BAB IV

IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi

Pada bab ini akan dilakukan implementasi dan pengujian terhadap sistem VPN dengan menggunakan *Virtual Private Server* yang dibangun. Implementasi dilakukan berdasarkan analisis dan perancangan yang telah dibuat. Setelah implementasi selesai, maka selanjutnya akan dilakukan pengujian untuk mengetahuan kinerja dari jaringan VPN yang telah dibangun dan keamanan yang didapat sebelum dan setelah menggunakan vpn.

4.1.1 Pengalamatan IP

Pada bagian ini diterapkan bagaimana pengalamatan IP terhadap *server* dan *client* sesuai dengan skema perancangan jaringan yang telah dilakukan pada bab sebelumnya. Adapun pengalamatan IP terhadap vpn *server*, *server wifi* dan *client* adalah sebagai berikut:

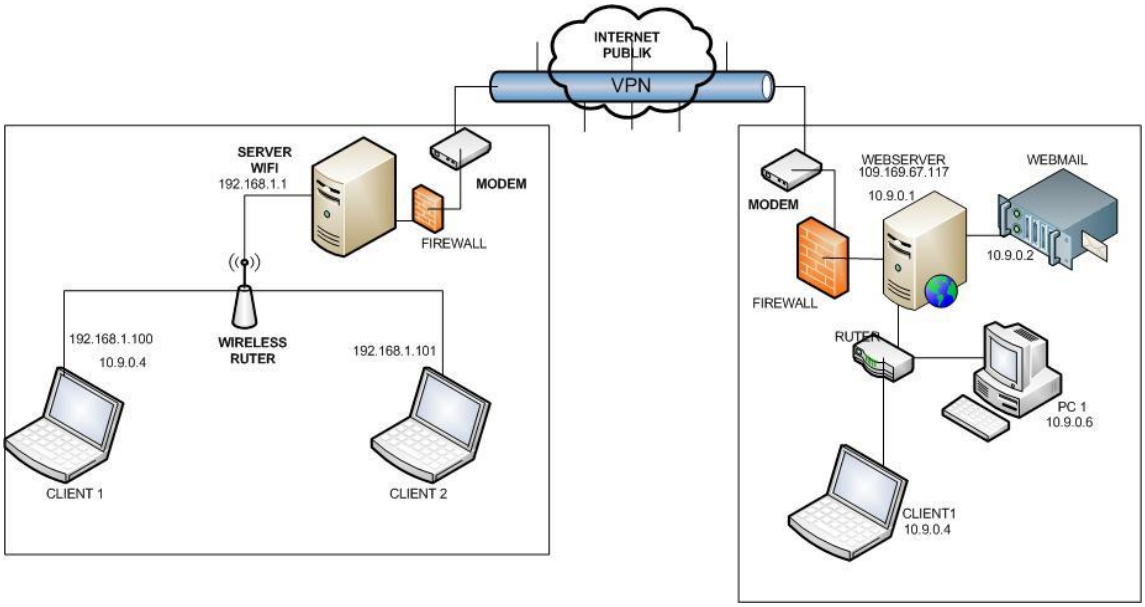
Tabel 4.1 Alokasi IP Addrees

Device	IP Address	Publik/Private	Interface
VPN Server	10.169.XXX.XXX	IP public	Modem
	109.169.67.117	IP Private	Eth0
	10.9.10.1	IP VPN	Virtual/tap adapter
Server Wifi	192.168.1.1	IP Server Wifi	Wifi /hospot
Client	192.168.1.xxx	IP public	Wifi / hostpot
	10.9.10.XX	IP VPN	Virtual/tap adapter

4.1.2 Skema Jaringan VPN

Skema atau ilustrasi vpn yang akan digunakan agar dapat menyelsaikan masalah yang terjadi dalam jaringan publik atau *wifi* adalah sebagai berikut.

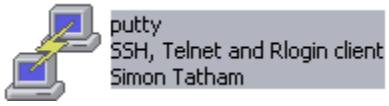
1. *notebook* atau pc yang terkoneksi ke jaringan *wifi*
2. melakukan *remote Acces* ke server Vpn dengan membuat jalur vpn sendiri secara aman untuk menanggulangi masalah penyadapan di wifi
3. setelah *client* terkoneksi ke vpn maka paket data terenkripsi hingga menjadi lebih aman dalam mengakses *webserver* dan *webmail* untuk lebih jelas nya dapat dilihat pada gambar 4.1



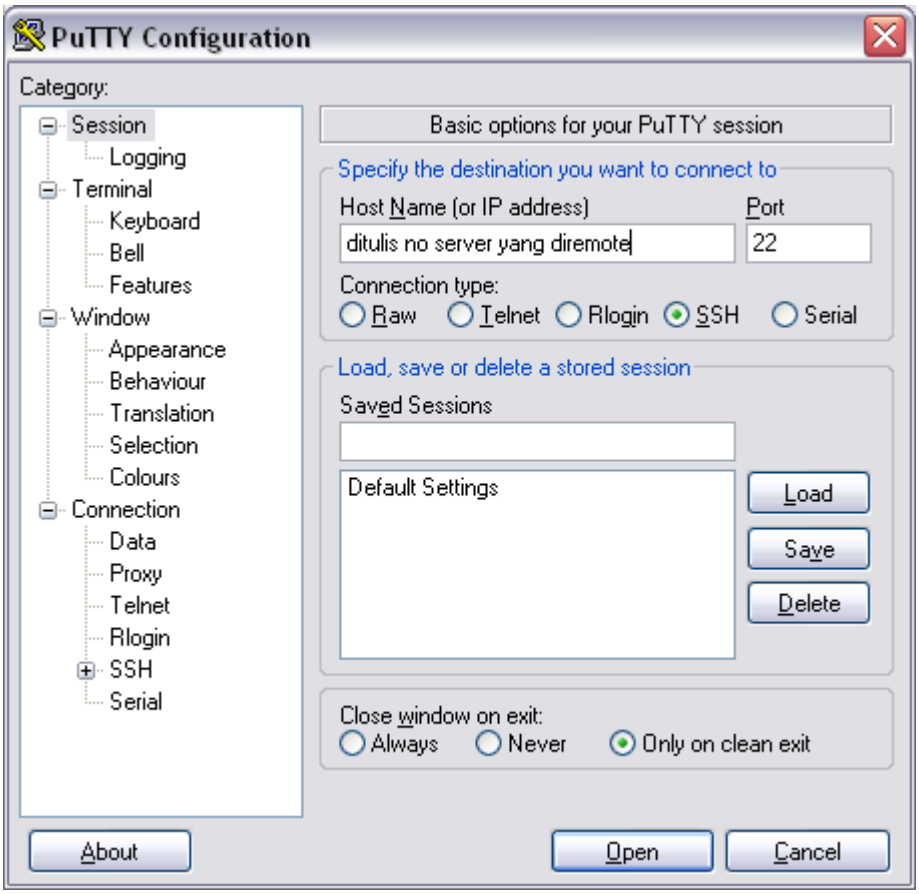
Gambar 4.1 Koneksi jaringan VPN dengan VPS

