MODUL PRAKTIKUM JARINGAN KOMPUTER

WWW.AJK.IF.ITS.AC.ID

MODUL 02

Laboratorium Arsitektur dan Jaringan Komputer
Jurusan Teknik Informatika Ruang IF 307
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember Surabaya

WIRESHARK

Pengertian Analisis Paket

Istilah *packet scanning* atau biasa disebut *packet sniffing* adalah proses pemindaian paket-paket data di dalam jaringan menggunakan *software* penyadap paket atau (*packet sniffer*).

Pengertian Wireshark

Wireshark merupakan perangkat lunak yang spesifik untuk melakukan analisa paket data (*packet sniffer*) pada jaringan secara *real time* dan menampilkan hasil analisa paket data tersebut dalam format yang dipahami oleh pengguna. Wireshark dapat melakukan paket *filtering*, paket color coding, dan fitur-fitur lain yang dapat mengizinkan untuk melihat detail *network traffic* dan inspeksi paket data secara individu.

Cara Mendapatkan Wireshark

Untuk mengunduh software wireshark, Anda dapat mengunjungi alamat website *official* wireshark di http://www.wireshark.org/download.html. Wireshark dapat digunakan pada sistem operasi Windows, Mac OS X, dan Linux.

Kapan Menggunakan Wireshark

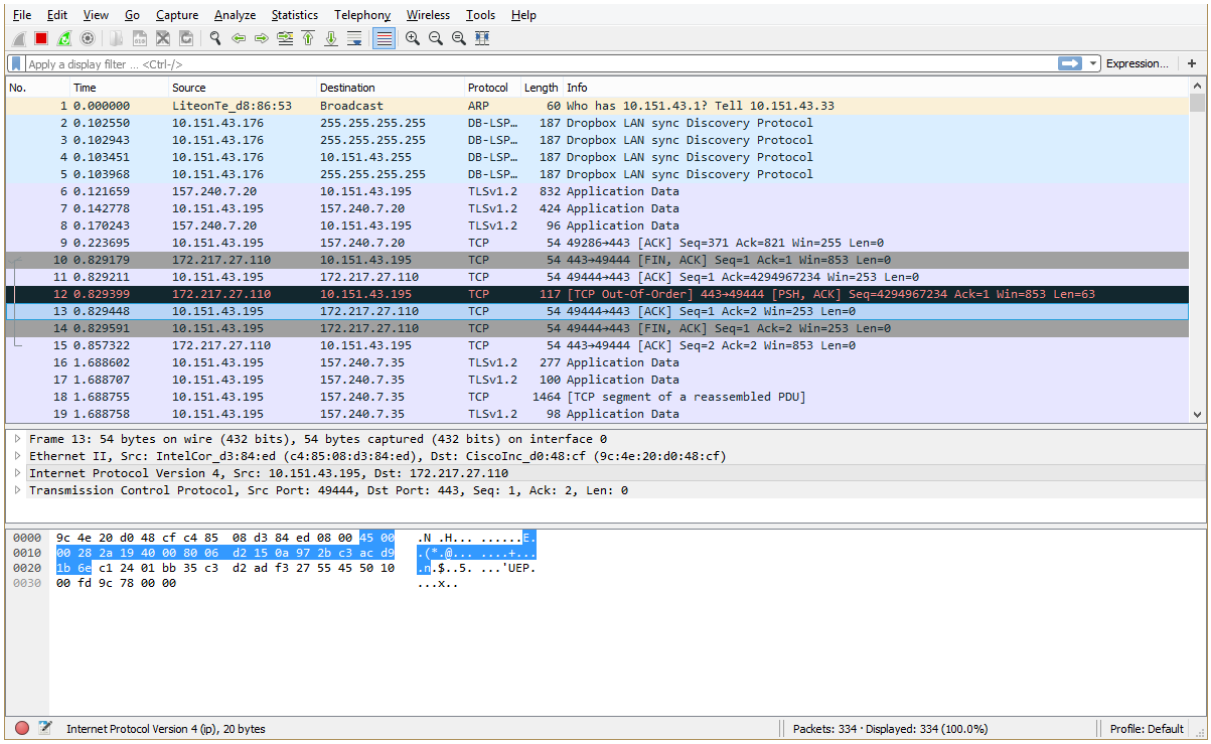
Ada banyak hal yang dilakukan menggunakan wireshark. Berikut ini merupakan contoh kasus yang mungkin dibutuhkan tools wireshark :

1. Melakukan troubleshoot permasalahan jaringan
2. Melakukan pengujian masalah keamanan
3. Melakukan debugging implementasi protokol
4. Belajar protokol jaringan

Wireshark ini dapat kita sebut sebagai tools yang powerful, karena dengan menggunakan tools ini, kita bisa saja dapat menggunakannya untuk mencuri informasi yang sensitif pada jaringan, seperti *password*, *cookie*, dan lain sebagainya.

Contoh Sniffing Packet

Penggunaan wireshark yang paling mudah adalah melihat paket-paket data yang ada di dalam jaringan secara real time. Contoh scanning packet secara realtime dapat dilihat pada gambar di bawah ini.

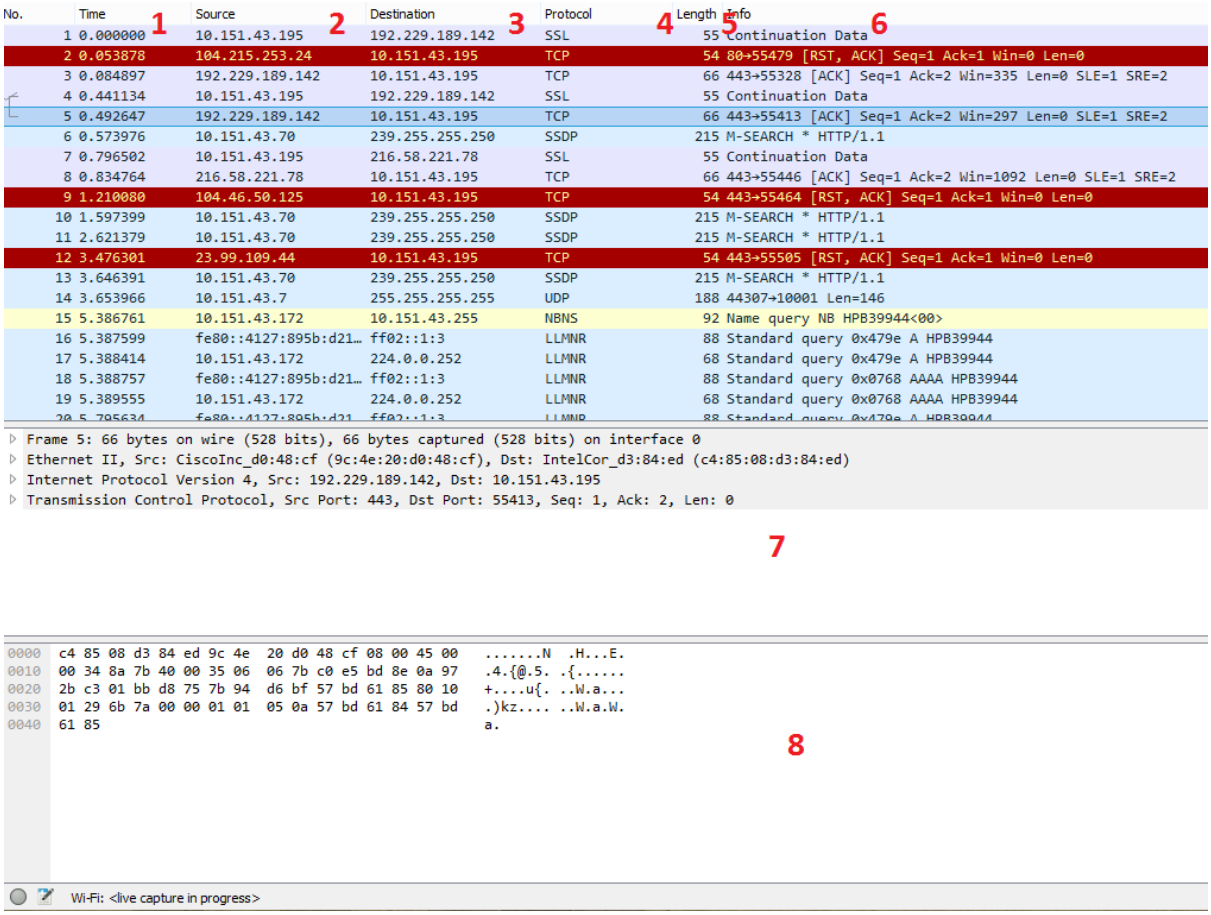


Tutotial Menggunakan Wireshark

Apabila sudah selesai meng-*install* wireshark, kita dapat langsung melakukan *scanning*, *sniffing* dan *capturing* terhadap paket data yang kita capture dari wireshark. Berikut ini adalah langkah langkah menggunakan wireshark:

