TUGAS TASK 5

JARINGAN KOMPUTER

Nama : Fifi Hariyani

Nim : 09011181419031

Kelas : SK.5A

Dosen Pengampuh : Dr. Deris Stiawan M.T

FAKULTAS ILMU KOMPUTER

JURUSAN SISTEM KOMPUTER

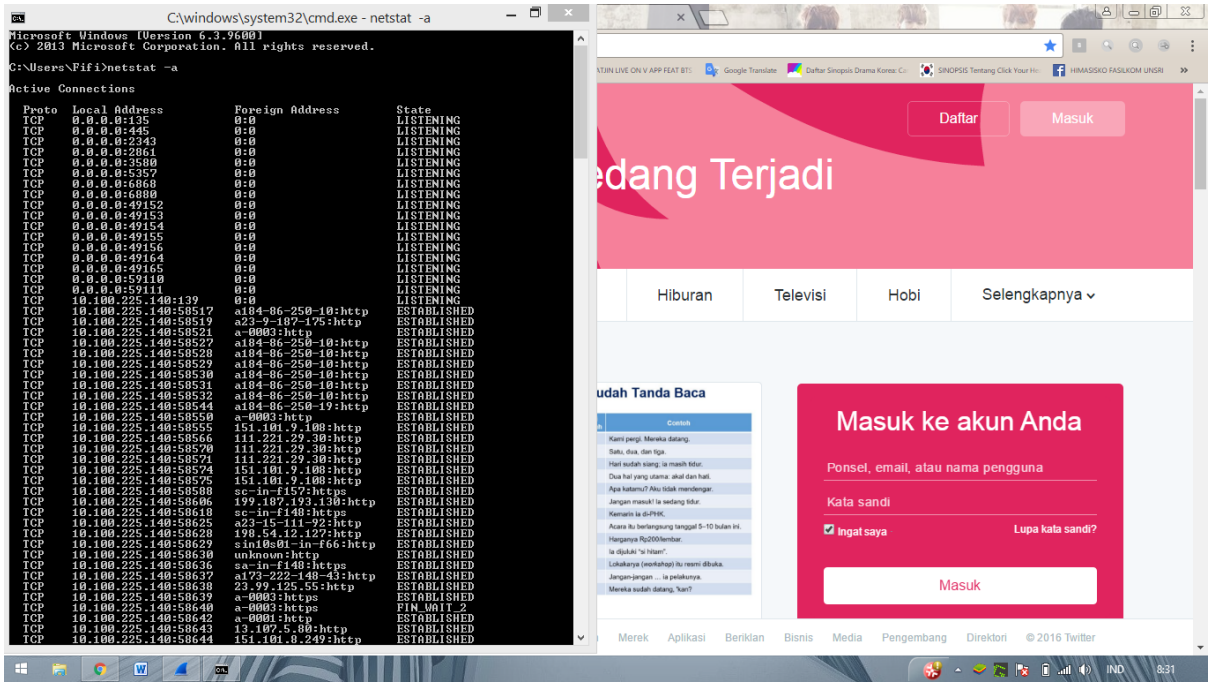
UNIVERSITAS SRIWIJAYA

2016

Tugas :

Analisa jaringan pada wireshark dan netstat a!

Ketika Url masuk ke http://twitter.com/ dengan perintah netstat -a di command prompt :



Analisa:

Saat melakukan perintah netstat-a akan muncul di jendela Command Prompt tulisan Active Connection. Dan dibawahnya terdapat listing "Proto" , "Lokal Address", "Foreign Address", dan "State". Active Connection menunjukkan bahwa dibawahnya merupakan koneksi-koneksi yang aktif.

