SISTEM INFORMASI BILLINGUAL

Analisa Data Menggunakan Wireshark

Oleh

DIRGA RAZZAK (09031381419071)

SI-4A

PROGRAM STUDY SISTEM INFORMASI BILLINGUAL

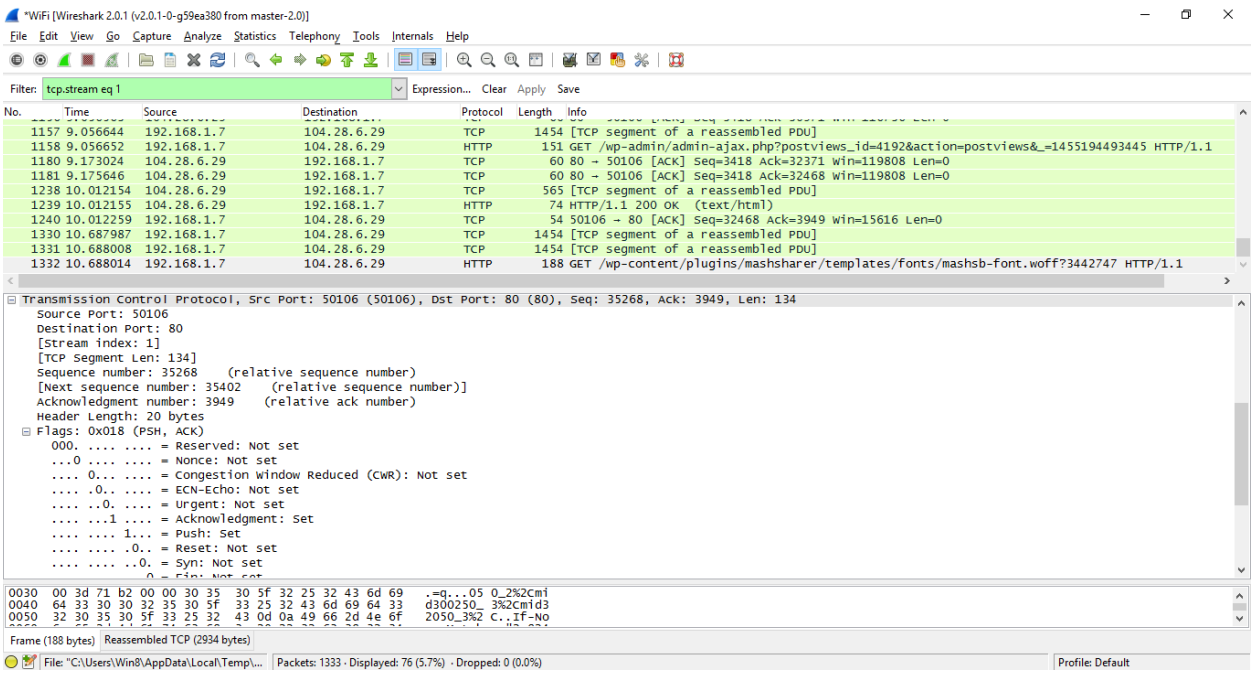
FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