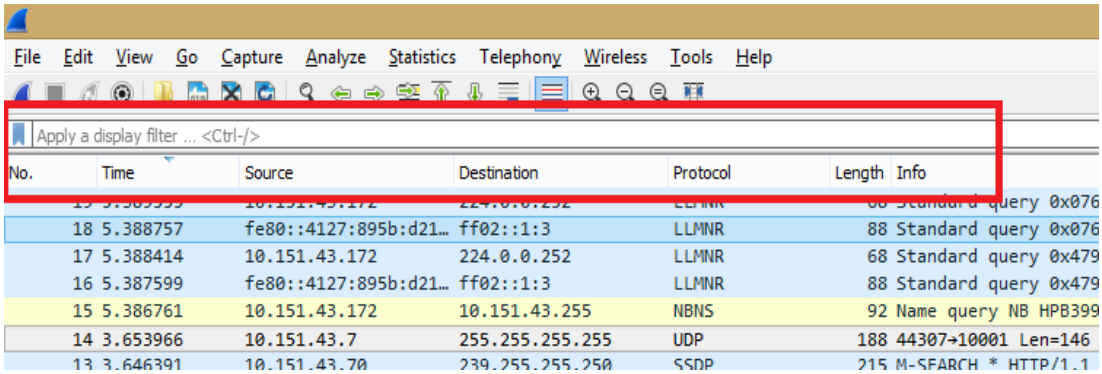
1. Pastikan komputer anda terhubung dengan sebuah jaringan.
2. Jalankan wireshark sebagai *administrator* (*root* jika di linux). Agar dapat Klik menu *capture* dan pilih *Interface* seperti yang terlihat pada gambar berikut.
3. Klik menu *capture* dan pilih *Interface* seperti yang terlihat pada gambar berikut.
4. Wireshark akan menampilkan *Interface* untuk dipilih, pada contoh ini kita akan memilih *interface* wifi untuk di-*scan*

5. Paket yang dikirim atau diterima pada jaringan akan otomatis muncul pada layar utama wireshark.



No.	Nama	Keterangan
1	Time	Waktu saat paket ditangkap, terhitung dari pertama kali melakukan scanning.
2	Source	Alamat sumber (darimana paket dikirimkan)
3	Destination	Alamat Tujuan (kemana paket dikirimkan)
4	Protocol	Menampilkan protocol apa yang dipakai oleh paket yang bersangkutan
5	Length	Panjang paket yang dikirimkan (byte)
6	Info	Informasi singkat tentang paket yang dikirimkan
7	Detail Column	Menampilkan detail paket yang bersangkutan
8	Hexadecimal Detail	Menampilkan detail paket yang bersangkutan (dalam format hexadecimal)

6. Untuk mempermudah pencarian maka anda dapat menggunakan fitur filter pada wireshark. Anda dapat menuliskan filter pada kolom input filter.



Ada dua macam filter pada wireshark, capture filter dan display filter. Capture filter bukanlah display filter, begitu juga sebaliknya. Capture filter digunakan untuk mengurangi size yang dibutuhkan saat scanning paket, sedangkan display filter hanya menyembunyikan paket yang tidak dibutuhkan.

A. Capture Filter

No.	Filter Syntax	contoh	Keterangan
1	host <ip address>	Host 10.151.36.15	capture trafik yang menuju atau dari suatu ip.
2	net <ip address> / <netmask>	Net 10.151.0.0/24 atau net 10.151.0.0 mask 255.255.255.0	capture trafik dari atau menuju sebuah range ip (netmask)
3	src net <ip address> / <netmask>	Src net 10.151.0.0/24	capture trafik yang berasal dari sebuah ip address
4	dst net <ip address> / <netmask>	Dst net 10.151.0.0/24	capture trafik yang menuju ke sebuah ip address
5	Port <port number>	Port 21	capture trafik yang menggunakan port tertentu

Untuk lebih lengkapnya silahkan buka: https://wiki.wireshark.org/CaptureFilters

B. Display Filter

No.	Filter Syntax	Contoh	Keterangan

1	Ip.src==<ip address> || ip.dst==<ip address>	Ip.src==10.151.36.15 || ip.dst==10.151.36.15	Menampilkan trafik yang berasal dari paket tertentu atau menuju ip tertentu
2	Ip.dst==<ip address> / <netmask>	Ip.dst==10.151.36.0.0/24	Menampilkan trafik yang berasal dari range ip tertentu (netmask)
3	tcp.port==<port number>	Tcp.port==53	Menampilkan trafik dengan protocol tcp yang menggukan port tertentu
4	http.host==”<host>”	http.host==”if.its.ac.id”	Menampilkan trafik pada host tertentu
5	http.host contains “<string>”	http.host contains “its.ac.id”	Menampilkan trafik pada host yang mengandung suatu string

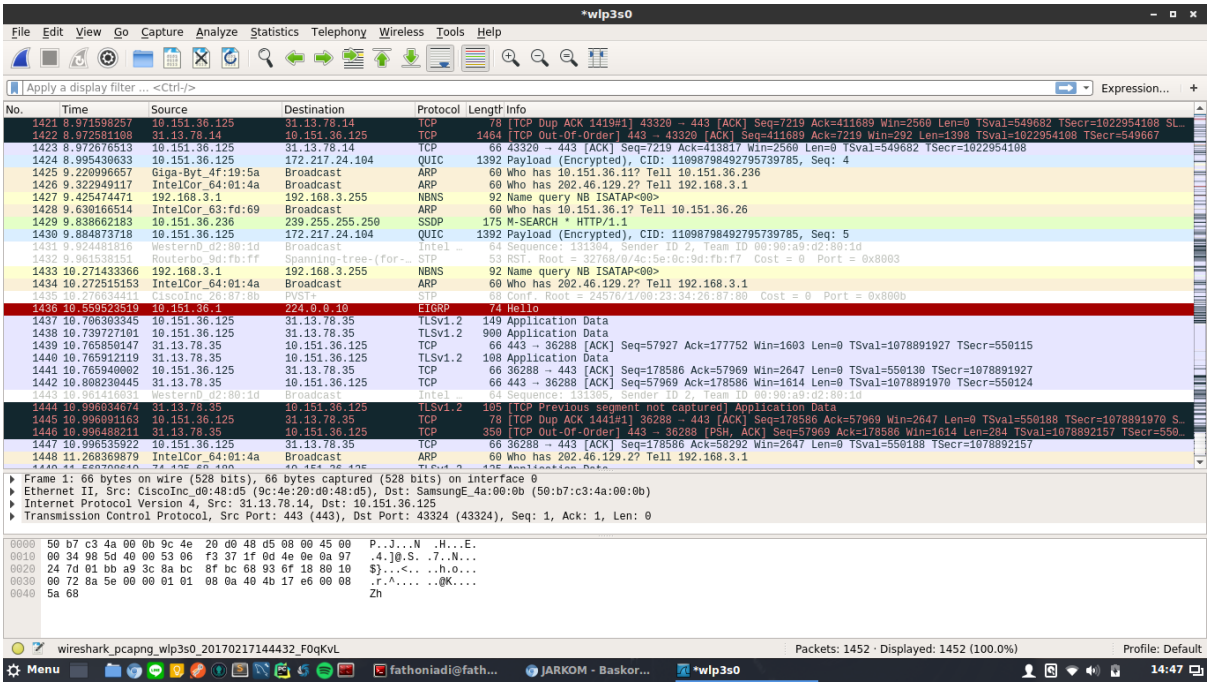
Untuk lebih lengkapnya silahkan buka: https://wiki.wireshark.org/DisplayFilters

Tutorial Export Data pada hasil Capture Wireshark

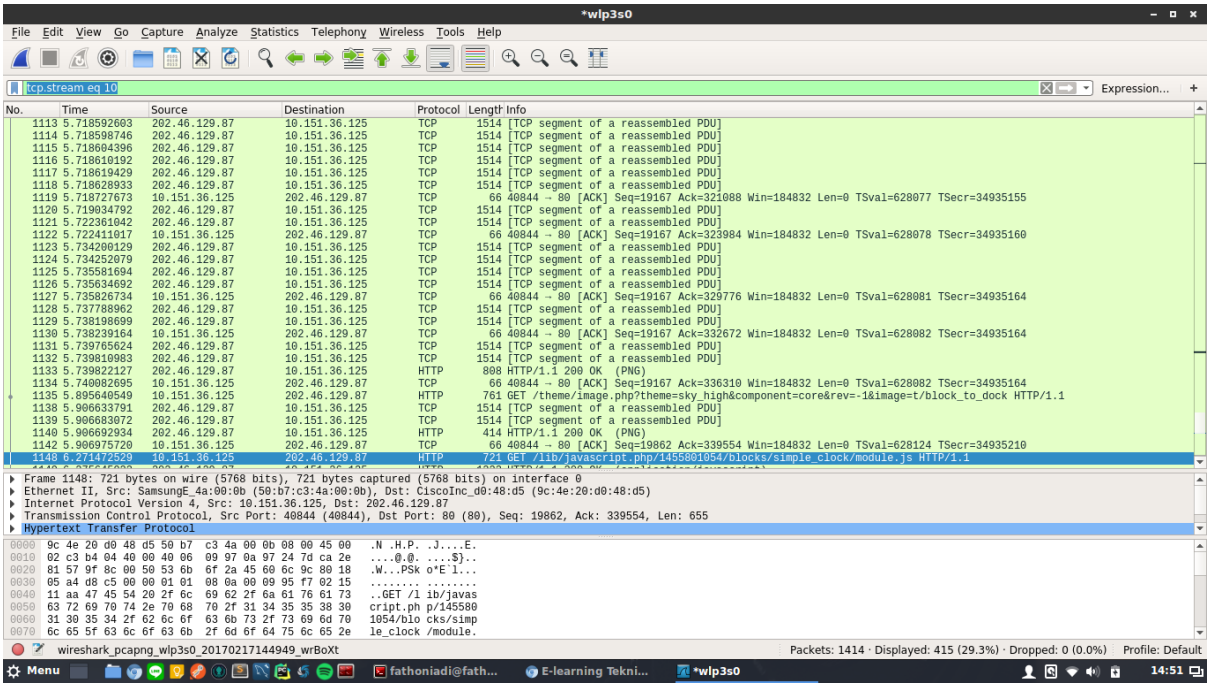
Selama proses sniffing pada jaringan, selain log akses kita juga bisa mengekstrak file-file yang terkirim maupun dikirim pada Jaringan.

