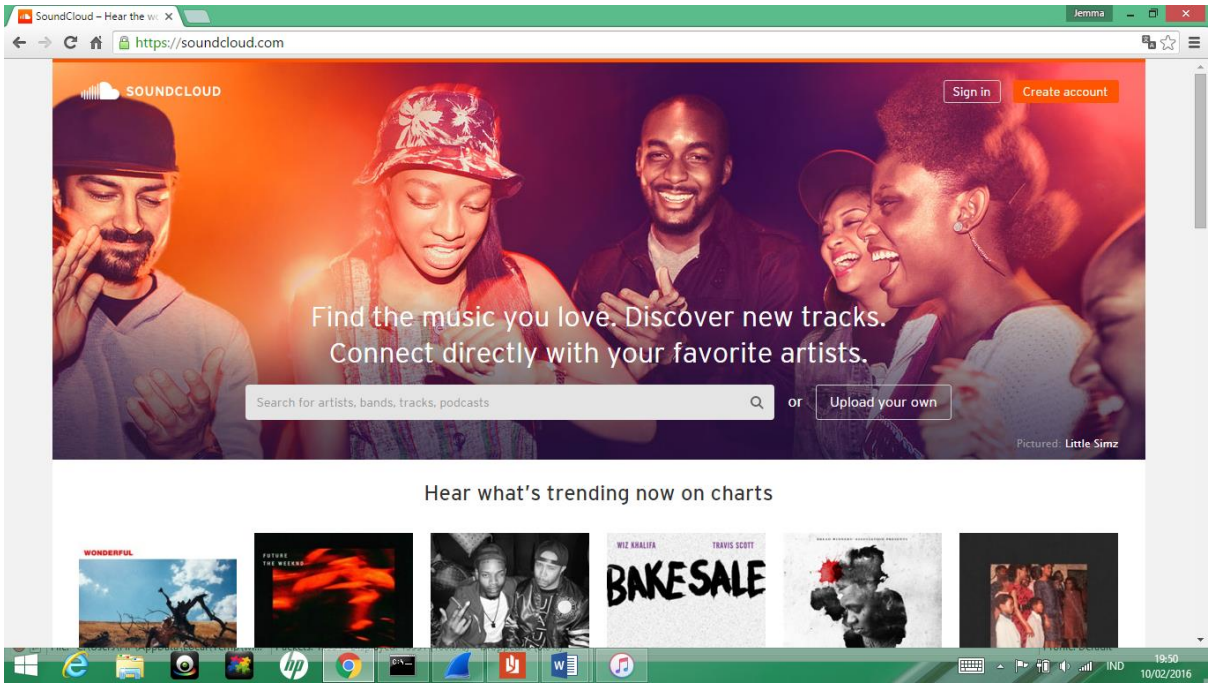
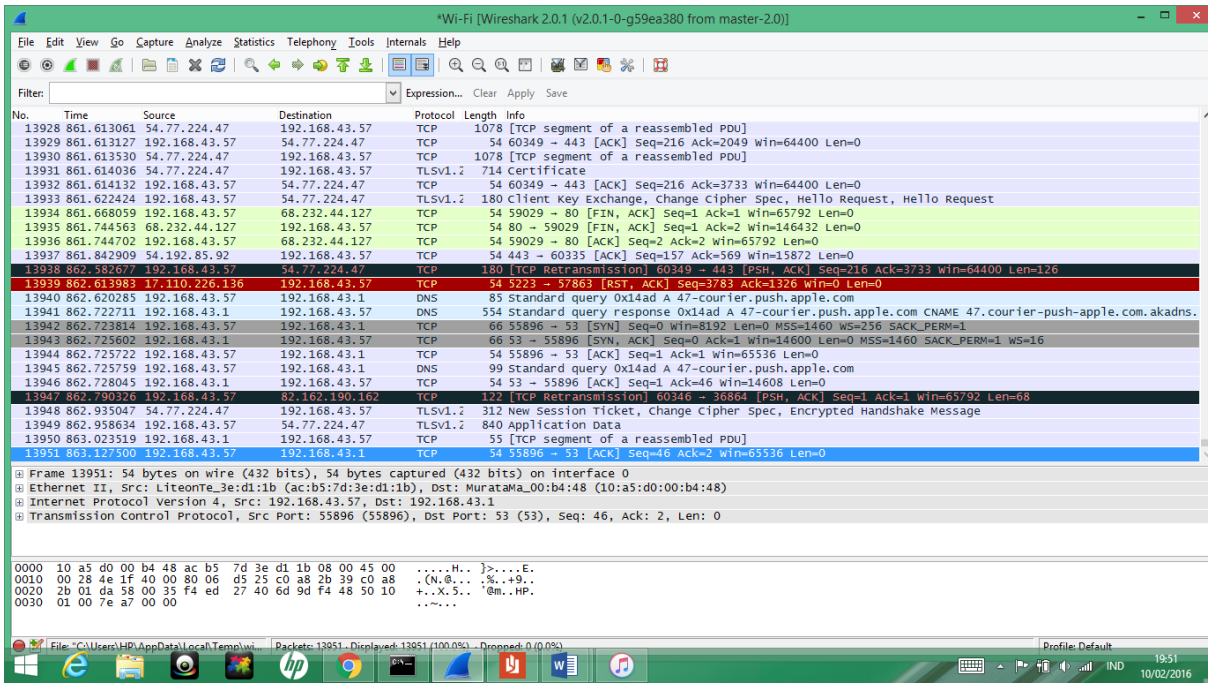
ANALISIS PROTOKOL DENGAN WIRESHARK

