

**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 :

```
C:\windows\system32\cmd.exe - netstat -a
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Fifi>netstat -a
Active Connections
Proto Local Address           Foreign Address         State
TCP 0.0.0.0:445              0.0.0.0:*               LISTENING
TCP 0.0.0.0:2343            0.0.0.0:*               LISTENING
TCP 0.0.0.0:2344            0.0.0.0:*               LISTENING
TCP 0.0.0.0:3580           0.0.0.0:*               LISTENING
TCP 0.0.0.0:3577           0.0.0.0:*               LISTENING
TCP 0.0.0.0:6888           0.0.0.0:*               LISTENING
TCP 0.0.0.0:49152          0.0.0.0:*               LISTENING
TCP 0.0.0.0:49153          0.0.0.0:*               LISTENING
TCP 0.0.0.0:49154          0.0.0.0:*               LISTENING
TCP 0.0.0.0:49155          0.0.0.0:*               LISTENING
TCP 0.0.0.0:49156          0.0.0.0:*               LISTENING
TCP 0.0.0.0:49164          0.0.0.0:*               LISTENING
TCP 0.0.0.0:49165          0.0.0.0:*               LISTENING
TCP 0.0.0.0:59110         0.0.0.0:*               LISTENING
TCP 0.0.0.0:59111         0.0.0.0:*               LISTENING
TCP 10.100.225.140:137     0.0.0.0:*               LISTENING
TCP 10.100.225.140:58517   a184-86-250-10:https   ESTABLISHED
TCP 10.100.225.140:58519   a23-9-107-175:https    ESTABLISHED
TCP 10.100.225.140:58521   a-0003:https           ESTABLISHED
TCP 10.100.225.140:58527   a184-86-250-10:https   ESTABLISHED
TCP 10.100.225.140:58528   a184-86-250-10:https   ESTABLISHED
TCP 10.100.225.140:58529   a184-86-250-10:https   ESTABLISHED
TCP 10.100.225.140:58530   a184-86-250-10:https   ESTABLISHED
TCP 10.100.225.140:58531   a184-86-250-10:https   ESTABLISHED
TCP 10.100.225.140:58532   a184-86-250-10:https   ESTABLISHED
TCP 10.100.225.140:58544   a184-86-250-19:https   ESTABLISHED
TCP 10.100.225.140:58550   a-0003:https           ESTABLISHED
TCP 10.100.225.140:58555   151.101.9.100:https     ESTABLISHED
TCP 10.100.225.140:58566   111.221.29.30:https     ESTABLISHED
TCP 10.100.225.140:58570   111.221.29.30:https     ESTABLISHED
TCP 10.100.225.140:58571   111.221.29.30:https     ESTABLISHED
TCP 10.100.225.140:58574   151.101.9.100:https     ESTABLISHED
TCP 10.100.225.140:58575   151.101.9.100:https     ESTABLISHED
TCP 10.100.225.140:58580   sc-in-f157:https       ESTABLISHED
TCP 10.100.225.140:58590   199.107.193.130:https  ESTABLISHED
TCP 10.100.225.140:58610   sc-in-f140:https       ESTABLISHED
TCP 10.100.225.140:58625   a23-15-111-22:https    ESTABLISHED
TCP 10.100.225.140:58628   198.54.12.127:https    ESTABLISHED
TCP 10.100.225.140:58629   sin10s01-in-f66:https  ESTABLISHED
TCP 10.100.225.140:58636   unknown:https          ESTABLISHED
TCP 10.100.225.140:58637   sc-in-f140:https       ESTABLISHED
TCP 10.100.225.140:58638   a173-222-148-43:https  ESTABLISHED
TCP 10.100.225.140:58639   23.99.125.55:https     ESTABLISHED
TCP 10.100.225.140:58639   a-0003:https           ESTABLISHED
TCP 10.100.225.140:58640   a-0003:https           FIN_WAIT_2
TCP 10.100.225.140:58642   a-0003:https           ESTABLISHED
TCP 10.100.225.140:58643   13.107.5.80:https      ESTABLISHED
TCP 10.100.225.140:58644   151.101.8.249:https    ESTABLISHED
```