Langkah-langkahnya :

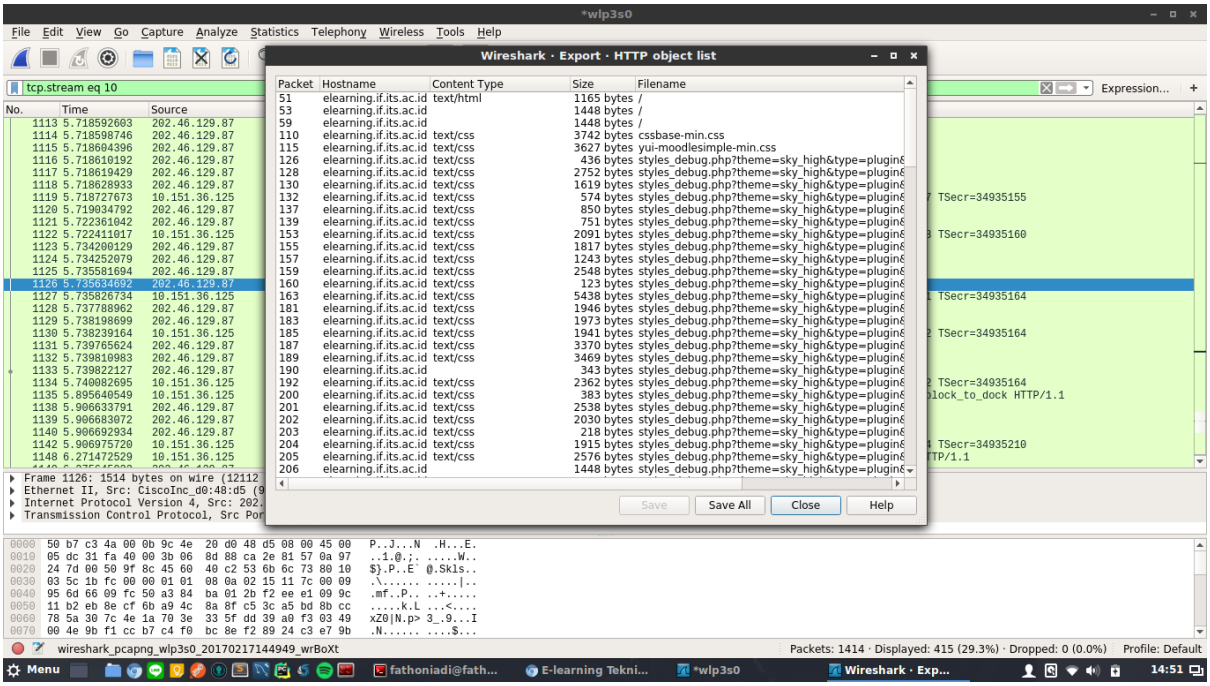
1. Capture paket dengan wireshark



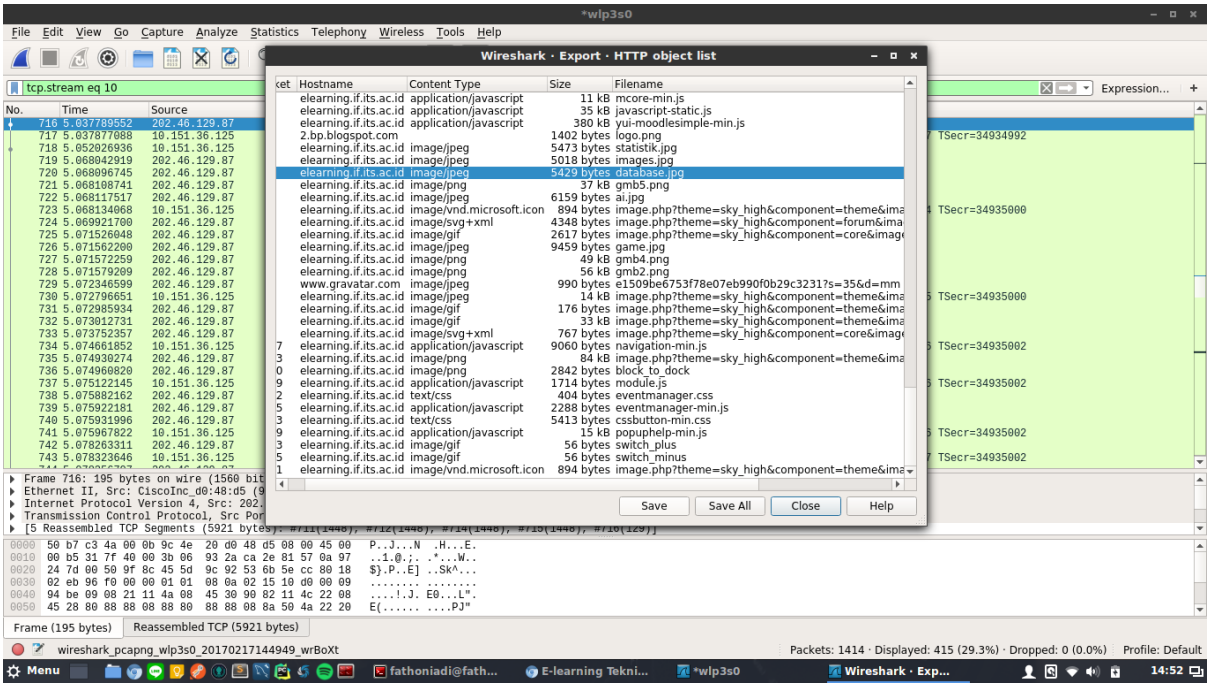
2. Filter paket yang dipilih



3. Klik menu File -> Export Object. Kemudian muncul kotak dialog list file.

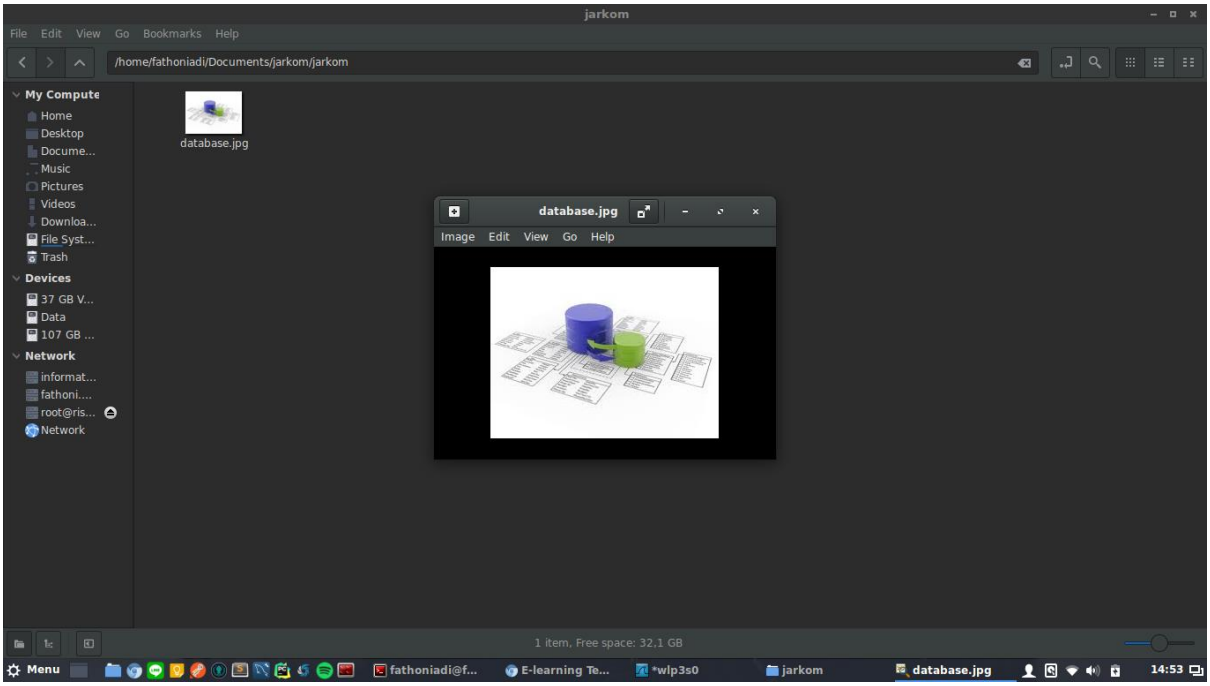


4. Pilih salah satu file.



5. Kemudian tekan save dan simpan di folder tujuan.

6. Hasil

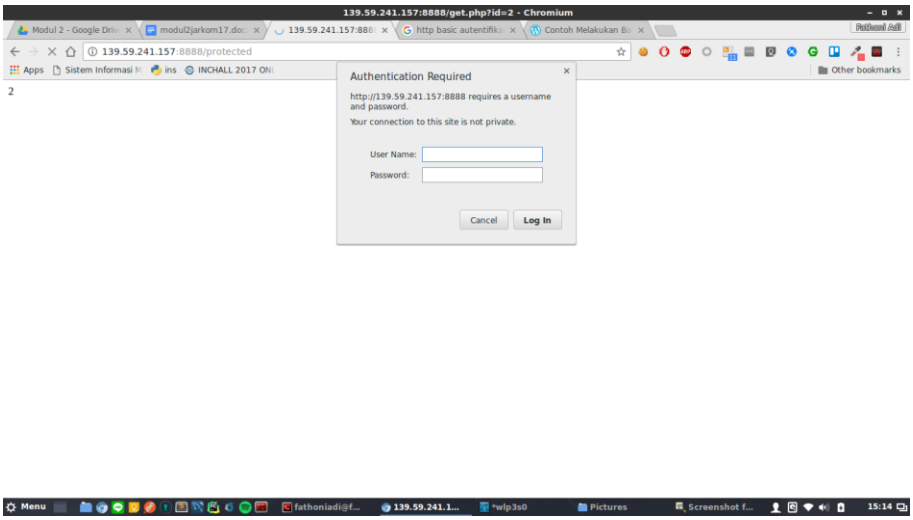


Penggunaan Wireshark pada HTTP Basic

HTTP Basic adalah salah satu model autentikasi dalam transaksi HTTP agar kita bisa masuk atau bisa menggunakan layanan dalam suatu web service.