VIYANKA WIDA RISWANDA / 09031381419065
SISTEM INFORMASI BILINGUAL 2014
UNIVERSITAS SRIWIJAYA

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



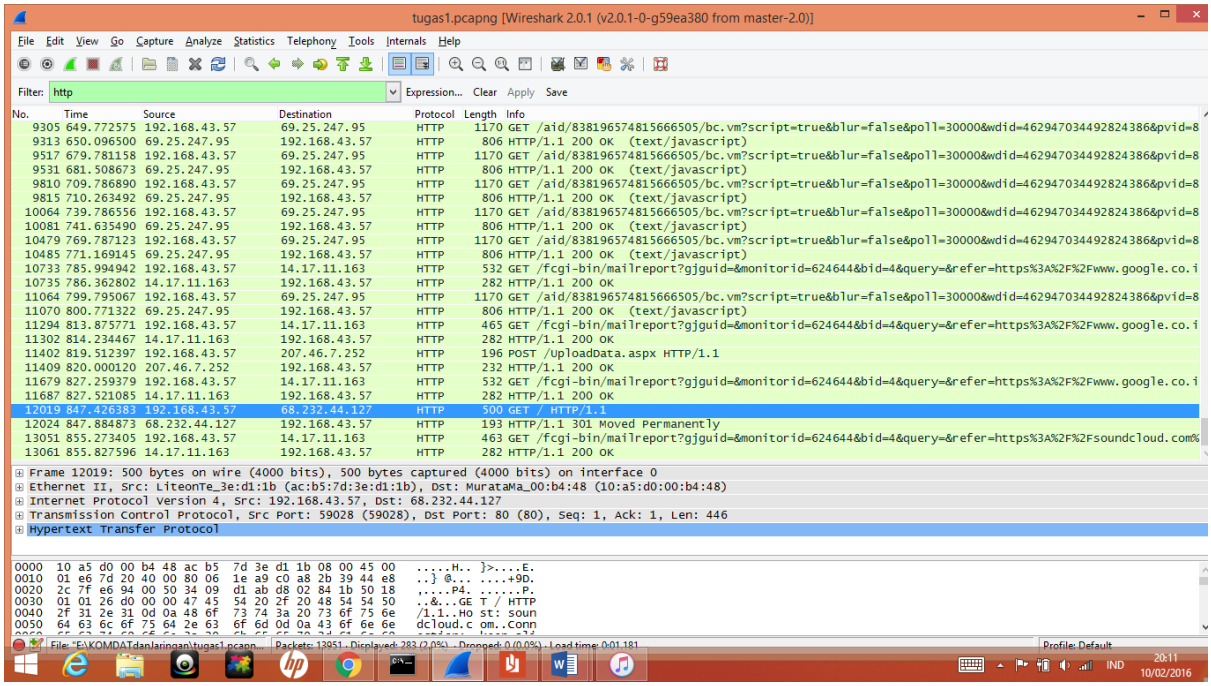
Berikut tampilan paket-paket data yang tertangkap selama me-load situs www.soundcloud.com seperti gambar dibawah.