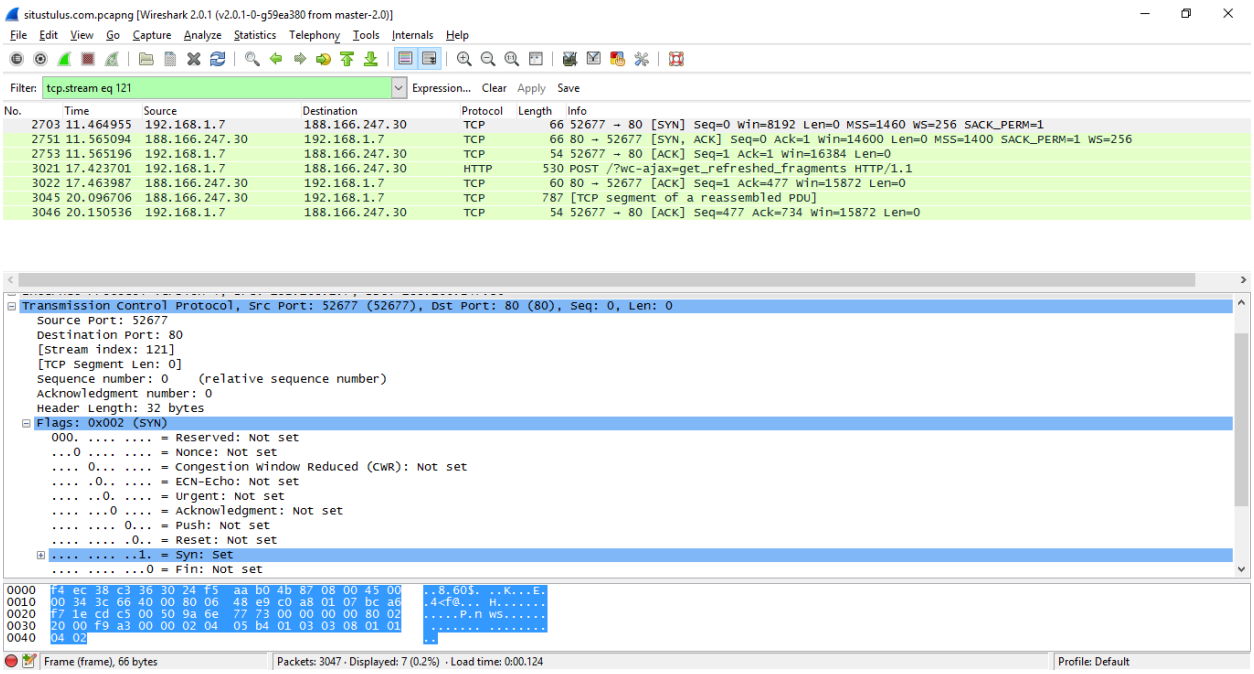
2015-2016

Wireshark adalah program yang berfungsi untuk mengetahui kejadian yang terjadi pada saat kita melakukan interaksi dengan internet.Dengan wireshark dapat dilihat proses pengiriman data dari komputer ke web yang dituju.berikut ini adalah analisa hasil dari capture yang dilakukan dengan menggunkan wireshark.

Capture pertama adalah capture pengunaan wireshark dengan membuka satu tab yaitu meminta request dari komputer ke www.segiempat.com :



(www.segiempat.com)

