TUGAS JARINGAN KOMPUTER

DISUSUN OLEH :

Nama : Dera Gustina

Nim : 09011181419003

Nama dosen : Dr. Deris Stiawan,M.T

Jurusan : Sistem Komputer

Fakultas : Ilmu Komputer

Universitas Sriwijaya

Menggunakan software wireshark dan command untuk mengetahui tentang network traffic

PENJELASAN :

● Pengertian protokol : Protokol adalah aturan main yang mengatur komunikasi diantara beberapa komputer di dalam sebuah jaringan sehingga komputer-komputer anggota jaringan dan komputer berbeda platform dapat saling berkomunikasi.

● Pengertian GET : Get adalah Sebuah permintaan GET mengambil data dari web server dengan menentukan parameter di bagian URL dari permintaan. Jika Anda memeriksa contoh permintaan HTTP bawah ini, kami minta index.html, dan melewati report_id parameter.

● Pengertian POST : post adalah Sebuah permintaan HTTP POST memanfaatkan badan pesan untuk mengirim data ke server web.

● Pengertian PUT : PUT adalah mirip dengan POST memanfaatkan badan pesan untuk mentransfer data. Namun, ada beberapa perbedaan mendasar antara keduanya. Pertama PUT dianggap idempotent, kedua tindakan seorang PUT ini selalu ditetapkan untuk URI tertentu, akhirnya PUT adalah untuk memuat data untuk sumber daya itu. Dengan kata lain Anda harus tahu lokasi yang tepat dari mana data yang Anda kirimkan akan diambil nanti.

● Pengertian HEAD : head adalah HTTP Metode yang digunakan untuk mengambil informasi tentang URL dari web server.

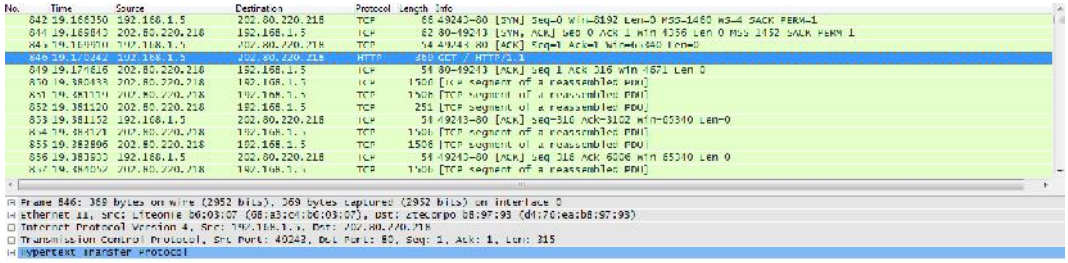
● Pengertian DELETE : Menghapus sumber daya tertentu dari web server.

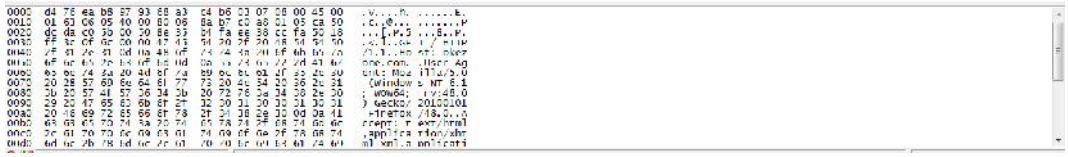
● Pengertian TRACE : Metode ini menggemakan kembali permintaan yang diterima sehingga klien HTTP dapat melihat apa server menengah menambahkan atau mengubah permintan.

● Pengertian OPTIONS : Metode ini membantu menentukan fungsi server seperti menentukan metode mana yang mendukung web server.

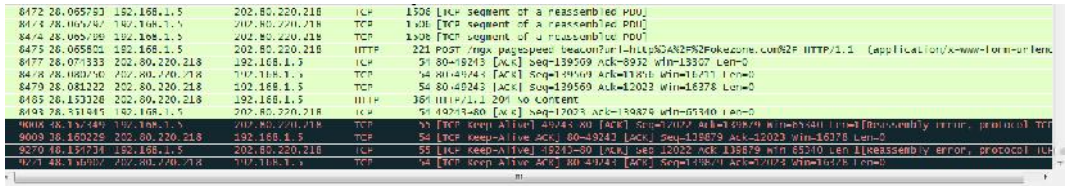
● Pengertian CONNECT : Metode connect mengubah Permintaan koneksi ke terowongan TCP / IP transparan. Hal ini membantu memfasilitasi Secure Socket Layer (SSL) berkomunikasi (HTTPS) melalui proxy HTTP yang tidak terenkripsi