4.1.3 Instalasi *software*

A. Instalasi *putty*

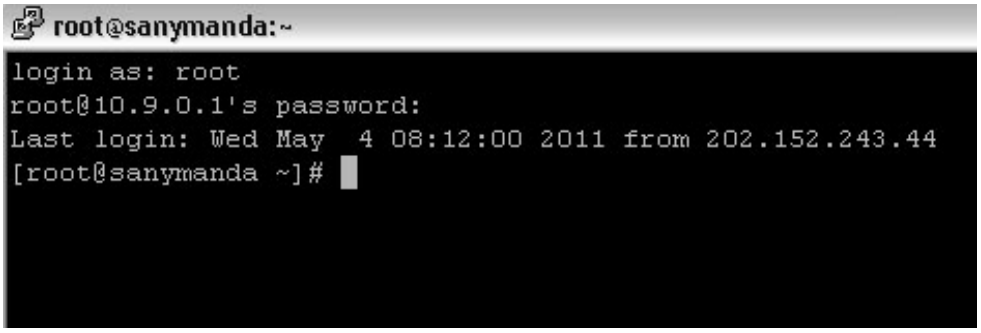
Putty 

Untuk menjalankan *putty* dengan *double click* pada *icon* maka *putty* secara otomatis langsung *running*,dan akan muncul tampilan Gambar 4.2



Gambar 4.2 Tampilan *Aplikasi Putty*

Untuk melakukan *Remote* ke server diharuskan mengisi *Hostname* (Ip server)yang akan *diremote* dengan port 22 dan *type connection SSH* setelah itu klik open maka putty akan langsung melakukan koneksi ke *server*,untuk lebih jelas nya bisa lihat Gambar 4.3

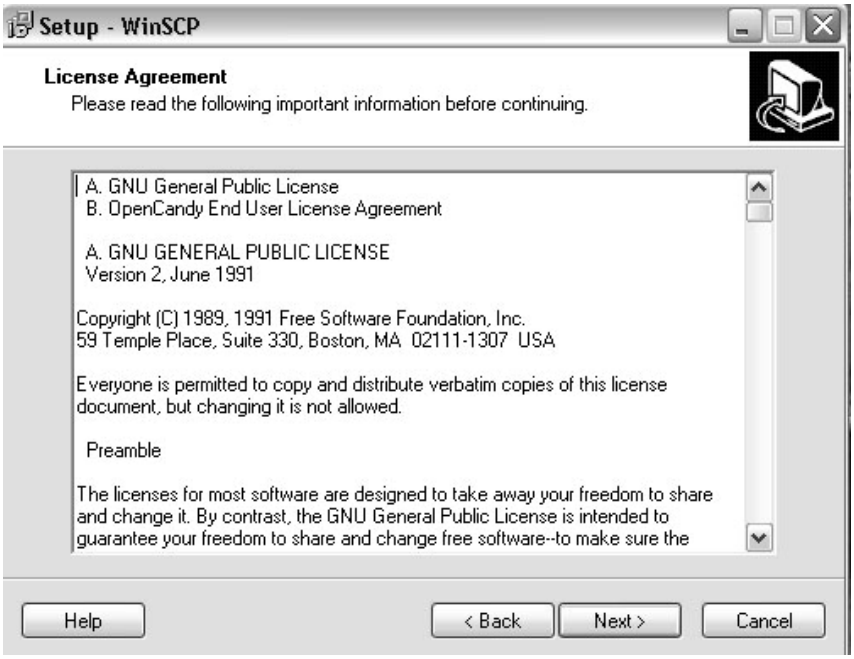


Gambar 4.3 Tampilan putty saat melakukan *remote*

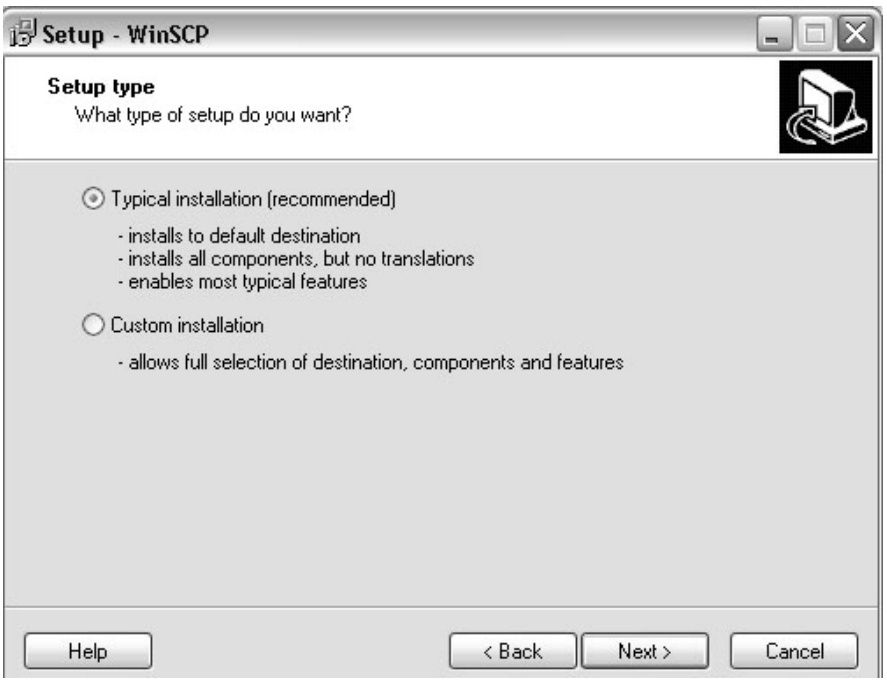
B. Instalasi WinSCP



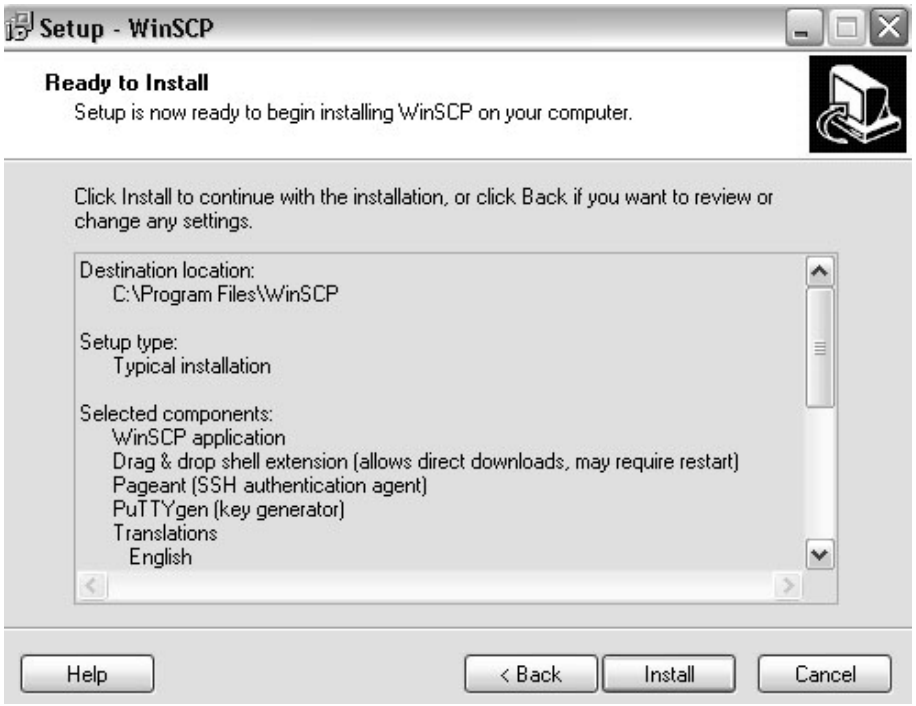
Gambar 4.4 Tampilan Awal Instalasi WinScp