## 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.

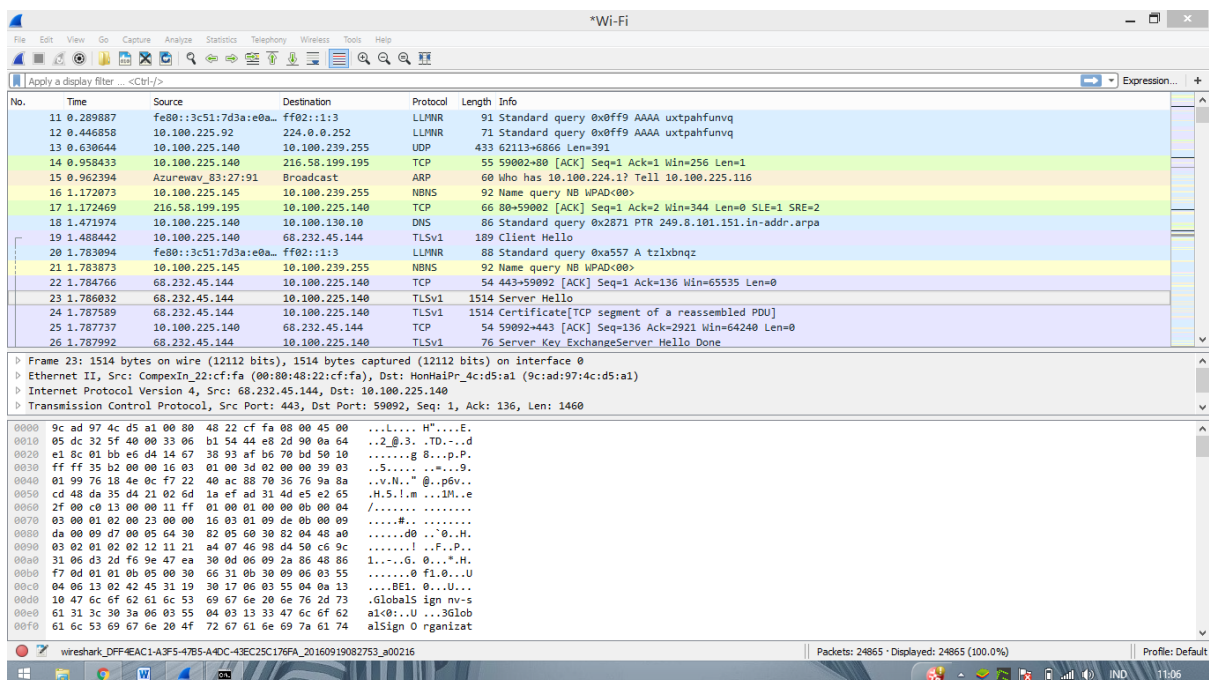
- State - Menunjukkan keadaan koneksi TCP. Mungkin negara adalah sebagai berikut: CLOSE\_WAIT, CLOSED, ESTABLISHED, FIN\_WAIT\_1, FIN\_WAIT\_2, LAST\_ACK, LISTEN, SYN\_RECEIVED, SYN\_SEND, dan TIME\_WAIT. Bila statenya close wait maka artinya tidak tersambung.