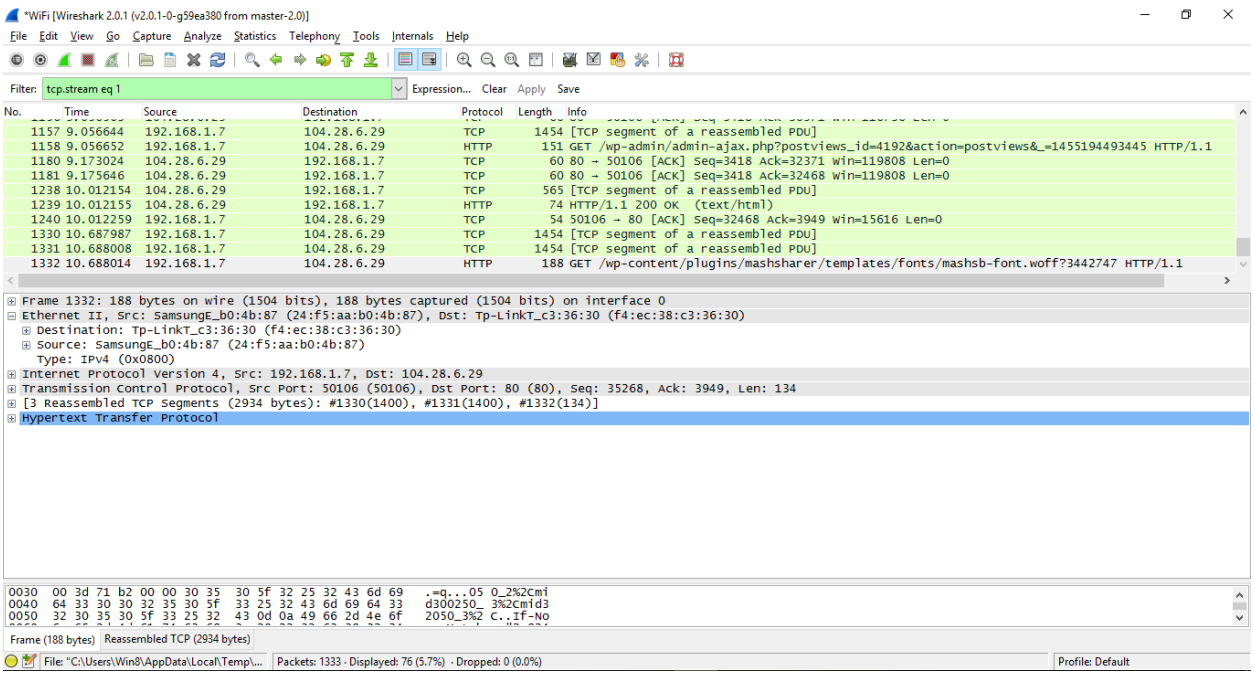


(www.situstulus.com)

