dari telnet itu berfungsi, salah satu aplikasi yang digunakan adalah **kts119c**.



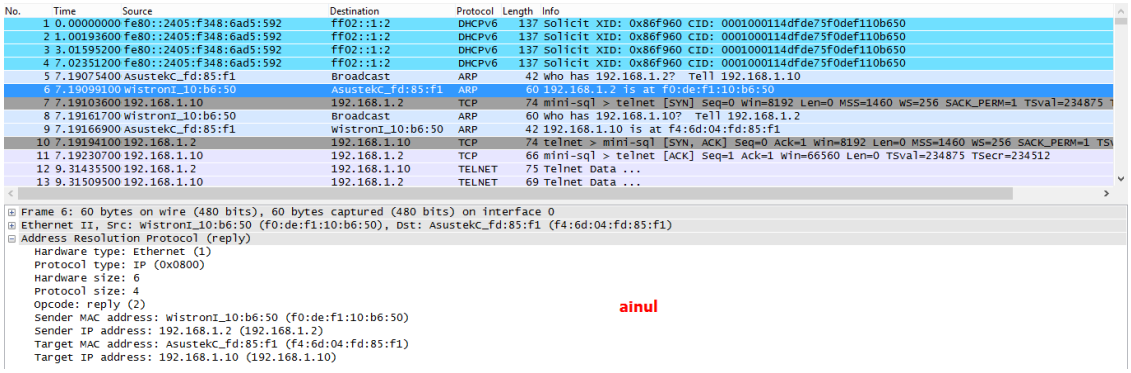
Dengan melakukan konfigurasi pada *use_ssh* dan *port* di atas kita memanfaatkan port 23 sebagai protokol Telnet.



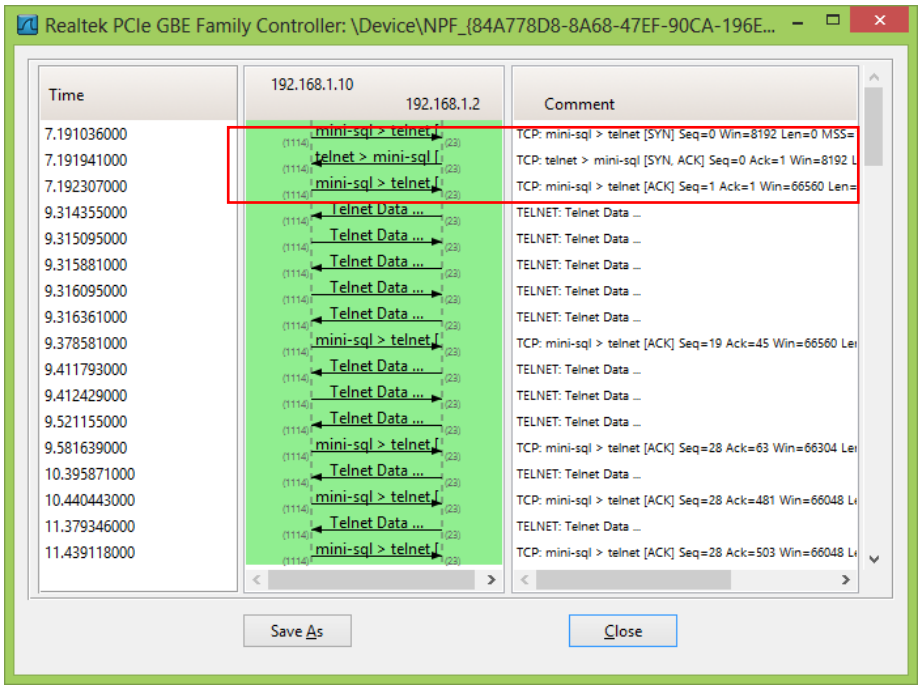
Dengan melakukan konfigurasi seperti di atas pada kedua laptop/komputer, berlangsunglah Telnet antara kedua perangkat. Berikut merupakan contoh dari telnet yang dilakukan dari laptop yang memiliki IP Address 192.168.1.10 ke 19.168.1.2 (Siti).



