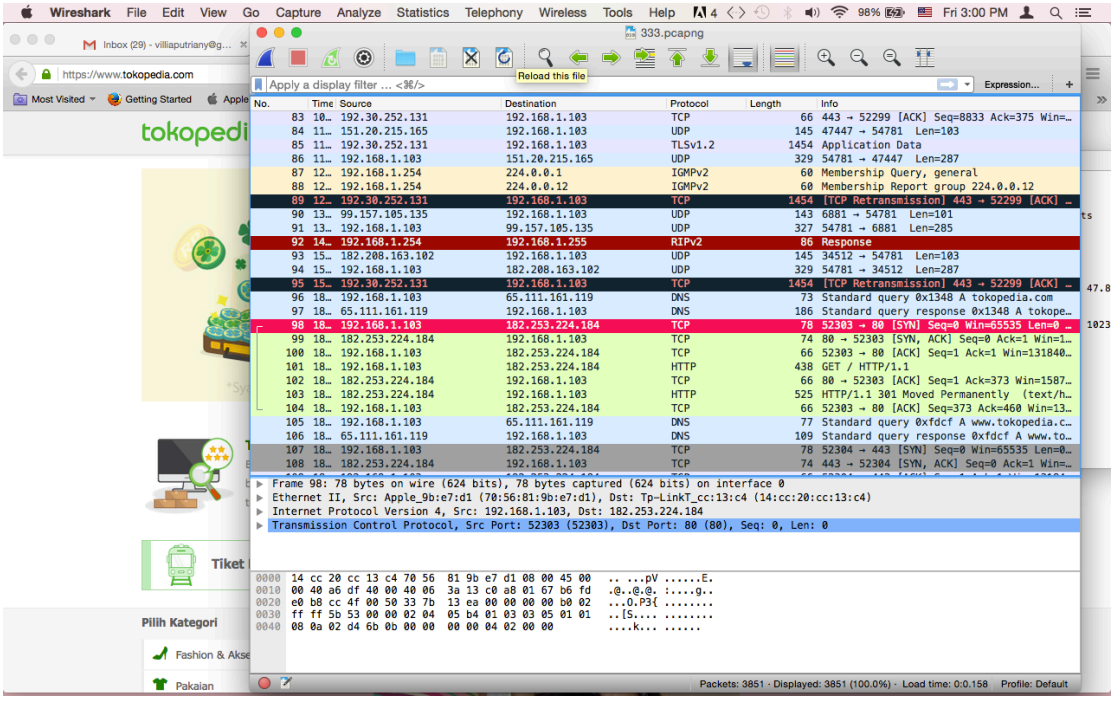
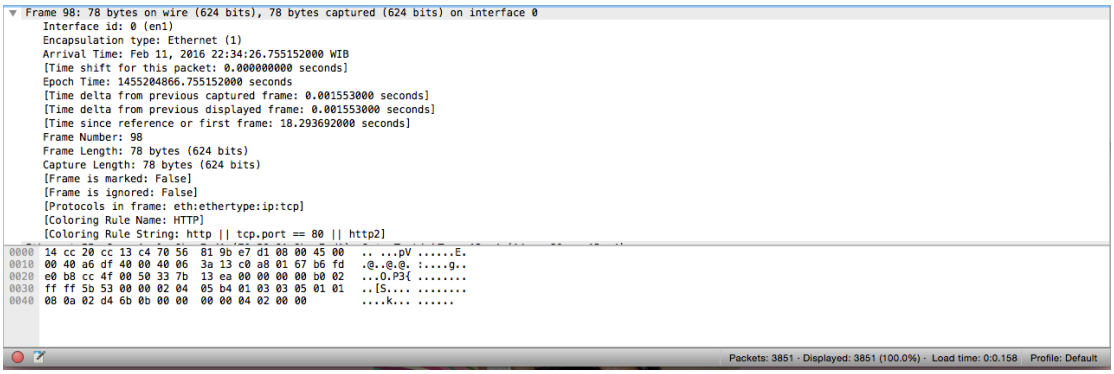
Nama: Villia Putriany
NIM: 09031381419103
Kelas: Sibil 4A