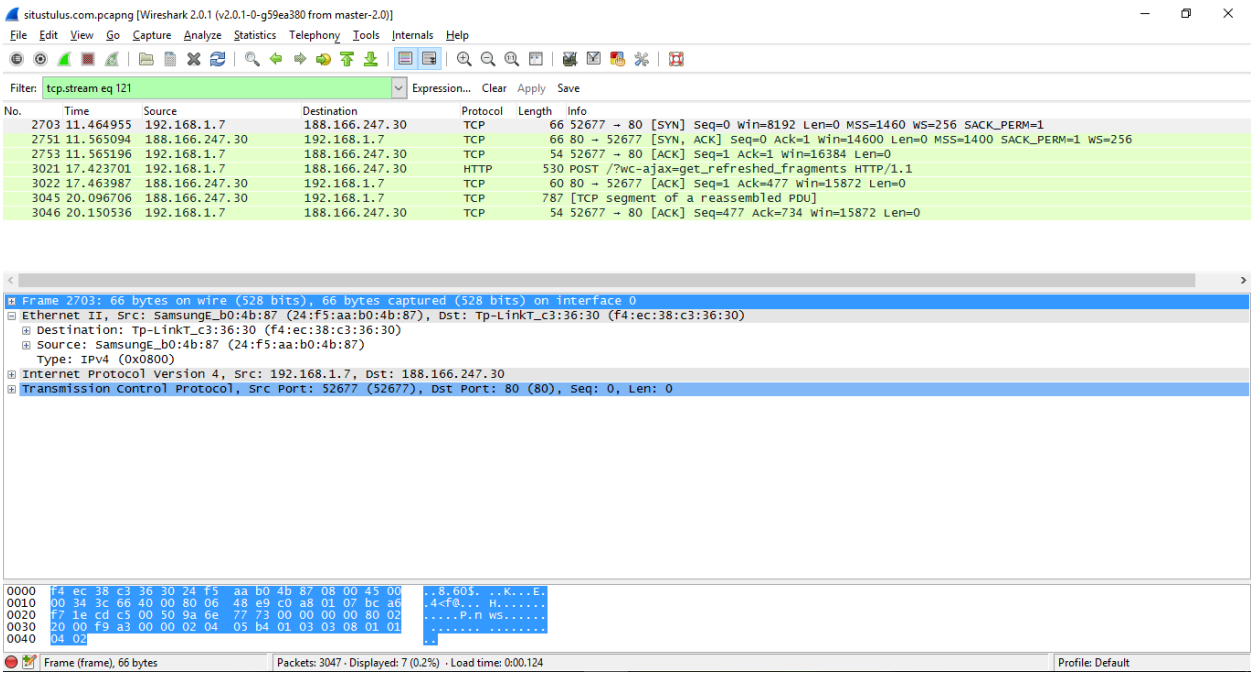
Gambar I

Pada gambar I komputer dengan IP 74.125.130.113 ketika memasukkan www.segiempat.com maka akan mengirimkan data data ke server dan juga data tersebut akan dikirim ke DNS untuk diketahui IP nya.Setelah IP diterjemahkan oleh DNS,maka DNS akan mengirimkan kembali IP segiempat ke komputer yang bertanya.Kemudian setelah dilakukan translasi dari www.segiempat.com ke 104.28.6.29 yang merupakan IP google maka komputer dengan IP 74.125.130.113 melakukan request ke destination 104.28.6.29 dengan menggunakan protocol TCP.Penggunaan TCP karena TCP merupakan protocol yang digunakan untuk melakukan browsing.Pada frame 1332 bisa dilihat Panjang headernya 20 byte,port yang diminta adalah 80 dan source port adalah 50106.

Setelah barulah di frame 2703 menyusul website www.situstulus.com diketahui IP nya 188.166.247.30 bisa di lihat panjang headernya 32 byte, port yang diminta adalah 80 dan source portnya 52677.



(www.segiempat.com)



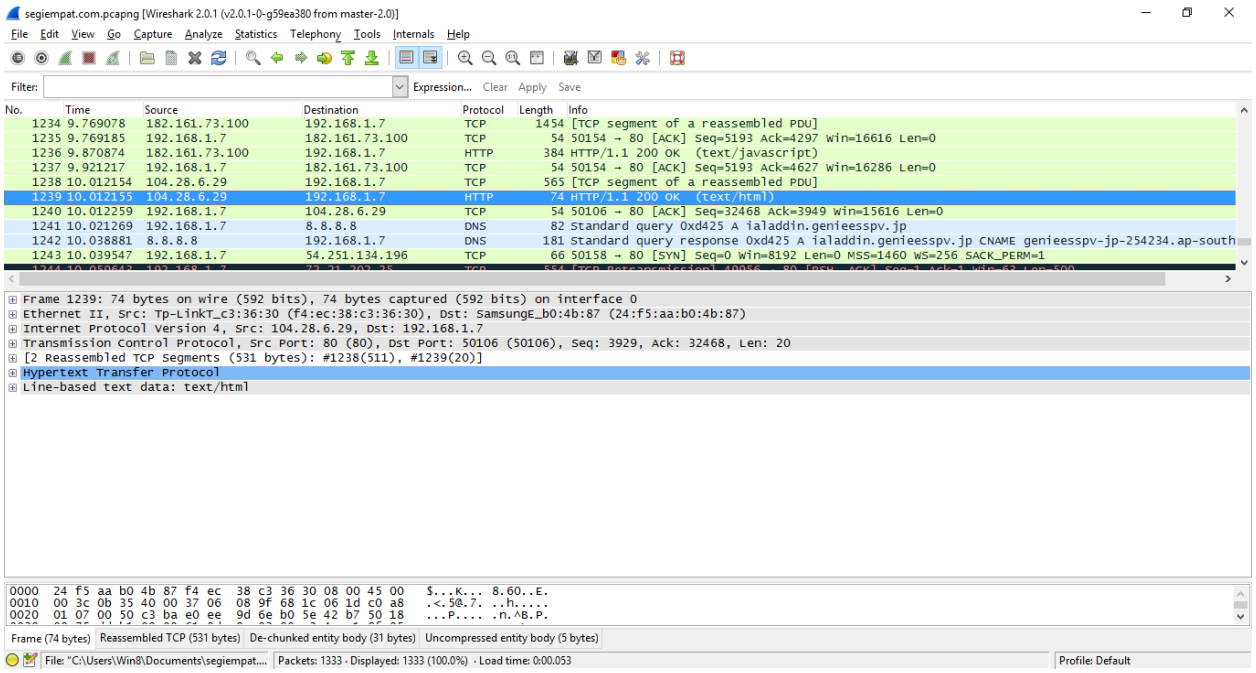
(www.situstulus.com)