Analisis :

Dari hasil capture di atas terdapat beberapa protocol yang tertangkap, diantaranya adalah hijau untuk http, biru dns, abu – abu arp, merah tcp dan lainnya.

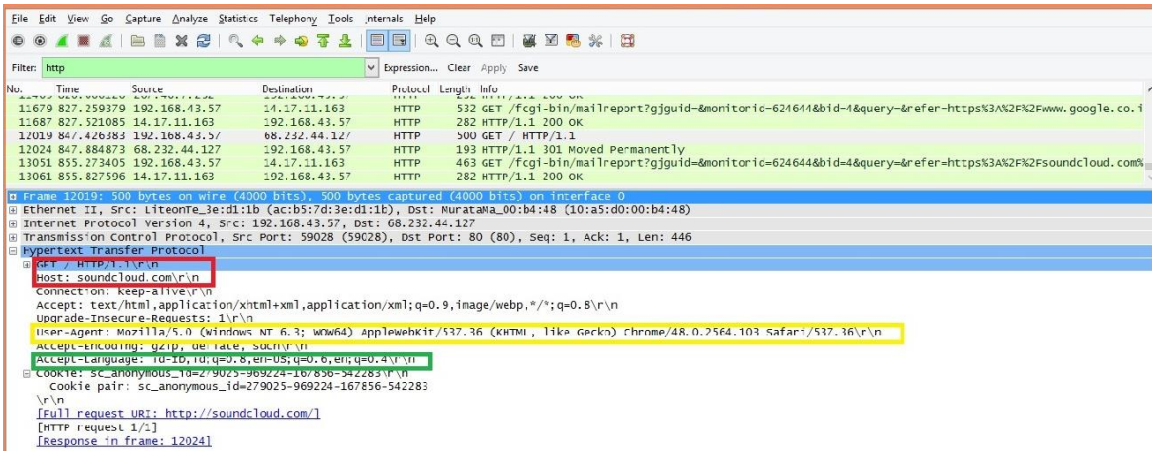
a. HTTP



Dari hasil capture di atas, dapat di lihat banyak sekali HTTP message yang di tangkap ketika membuka www.soundcloud.com. Berdasarkan sumber nya ada 2 macam HTTP messagge, yaitu GET message dan OK message. Pertama GET dari IP komputer meminta data ke IP Soundcloud, lalu setelah dari Soundcloudnya merespon, maka akan ada OK message dari soundcloud ke IP komputer, hal tersebut dapat dilihat dari IP source dan destination. Itu berarti kita mempunyai IP address 192.168.43.57 dan Server Soundcloud adalah 68.232.44.127. Untuk membuktikan hal tersebut dapat dilakukan dengan menggunakan command promt seperti gambar dibawah.

```
C:\Users\HP>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::21b3:25cf:512c:dfea%6
   IPv4 Address. . . . . . . . . . . : 192.168.43.57
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.43.1
```

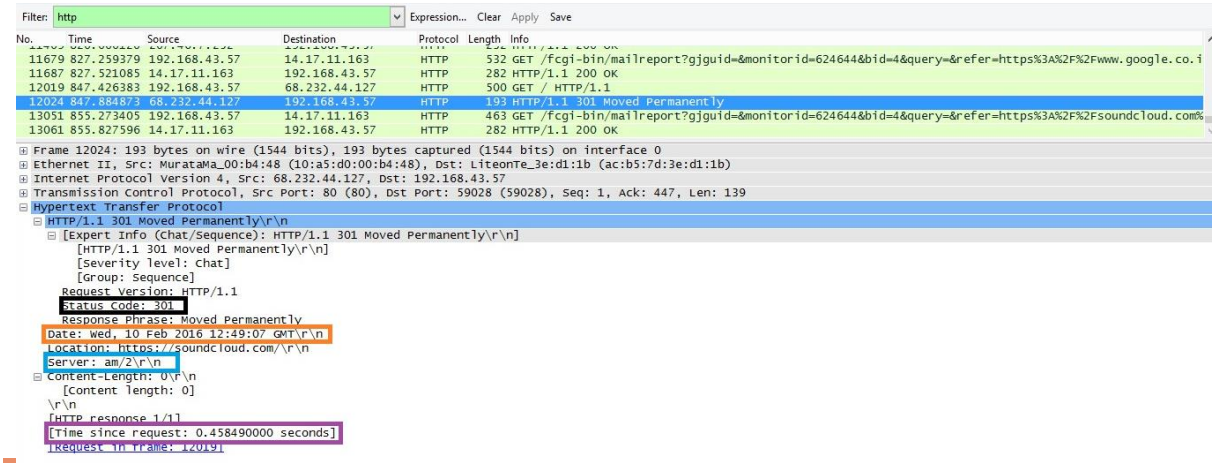
Untuk menganalisis protokol HTTP sebagai analogi kita akan membuka detail dari GET dan OK message dari HTTP ini.