Analisis Packets dengan aplikasi Wireshark

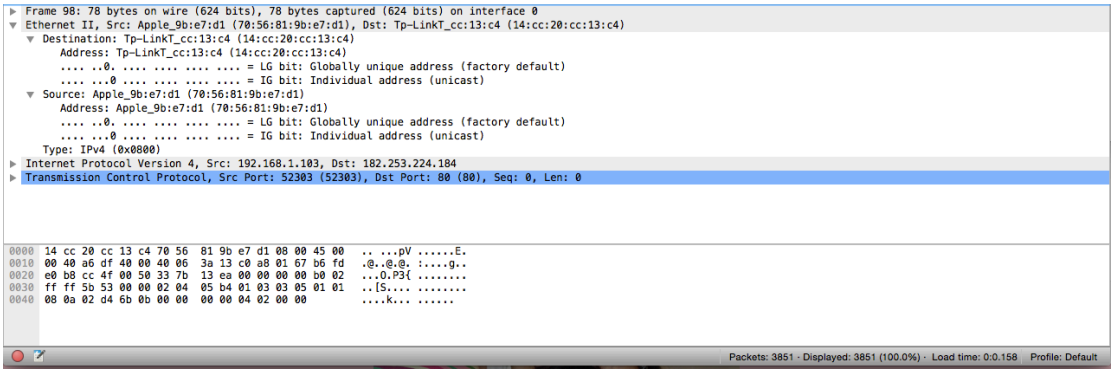
WIRESHARK adalah satu dari sekian banyak tool Network Analyzer yang dipakai oleh orang – orang yang bekerja di bidang jaringan yang ingin melihat atau menganalisa paket jaringan, pengembangan protokol jaringan serta edukasi bagi yang ingin memperdalam ilmu nya dalam jaringan komputer.
Aplikasi ini juga dapat menangkap paket-paket data/informasi yang ada dalam jaringan yang kita ingin liahat. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Kali ini saya akan menganalisa packet protocol yang ter-capture saat membuka situs website Tokopedia (tokopedia.com).



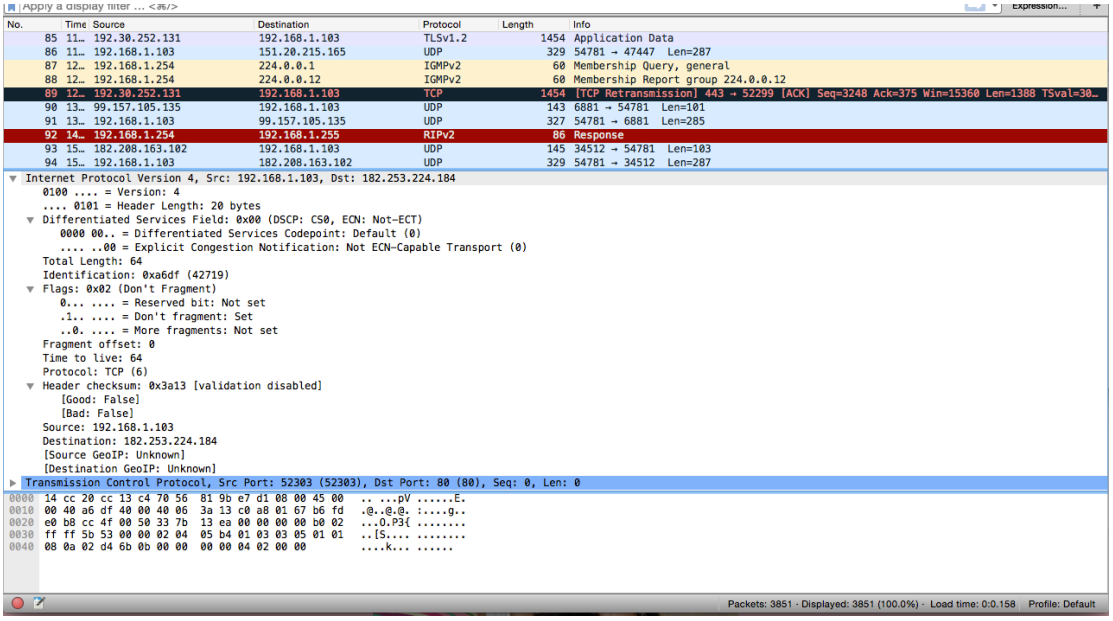
Berikut adalah hasil analisa jaringan yang ter-capture saat membuka dua tab website yaitu gmail.com dan tokopedia.com. Pertama saya akan menjelaskan per-layer (lapisan) pada analisis capture lalu saya akan menjelaskan jenis protocol yang tertangkap pada saat membuka website (HTTP, TCP, DNS, UDP)



