

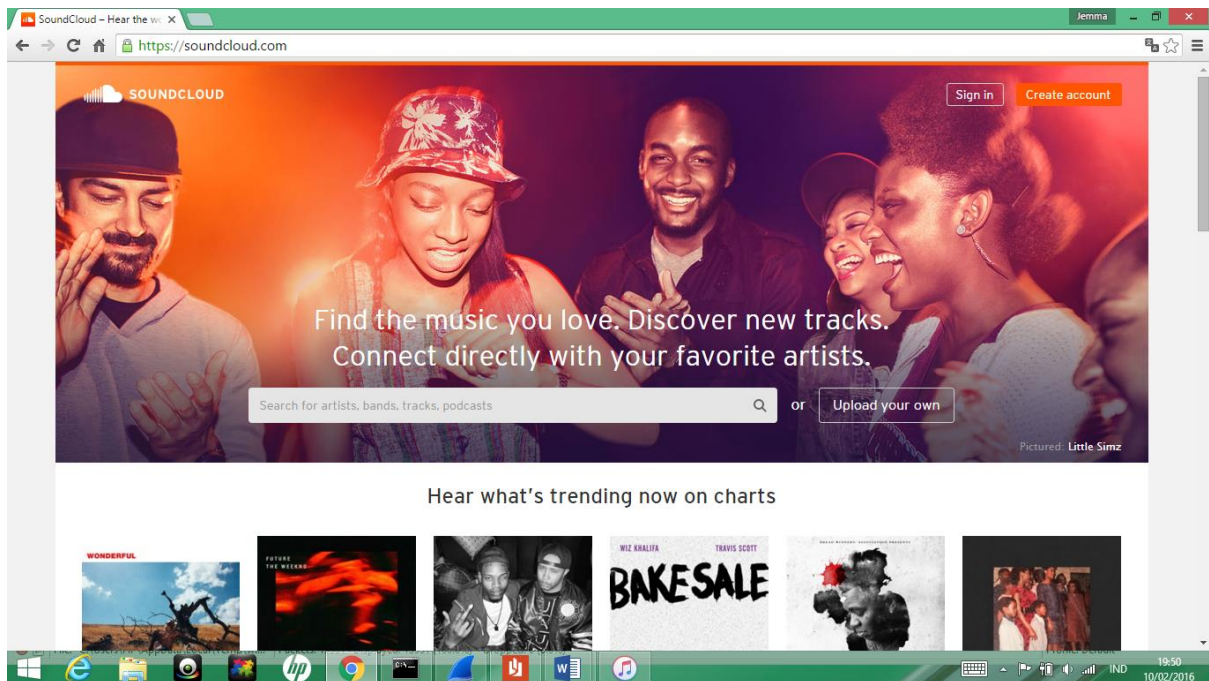
ANALISIS PROTOKOL DENGAN WIRESHARK

VIYANKA WIDA RISWANDA / 09031381419065

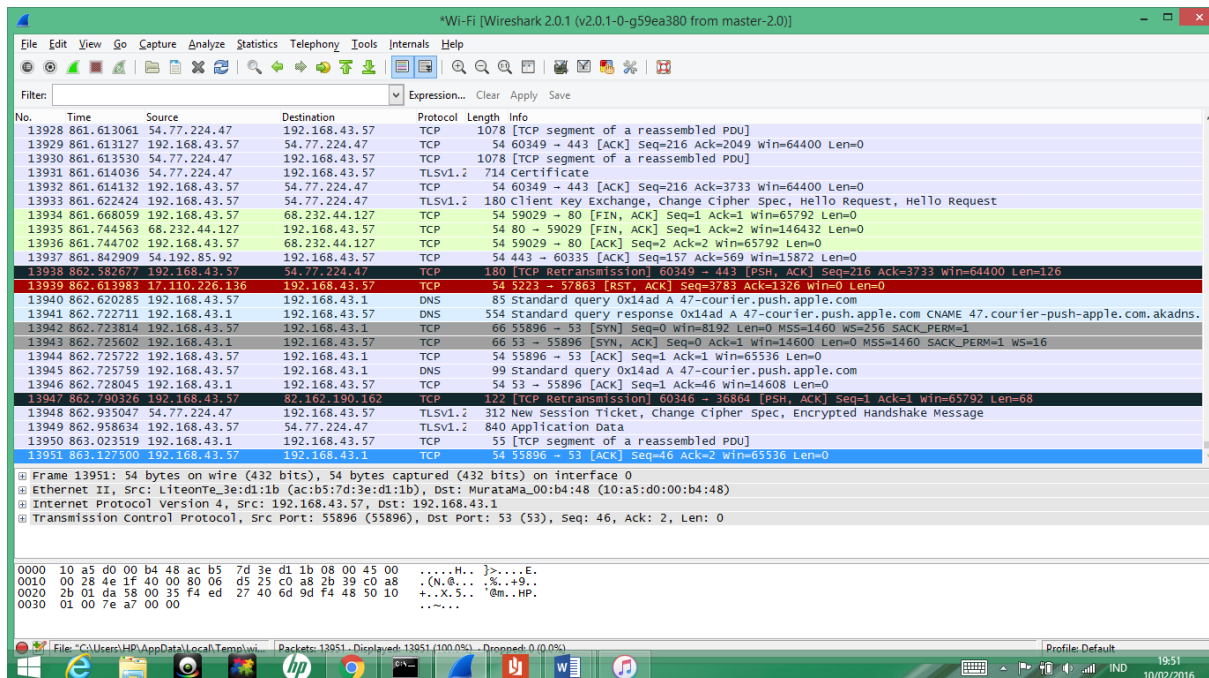
SISTEM INFORMASI BILINGUAL 2014

UNIVERSITAS SRIWIJAYA