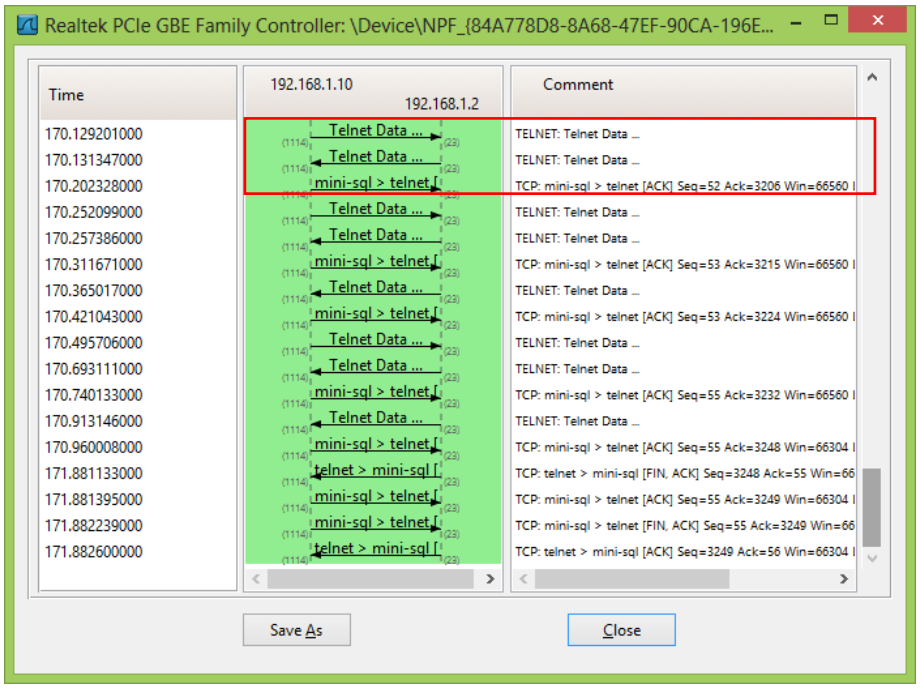
Nah dari telnet yang telah berhasi tersebut, ada protokol-protokol yang berlalu lalang, seperti biasa kita menggunakan Wireshark guna melakukan *capture* protokol yang berlalu lalang tadi.



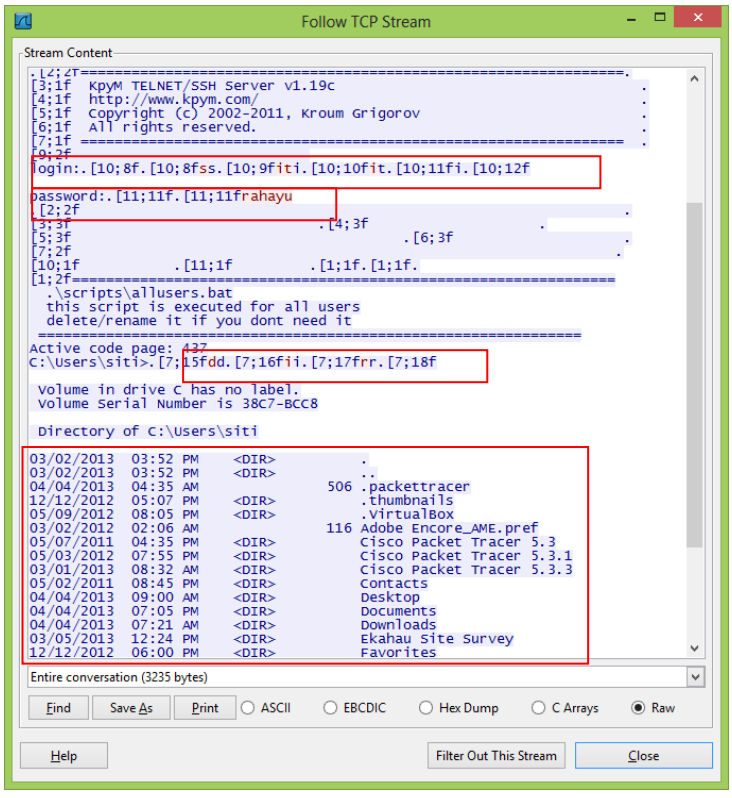
Dari beberapa protokol frame di atas terlihat bahwa Laptop dengan IP Add 192.168.1.10 sedang mengirim ARP dulu untuk melakukan **3Ways Handshaking** ketika akan melakukan *log in* ke laptop dengan IP Add 192.168.1.2, yang berisi [SYN], [SYN ACK], dan [ACK].



