TUGAS V

JARINGAN KOMPUTER

Nama : Randa Fratelli Junaedi

Nim : 09011181419006

Nama Dosen : Deris Stiawan, M.T. PH.D

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2016

TASK V

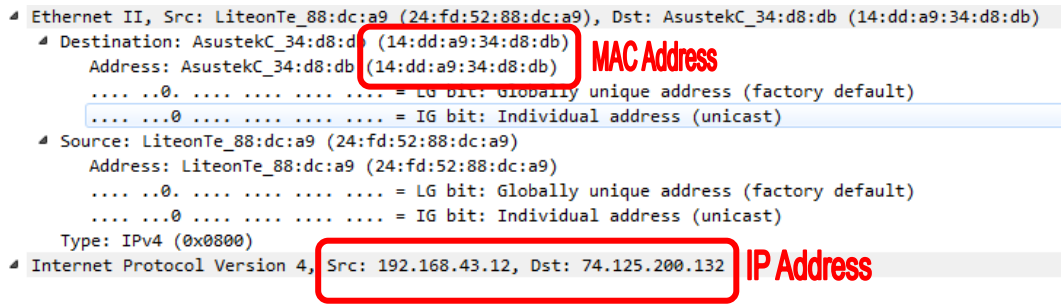
CAPTURING PAKET PADA DENGAN WIRESHARK

Wireshark adalah sebuah tool yang sangat berguna untuk analisa forensik paket data yang ada pada sebuah jaringan secara real time berdasarkan protokol pengirimanya.

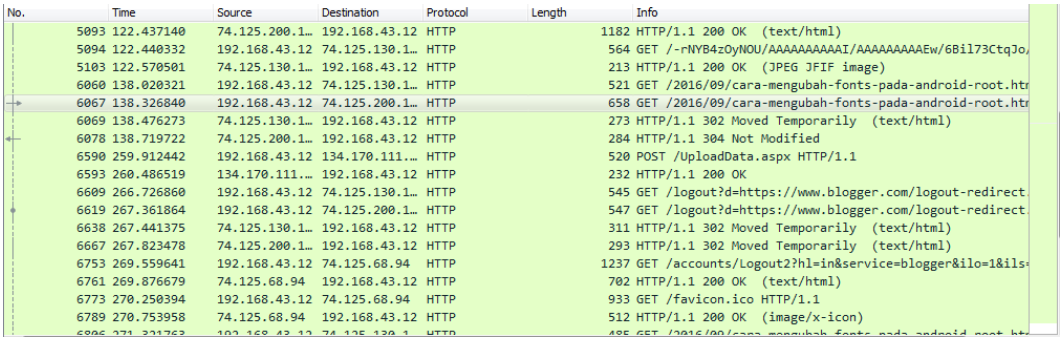
Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya. Pada tingkatan yang terendah, protokol mendefinisikan koneksi perangkat keras. Paket data antar komputer dikirimkan melalui sebuah protokol untuk berkomunikasi, mulai dari penamaan suatu komputer, penentuan media pengiriman, rute pengiriman, error correction, enkripsi paket, hingga menentukan jenis paket yang dikirim.

MAC Address (Media Access Control Address) adalah sebuah alamat jaringan yang diimplementasikan pada lapisan data-link dalam tujuh lapisan model OSI, yang merepresentasikan sebuah node tertentu dalam jaringan. Dalam sebuah jaringan berbasis Ethernet, MAC address merupakan alamat yang unik yang memiliki panjang 48-bit (6 byte) yang mengidentifikasikan sebuah komputer, interface dalam sebuah router, atau node lainnya dalam jaringan. MAC Address juga sering disebut sebagai Ethernet address, physical address, atau hardware address.