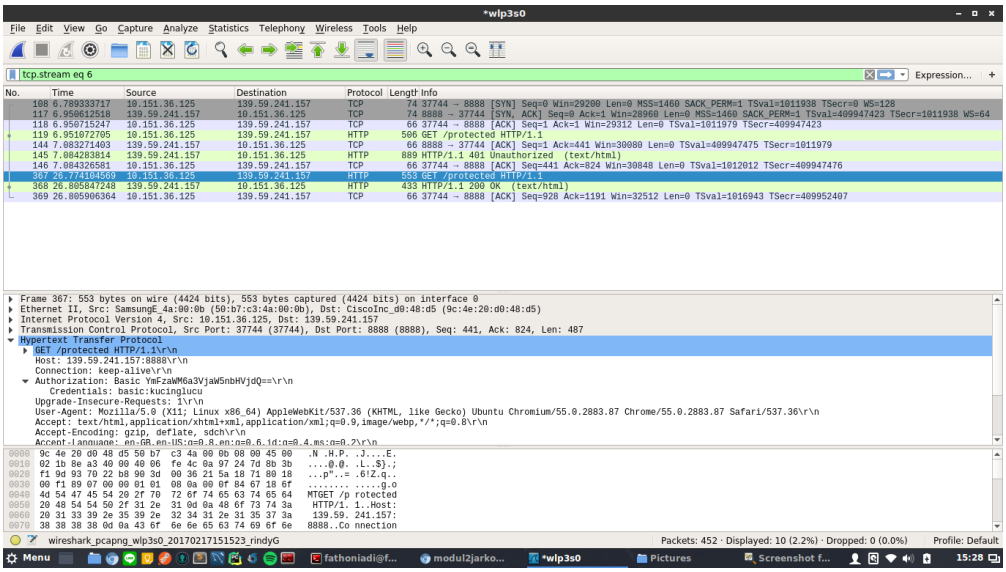
Langkah - langkah :

1. Siapkan aplikasi wireshark, start capture paket.
2. Buka http://139.59.241.157:8888/protected
3. Kemudian muncul kotak dialog autentifikasi



4. Masukan username: basic, password: kucinglucu
5. Kemudian lihat hasil capture wireshark, cari menggunakan filter ip.addr == 139.59.241.157

6. Klik GET /protected HTTP1.1. Kemudian lihat di paket detail selanjutnya pilih hypertext transfer protocol kemudian ada field Authorization:Basic YmFzaWM6a3VjaW5nbHVjdQ==



Field diatas menujukan bahwa terdapat autentifikasi HTTP Basic dengan username basic dan password yang dikirim adalah kucing lucu.

Penggunaan Wireshark untuk Protocol FTP

Langkah-Langkah :

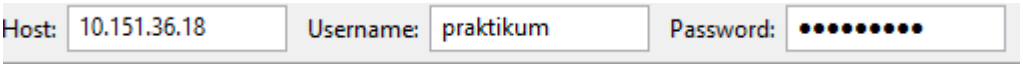
1. Start capture pada wireshark
2. Buka FileZilla
3. Isikan alamat host, username dan password

   Host : 10.151.36.18

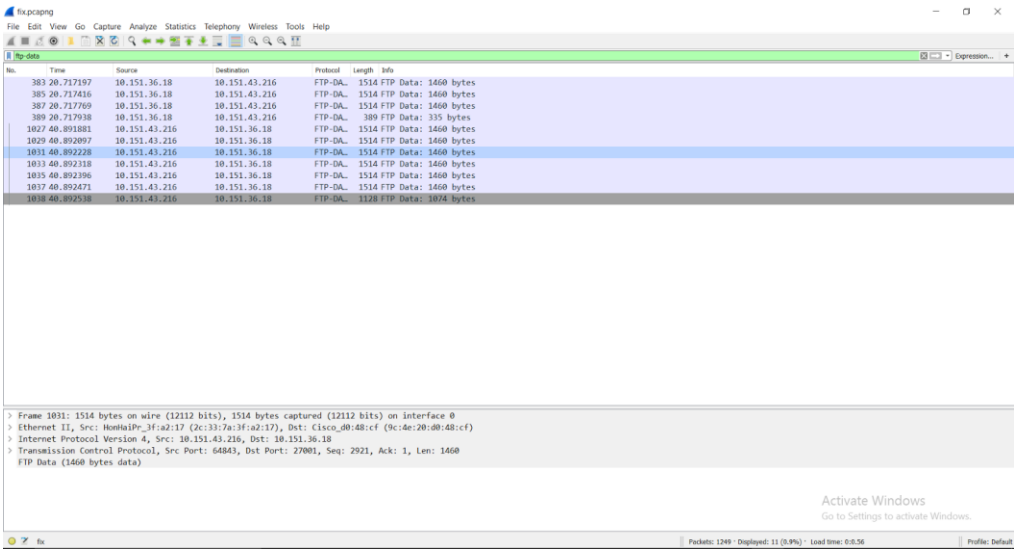
   Username : praktikum

   Password : praktikum

   Port : 21 (Default File ZIla akan otomatis mengarah ke port 21)



4. Gunakan capture filter ftp-data
5. Hasil seperti berikut :



Penggunaan Wireshark untuk Protocol HTTP Request Method GET

1. Ketikkan : 139.59.241.157:8888/get.php?id=22 pada browser
2. Filter packet menggunakan IP, kemudian pilih GET /get.php?id=22 HTTP/1.1

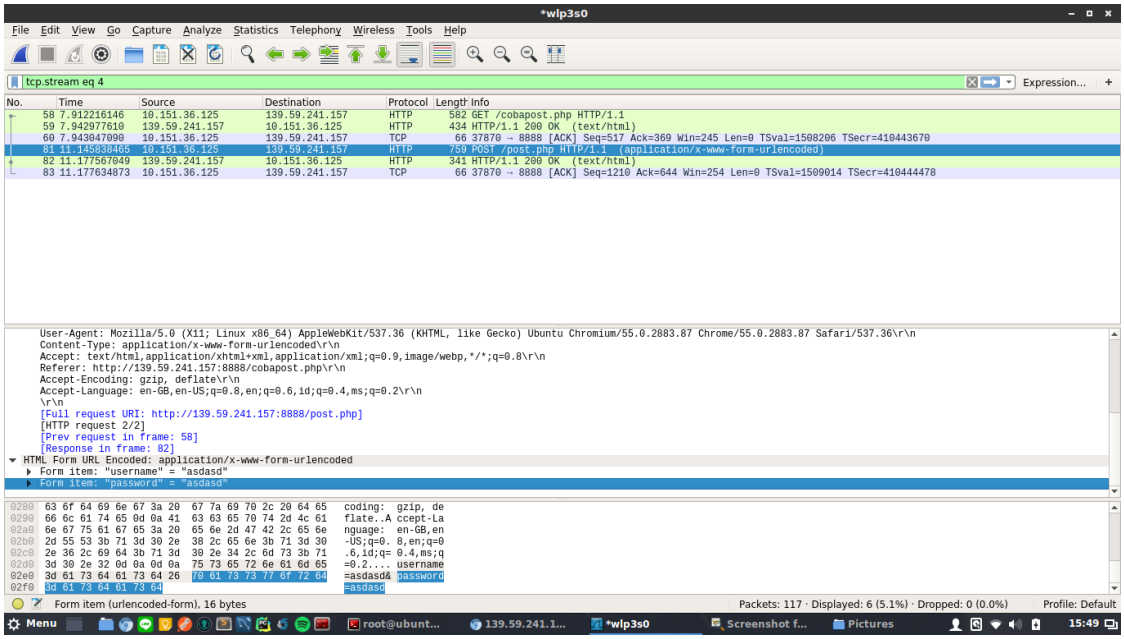
```
  76 6.955262    10.151.43.197 139.59.241.1… HTTP      468 GET /get.php?id=1 HTTP/1.1
  77 6.992429    139.59.241.1… 10.151.43.197 HTTP      289 HTTP/1.1 200 OK  (text/html)
  78 7.042446    10.151.43.197 139.59.241.1… TCP        54 64079 → 8888 [ACK] Seq=829 Ack=471 Win=252 Len=0
  99 11.081887   10.151.43.197 139.59.241.1… HTTP      443 GET /get.php?id=22 HTTP/1.1
 100 11.111028   139.59.241.1… 10.151.43.197 HTTP      290 HTTP/1.1 200 OK  (text/html)
 101 11.166836   10.151.43.197 139.59.241.1… TCP        54 64079 → 8888 [ACK] Seq=1218 Ack=707 Win=251 Len=0
```