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



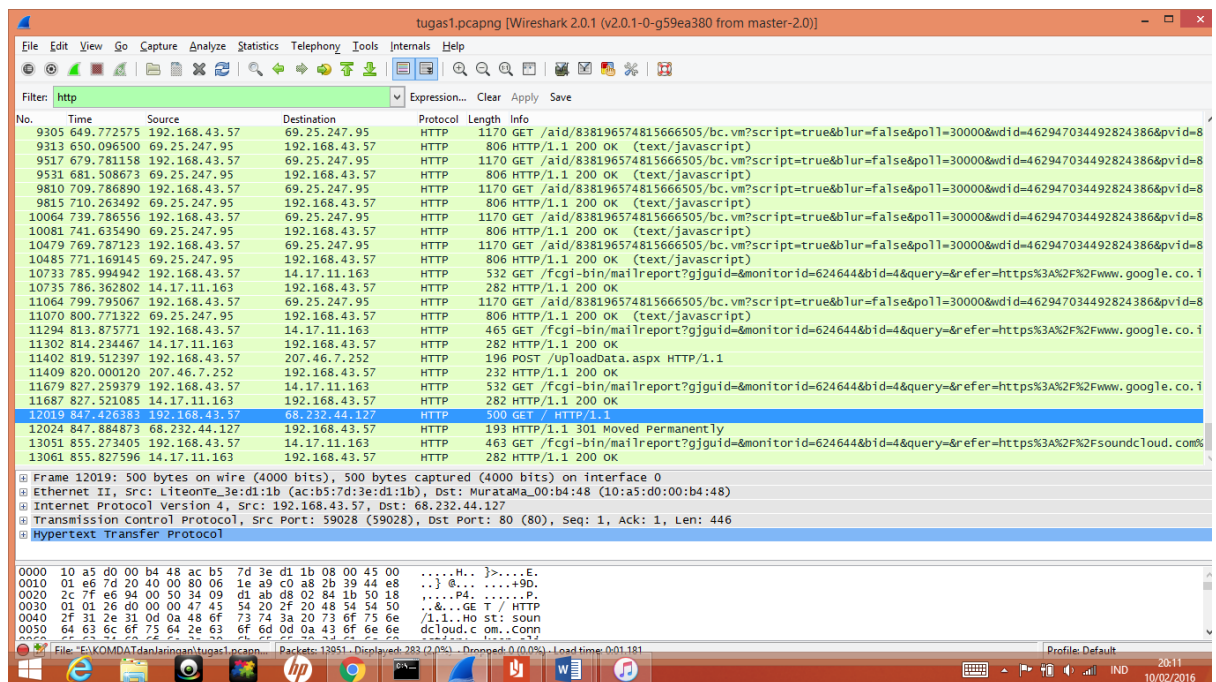
Berikut tampilan paket-paket data yang tertangkap selama me-load situs www.soundcloud.com seperti gambar dibawah.