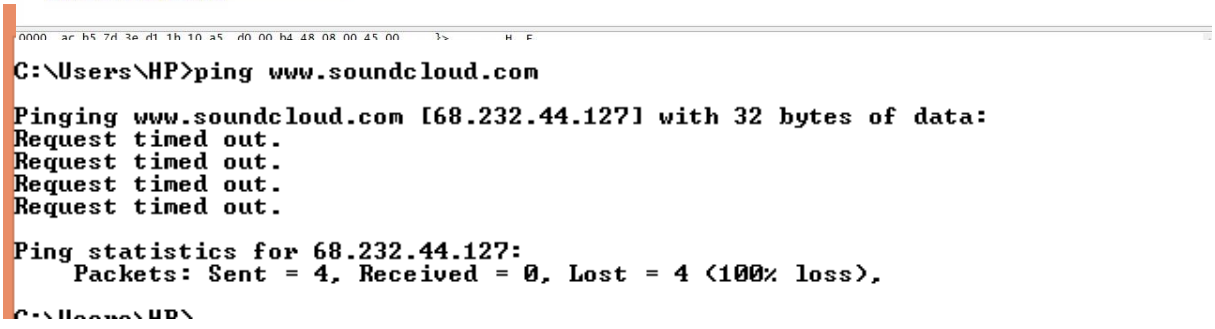


Dari gambar di atas dapat di jelaskan

- Kotak yang berwana merah menjelaskan bahwa Web browser dan server soundcloud sama-sama running HTML versi 1.1;
- Pada kotak warna kuning dapat di jelaskan kemungkinan Web browser yang digunakan adalah Mozilla 5.0/Chrome 48.0.2564.103/Safari 537.36 dengan operating sistem Windows 64bit;
- Lalu pada kotak warna hijau dapat di jelaskan bahwa bahasa yang di gunakan adalah Indonesia dan English US.