Contoh MAC Address :



HTTP (HyperText Transfer Protocol)



No.	Time	Source	Destination	Protocol	Length	Info
5093	122.437140	74.125.200.1…	192.168.43.12	HTTP	1182	HTTP/1.1 200 OK (text/html)
5094	122.440332	192.168.43.12	74.125.130.1…	HTTP	564	GET /-rNYB4zOyNOU/AAAAAAAAAAI/AAAAAAAAAEw/6Bil73CtqJo/
5103	122.570501	74.125.130.1…	192.168.43.12	HTTP	213	HTTP/1.1 200 OK (JPEG JFIF image)
6060	138.020321	192.168.43.12	74.125.130.1…	HTTP	521	GET /2016/09/cara-mengubah-fonts-pada-android-root.htr
6067	138.326840	192.168.43.12	74.125.200.1…	HTTP	658	GET /2016/09/cara-mengubah-fonts-pada-android-root.htr
6069	138.476273	74.125.130.1…	192.168.43.12	HTTP	273	HTTP/1.1 302 Moved Temporarily (text/html)
6078	138.719722	74.125.200.1…	192.168.43.12	HTTP	284	HTTP/1.1 304 Not Modified
6590	259.912442	192.168.43.12	134.170.111.…	HTTP	520	POST /UploadData.aspx HTTP/1.1
6593	260.486519	134.170.111.…	192.168.43.12	HTTP	232	HTTP/1.1 200 OK
6609	266.726860	192.168.43.12	74.125.130.1…	HTTP	545	GET /logout?d=https://www.blogger.com/logout-redirect
6619	267.361864	192.168.43.12	74.125.200.1…	HTTP	547	GET /logout?d=https://www.blogger.com/logout-redirect
6638	267.441375	74.125.130.1…	192.168.43.12	HTTP	311	HTTP/1.1 302 Moved Temporarily (text/html)
6667	267.823478	74.125.200.1…	192.168.43.12	HTTP	293	HTTP/1.1 302 Moved Temporarily (text/html)
6753	269.559641	192.168.43.12	74.125.68.94	HTTP	1237	GET /accounts/Logout2?hl=in&service=blogger&ilo=1&ils=
6761	269.876679	74.125.68.94	192.168.43.12	HTTP	702	HTTP/1.1 200 OK (text/html)
6773	270.250394	192.168.43.12	74.125.68.94	HTTP	933	GET /favicon.ico HTTP/1.1
6789	270.753958	74.125.68.94	192.168.43.12	HTTP	512	HTTP/1.1 200 OK (image/x-icon)

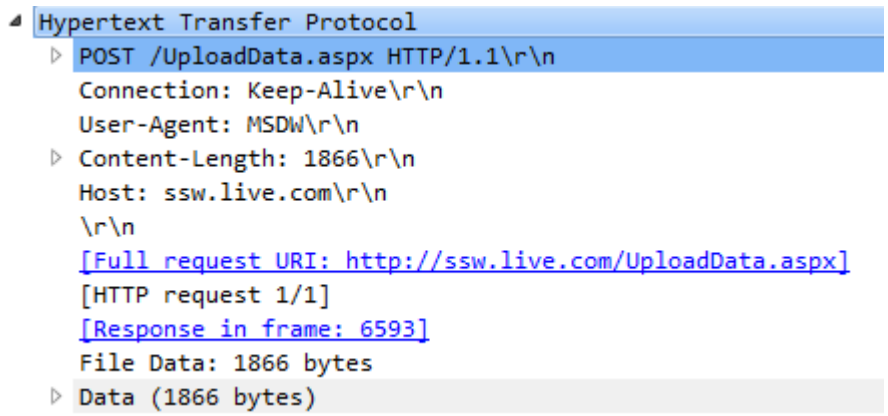
definisi HTTP (HyperText Transfer Protocol) adalah sebuah protokol untuk meminta dan menjawab antara client dan server. Sebuh client HTTP seperti web browser, biasanya memulai permintaan dengan membuat hubungan TCP/IP ke port tertentu di tempat yang jauh. Sebuah server HTTP yang mendengarkan di port tersebut menunggu client mengirim kode permintaan (request) yang akan meminta halaman yang sudah ditentukan, Klien HTTP terhubung ke server HTTP menggunakan TCP. Setelah membuat sambungan, klien dapat mengirim pesan permintaan HTTP Ke server.

HTTP digunakan untuk mengirimkan permintaan dari klien web (browser) ke web server, dikembali kan ke konten web (halaman web) dari server ke klien.

HTTP tidaklah terbatas untuk penggunaan dengan TCP/IP, meskipun HTTP merupakan salah satu protokol aplikasi TCP/IP paling populer melalui Internet. Memang HTTP dapat diimplementasikan di atas protokol yang lain di atas Internet atau di atas jaringan lainnya.