3. Hasil

```
▲ Hypertext Transfer Protocol
  ▷ HTTP/1.1 200 OK\r\n
    Server: nginx/1.10.0 (Ubuntu)\r\n
    Date: Fri, 17 Feb 2017 08:19:05 GMT\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Transfer-Encoding: chunked\r\n
    Connection: keep-alive\r\n
    Content-Encoding: gzip\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.032059000 seconds]
    [Request in frame: 264]
  ▷ HTTP chunked response
    Content-encoded entity body (gzip): 22 bytes -> 2 bytes
    File Data: 2 bytes
▲ Line-based text data: text/html
    22
```

Penggunaan Wireshark untuk Protocol HTTP Request Method POST

1. Buka http://139.59.241.157:8888/cobapost.php pada browser, isi username dan password. Bebas masukkan username dan password apa saja.
2. Lakukan seperti cara GET untuk mengetahui apa isi body paketnya.
3. Hasilnya



Perbedaan Menggunakan Persisten Connection Dan Non-Persistent Connection

Pada Persistent Connection, server akan terus menggunakan koneksi TCP yang sudah ada untuk transmisi data ke klien. Sehingga untuk request request berikutnya akan berlangsung lebih cepat karena tidak perlu membuat koneksi TCP baru lagi.

Sementara Non Persistent Connection, begitu request berhasil di respon, koneksi TCP tersebut akan ditutup sehingga jika klien melakukan request lagi, perlu membuat koneksi baru lagi. Hal ini tentu memakan waktu lebih.

Pada HTTP 1.0, akan didefinisikan di HTTP header, apakah koneksi request tersebut Persistent / Non Persistent.

Ciri-Ciri :

Connection : Keep-Alive berarti koneksinya bersifat Persistent

Connection : Close berarti koneksinya bersifat non-persistent Pada HTTP 1.1, semua koneksi yang dibuat adalah persistent by default, kecuali jika di spesifikasikan non-persistent

Contoh :

```
Hypertext Transfer Protocol
  GET /shout/show/getNewShout.php?&callback=jsonp1487521879899&_=1487522490060&shoutname=tinggalkan_jejak_anda__&start_id=7 HTTP/1.1\r\n
  Host: shoutcamp.com\r\n
  Connection: keep-alive\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36\r\n
  Accept: */*\r\n
  Referer: http://depeen.blogspot.co.id/2013/03/tutorial-wireshark-next-level_9.html\r\n
  Accept-Encoding: gzip, deflate, sdch\r\n
  Accept-Language: en-US,en;q=0.8\r\n
  \r\n
  [Full request URI: http://shoutcamp.com/shout/show/getNewShout.php?&callback=jsonp1487521879899&_=1487522490060&shoutname=tinggalkan_jejak_anda__&start_id=7]
  [HTTP request 1/1]
  [Response in frame: 1390]
```

ACCESS POINT

Pengertian Access Point

Jaringan WiFi merupakan jaringan tanpa kabel yang populer digunakan. Dan untuk membuat sendiri jaringan WiFi, kita butuh yang namanya **Access Point.** Access Point ini memiliki cara kerja yang hampir sama dengan Hub. Dan dia yang menjadi titik pusat pengiriman data di jaringan WiFi. Sehingga ketika komputer ingin mengirimkan data, dia pasti akan mengirimkannya melalui Access Point terlebih dahulu.

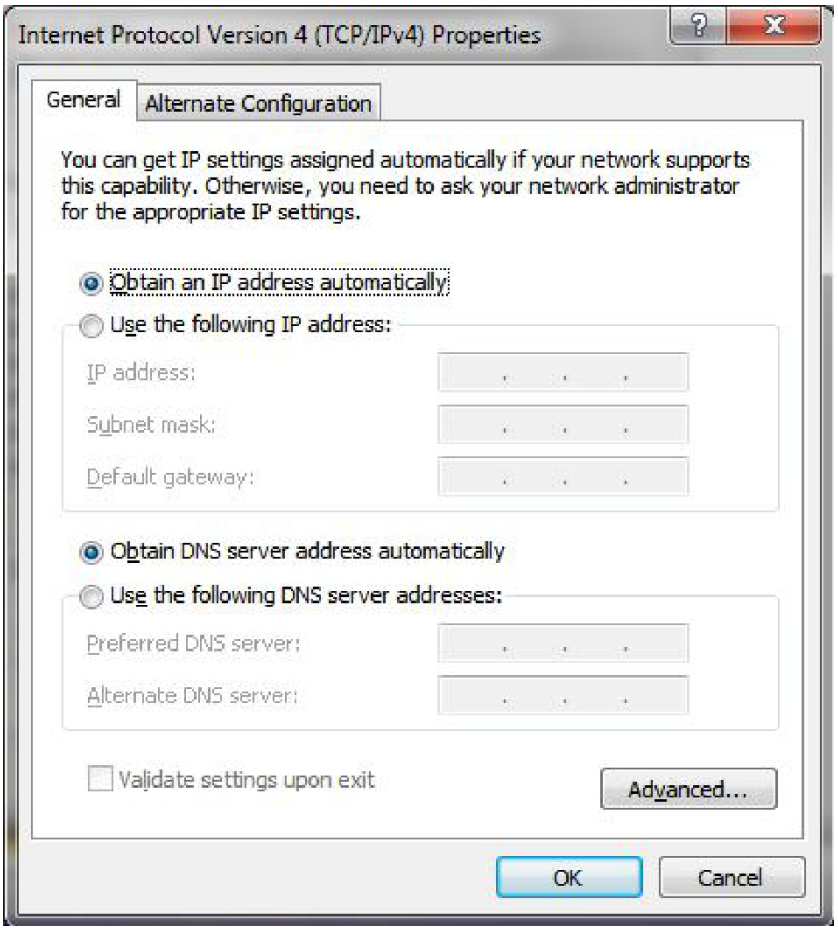
Sebuah Access Point biasanya dilengkapi juga dengan antenna untuk memancarkan sinyal. Kelemahan dari Access Point ini adalah kekuatan sinyal akan menurun jika terhalang benda padat. Karena itu peletakan sebuah Access Point perlu dipikirkan juga. Yang perlu diperhatikan lagi adalah konfigurasi Channel yang digunakan oleh masing-masing Access Point. Karena dua Access Point yang berdekatan tidak disarankan menggunakan Channel yang sama. Jika dipaksakan akan menyebabkan gangguan komunikasi antar Access Point. Sedangkan untuk masalah keamanan, Access Point masih lebih baik dari Hub, meski cara kerjanya hampir sama.

Access Point dapat melindungi penggunanya dengan menggunakan fitur keamanan WEP atau WPA. Dengan menggunakan WEP/WPA, tidak sembarang orang dapat menggunakan Access Point yang kita miliki. Selain itu, data yang dikirimkan juga lebih aman karena terenkripsi. Dan sangat disarankan untuk menggunakan WPA versi 2 apabila Access Point mendukung, karena apabila menggunakan WEP dapat dengan mudah dijebol. Seperti telah disebutkan di atas, saat ini banyak router yang sudah terintegrasi dengan Access Point.

Konfigurasi Access Point

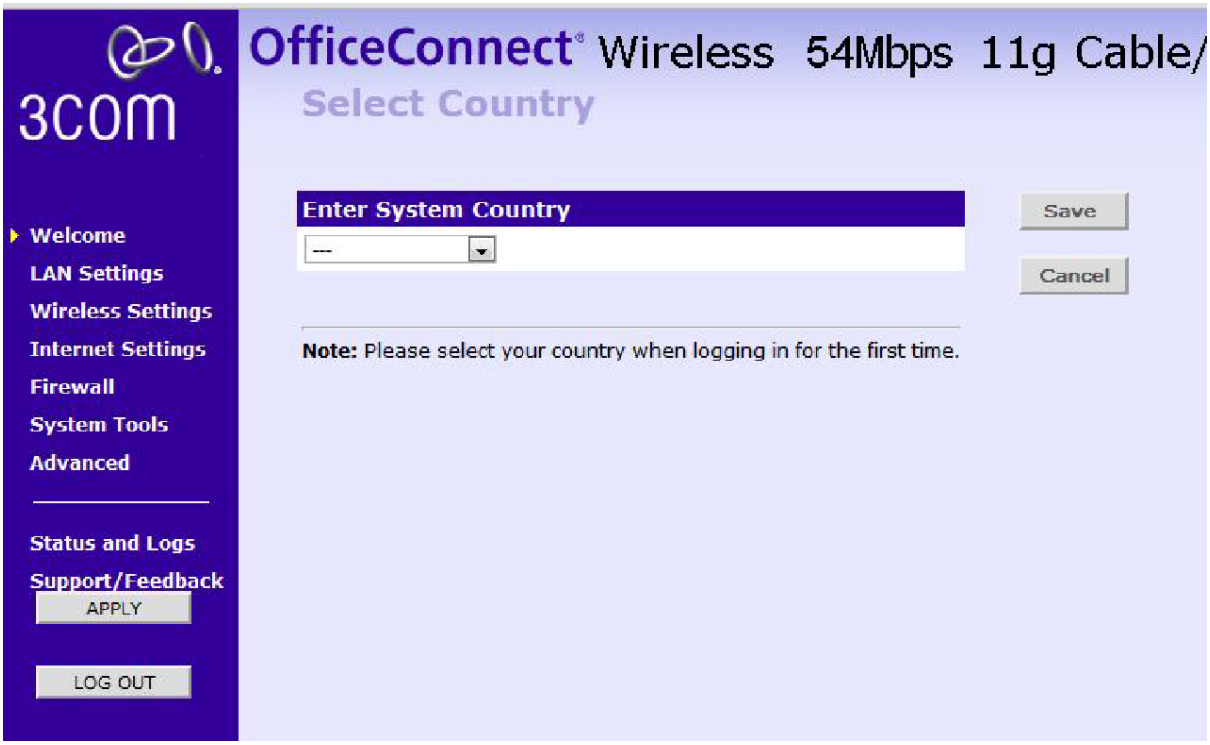
Langkah awal yang perlu dilakukan adalah memastikan access point sudah dalam kondisi default. Karena bisa saja access point yang akan dikonfigurasi sudah berubah dari aslinya, sehingga untuk login saja tidak bisa. Berikut ini adalah langkah-langkah untuk mengembalikan/memastikan access point sudah dalam kondisi default :