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



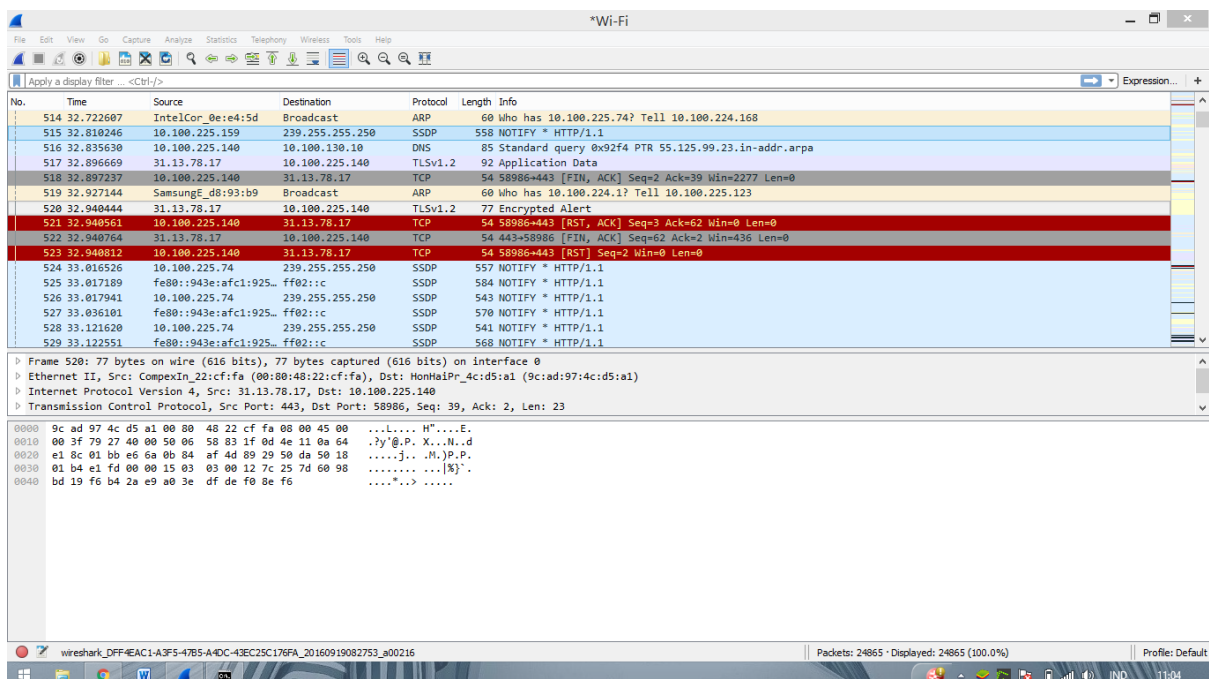
### Analisa :

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

Dari hasil sniffing menggunakan wireshark akan menangkap aktifitas jaringan, 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 gateway 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 gateway 216.58.199.195 (komputer tujuan). setiap komputer sumber mau melakukan koneksi sniffing akan melakukan koneksi ke komputer tujuan /gateway dahulu seperti pada gambar di atas koneksi ini menggunakan metode three way handshake dan sinkronisasi,

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



Wireshark capture showing a DHCP ACK packet. The packet list shows a DHCP ACK from 10.100.225.92 to 10.100.225.140. The packet details show it's a DHCP ACK for transaction ID 0xb6f9ae7. The raw data shows the IP header and the beginning of the DHCP message.

## 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.

Wireshark capture showing a series of DNS and DHCP packets. The packet list shows a sequence of DNS queries and responses, followed by a DHCP ACK. The packet details show the DHCP ACK packet from 10.100.225.92 to 10.100.225.140. The raw data shows the IP header and the beginning of the DHCP message.