Gambar dibawah ini adalah analisis cappture menganalisis traffic websate www.okezone.com menggunakan software wirkshark :

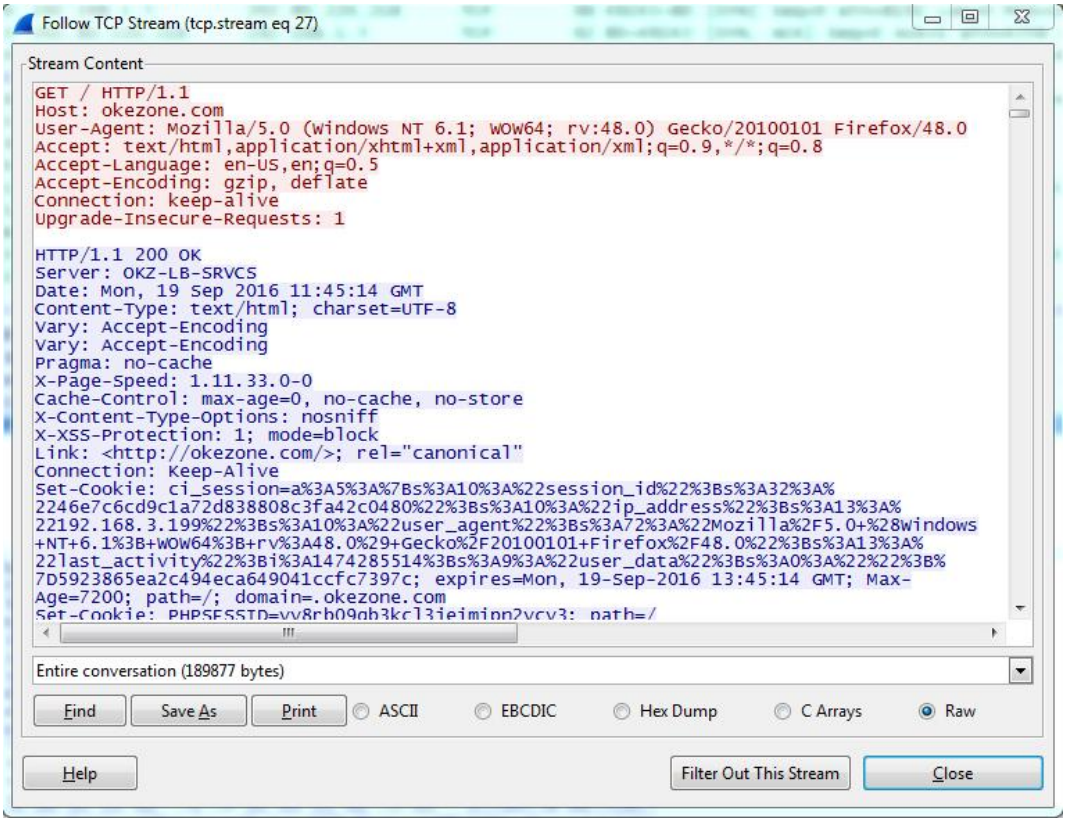




Okezone.com



Okezone.com



Sotware Wireshark memiliki kemampuan untuk menangkap lalu lalang kegiatan yang terjadi pada jaringan milik kita. Selain itu juga bisa mem-filter protokol lain selain ICMP, seperti HTTP dan lain-lain.