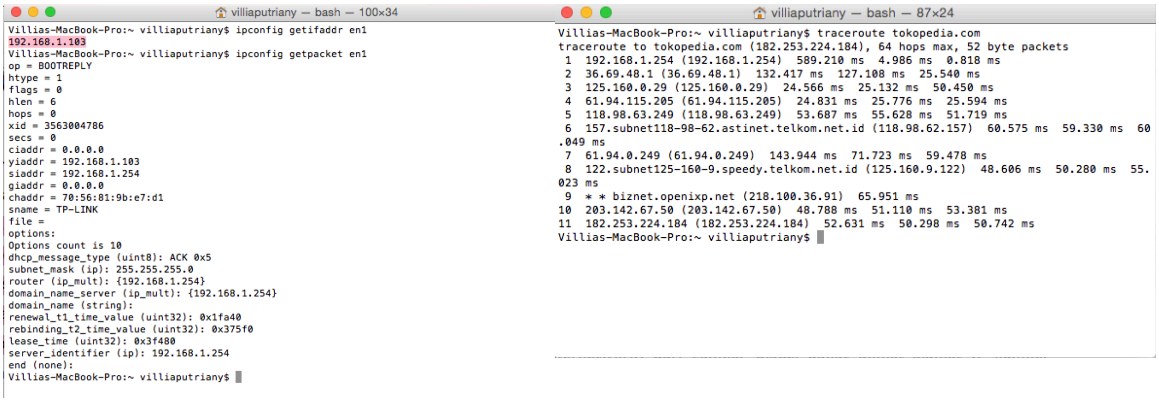
Pada baris kedua terdapat beberapa layer, pada layer pertama, Frame layer, menjelaskan ringkasan dari frame.



Layer kedua , Ethernet Layer, terdapat alamat destinasi dan alamat sumber. Data link layer biasanya cukup sederhana hanya terpaku dalam mendapatkan frame ke simpul yang berdekatan berikutnya pada medium fisik.