Analisis :

Dari hasil capture di atas terdapat beberapa protokol 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 message, 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 prompt seperti gambar dibawah.

```
C:\Users\HP>ipconfig

Windows IP Configuration

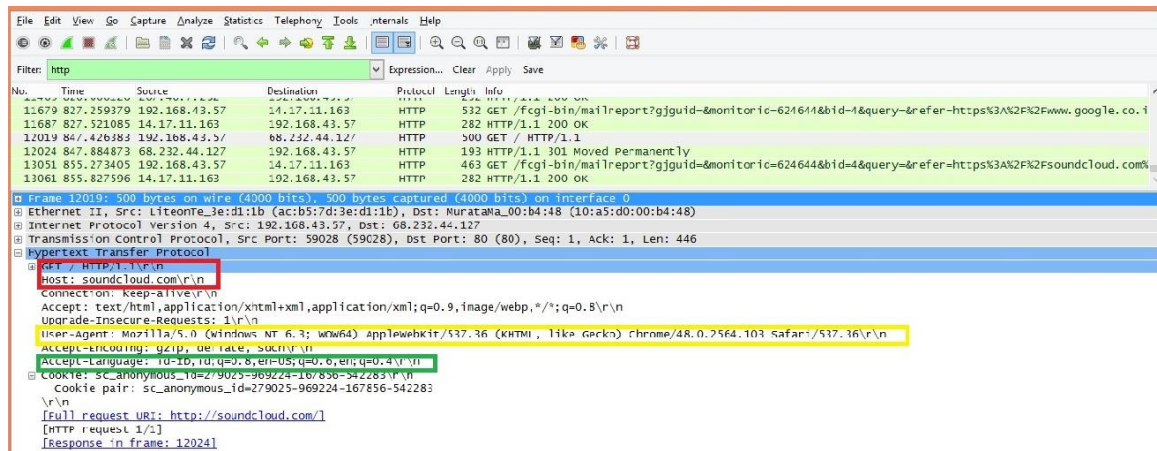
Wireless LAN adapter Local Area Connection* 3:

    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
```

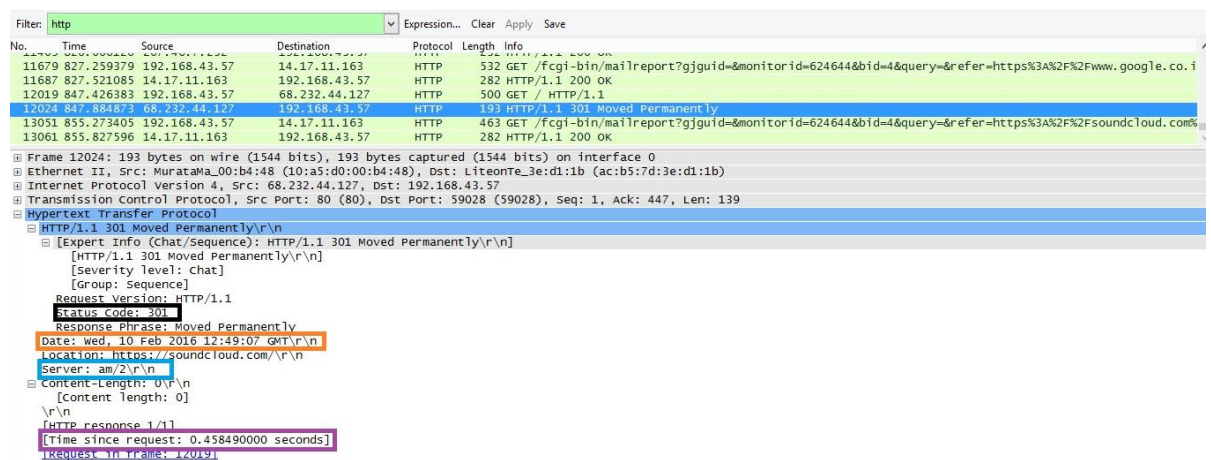
Untuk menganalisis protokol HTTP sebagai analogi kita akan membuka detail dari GET dan OK message dari HTTP ini.