Penjelasan :

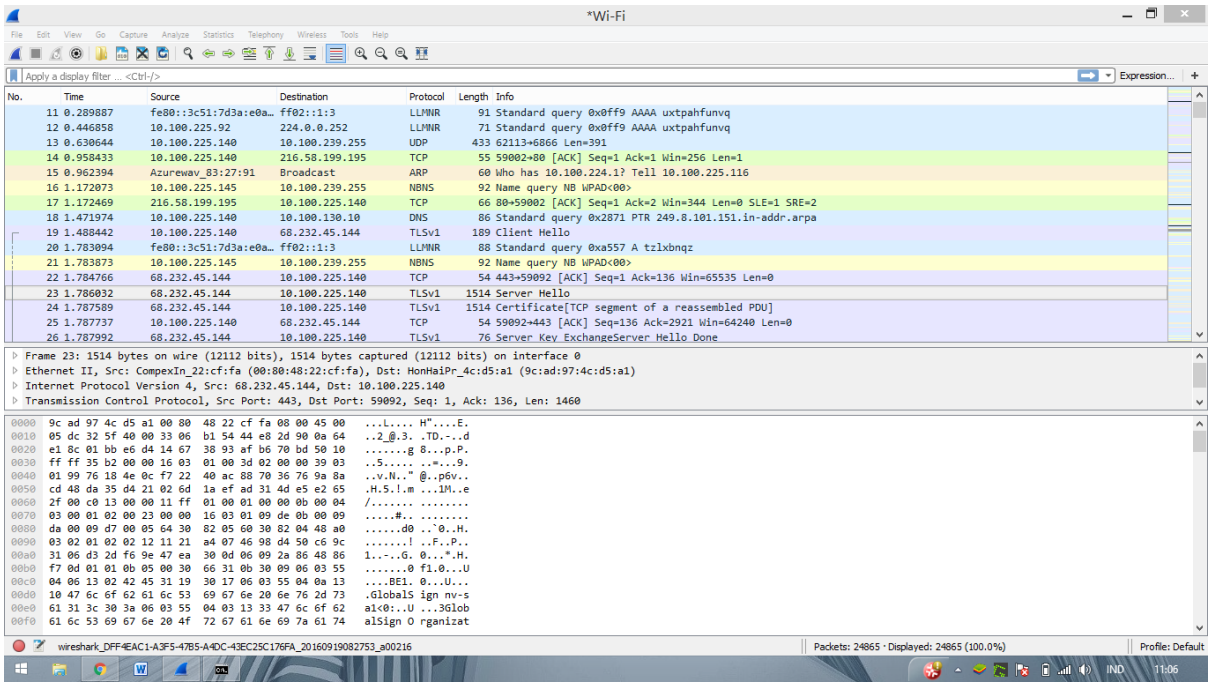
- Proto - Nama protokol (TCP atau UDP). Mengindikasikan Protocol yang digunakan
- Local Address - Alamat IP dari komputer lokal dan nomor port yang digunakan. Nama komputer lokal yang sesuai dengan alamat IP dan nama port ditampilkan kecuali parameter -n ditentukan. Tanda bintang (*) ditampilkan untuk tuan rumah jika server mendengarkan pada seluruh interface. Jika port tersebut belum ditetapkan, nomor port ditampilkan sebagai tanda bintang.
- Foreign Address - Alamat IP dan nomor port dari komputer remote yang soket terhubung. Nama-nama yang sesuai dengan alamat IP dan port akan

ditampilkan kecuali parameter -n ditentukan. Jika port tersebut belum ditetapkan, nomor port akan ditampilkan sebagai tanda bintang (*). Foreign Address : alamat computer yang kita hubugi.

- State - Menunjukkan keadaan koneksi TCP. Mungkin negara adalah sebagai berikut: CLOSE_WAIT, CLOSED, ESTABLISHED, FIN_WAIT_1, FIN_WAIT_2, LAST_ACK, LISTEN, SYN_RECEIVED, SYN_SEND, dan TIME_WAIT. Bila statenya close wait maka artinya tidak tersambung.
  Maksud dari state yang terdapat pada netstat:
  - Close wait artinya terputus.
  - Established artinya aktif / tersambung.
  - Time wait artinya menunggu.