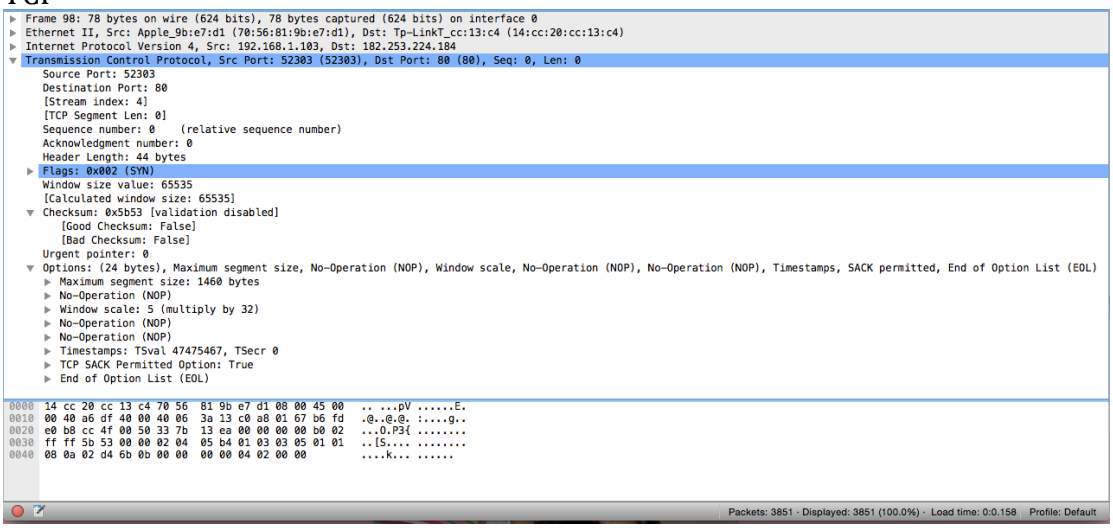


Jika Ethernet layer terpaku pada simpul ke simpul, IP layer terpaku pada pergerakan antar jaringan (internetwork) dari gambar diatas dapat dilihat alamat IP sumber (192.168.1.103) dan IP tujuan (182.253.224.184) serta IP header length (20 bytes pada gambar). Dapat diperhatikan gambar dibawah adalah pengecekan IP komputer dengan ipconfig dan IP tokopedia dengantraceroute.



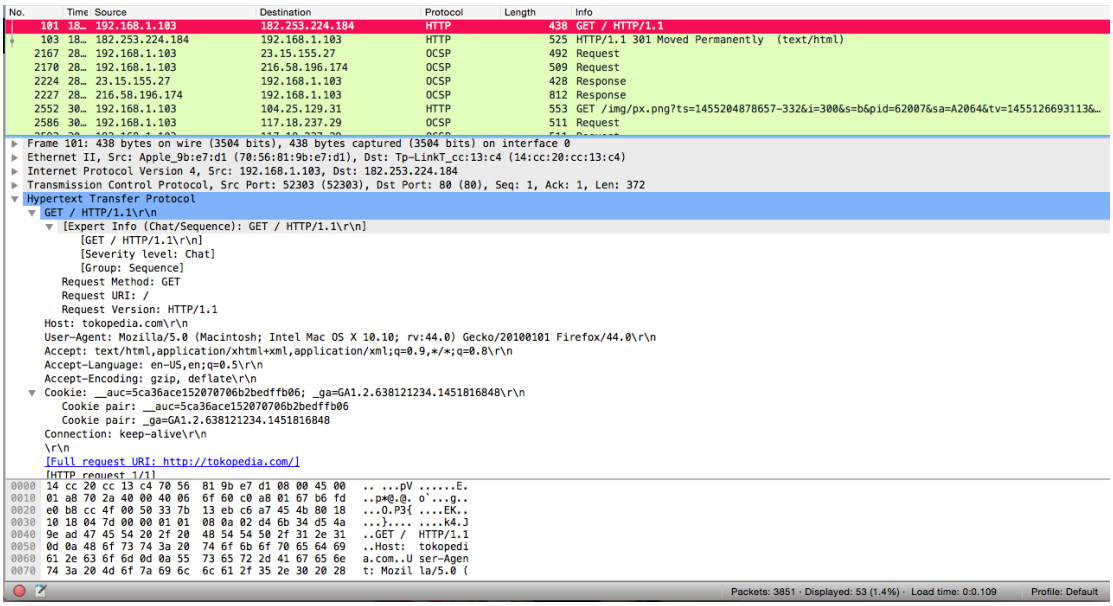
Kita juga bisa melihat Layanan Differentiated (DiffServ) daerah. Ini akan menjadi tempat informasi tambahan yang berkaitan dengan jenis paket layanan yang pergi. Bagi kebanyakan paket pada LAN ini diatur ke nol, yang berarti usaha terbaik. Ada beberapa tingkatan lain, seperti Expedited Forwarding, yang umumnya memiliki kehilangan rendah, delay rendah, dan jitter rendah. tingkat Diff Serv dapat digunakan ketika ingin menerapkan Quality of Service pada jaringan IP.