1. Cari tombol Reset (no 11) di access point, biasanya berbentuk tombol hitam keci
2. Nyalakan Access Point
3. Tekan tombol kecil tersebut, dan tahan beberapa detik (5-10 detik)
4. Kemudian lepaskan, maka akan ada indikator ketika perangkat sudah tereset. (Contoh : Lampu LED LAN Status akan menyala bergantian)
5. Untuk mulai mengkonfigurasi, gunakan kabel LAN jenis Straight, hubungkan antara komputer anda dengan salah satu 10/100 LAN Ports yang ada
6. Pastikan konfigurasi IP di komputer anda mengunakan IP dinamis
7. Caranya dengan membuka Network & Sharing Center dan buka konfigurasi IP (ipv4) sehingga muncul tampilan seperti ini



8. Pastikan konfigurasi IP default seperti pada gambar diatas. Lalu klik ok dan keluar.
9. Buka browser Firefox/Chrome yang ada, kemudian masukkan alamat ip router (pada contoh disini menggunakan http://192.168.1.1) maka akan tampak seperti gambar di bawah ini :

10. Lalu masukkan default password yang ada, dalam hal ini adalah “admin” (tanpa tanda petik), maka akan masuk ke halaman konfigurasi yang ada seperti terlihat pada gambar berikut.



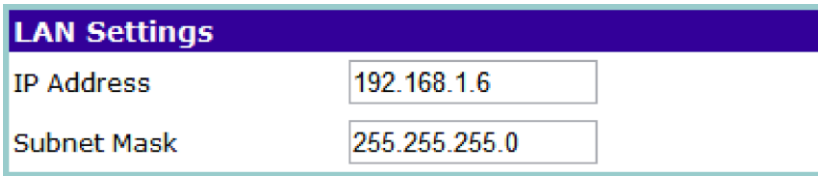
11. Setelah itu pilih USA pada System Country, dan klik tombol Save

Konfigurasi LAN (DHCP)

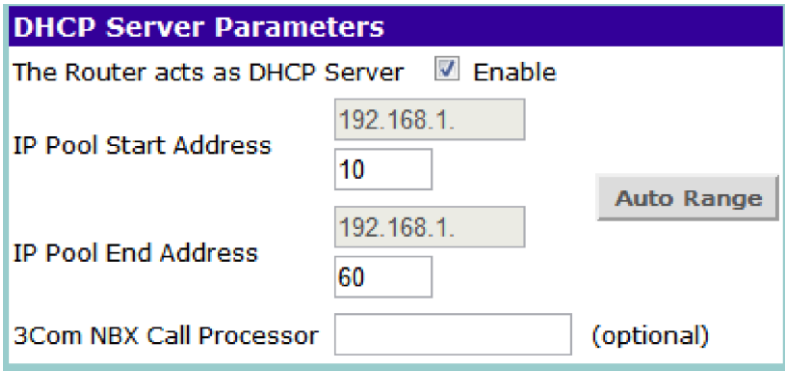
Yang pertama akan dibahas setelah konfigurasi awal adalah konfigurasi LAN pada access point, yang termasuk di dalamnya adalah konfigurasi DHCP Server pada access point. Berikut ini adalah apa saja yang bisa dilakukan pada konfigurasi LAN di access point:

1. Klik LAN Settings yang ada di sebelah kiri

2. Yang pertama dikonfigurasi adalah alamat IP dari access point ini, hal ini berguna jika nanti kita akan mengkonfigurasi ulang access point ini.



3. Misalkan saja diubah menjadi 192.168.1.6 dengan netmask 255.255.255.0
4. Kemudian, berikutnya adalah mengkonfigurasi DHCP server. Jika ingin access point ini dapat memberikan IP secara dinamis, maka centang The router act as DHCP Server
5. Lalu berikan range alamat IP yang dapat diberikan, misalkan saja 192.168.1.10-192.168.1.60, maka akan tampak seperti gambar berikut :



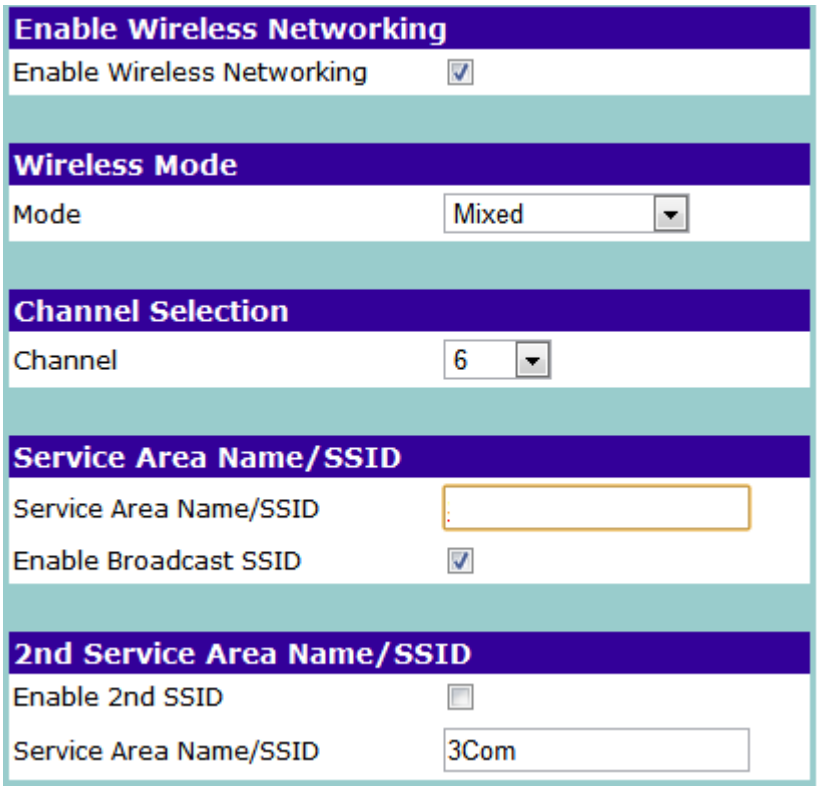
6. Kemudian klik tombol Save yang ada di sebelah kanan
7. Setelah klik Save, maka akan ada peringatan dan anda akan kembali ke halaman login setelah menunggu beberapa detik

Konfigurasi Wireless

Setelah konfigurasi LAN selesai, berikutnya adalah konfigurasi Wireless. Konfigurasi ini termasuk penting karena bila tidak berjalan, maka access point kita tidak akan bisa berfungsi sebagai access point yang sebenarnya. Berikut ini adalah apa saja yand dikonfigurasi pada bagian ini.

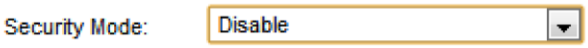
1. Klik LAN Settings yang ada di sebelah kiri

2. Di halaman berikutnya yang muncul, pilih enable Wireless Networking
3. Kemudian untuk Mode, pilih yang Mixed

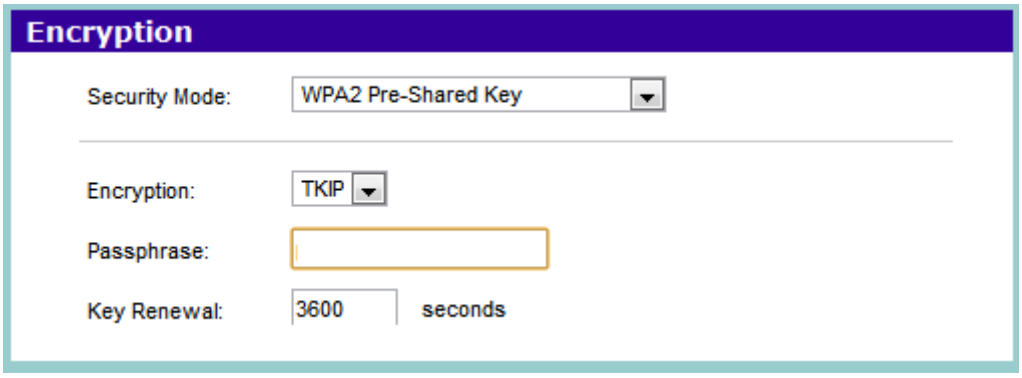


4. Untuk Channel, pastikan terlebih dahulu access point lain di sekitar Access Point anda menggunakan channel berapa. Usahakan tidak menggunakan channel yang sama dengannya, pada contoh ini akan menggunakan channel 6
5. Berikutnya untuk SSID atau nama access point, buatlah juga yang unik, sehingga tidak ada access point lain dengan nama yang sama (Jangan gunakan karakter spasi untuk SSID).
6. Klik tombol Save
7. Setelah selesai pada bagian ini, berikutnya adalah konfigurasi fitur keamanan pada access point dengan menggunakan enkripsi, sehingga tidak sembarang orang dapat menggunakan access point yang anda miliki
8. Klik tab Encryption