Gambar 4.5 Tampilan *License Agreement* WinScp



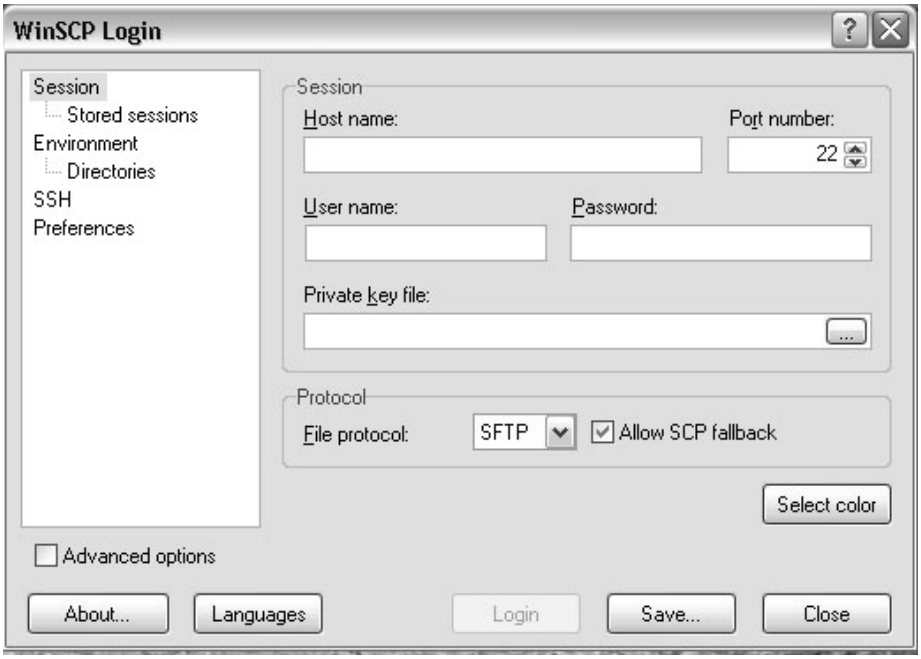
Gambar 4.6 Tampilan *Setup Type Winscp*



Gambar 4.7 Tampilan lokasi Instalasi WinScp

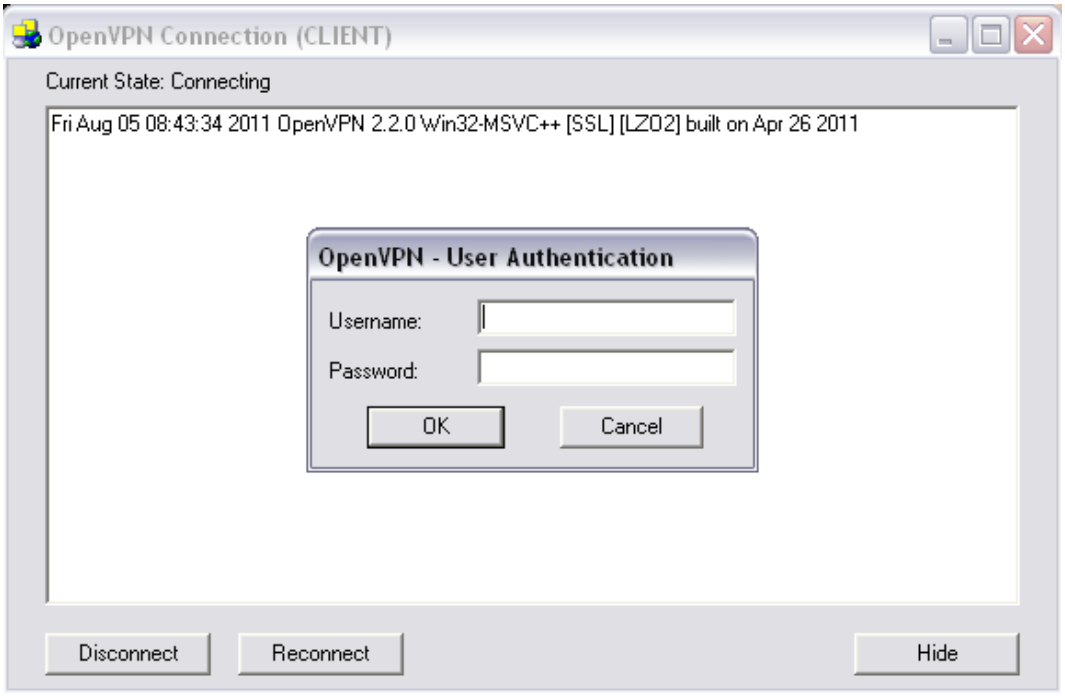


Gambar 4.8 Tampilan *User interface style*



Gambar 4. 9 Tampilan Login WinSCP

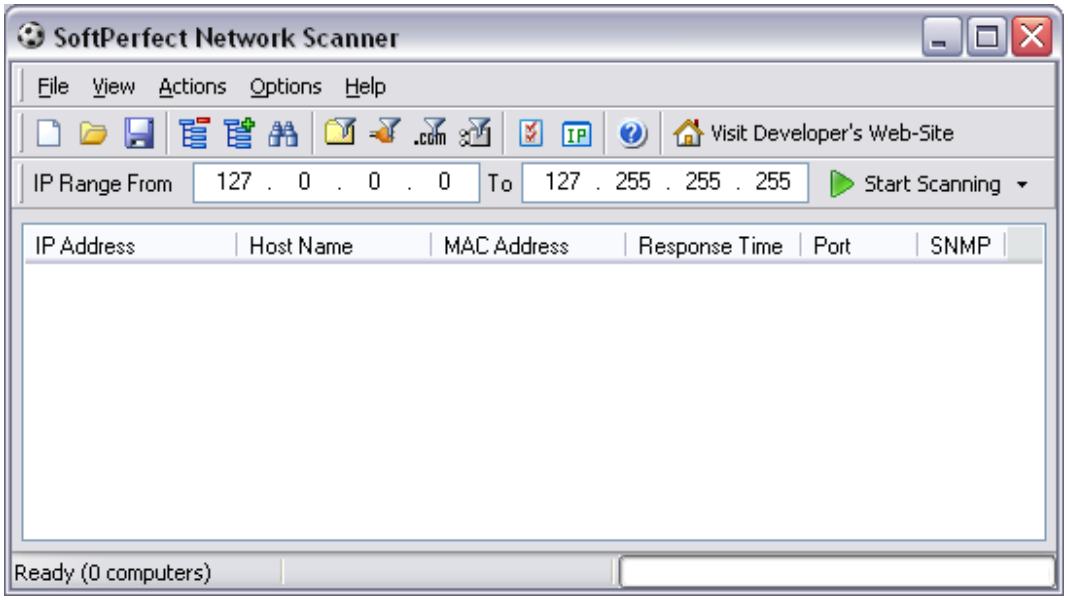
C.Client Openvpn



Gambar 4.10 Tampilan Login *Client Openvpn*

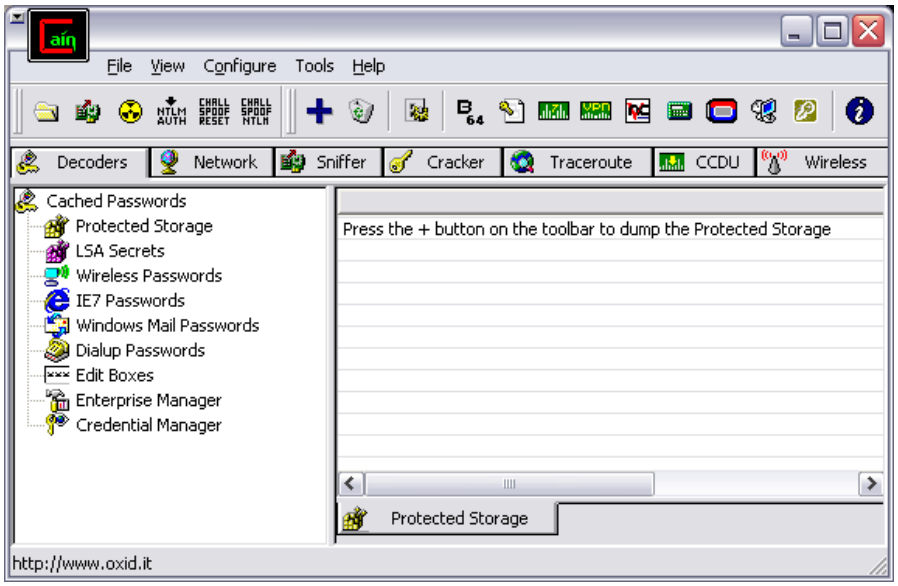
D.NetScan

Untuk instalasi tinggal *double click* pada program yang telah di download



Gambar 4.11 Tampilan Aplikasi Netscan

D.Cain & Abel



Gambar 4.12 Tamilan Awal Cain dan abel

4.1.4 Konfigurasi *server* dan *client VPN*

Agar VPN dapat terkoneksi sesuai pembangunan Vpn yang digunakan maka perlu dilakukan konfigurasi antara Client dan server,untuk mengetahui konfigurasi nya di jelaskan di bawah ini

4.1.1.1 Pada Server VPN

Membuat file konfigurasi TCP:

Ketikan command dibawah:

```
$ cat > 443.conf
Lalu isi / copy paste setting dibawah ini:
local 109.169.67.117
port 443
proto tcp
dev tun
ca vpn443/ca.crt
cert vpn443/vpn443.crt
key vpn443/vpn443.key
dh vpn443/dh1024.pem
# server utk beda port beda server, misal port
1194: 10.8.0.0 port 443: 10.9.0.0
server 10.8.10.0 255.255.255.0
ifconfig-pool-persist vpn443/logs/ipp.txt # supaya
alokasi IP client tdk berubah2
push "route 10.8.10.0 255.255.255.0"
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 4.2.2.1" # DNS resolver
push "dhcp-option DNS 4.2.2.2" # DNS resolver
keepalive 5 60
comp-lzo
#max-clients 100
daemon
#user nobody
```

```
#group nobody
persist-tun
persist-key
status vpn443/logs/openvpn-status.log # openvpn
status log
log-append vpn443/logs/openvpn.log # openvpn log
verb 6
#mute 20
#ping-timer-rem
# VPN Access Method
plugin /usr/lib64/openvpn/plugin/lib/openvpn-auth-
pam.so login
  client-cert-not-required
  username-as-common-name
#management localhost 7500
```

konfigurasi simpan di

```
# openvpn /etc/openvpn/nama443.conf
```

Konfigurasi port UDP :

Ketikan command dibawah:

```
$ cat > 53.conf