Dari gambar di atas dapat di jelaskan

- Kotak yang berwarna 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



```
C:\Users\HP>ping www.soundcloud.com

Pinging www.soundcloud.com [68.232.44.127] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 68.232.44.127:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    0 ms round trip time.
```

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 A 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

No.	Time	Source	Destination	Protocol	Length	Info
12793	850.404962	192.168.43.1	192.168.43.57	DNS	262	Standard query response 0x729d A va.sndcdn.com CNAME cs70.wac.edgecastcdn.net A 68.232.44.96 NS ns
12878	850.528202	192.168.43.1	192.168.43.57	DNS	696	Standard query response 0xa99d A secure.quantserve.com CNAME akamai-pixel.quantserve.com.akadns.net
13057	855.819713	192.168.43.57	192.168.43.1	DNS	84	Standard query 0x7b5b A www.googletagmanager.com
13065	855.903647	192.168.43.1	192.168.43.57	DNS	280	Standard query response 0x7b5b A www.googletagmanager.com CNAME www-googletagmanager-1.google.com
13537	857.929341	192.168.43.57	192.168.43.1	DNS	80	Standard query 0xc43c A connect.facebook.net
13542	858.023013	192.168.43.1	192.168.43.57	DNS	251	Standard query response 0xc43c A connect.facebook.net CNAME scontent.xx.fbcdn.net A 31.13.79.251 N

Frame 12878: 696 bytes on wire (5568 bits), 696 bytes captured (5568 bits) on interface 0
Ethernet II, Src: MurataMa_00:b4:48 (10:a5:d0:00:b4:48), Dst: LiteontE_3e:d1:1b (ac:b5:7d:3e:d1:1b)
Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.57
Transmission Control Protocol, Src Port: 53 (53), Dst Port: 60318 (60318), Seq: 2, Ack: 42, Len: 642
[2 Reassembled TCP Segments (643 bytes): #12779(1), #12878(642)]
Domain Name System (response)
Request ID: 12210
Time: 1.049591000 seconds
Length: 641
Transaction ID: 0xa99d
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 10
Authority RRs: 10
Additional RRs: 11
Queries
Answers
Authoritative nameservers
Additional records

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

The screenshot shows a Wireshark capture of ARP traffic. The filter is set to 'arp'. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
11137	810.873464	LiteonTe_3e:d1:1b	MurataMa_00:b4:48	ARP	42	who has 192.168.43.1? Tell 192.168.43.57
11138	810.875316	MurataMa_00:b4:48	LiteonTe_3e:d1:1b	ARP	42	192.168.43.1 is at 10:a5:d0:00:b4:48
11744	831.112688	MurataMa_00:b4:48	LiteonTe_3e:d1:1b	ARP	42	who has 192.168.43.57? Tell 192.168.43.1
11745	831.112722	LiteonTe_3e:d1:1b	MurataMa_00:b4:48	ARP	42	192.168.43.57 is at ac:b5:7d:3e:d1:1b
11819	836.873325	LiteonTe_3e:d1:1b	MurataMa_00:b4:48	ARP	42	who has 192.168.43.1? Tell 192.168.43.57
11820	836.875227	MurataMa_00:b4:48	LiteonTe_3e:d1:1b	ARP	42	192.168.43.1 is at 10:a5:d0:00:b4:48

The details pane for packet 11744 shows:

- Frame 11744: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
- Ethernet II, Src: MurataMa_00:b4:48 (10:a5:d0:00:b4:48), Dst: LiteonTe_3e:d1:1b (ac:b5:7d:3e:d1:1b)
- Address Resolution Protocol (request)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)