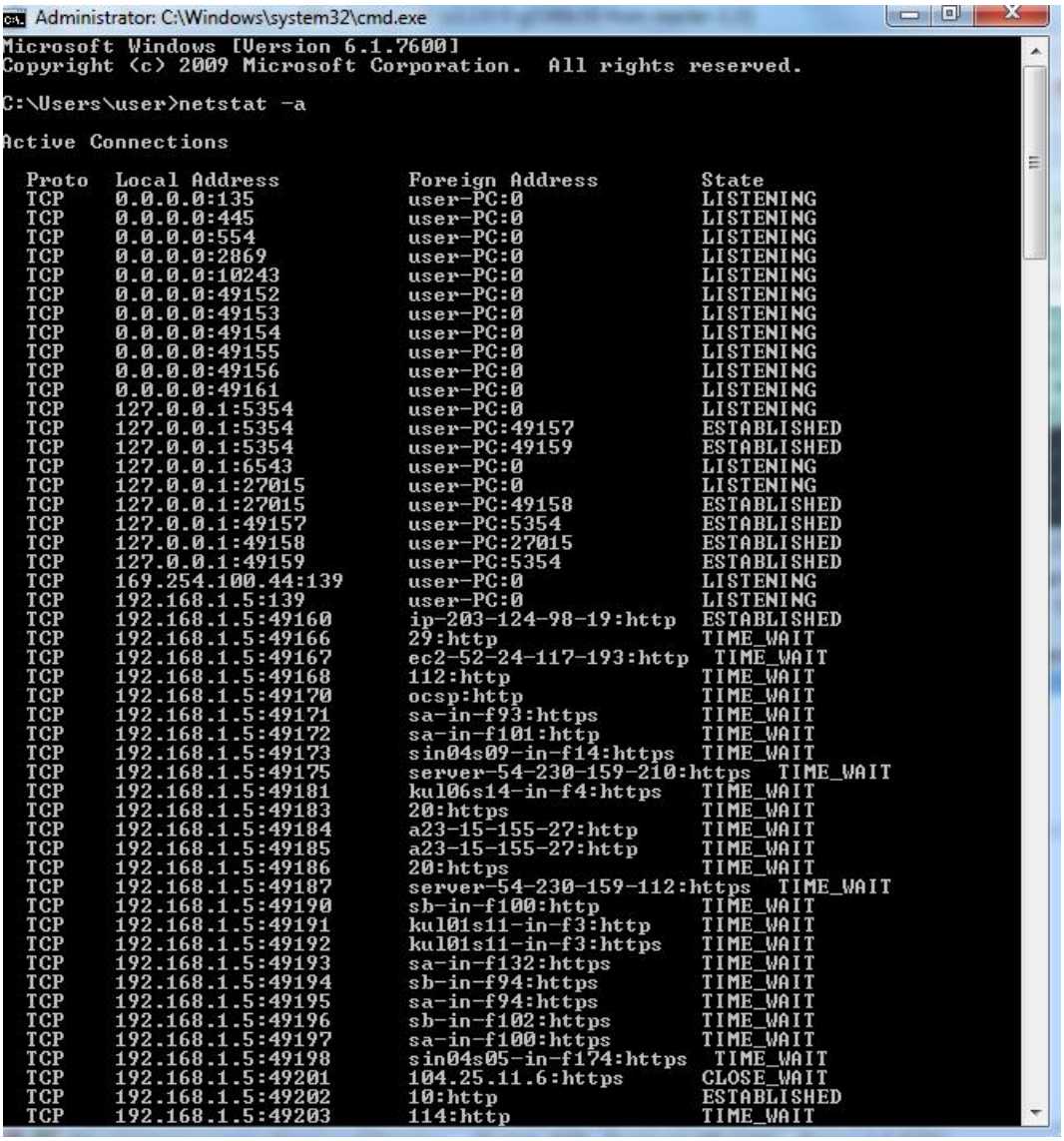
Panel pertama merupakan daftar dari data packet yang telah dicapture. Biasanya diurutkan berdasarkan waktu. Panel ini berisi no packet, waktu saat packet di capture, tujuan dan sumber dari packet, protocol yang digunakan dan panjangnya. Hasil yang difilter merupakan hasil dari filter dari packet yang berisi method ‘GET’.