Dengan Menggunakan Wireshark

Ke twitter.com



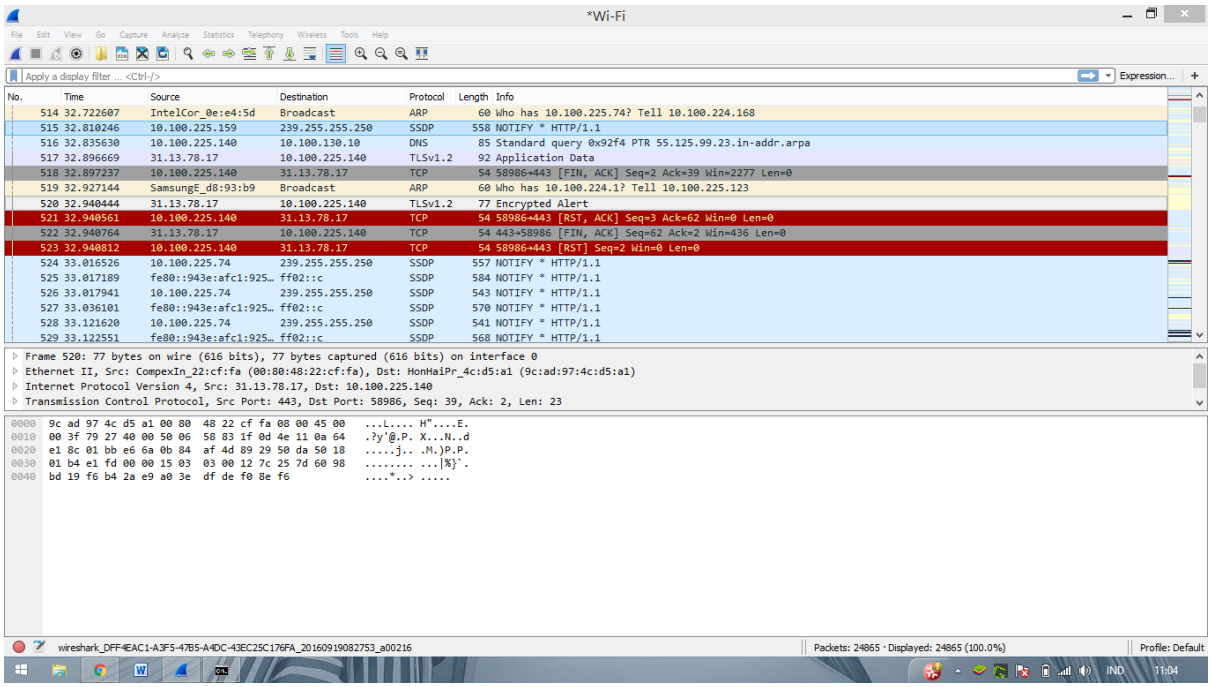
Analisa :