TCP



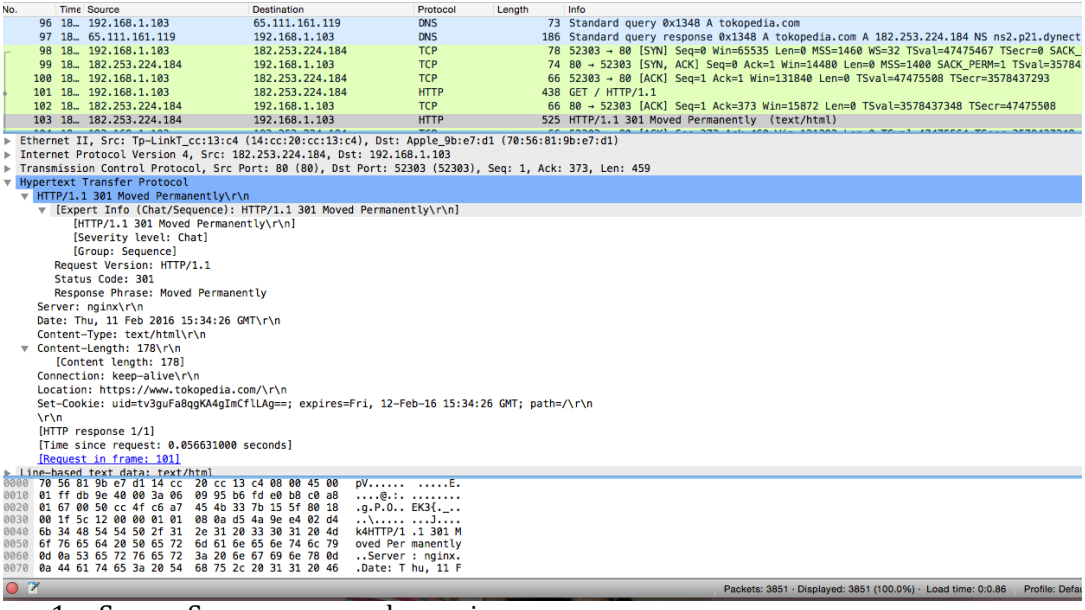
Transport layer menjelaskan di mana aplikasi berkomunikasi melalui port yang digunakan. Melihat capture ditunjukkan pada gambar diatas, kita dapat melihat bahwa port sumber adalah 52303, sedangkan port tujuan adalah 80. Hal menarik yang lain adalah panjang header (44 byte) dan nomor urut. Nomor urut umumnya akan berubah untuk setiap paket.

HTTP



Dari data yang dicapture diatas kita dapat menganalisis beberapa informasi sebagai berikut.

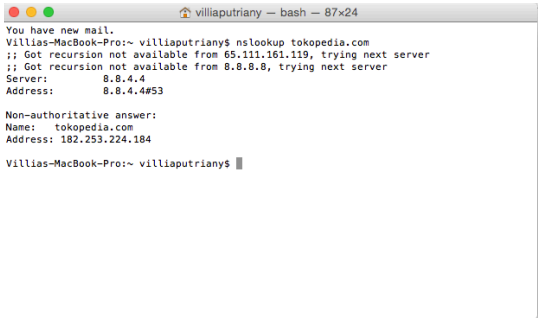
1. Kemungkinan Web browser yang digunakan adalah Mozila 5.0/Crome 25.0.1364/Safari 537.22 dengan operating sistem Macintosh; Intel Mac OS X 10.10
2. Web browser dan server Tokopedia sama-sama running HTML versi 1.1
3. Bahasa yang digunakan Web browser yang dapat diterima server adalah bahasa English US.
4. Akses ke tokopedia.com browser ini dah pernah dilakukan hinnga terdapat cookie tersimpan di browser user.