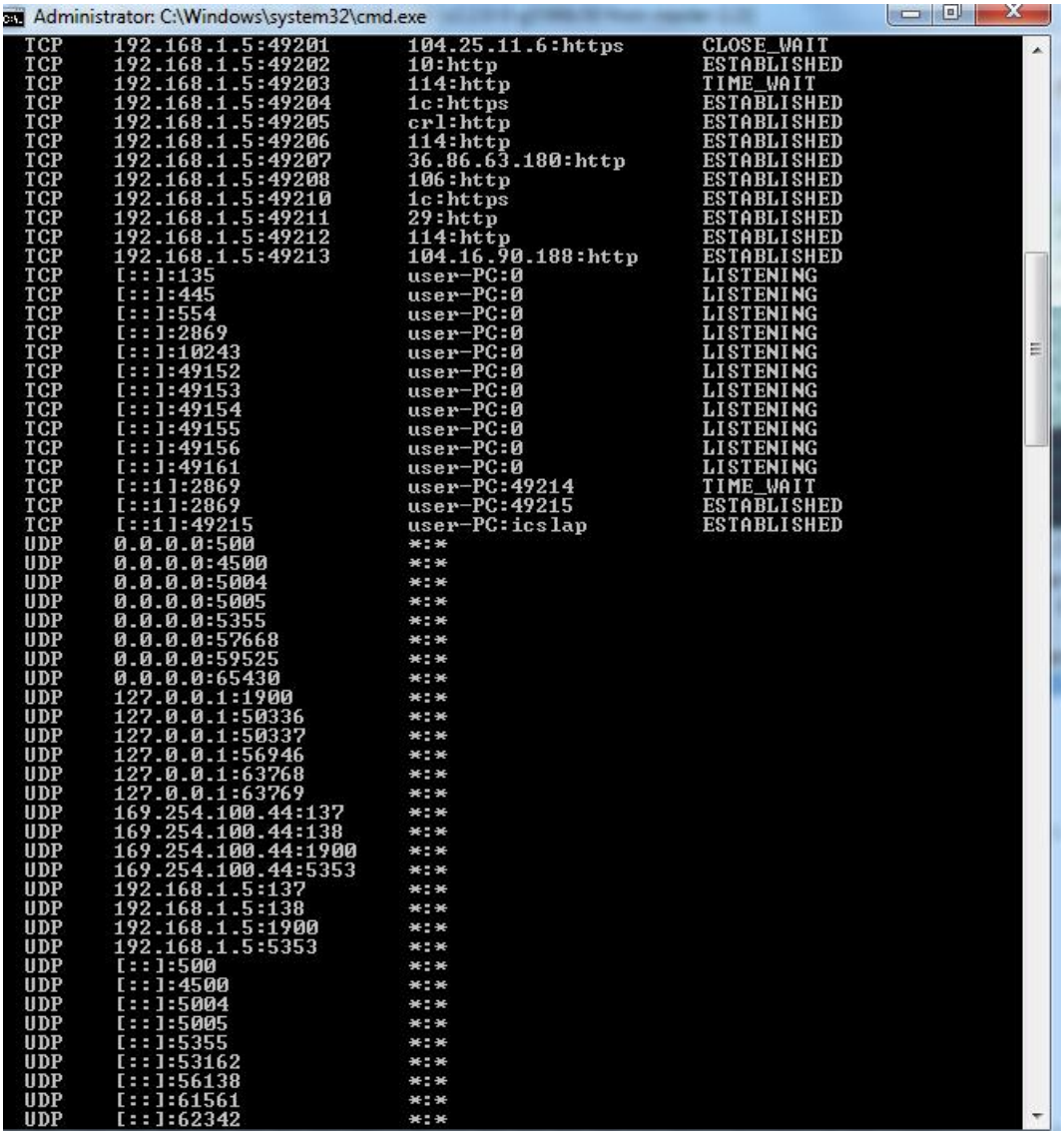
Panel ini berisi detail data dari packet yang dipilih di daftar packet. Di baris pertama terdapat frame 93 yang pada umumnya berisi data dari waktu dan panjang paket. Baris Kedua yang terdapat tulisan Ethernet II berisi informasi hardware dari pengirim dan penerima paket. Baris Ketiga berisi versi Internet Protocol. Dari screenshot diatas terlihat IP yang digunakan IPv4 dan jug terlihat IP pengirim dan penerima. Baris Keempat berisi Transmission Control Protocol,

ini berisi daftar port pengirim dan port penerima dan flag yang diset untuk paket yang menandakan apakah paket itu sekuensial atau request acknowledgment. Baris Kelima berisi Hyper Text Transfer Protocol yaitu packet tersebut menggunakan protocol HTTP.
Panel ketiga merupakan Bytes dari paket. Panel ini berisi data yang diterima atau dikirim dalam bentuk hexadecimal. Karena kita tidak bisa membaca hexadecimal secara langsung maka dibagian kanan dari data hexadcimal terdapat 'terjemahan'nya.

Ip yang ada pada komputer saya adalah 192.168.1.5 dan ip destination adalah 202.80.220.218 . Terlihat bahwa respon server terhadap Method GET tersebut adalah OK dan pada bagian bawahnya berisi element website tersebut dengan bahasa html, Namun tidak ditemukan Methode POST maupun RESPONS. Pada method POST sendiri, Permintaan POST digunakan untuk mengirim data ke server, misalnya, informasi pelanggan, file upload, dll menggunakan bentuk HTML sedangkan dalam kasus ini hanya ditugaskan untuk mengunjungi sebuah situs kemudian dicapture dan method POST tidak terbaca karena kita tidak melakukan login,search pada website maupun login ke website tersebut. Sedangkan untuk method RESPONS dapat dilihat pada bagian GET yang didalamnya merupakan respon dari server yang dituju dalam kasus ini jika website berhasil dikunjungi maka akan menghasilkan RESPONS OK.