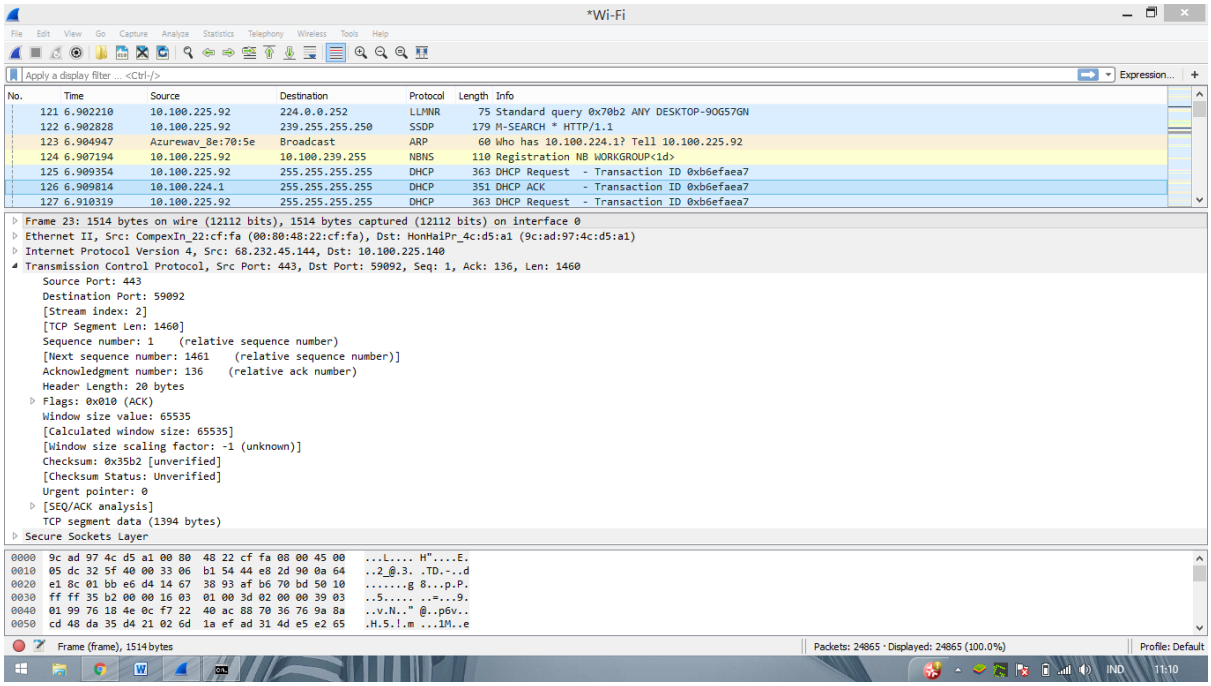
Dari gambar diatas, wireshark manangkap aktifitas jaringan ke twitter.com.

Dari hasil sniffing menggunakan wireshark akan menangkap aktifitas dijaringan, informasi yang dapat dihasilkan yaitu menampilkan port. Namun ketika aktifitas login password, maka akan dienkripsi oleh ssl .

Berdasarkan hasil SysRq gambar di atas saat wireshark baru dibuka, saat itu jg setiap melakukan koneksi ke sebuah alamat website maka komputer akan melakukan koneksi ke gateaway dan disitu dapat dilihat komputer yang menggunakan wireshark (komputer sumber) adalah 31.13.78.17 dengan acces point melalui ip 10.100.225.140 dan komputer gateaway 216.58.199.195 (komputer tujuan). setiap komputer sumber mau melakukan koneksi sniffing akan melakukan koneksi ke komputer tujuan /gateaway dahulu seperti pada gambar di atas koneksi ini menggunakan metode three way handshake dan sinkronisasi,