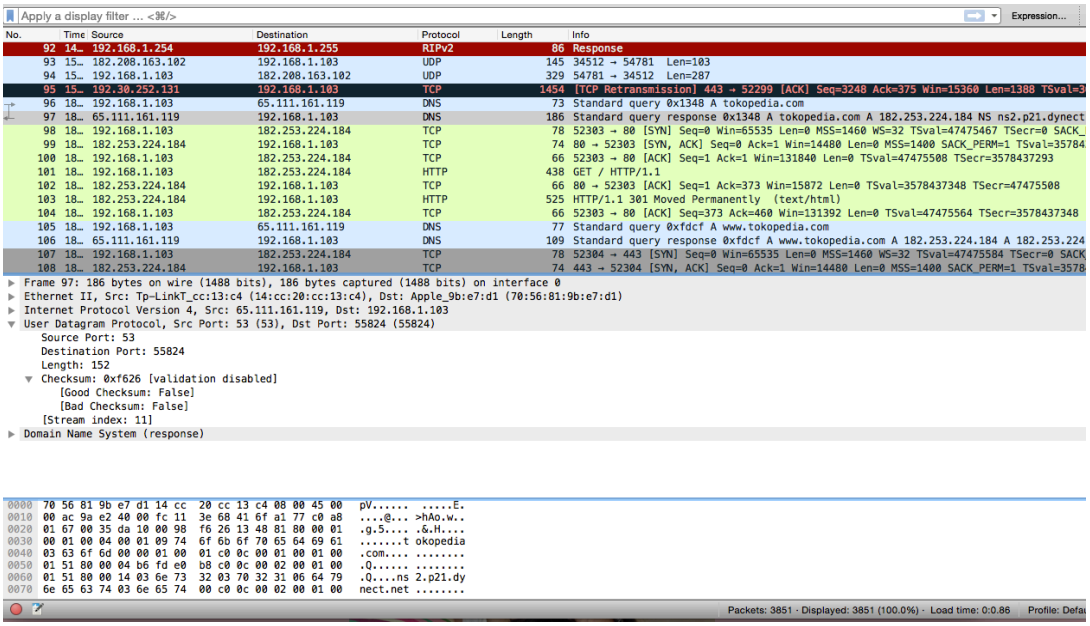
1. Server Sony menggunakan nginx
2. Status Code dari server ke browser kita adalah 301 yang artinya Moved Permanently
3. Website diakses pada Hari Kamis 11 Februari 2016 15:34:26 GMT
4. Content yang ditransfer pada sesi ini bertipe teks
5. Panjang Content-nya adalah 178 bytes

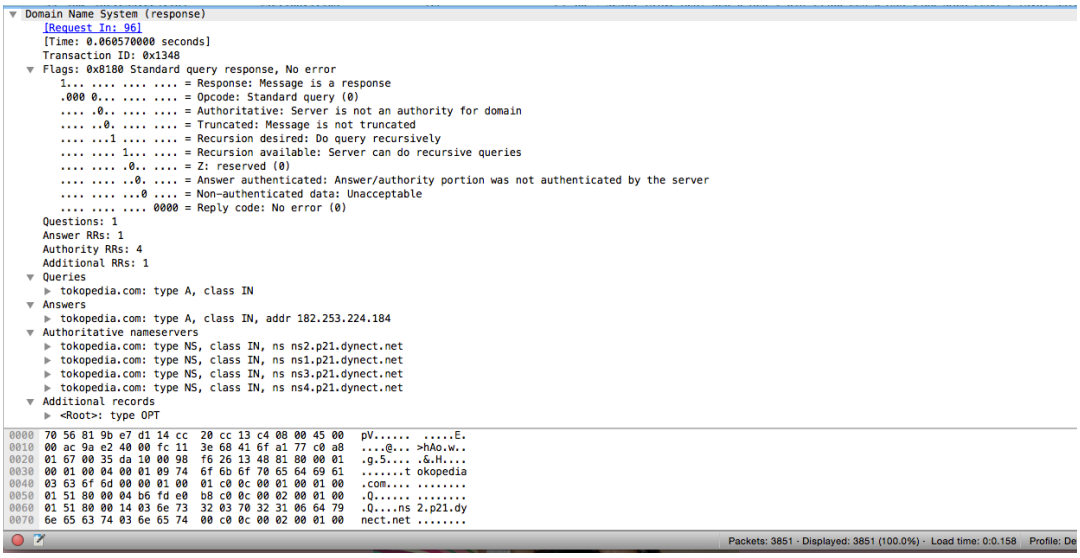
DNS

Dapat diketahui bahwa server DNS kita adalah 8.8.4.4 yang mempunyai IP address 192.168.203.1. Hal tersebut berdasar pada IP source dan destination pada penangkapan paket oleh wireshark. Untuk membuktikannya kita juga dapat mengecek melalui Terminal.