Lalu kita buka detail dari OK message HTTP



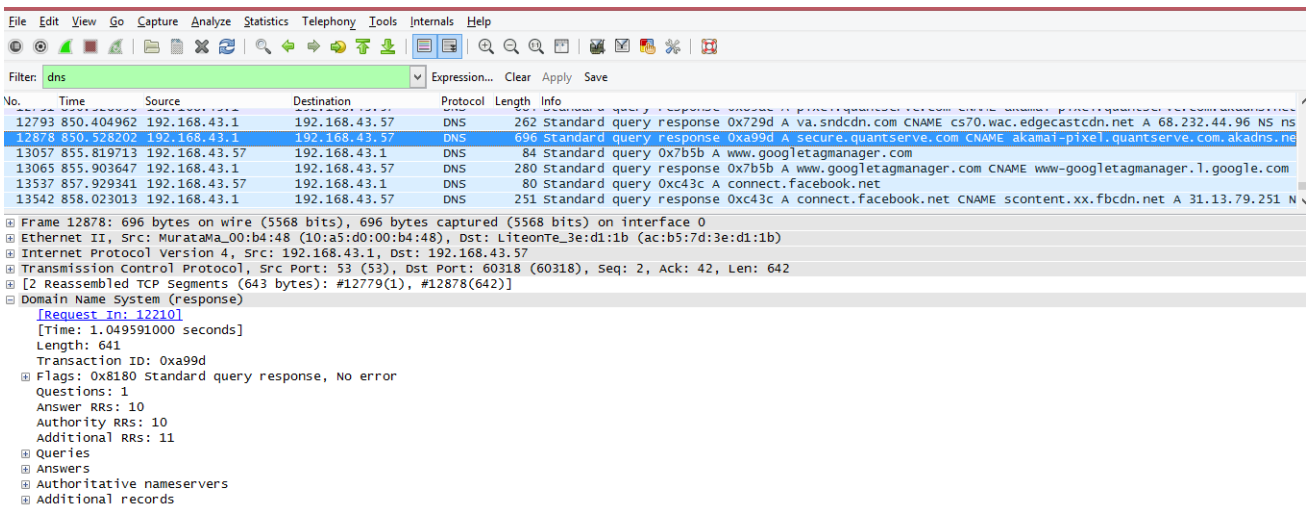


Dari gambar di atas dapat di jelaskan

- Pada kotak warna hitam dapat dilihat Status Code dari server ke browser kita adalah 301 yang berarti Moved Permanently;
- Pada kotak warna orange dapat di lihat bahwa soundcloud di akses pada hari Rabu, 10 Februari 2016 pada pukul 12.49 GMT;
- Pada kotak berwarna biru bisa di jelaskan bahwa server yang di gunakan adalah am/2\r\n;
- Lalu pada kotak berwarna ungu yaitu time since request yaitu waktu yang di butuhkan ketika antara GET message sampai OK message adalah 0.458490000 second.

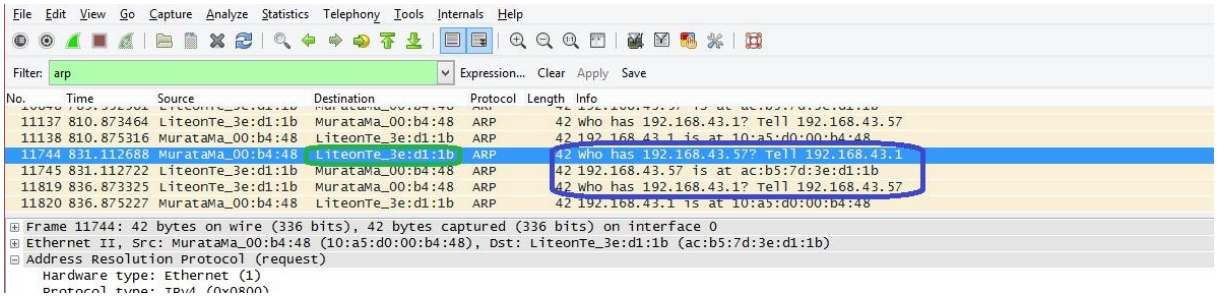
b. DNS

Berikut merupakan hasil capture DNS dari wireshark

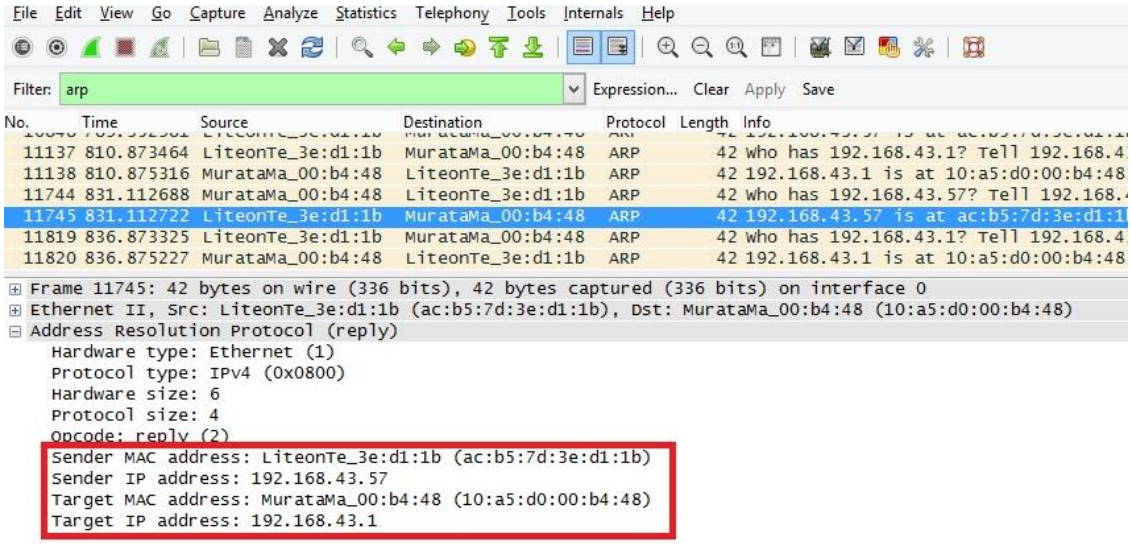


Pada wireshark DNS menerjemahkan alamat IP ke hostname dan sebaliknya. Host meminta alamat yang akan dituju (www.soundcloud.com) kepada DNS server. Dapat dilihat untuk melakukan proses ini diperlukan 1.049591000 second. Server DNS yang menjawab host memiliki IP address 192.168.43.1.