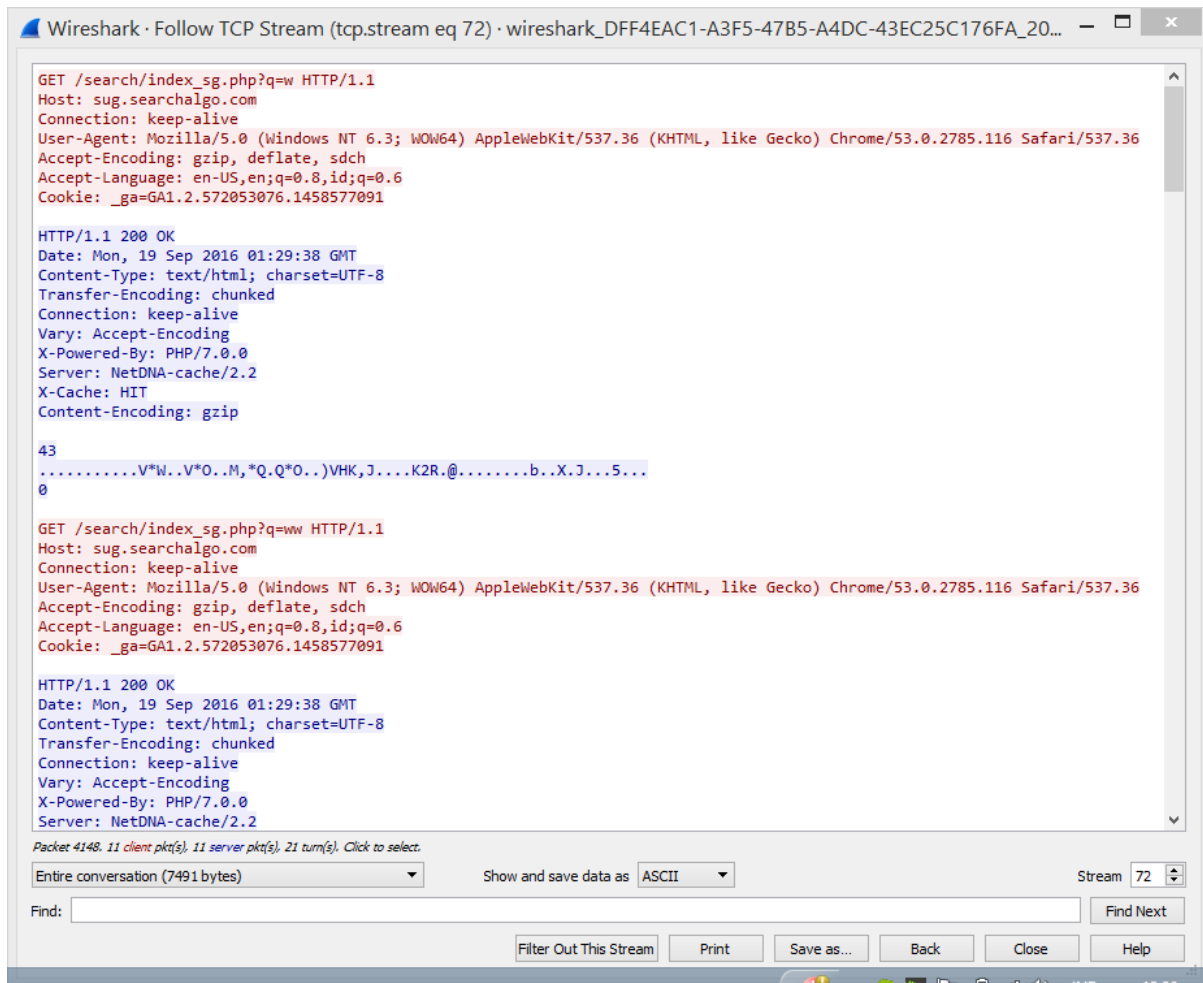
Nampak pada gambar di atas terlihat jelas ketika kita mengetikkan username serta password maka akan langsung di encrypted oleh server twitter itu sendiri yang penyimpanan username dan password tersimpan di tempat lain dengan ip 10.100.225.140 dengan source port 443 destination port https (59092) proses pengencrypt 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-encrypt

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 mengetikkan username dan password maka server akan mengencrypted file yang penting tersebut agar aman yang proses pengencryptednya menggunakan ssl dengan cara mengaktifkan proses encrpsi di server website jalur aman ini yang disebut dengan https menggunakan ssl.