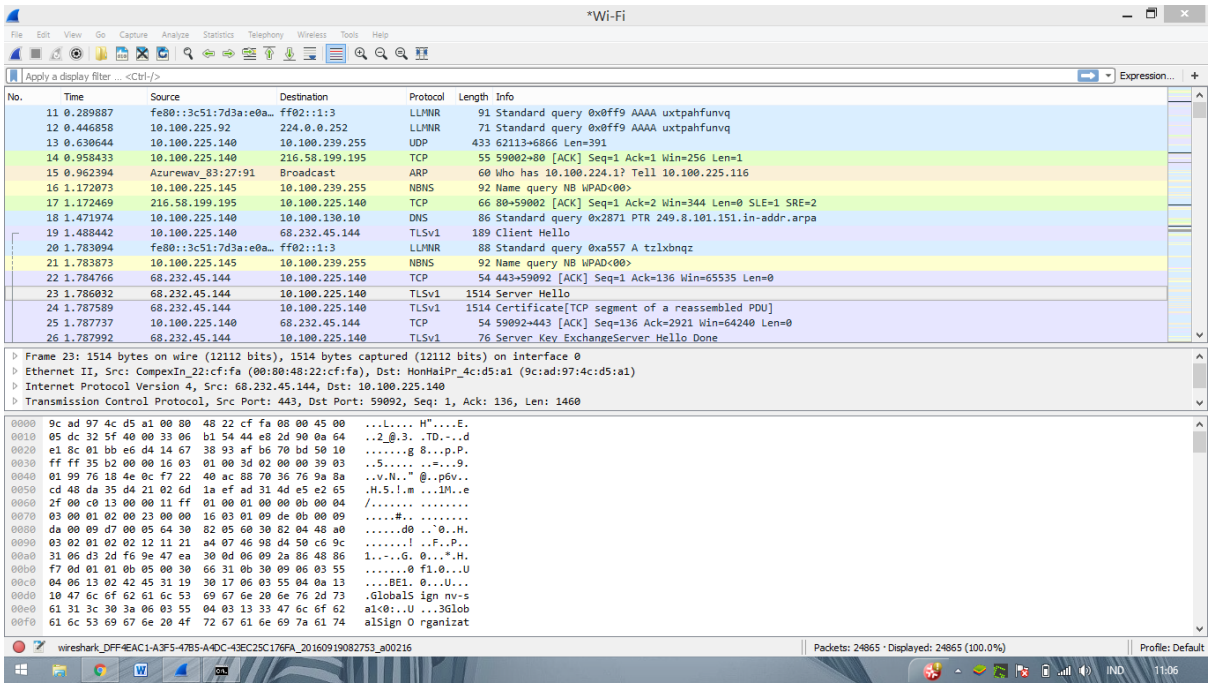
- komputer client mengirimkan broadcast (DHCP DISCOVER).
- komputer server mengirimkan (DHCPOFFER)beserta alamat ip dan waktu penyewaan.
- client menerima penawaran ip dari dhcp server mengirimkan (DHCPREQUEST)
- proses terakhir,DHCP server mengirimkan DHCPPACK begitu juga dengan koneksi ke website dengan menggunakan protocol tcp komputer akan mengirimkan paket ke server website tersebut seperti pada gambar di bawah ini:





Analisa :

Komputer sumber ip 31.13.78.17 akan mengirimkan paket ke alamat http://twitter.com. Setelah itu komputer sumber akan melakukan koneksi ke ip tujuan yaitu ip 68.232.45.144 dari source port 443 ke destination port 59092 setelah itu ip dari twitter akan mengirimkan paket data ke ip 10.100.225.140 dengan source port 443 yang merupakan port default website server untuk diakses berjuta-juta umat ke port 59092 yang isinya adalah isi dari halaman website twitter.