Saat Client mengakses web, Akan ada dua paket HTTP yaitu GET dimana client melakukan request pada webserver dan POST dimana client mengirimkan data ke webserver.

Contoh POST :



```
▲ Hypertext Transfer Protocol
  ▷ POST /UploadData.aspx HTTP/1.1\r\n
    Connection: Keep-Alive\r\n
    User-Agent: MSDW\r\n
  ▷ Content-Length: 1866\r\n
    Host: ssw.live.com\r\n
    \r\n
    [Full request URI: http://ssw.live.com/UploadData.aspx]
    [HTTP request 1/1]
    [Response in frame: 6593]
    File Data: 1866 bytes
  ▷ Data (1866 bytes)
```

POST dimana client mengirimkan data ke webserver, pada informasi paket POST kita Bisa melihat informasi apa saja yang dikirim client ke webserver, pada gambar diatas POST melakukan pengiriman upload data.

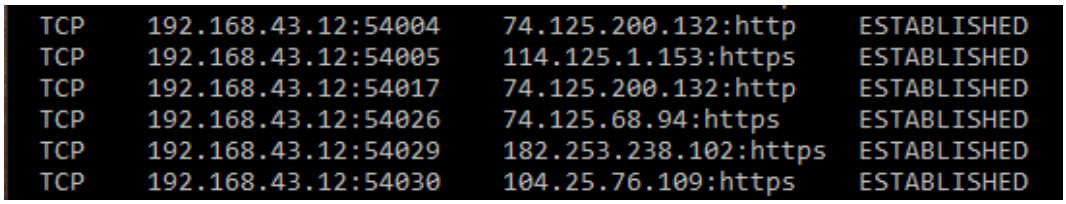
Contoh GET :

GET merupakan dimana client melakukan request pada webserver, dan pada gambar diatas client meminta request pada webserver yang berupa situs http://familyr3i1.blogspot.co.id/2016/09/cara-mengubah-fonts-pada-android-root.html

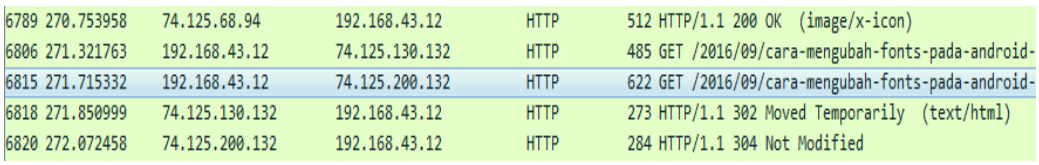
Netstat

Netstat merupakan salah satu perintah dasar pada GNU/Linux yang mempunyai fungsi untuk memantau aktifitas yang ada di jaringan dan tentunya dijalankan dengan mode teks alias dengan terminal/konsol.

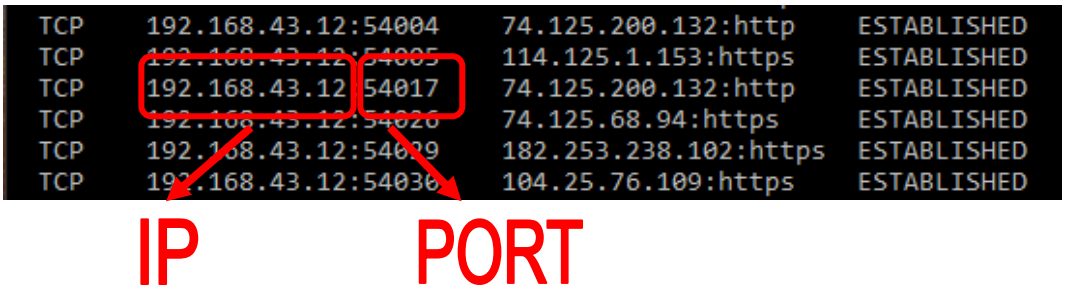
Contoh Netstat



Contoh HTTP menggunakan wireshark



Dalam netstat mendapatkan 192.168.43.12 dan port 54017



Dan dalam wireshark yang dimana IP Source 192.168.43.12 dan port 54017, dan pada IP Destination 74.125.200.132 dan port 80