Ketika laptop akan *log out* dari Telnet maka akan ditutup dengan **3Ways Handshaking** yang berisi seperti berikut.



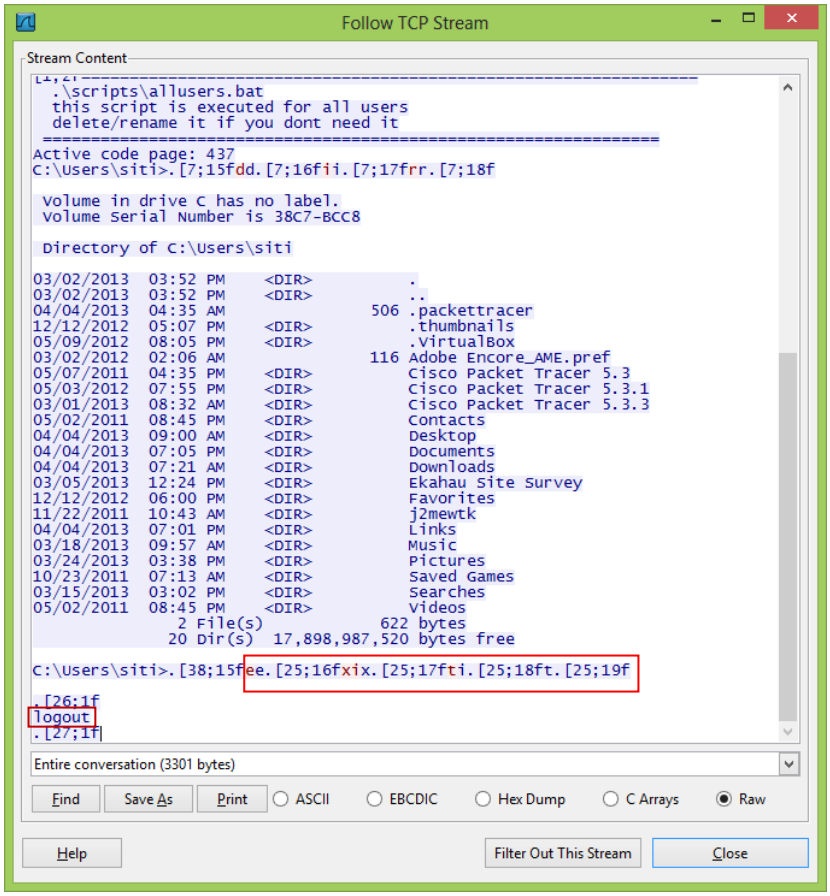
Itu tadi merupakan *capture* bagaimana 3ways handshaking ketika Laptop melakukan *log in* dan *log out*. Nah, ada lagi yang tercapture, yaitu *user* dan *password* dari laptop yang ditelnet berserta isi direktori. Dengan kita melakukan "Follow TCP Stream" pada salah satu protokol TCP yang ada pada frame yang tercapture Wireshark. Hasilnya adalah sebagai berikut.



Dari "Flow Graph" tersebut terlihat *user login* yang digunakan adalah siti dan *password login*

yang digunakan adalah rahayu. Perintah cmd yang digunakan adalah dir. Terlihat bahwa directory dari laptop tersebut berisi packettracer, virtualbox, cisco packet tracer, dsb.

Beda lagi "Flow Graph" yang ditampilkan ketika melakukan *logout*.



Perintah yang dilakukan untuk *logout* adalah exit.

Nah begitulah monitoring pada Telnet menggunakan Wireshark.

Terimakasih, semoga bermanfaat.

Referensi:

http://www.dq-online.com/index.php?option=com_content&view=article&id=68:telnet&catid=50:network&Itemid=64

http://id.wikipedia.org/wiki/Telnet

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