konfigurasi
local 109.169.67.117
port 53
proto udp
dev tun
ca vpn53/ca.crt
cert vpn53/vpn53.crt
key vpn53/vpn53.key
dh vpn53/dh1024.pem
```

```
# server utk beda port beda server, misal port 1194:
10.8.0.0 port 443: 10.9.0.0
server 10.9.10.0 255.255.255.0
ifconfig-pool-persist vpn53/logs/ipp.txt # supaya
alokasi IP client tdk berubah2
push "route 10.9.10.0 255.255.255.0"
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 4.2.2.1" # DNS resolver
push "dhcp-option DNS 4.2.2.2" # DNS resolver
keepalive 5 60
comp-lzo
#max-clients 100
daemon
#user nobody
#group nobody
persist-tun
persist-key
status vpn53/logs/openvpn-status.log # openvpn status
log
log-append vpn53/logs/openvpn.log # openvpn log
verb 6
#mute 20
#ping-timer-rem
# VPN Access Method
plugin /usr/lib64/openvpn/plugin/lib/openvpn-auth-
pam.so login
client-cert-not-required
username-as-common-name
#management localhost 7500
```

konfigurasi simpan di

```
# openvpn /etc/openvpn/nama53.conf
```

4.1.5 Konfigurasi pada client

File konfigurasi, untuk client

```
client
proto udp
dev tun
remote 109.169.67.117 53
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
auth-user-pass
comp-lzo
verb 3
```

4.2 Pengujian

Pada penelitian ini dilakukan pengujian terhadap *remote access virtual private network menggunakan vps* dengan beberapa scenario untuk melihat keamanan dari vpn yang telah dibangun. Simulasi akan dilakukan melalui jaringan *wifi mall dan caffee free hostpot,* dengan arsitektur simulasi seperti yang telah dirancang pada gambar dan dilakukan menggunakan *windows xp,windows vista,windows 7*

4.2.1 Skenario Pengujian

Pada skenario pengujian akan dilakukan terhadap konektivitas vpn dengan virtual private server dengan skenario dan keamanan sebelum dan sesudah menggunakan vpn di jaringan wifi . Adapun skenario-skenario yang akan dilakukan adalah sebagai berikut:

1. Pengujian koneksi VPN (koneksi Server dan koneksi Client), pengujian bertujuan apakah konfigurasi yang telah dilakukan pada *server* maupun *client* telah benar atau tidak.