Gambar II

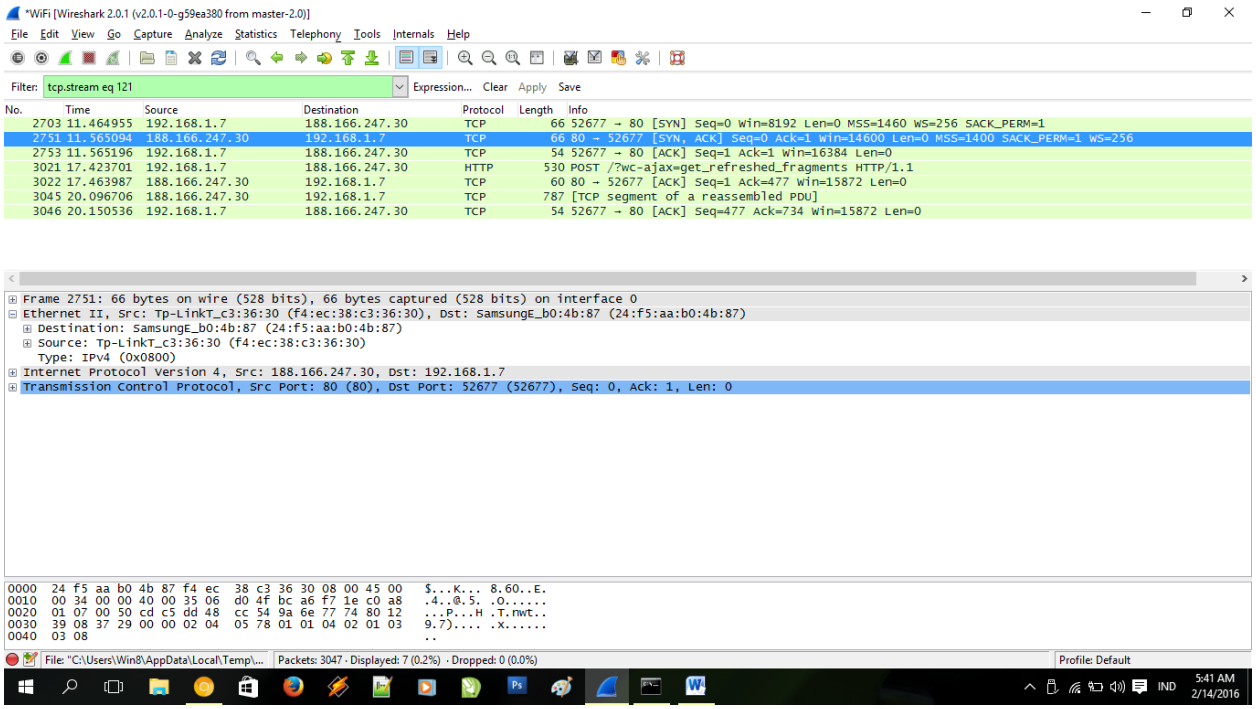
Pada layer ethernet II, dijelaskan bahwa pada source (74.125.130.113) memiliki mac

address 24:f5:aa:b0:4b:87 , dan pada destination(104.28.6.29) memiliki mac address f4:ec:38:c3:36:30.

Dan selanjutnya source (74.125.130.113) yang memiliki mac address 24:f5:aa:b0:4b:87 dan pada destination (188.166.247.30) memiliki mac address f4:ec:38:c3:36:30



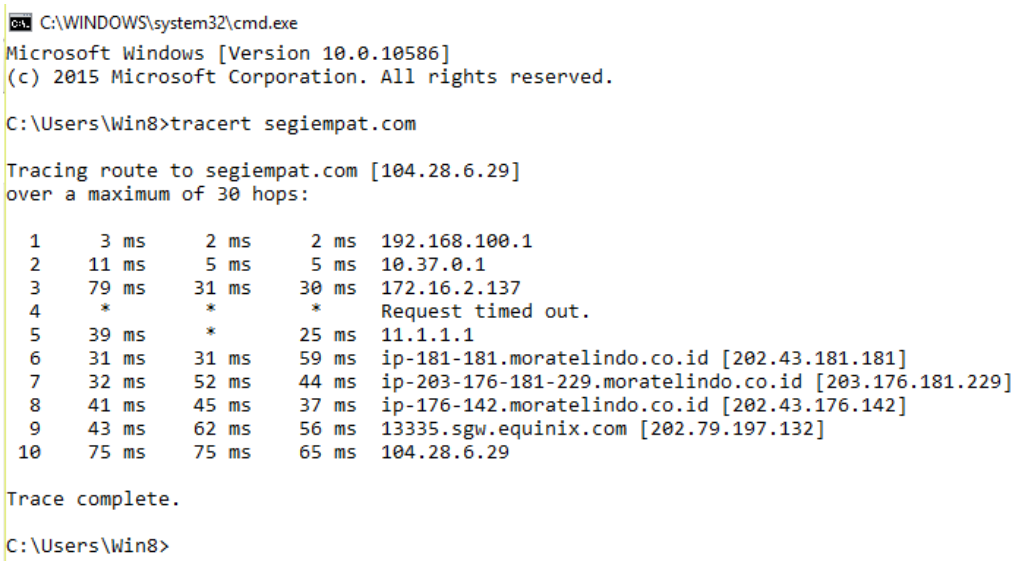
(www.segiempat.com)