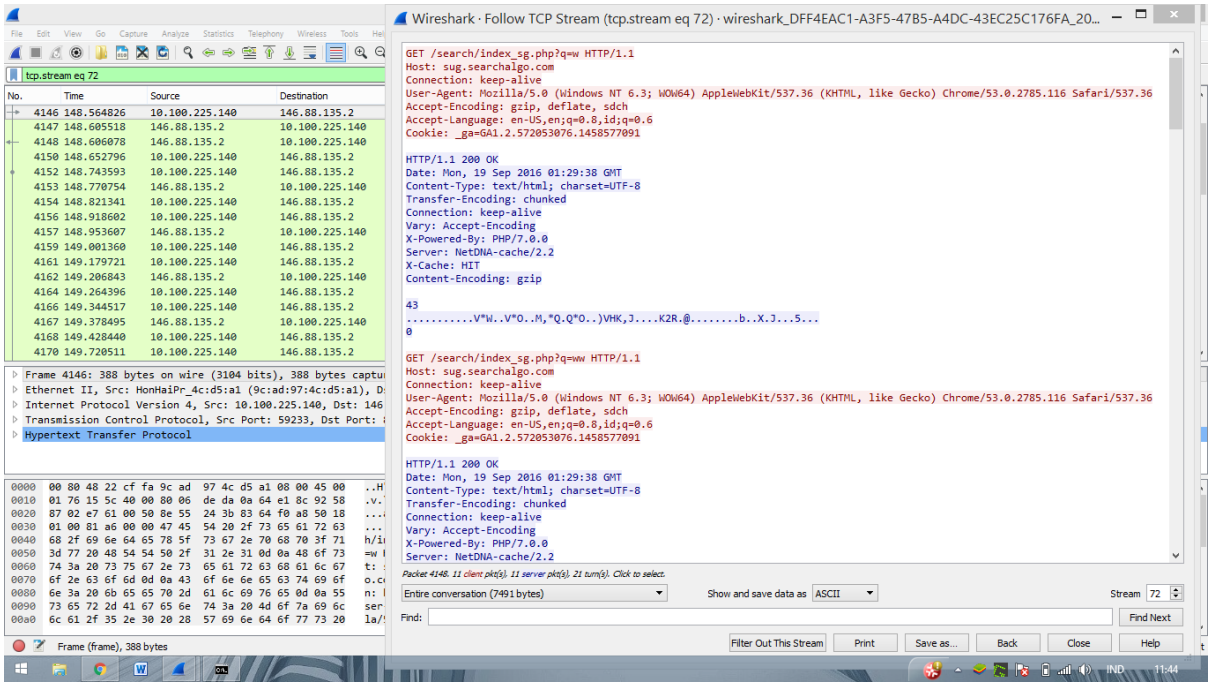


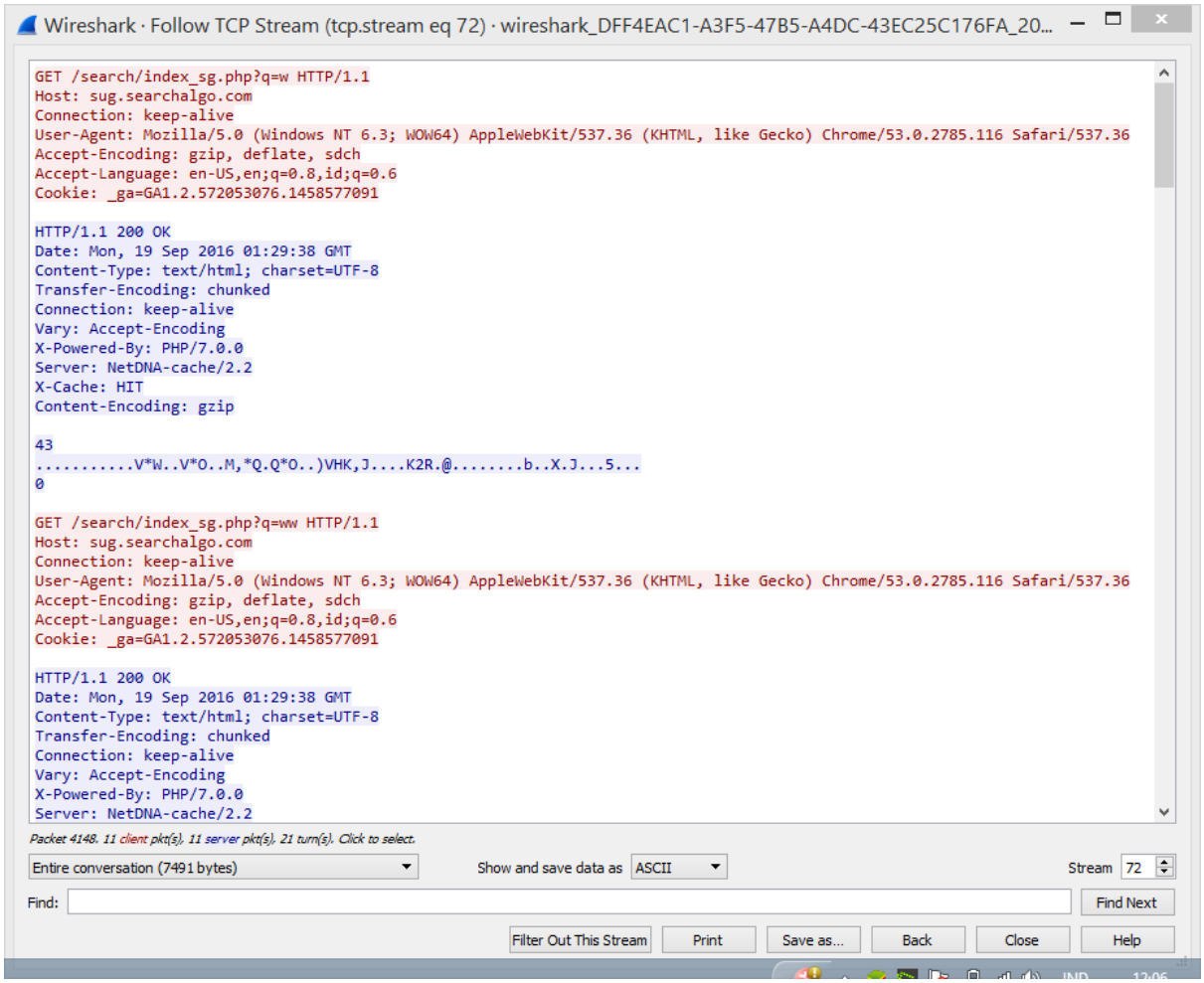
Nampak pada gambar di atas terlihat jelas ketika kita mengetikan username serta password maka akan langsung di encrypted oleh server twitter itu sendiri yang penyimpanan username dan password tersimpan di tempat lain dengan ip 10.100.225.140 dengan source port 443 desination port https (59092) proses peng encrypt an adalah dengan menggunakan protocol ssl