2. Pengujian Koneksi VPN yang berupa tes koneksi *PING* dan ip yang di dapat

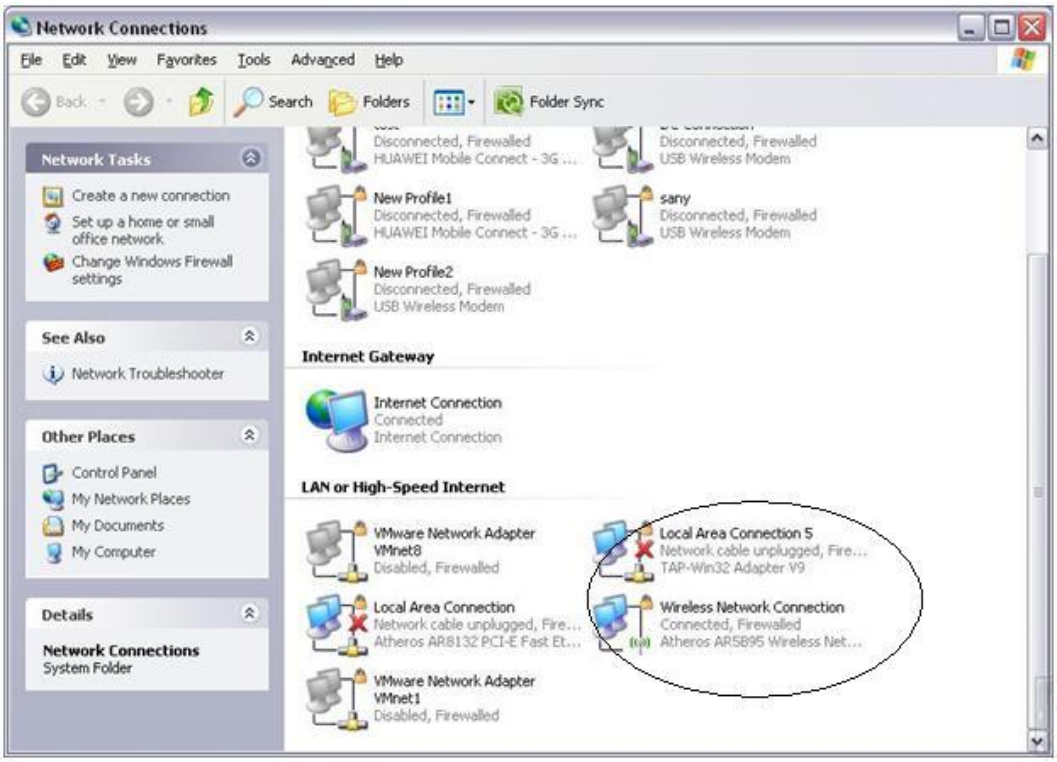
3. Pengujian Akses *Server* dimana *client* melakukan akses terhadap *webserver* dan *webmail*

4. Pengujian keamanan dilakukan di jaringan *wifi mall* dan *caffe free hostpot* dengan menggunakan *software cain abel*
5. pengujian menggunakan *windows xp,windows vista,windows 7*

4.3 Pengujian Server dan Client VPN

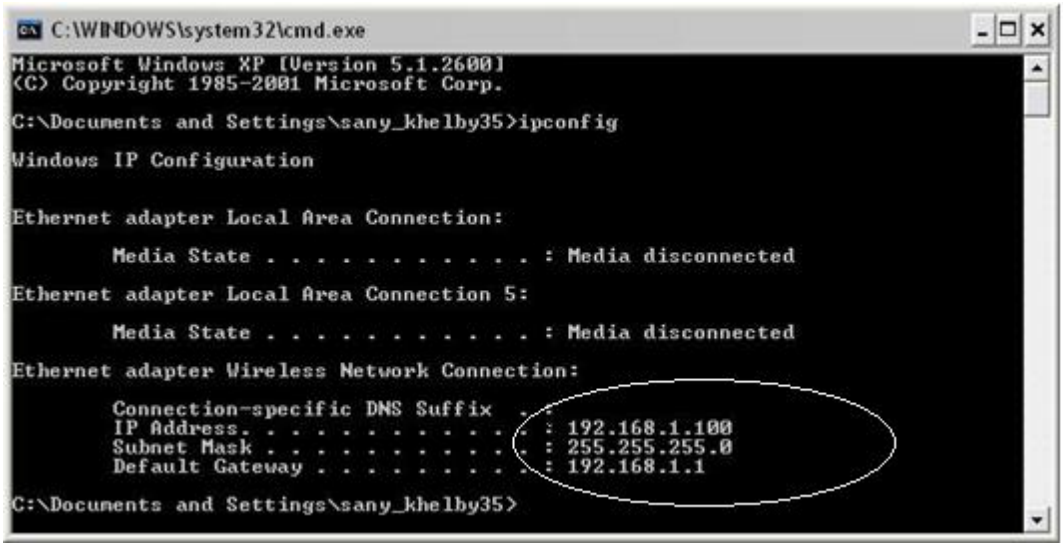
Di bagian ini dibahas koneksi dari *client* ke *server* vpn sebelum melakukan test dilakukan instalasi dulu di sisi *Client* menggunakan Openvpn,kenapa menggunakan openvpn karena dari segi lisensi openvpn adalah *software* gratis, untuk instalasi openvpn ada di bab sebelumnya,di sini dianggap openvpn telah terinstal di *notebook/PC* untuk lebih jelas tentang koneksi vpn dapat dilihat sebagai berikut

A. Kondisi ketika Client belum terhubung dengan VPN server



Gambar 4.13 Tampilan *Network Connection* dengan 1 IP *Connec*t

Pada gambar diatas terlihat bahwa hanya ada satu jaringan yang terkoneksi yaitu jaringan wireless jadi vpn belum terkoneksi.



Gambar 4.14 Tampilan *Command* terdapat satu no IP *Address*

Pada gambar diatas ketika client melakukan perintah *ipconfig* maka hanya diperoleh satu ip yaitu dari adapter wireless 192.168.1.100 dengan Gatway ip 192.168.1.1 adalah *server wireless*

B. Melakukan koneksi *client* ke VPN *server*

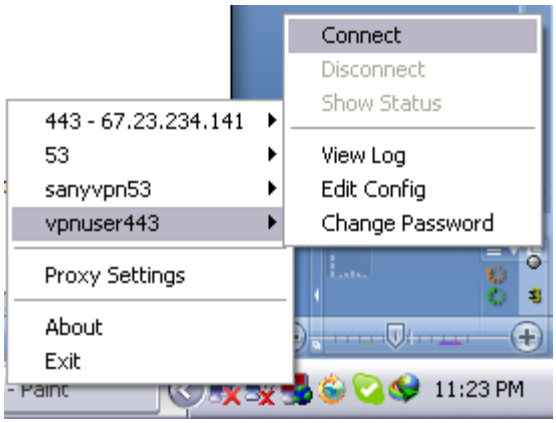
1. Pada *desktop double click icon* 

maka ada muncul pada *taskbar* menu



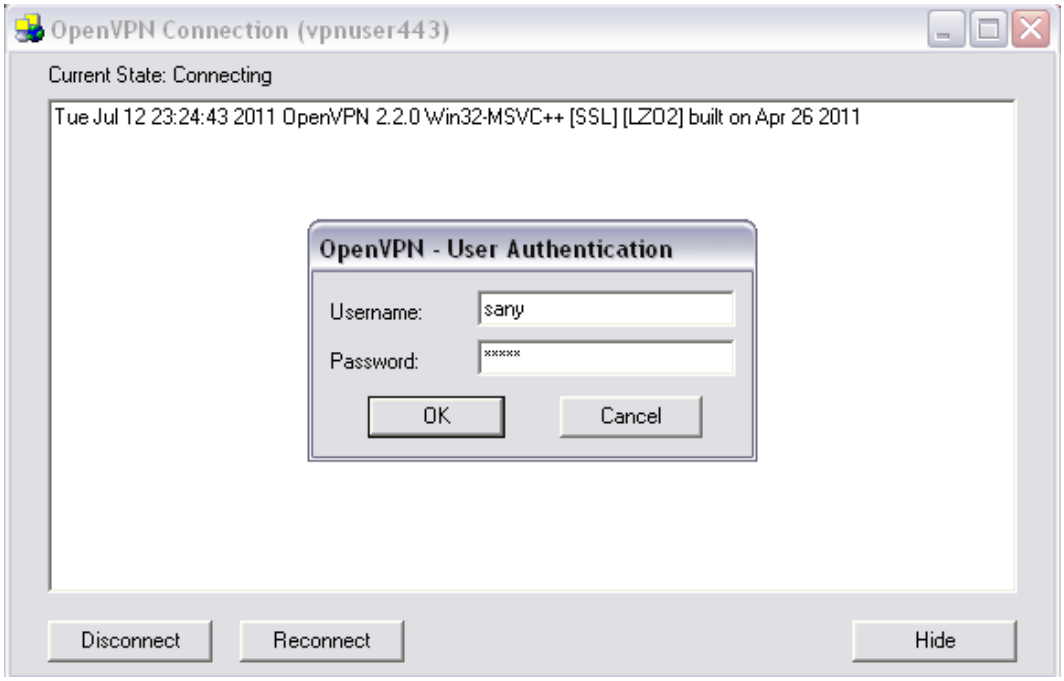
Gambar 4.15 Tampilan *icon* VPN pada *Taskbar*