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

The screenshot shows a Wireshark capture of ARP traffic. The filter is set to 'arp'. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
11137	810.873464	LiteonTe_3e:d1:1b	MurataMa_00:b4:48	ARP	42	who has 192.168.43.1? Tell 192.168.43.57
11138	810.875316	MurataMa_00:b4:48	LiteonTe_3e:d1:1b	ARP	42	192.168.43.1 is at 10:a5:d0:00:b4:48
11744	831.112688	MurataMa_00:b4:48	LiteonTe_3e:d1:1b	ARP	42	who has 192.168.43.57? Tell 192.168.43.1
11745	831.112722	LiteonTe_3e:d1:1b	MurataMa_00:b4:48	ARP	42	192.168.43.57 is at ac:b5:7d:3e:d1:1b
11819	836.873325	LiteonTe_3e:d1:1b	MurataMa_00:b4:48	ARP	42	who has 192.168.43.1? Tell 192.168.43.57
11820	836.875227	MurataMa_00:b4:48	LiteonTe_3e:d1:1b	ARP	42	192.168.43.1 is at 10:a5:d0:00:b4:48

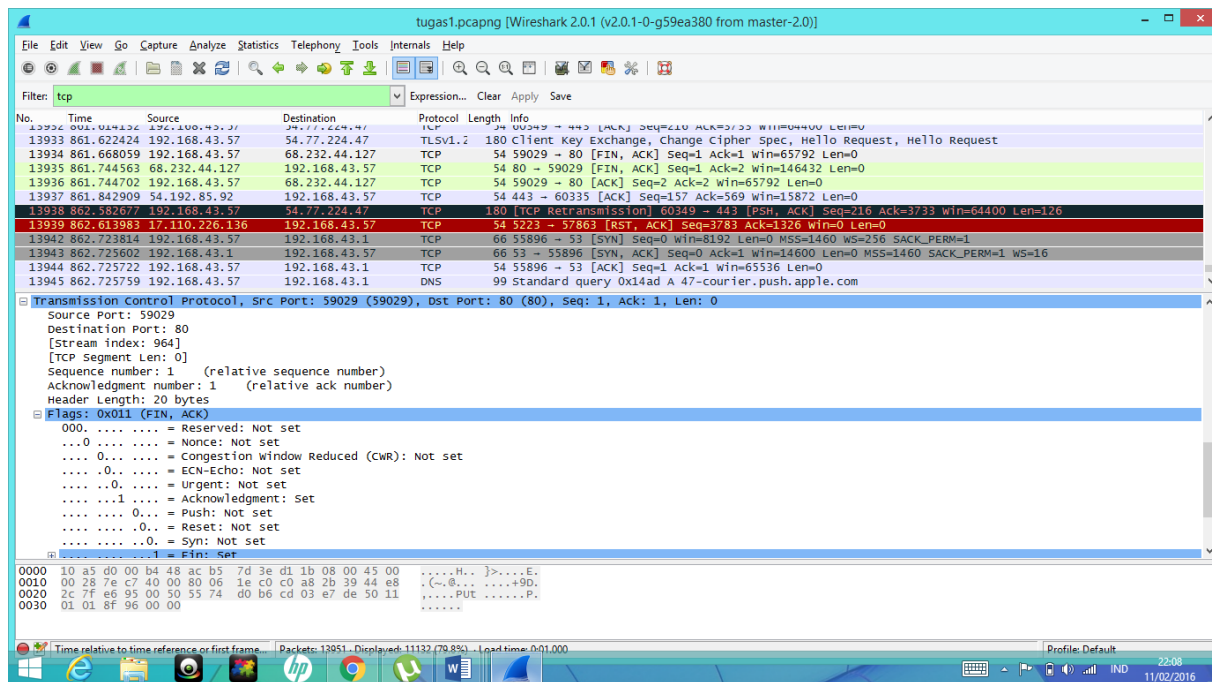
The details pane for packet 11745 shows:

- Frame 11745: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
- Ethernet II, Src: LiteonTe_3e:d1:1b (ac:b5:7d:3e:d1:1b), Dst: MurataMa_00:b4:48 (10:a5:d0:00:b4:48)
- Address Resolution Protocol (reply)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: reply (2)

The packet bytes pane for packet 11745 shows:

- Sender MAC address: LiteonTe_3e:d1:1b (ac:b5:7d:3e:d1:1b)
- Sender IP address: 192.168.43.57
- Target MAC address: MurataMa_00:b4:48 (10:a5:d0:00:b4:48)
- Target IP address: 192.168.43.1

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.