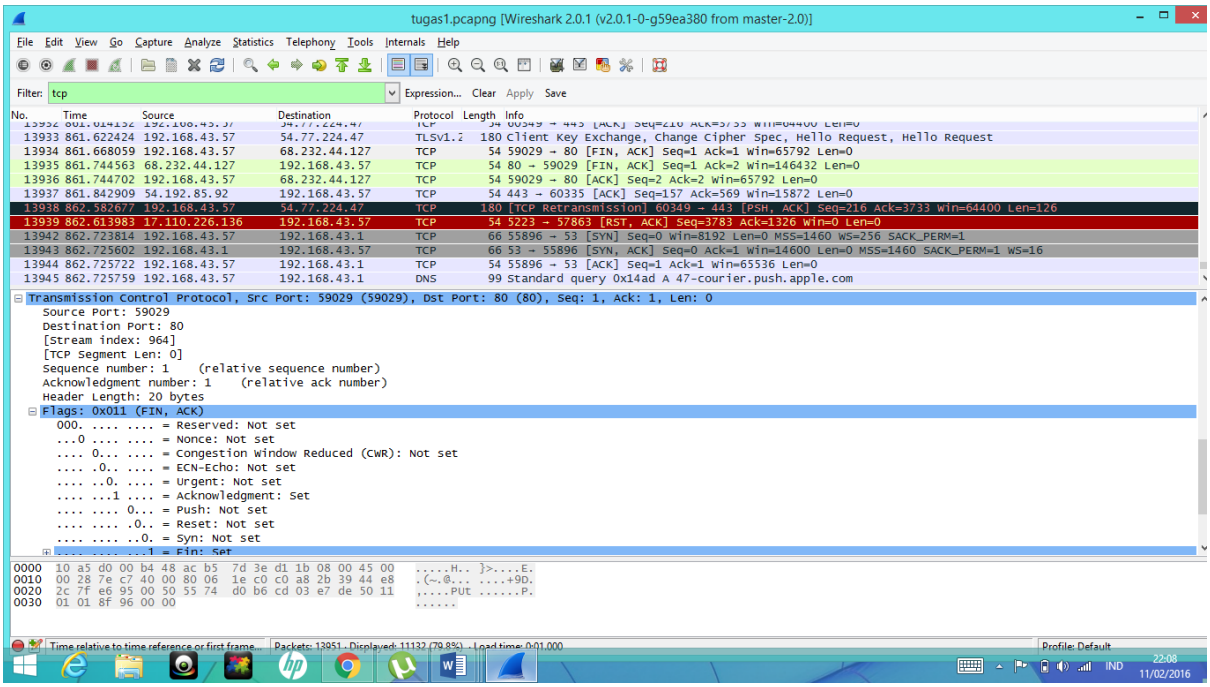
c. ARP



Pada gambar di atas dapat di jelaskan server MurataMa_00:b4:48 menanyakan kepada server LiteonTe_3e:d1:1b siapa yang memiliki IP 192.168.43.57 kepada IP komputer yaitu 192.168.43.1. Lalu setelah itu server LiteonTe_3e:d1:1b memberi jawaban kepada server MurataMa_00:b4:48 jika IP 192.168.43.57 memiliki MAC address ac:b5:7d:3e:d1:1b



d. TCP



TCP merupakan protocol yang digunakan untuk melakukan browsing. Pada layer ke 5 bisa dilihat panjang headernya 20 byte, port yang diminta adalah 80 dan source port adalah 59029. Pada layer ke5 di frame 13934 terdapat flag fin yang bernilai 1 karena ketika sebuah koneksi TCP akhirnya dihentikan (akibat sudah tidak ada data yang dikirimkan lagi), setiap host TCP akan mengirimkan sebuah segmen TCP dengan flag FIN diset ke nilai 1.