9. Ubah Security Mode yang awalnya disabled



10. Menjadi WPA2-PreShared Key seperti pada gambar di bawah ini



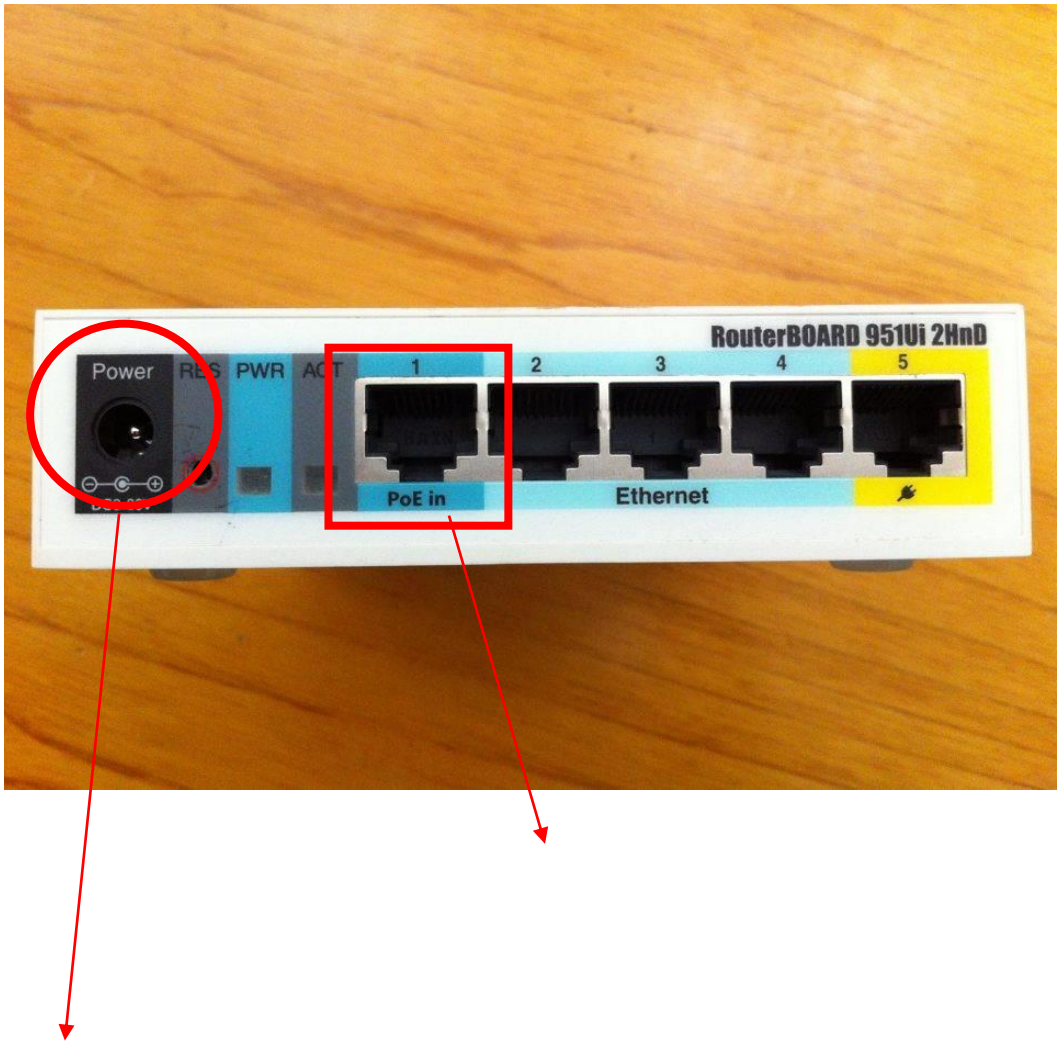
11. Berikan juga Passphrase atau Password yang nanti akan digunakan oleh user untuk mengakses access point
12. Klik tombol Save
13. Klik tombol Apply yang berkedip di kanan bawah

14. Setelah klik Apply, maka akan ada peringatan dan anda akan kembali ke halaman login setelah menunggu beberapa detik

MIKROTIK

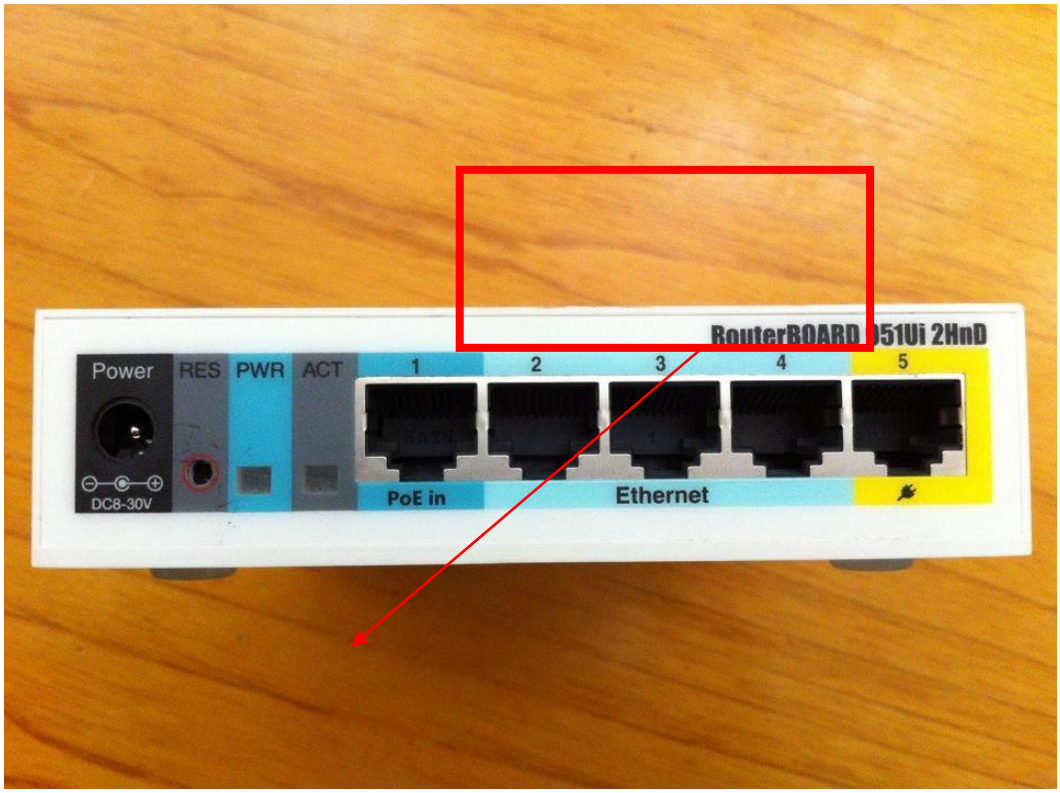
Mikrotik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer manjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk IP network dan jaringan wireless, cocok digunakan oleh ISP, provider hotspot dan warnet.

Interface Mikrotik

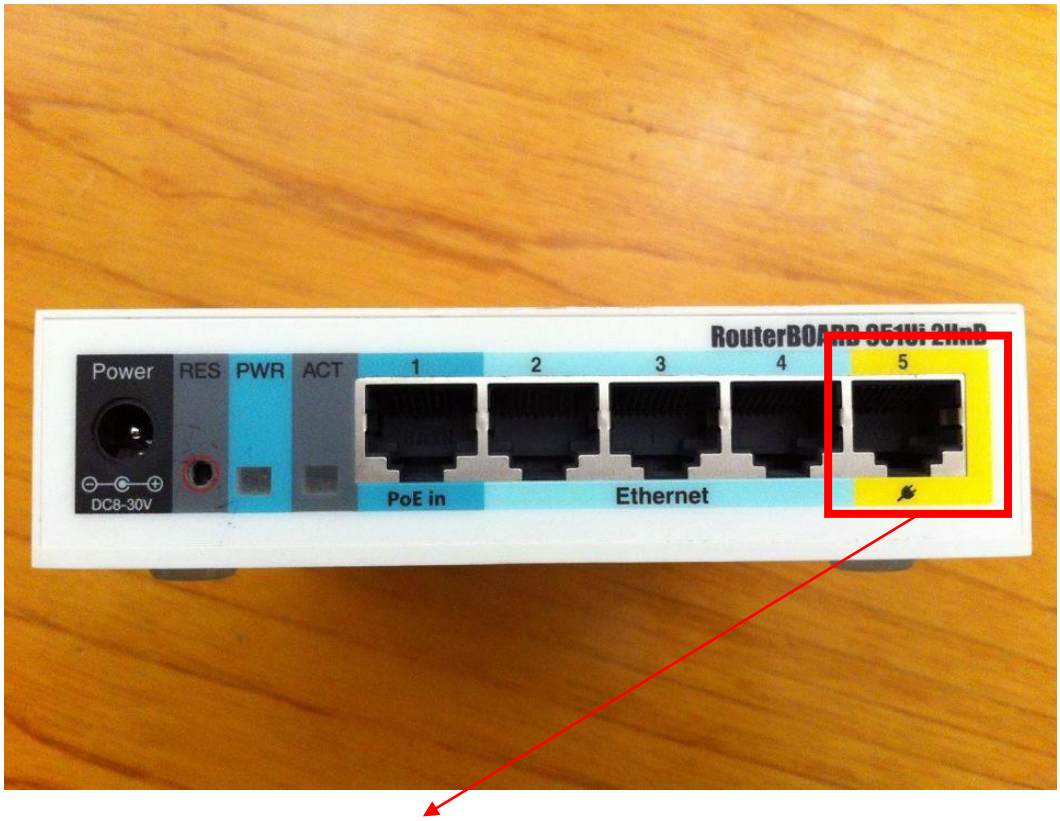


PoE in adalah port yang menerima daya yang dilewatkan oleh kabel ethernet .