2. Untuk memulai koneksi *click* kanan pada openVPN lalu pilih *connect*



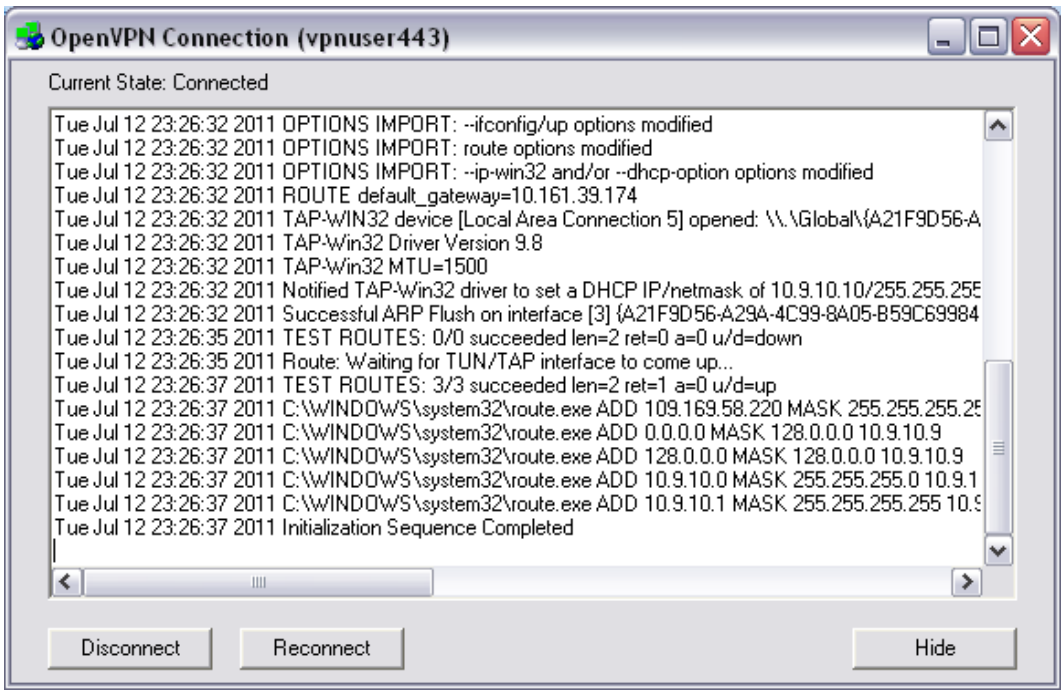
Gambar 4. 16 Tampilan VPN yang ingin dikoneksikan

3. Maka akan keluar tampilan dan disana harus isi *username* dan *password* vpn liat gambar dibawah ini

4. 

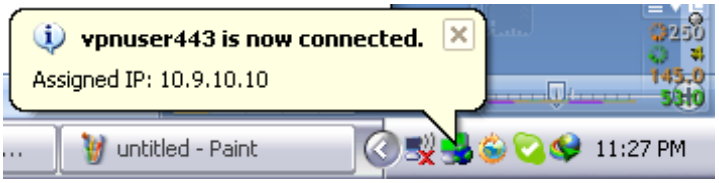
Gambar 4.17 Tampilan Openvpn Authentication

5. Setelah isi *username* dan *password* maka openvpn akan mulai memverifikasi liat gambar dibawah ini



Gambar 4.18 Tampilan Openvpn berhasil terkoneksi

6. Jika username dan password benar maka icon openvpn gui yang tadi nya merah berubah menjadi hijau seperti gambar dibawah ini