Capture dengan wireshark:



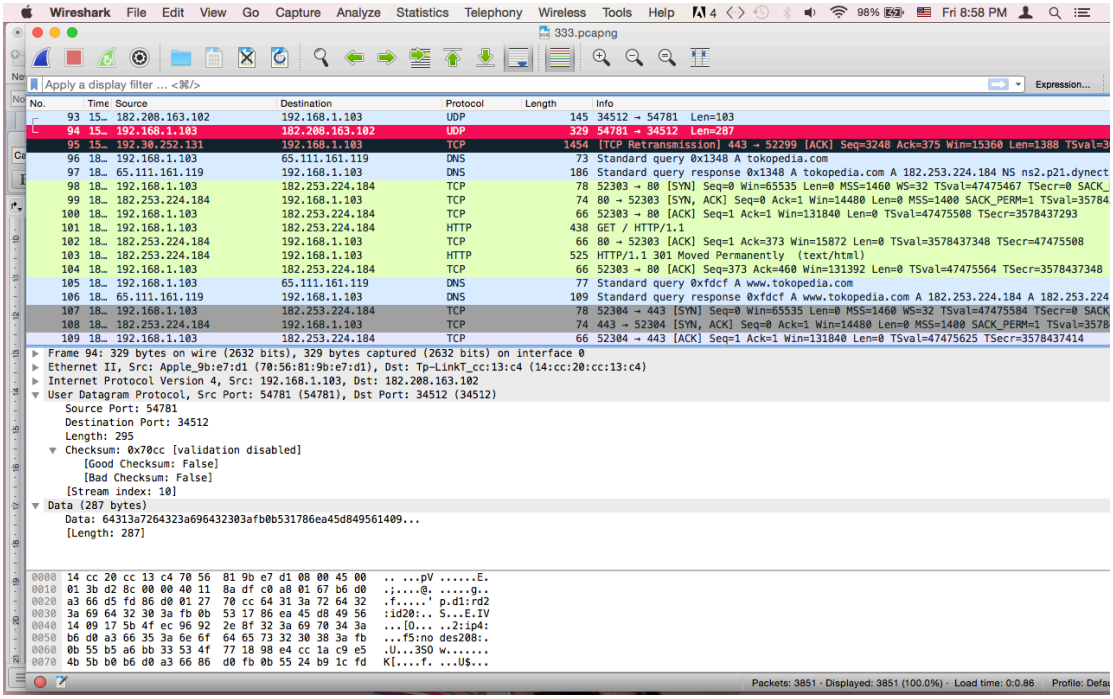


Pada dasarnya DNS (Domain Name System) adalah penerjemahan alamat IP ke hostname dan sebaliknya. Host meminta alamat yang akan dituju (tokopedia.com) kepada DNS server. Dapat dilihat untuk melakukan proses ini diperlukan 0.060570000 second.

Server DNS menjawab kepada host bahwa tokopedia.com dengan IP address 182.253.224.184. Ternyata data ini sama persis dengan informasi yang diperoleh pada nslookup Terminal. Kita dapat mengetahui bahwa queries alamat Tokopedia ini type A (host Address) dan Class IN (0x0001).

UDP

UDP adalah TCP yang connectionless. Hal ini berarti bahwa suatu paket yang dikirim melalui jaringan dan mencapai komputer lain tanpa membuat suatu koneksi. Sehingga dalam perjalanan ke tujuan paket dapat hilang karena tidak ada koneksi langsung antara kedua host, jadi UDP sifatnya tidak realibel. UDP tidak pernah digunakan untuk mengirim data penting seperti halaman web, informasi database, dan sebagainya. Tetapi UDP biasanya digunakan untuk streaming audio dan video, karena UDP mempunyai kelebihan yaitu pada kecepatan transfer. UDP lebih cepat dari TCP karena pada protokol UDP tidak ada bentuk kontrol aliran dan koreksi kesalahan.



Dari gambar diatas dapat dilihat protokol UDP yang tercapture wireshark diaman IP source 192.168.1.103 menggunakan port 54781 dimana pada sesi ini dia adalah pengirim data atau informasi dan IP destination 182.208.163.102 port 34512 adalah yang akan menerima informasi dari source. Pada UDP tidak ada proses koreksi kesalahan/flow control.