Fungsi dari power adalah sebagai media transmisi power/daya.



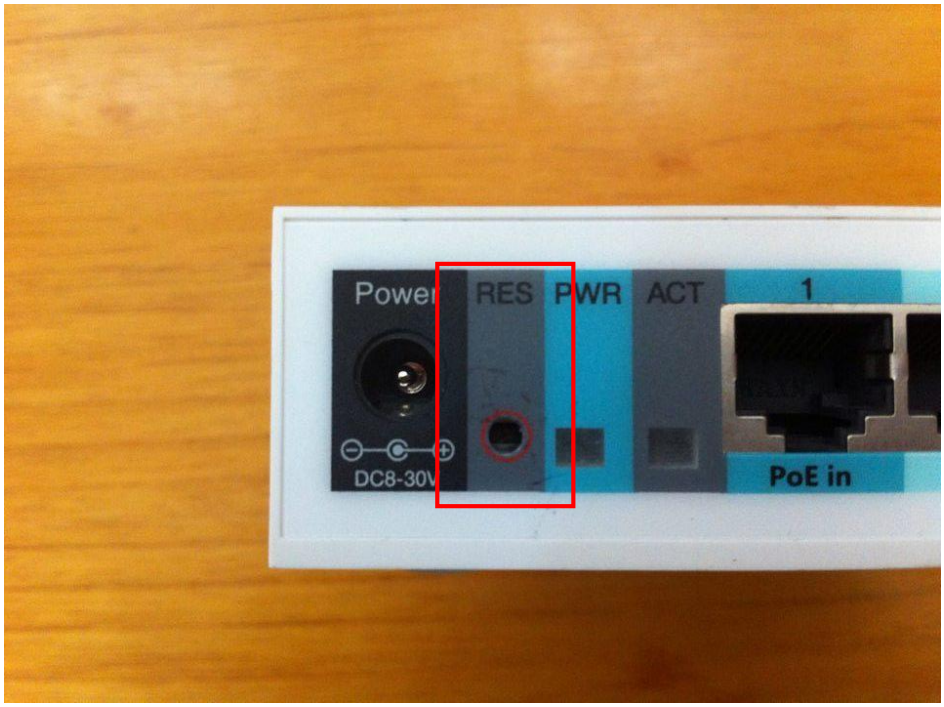
Ethernet adalah port untuk menyambungkan kabel LAN antara mikrotik dengan PC atau perangkat yang lain.



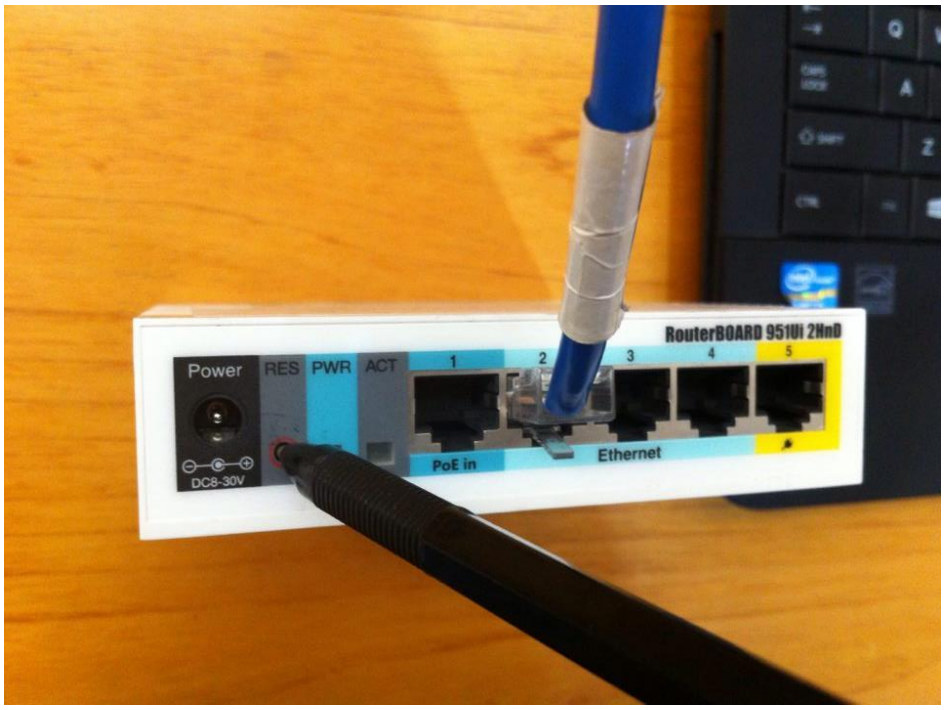
Port nomor 5 ini adalah PoE out, dimana berfungsi untuk memberikan daya kepada perangkat lain yang support oleh PoE in.

Jika melakukan “reset” pada hardware dengan cara berikut:

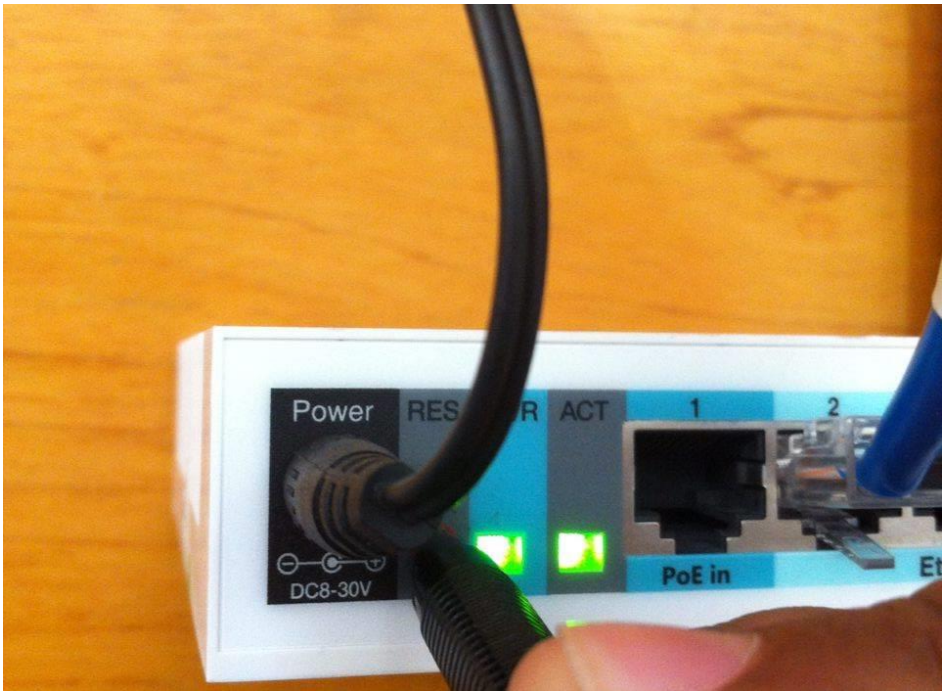
- Masukkan bolpoin/benda logam lainnya pada lubang RES untuk melakukan reset mikrotik.



- Lakukan seperti pada gambar berikut. Pada saat bolpoin/benda logam tersebut menancap, pastikan mikrotik dalam keadaan mati/power tidak menyala.



- Tekan bolpoin/logam tersebut, saat sedang menekan, nyalakan mikrotik dengan menancapkan power supply ke mikrotik seperti pada gambar dibawah. Jangan lepas bolpoin dulu. Kemudian perhatikan indikator pada ACT. Setelah lampu indikator pada ACT berkedip-kedip, kemudian mati, lepas bolpoin, maka mikrotik sudah berhasil di reset.



SOAL LATIHAN

SOAL 1

Buka facebook.com kemudian login sampai akun masuk ke beranda (Timeline). Tutup browser dan kemudian buka lagi facebook.com.

Mengapa akun masih terautentifikasi dan kita tidak perlu login lagi? Cobalah analisa menggunakan wireshark mulai dari sebelum login hingga membuka ulang facebook.com tanpa logout.

SOAL 2

(Ping tanpa limit) Coba ping its.ac.id dan 192.168.101.101. Menggunakan protocol apakah ping itu? Bagaimana hasil sniffing menggunakan wireshark (lihat detail)? Analisalah dan lihat apa perbedaan ping its.ac.id dan 192.168.101.101

SOAL 3

Bagaimana respon yang diterima komputer ketika mencari IP untuk nama domain akademik3.its.ac.id dan fablius.its.ac.id?

(Uji Coba DNS) Kegunaan perintah: host –t A (url)