Jalannya sebuah websites yang di akses oleh komputer terlihat jelas dapat di tangkap oleh wireshark dari mulai dari ip, jenis koneksi sampai port kecuali http yang menggunakan jalur ssl yang merupakan jalur yang aman tidak dapat di sniffing karena ketika mengisi file username dan password sudah langsung ter-endkripsi

Dapat di simpulkan bahwa, ketika komputer sumber akan melakukan koneksi ke suatu situs maka komputer sumber akan mengirimkan paket atau broadcast ke server website melalui koneksi tcp/ip beserta portnya kemudian webserver akan mengirimkan balik paket data ke komputer sumber beserta ip dan port untuk di akses dan ketika user akan mengetikan username dan password maka server akan mengencrypted file yang penting tersebut agar aman yang proses pengencryptednya menggunakan ssl dengan cara mengaktifkan proses encripsi di server website jalur aman ini yang disebut dengan https menggunakan ssl.

Get, Respon, dan Post





Analisa :

Membaca Request (Get & Post) :

- GET menunjukkan metode yang digunakan (GET atau POST).
- URL menunjukkan URL untuk permintaan sedang dikirim.
- Protokol dalam hal ini akan menjelaskan HTTP. Hal ini juga menunjukkan versi, yaitu 1.1
- User-Agent berisi informasi tentang browser yang digunakan.
- Accept-Encoding juga merupakan salah satu dari header message yang menunjukkan metode encoding yang berbeda yang dapat diterjemahkan oleh browser dari permintaan yang sedang dikirim.
- Accept-Language adalah
- Cookie, berisi data yang disimpan dalam cookie browser Anda saat ini.

membaca Respon :

- HTTP / 1.1 menunjukkan protokol / versi yang digunakan.

- 200 adalah kode status "OK". Menunjukkan Permintaan telah berhasil. Informasi kembali dengan respon yang tergantung pada metode yang digunakan dalam permintaan, misalnya:
    - GET, entitas sesuai dengan sumber daya yang diminta dikirim dalam respon;
    - HEAD, entitas-header yang sesuai dengan sumber daya yang diminta dikirim dalam respon tanpa message-body;
    - POST, suatu entitas yang menggambarkan atau mengandung hasil dari tindakan;
    - TRACE entitas yang berisi pesan permintaan seperti yang diterima oleh server akhir.
- Tanggal menunjukkan waktu selama respon yang dihasilkan.

IP dan Port pada Comand Prompt