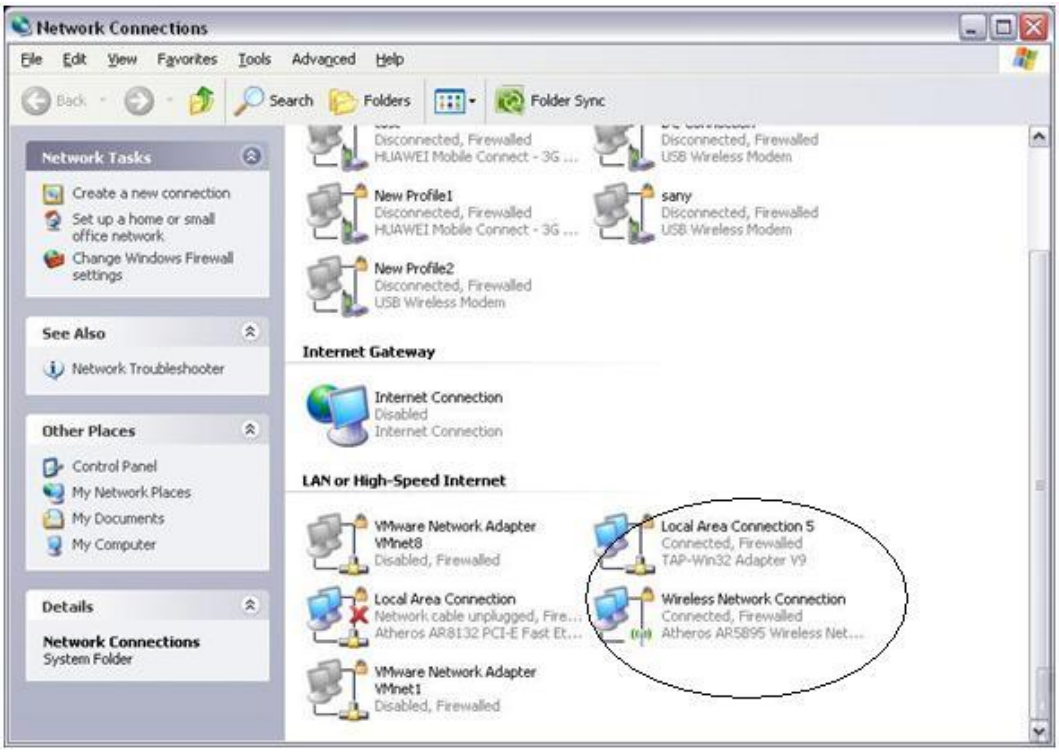


Gambar 4.19 Tampilan icon taskbar Openvpn menjadi hijau

7. Koneksi dari *Client* ke *Server* VPN telah berhasil

C. Setelah computer terkoneksi dengan VPN

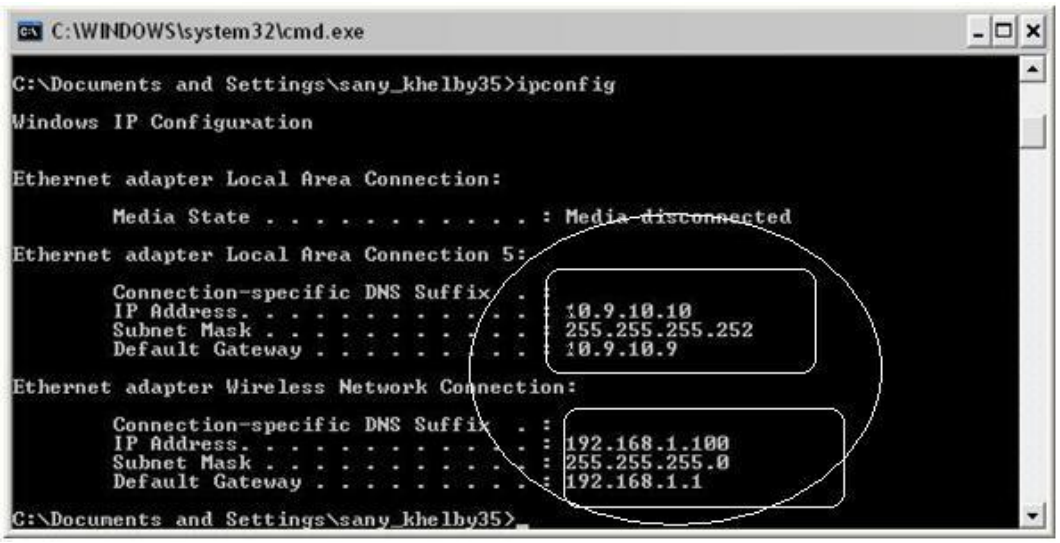
1. Maka ketika dilihat dalam *All Connection* maka terlihat seperti gambar dibawah ini



Gambar 4. 20 Tampilan *Network connection* dengan dua IP terkoneski

Pada gambar diatas terlihat ada dua ip yang terkoneksi yaitu ip wireless dan ip dari VPN virtual tap adapter V9

2.ketika dilakukan perintah di command *ipconfig* maka muncul tampilan dibawah ini



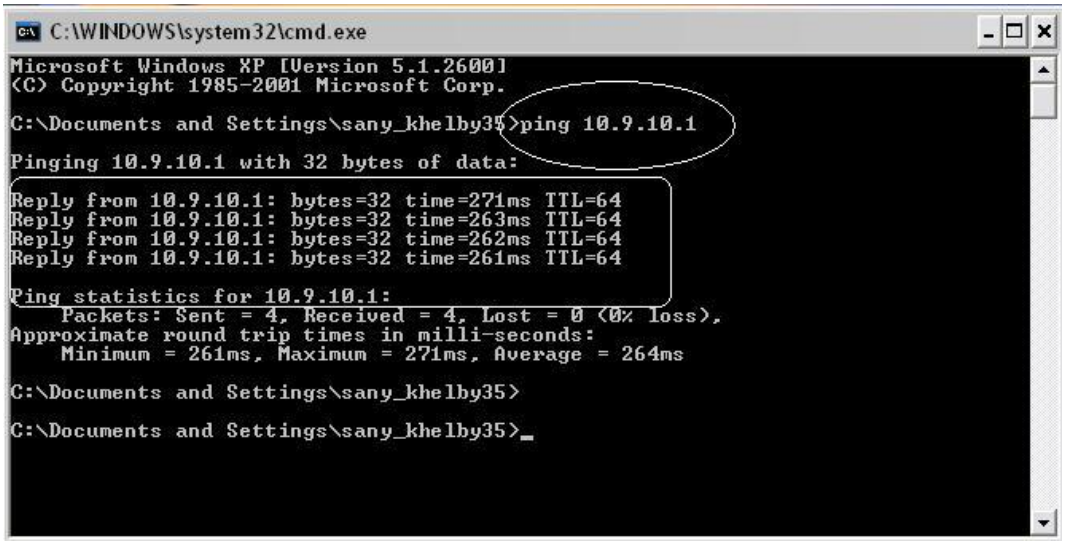
Gambar 4.21 Tampilan pada Command terdapat dua IP Address

Maka terdapat dua no ip address di computer *client* yaitu *Ethernet adapter Lan* dan dan ip dari *wireless*

Maka Vpn telah terkoneksi dengan baik.

4.4 Pengujian Ping

Pengujian Ping pengujian ping dilakukan agar dapat diketahui apakah computer Client dan Server terhubung dengan baik,pengujian ping dapat di lihat dibawah ini



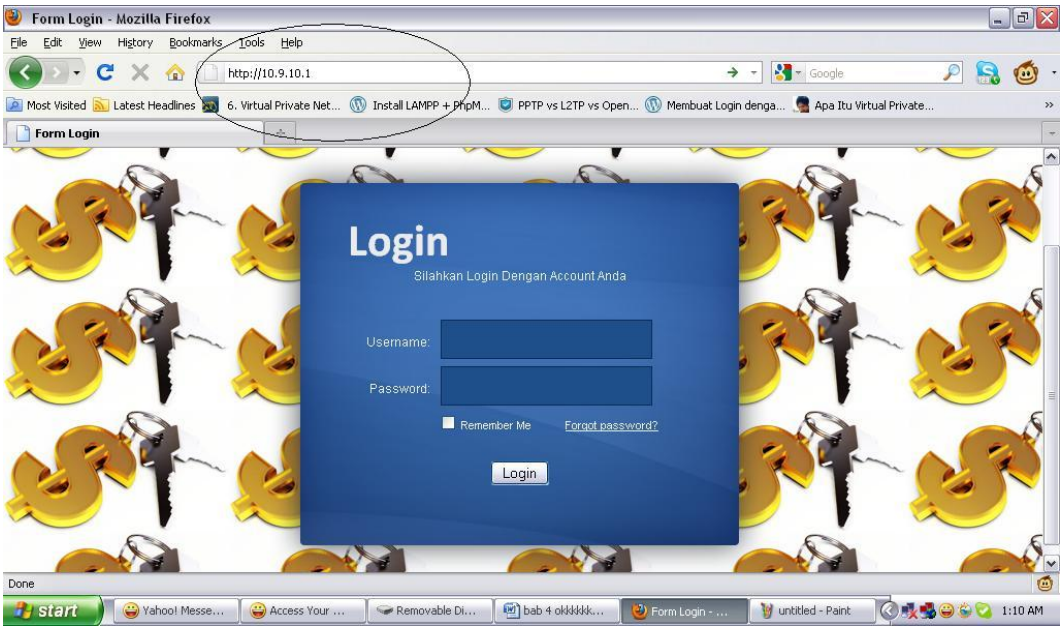
Gambar 4.22 Tampilan ketika test ping

Dapat dilihat pada gambar ping yang dilakukan berhasil atau dapat Replay dari *server* berarti koneksi VPN *Client* dan *Server* terkoneksi dengan baik.

4.5 Pengujuan akses webserver dan webmain yang berada di vpn

Pengujian ini dilakukan untuk mengetahui apakah webserver di vpn dan webmain telah berjalan dengan baik.