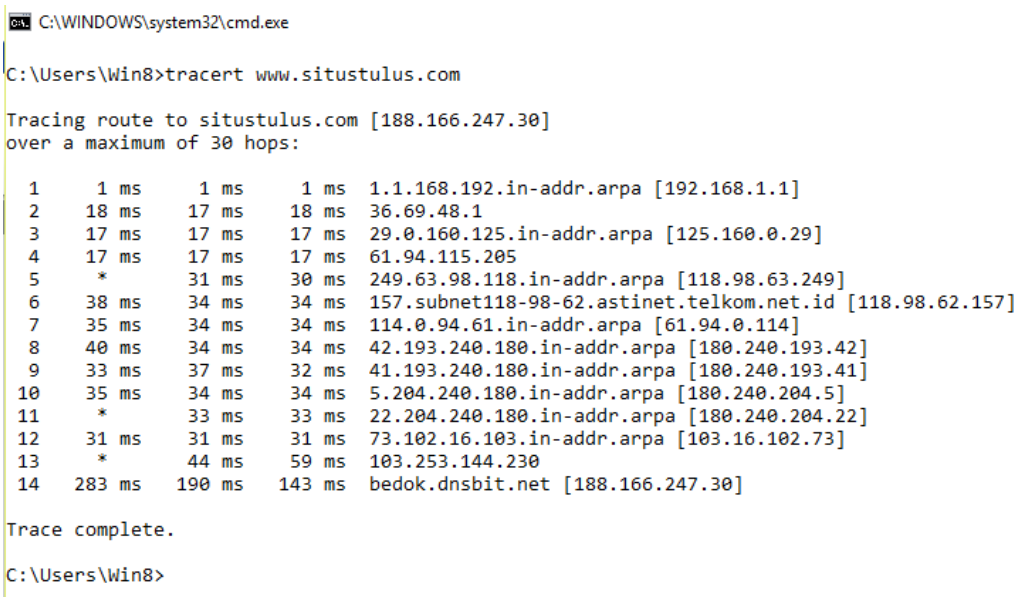
(www.situstulus.com)

Gambar III

Setelah paket data dikirim dari komputer client ke server maka server akan memberikan balasan ke client dengan cara mengirimkan data dari server ke client.Dalam hal ini yang menjadi source adalah 104.28.6.29 (www.segiempat.com) dan menjadi destination adalah 74.125.130.113



(www.segiempat.com)



(www.situstulus.com)

Gambar IV

Traceroute mengirimkan sebuah paket ke port UDP yang tidak dipakai oleh servis lain pada komputer tujuan (defaultnya adalah port 33434). Untuk tiga paket pertama, traceroute mengirimkan paket yang memiliki TTL satu, maka sesampainya paket tersebut pada router pertama (menghasilkan loncatan yang pertama) TTL akan dikurangi dengan satu sehingga menjadi 0 kemudian paket tersebut akan di drop. Berikutnya router tersebut akan mengirimkan paket ICMP ke komputer kita yang berisi pemberitahuan bahwa TTL dari paket yang kita kirimkan sudah habis dan paket yang kita kirimkan di drop.