Selain menggunakan software wirshark analisis yang saya gunakan juga menggunakan commad promnt dimana hasilnya adalah sebagai berikut :


Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\user>netstat -a
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 user-PC:0 LISTENING
TCP 0.0.0.0:445 user-PC:0 LISTENING
TCP 0.0.0.0:554 user-PC:0 LISTENING
TCP 0.0.0.0:2869 user-PC:0 LISTENING
TCP 0.0.0.0:10243 user-PC:0 LISTENING
TCP 0.0.0.0:49152 user-PC:0 LISTENING
TCP 0.0.0.0:49153 user-PC:0 LISTENING
TCP 0.0.0.0:49154 user-PC:0 LISTENING
TCP 0.0.0.0:49155 user-PC:0 LISTENING
TCP 0.0.0.0:49156 user-PC:0 LISTENING
TCP 0.0.0.0:49161 user-PC:0 LISTENING
TCP 127.0.0.1:5354 user-PC:0 LISTENING
TCP 127.0.0.1:5354 user-PC:49157 ESTABLISHED
TCP 127.0.0.1:5354 user-PC:49159 ESTABLISHED
TCP 127.0.0.1:6543 user-PC:0 LISTENING
TCP 127.0.0.1:27015 user-PC:0 LISTENING
TCP 127.0.0.1:27015 user-PC:49158 ESTABLISHED
TCP 127.0.0.1:49157 user-PC:5354 ESTABLISHED
TCP 127.0.0.1:49158 user-PC:27015 ESTABLISHED
TCP 127.0.0.1:49159 user-PC:5354 ESTABLISHED
TCP 169.254.100.44:139 user-PC:0 LISTENING
TCP 192.168.1.5:139 user-PC:0 LISTENING
TCP 192.168.1.5:49160 ip-203-124-98-19:http ESTABLISHED
TCP 192.168.1.5:49166 29:http TIME_WAIT
TCP 192.168.1.5:49167 ec2-52-24-117-193:http TIME_WAIT
TCP 192.168.1.5:49168 112:http TIME_WAIT
TCP 192.168.1.5:49170 ocsp:http TIME_WAIT
TCP 192.168.1.5:49171 sa-in-f93:https TIME_WAIT
TCP 192.168.1.5:49172 sa-in-f101:http TIME_WAIT
TCP 192.168.1.5:49173 sin04s09-in-f14:https TIME_WAIT
TCP 192.168.1.5:49175 server-54-230-159-210:https TIME_WAIT
TCP 192.168.1.5:49181 kul06s14-in-f4:https TIME_WAIT
TCP 192.168.1.5:49183 20:https TIME_WAIT
TCP 192.168.1.5:49184 a23-15-155-27:http TIME_WAIT
TCP 192.168.1.5:49185 a23-15-155-27:http TIME_WAIT
TCP 192.168.1.5:49186 20:https TIME_WAIT
TCP 192.168.1.5:49187 server-54-230-159-112:https TIME_WAIT
TCP 192.168.1.5:49190 sb-in-f100:http TIME_WAIT
TCP 192.168.1.5:49191 kul01s11-in-f3:http TIME_WAIT
TCP 192.168.1.5:49192 kul01s11-in-f3:https TIME_WAIT
TCP 192.168.1.5:49193 sa-in-f132:https TIME_WAIT
TCP 192.168.1.5:49194 sb-in-f94:https TIME_WAIT
TCP 192.168.1.5:49195 sa-in-f94:https TIME_WAIT
TCP 192.168.1.5:49196 sb-in-f102:https TIME_WAIT
TCP 192.168.1.5:49197 sa-in-f100:https TIME_WAIT
TCP 192.168.1.5:49198 sin04s05-in-f174:https TIME_WAIT
TCP 192.168.1.5:49201 104.25.11.6:https CLOSE_WAIT
TCP 192.168.1.5:49202 10:http ESTABLISHED
TCP 192.168.1.5:49203 114:http TIME_WAIT



Pada hasil capture diatas command yang dugunakan yaitu “netstat –a” dan muncul tampilan seperti diatas. Cara membaca hasil capture menggunakan

command netstat –a adalah melihat Local Address yang merupakan IP Address komputer kita sendiri atau merupakan source dan untuk Destination dapat dilihat pada bagian Foreign Address. Sedangkan untuk state merupakan keadaan dari proses lalu lintas data tersebut misalkan listening dapat diartikan menunggu respon user, time wait merupakan proses menunggu respon dari destination.

Gambar diatas adalah gambar ip yang ada pada komputer yang saya gunakan