## Get, Respon, dan Post

The screenshot displays the Wireshark interface with a TCP stream capture. The main pane shows a list of packets with columns for No., Time, Source, and Destination. Packet 4146 is highlighted, showing a GET request to /search/index\_sg.php?q=w. The details pane below shows the structure of the request, including the Host (sug.searchaigo.com), User-Agent (Mozilla/5.0), Accept-Encoding (gzip, deflate, sdch), and Cookie (\_ga=GA1.2.572053076.1458577091). The response pane shows an HTTP/1.1 200 OK status, Date (Mon, 19 Sep 2016 01:29:38 GMT), Content-Type (text/html; charset=UTF-8), and Transfer-Encoding (chunked). The raw data pane shows the hexadecimal and ASCII representation of the response body, which appears to be a large block of data.



## 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

```

C:\windows\system32\cmd.exe
C:\Users\Fifi>netstat
Active Connections

Proto Local Address          Foreign Address        State
TCP   10.100.225.140:60427    sa-in-f188:5228       ESTABLISHED
TCP   10.100.225.140:61487    sa-in-f139:https      ESTABLISHED
TCP   10.100.225.140:61589    s-prd-umpxl-adcom_nwa_blue:https TIME_WAIT
TCP   10.100.225.140:61698    kul01s10-in-f14:https CLOSE_WAIT
TCP   10.100.225.140:61699    kul01s10-in-f14:https TIME_WAIT
TCP   10.100.225.140:61766    sc-in-f132:http       CLOSE_WAIT
TCP   10.100.225.140:61774    sa-in-f132:http       CLOSE_WAIT
TCP   10.100.225.140:61775    sc-in-f132:http       CLOSE_WAIT
TCP   10.100.225.140:61921    151.101.1.69:http     ESTABLISHED
TCP   10.100.225.140:61922    sc-in-f141:https      TIME_WAIT
TCP   10.100.225.140:61925    151.101.129.69:http   ESTABLISHED
TCP   10.100.225.140:61926    151.101.129.69:http   ESTABLISHED
TCP   10.100.225.140:61927    104.16.111.18:https   CLOSE_WAIT
TCP   10.100.225.140:61936    104.16.13.8:http      CLOSE_WAIT
TCP   10.100.225.140:61937    a173-222-148-40:http  ESTABLISHED
TCP   10.100.225.140:61938    104.16.13.8:http      CLOSE_WAIT
TCP   10.100.225.140:61942    sin04s09-in-f206:https ESTABLISHED
TCP   10.100.225.140:61944    a173-222-148-35:http  ESTABLISHED
TCP   10.100.225.140:61945    ec2-23-23-73-103:http CLOSE_WAIT
TCP   10.100.225.140:61947    ec2-23-23-73-103:http CLOSE_WAIT
TCP   10.100.225.140:61948    stackoverflow:https   ESTABLISHED
TCP   10.100.225.140:61952    kul01s11-in-f2:http   ESTABLISHED
TCP   10.100.225.140:61954    sa-in-f149:https      ESTABLISHED
TCP   10.100.225.140:61956    sa-in-f156:https      ESTABLISHED
TCP   10.100.225.140:61957    sa-in-f149:https      ESTABLISHED
TCP   10.100.225.140:61958    kul01s11-in-f2:https  ESTABLISHED
TCP   10.100.225.140:61984    s3-1-w:https          CLOSE_WAIT
TCP   10.100.225.140:61985    s3-1-w:https          CLOSE_WAIT
TCP   127.0.0.1:49157        Lenovo-PC:49160       ESTABLISHED
TCP   127.0.0.1:49158        Lenovo-PC:49159       ESTABLISHED
TCP   127.0.0.1:49159        Lenovo-PC:49158       ESTABLISHED
TCP   127.0.0.1:49160        Lenovo-PC:49157       ESTABLISHED
TCP   127.0.0.1:49161        Lenovo-PC:49162       ESTABLISHED
TCP   127.0.0.1:49162        Lenovo-PC:49161       ESTABLISHED
TCP   127.0.0.1:58325        Lenovo-PC:58326       ESTABLISHED
  
```