A.Akses halaman webserver (website gaji karyawan)

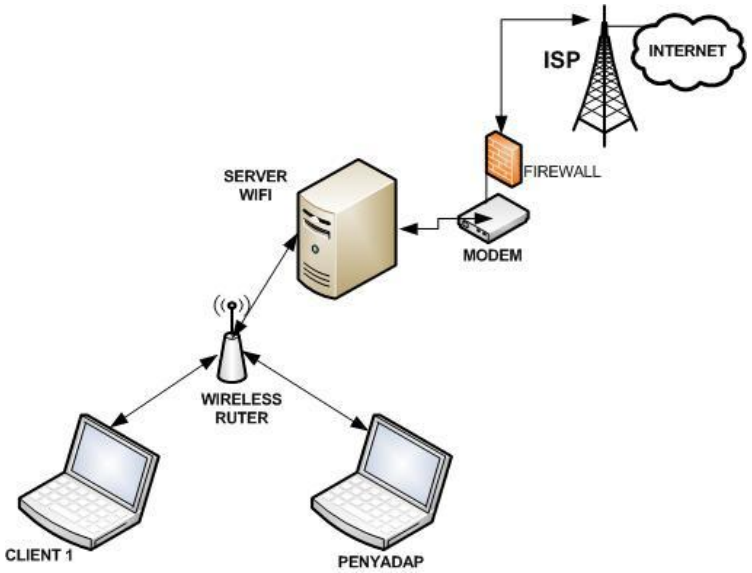


Gambar 4.23 Tampilan Webserver Penggajian di Dalam server VPS

4.6 Pengujian keamanan sebelum dan setelah menggunakan vpn

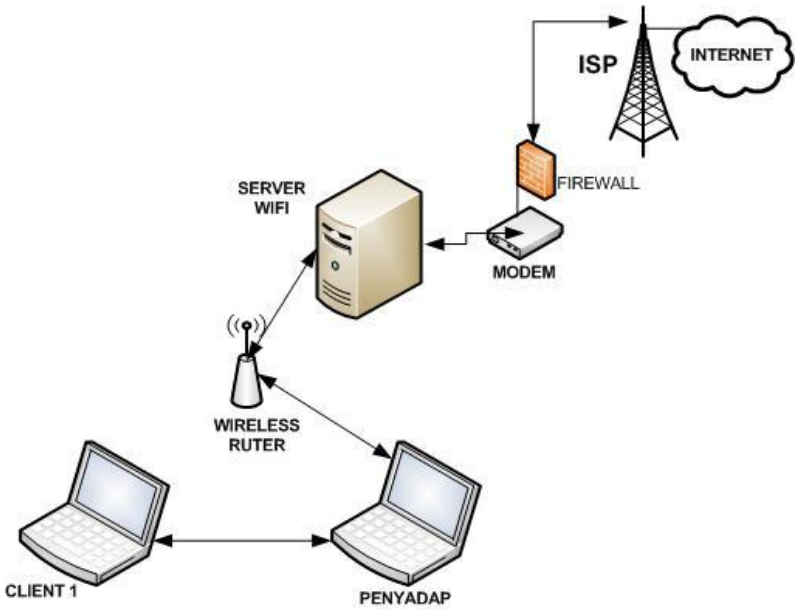
Pada bagian ini akan dibahas beberapa skenario keamanan paket data yang dilakukan di jaringan wifi free seperti di mall atau caffee.

A.Gambaran keadaan wifi Normal dapat dilihat dibawah ini



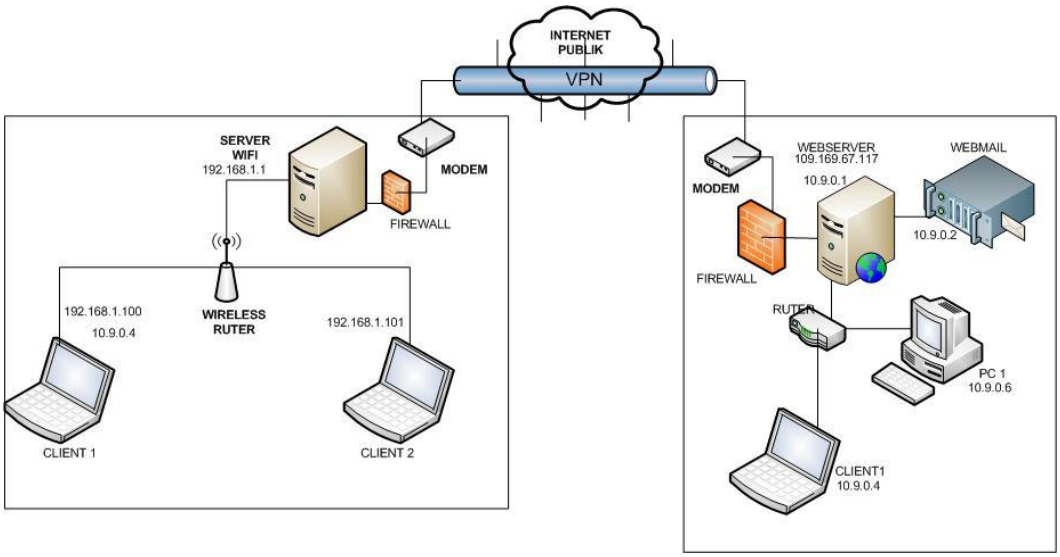
Gambar 4.24 Aliran Paket Data normal pada Jaringan Wifi

B.Gambaran ketika wifi dilakukan penyadapan dapat dilihat dibawah ini



Gambar 4.25 Aliran Paket Data Tidak normal Akan Melalui Penyadap

C . Koneksi VPN dengan menggunakan Virtual Private Server



Gambar 4. 26 Proses Koneksi Jaringan VPN Dengan VPS

4.7 Persiapan penyadapan di jaringan

A. Dilakukan penyadapan di *windows xp* dengan *cain & Abel* tanpa vpn

A. Client

1. *firewall* diaktifkan

B. Penyadap

1.menggunakan *scanner NetScan*

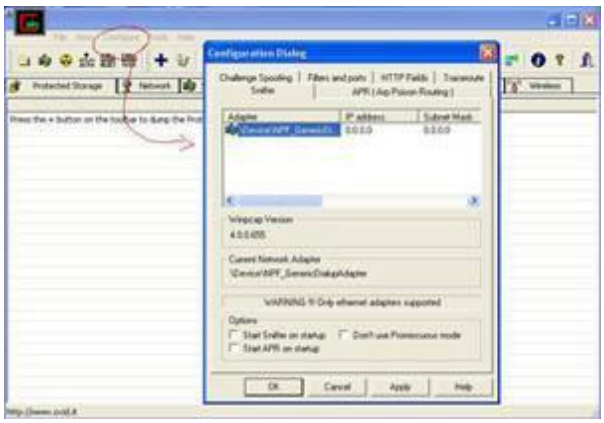
2.*cain & Abel*

1.Untuk memulai melakukan *sniffing* sangat mudah. Pilih tab ***"Sniffer"*** kemudian klik icon *Start/Stop Sniffer* (nomor dua dari kiri pada bagian atas).liat gambar dibawah ini



Gambar 4.27 Tampilan Menu Pilih kartu jaringan *Cain Abel*

2.Jika menggunakan kartu jaringan lebih dari satu, jangan lupa dikonfigurasikan Cain tersebut lebih dulu untuk menggunakan kartu yang mana. Cukup dengan klik *Configure*, kemudian pada tab *Sniffer*, pilih kartu yang anda gunakan kemudian klik OK.liat gambar dibawah ini



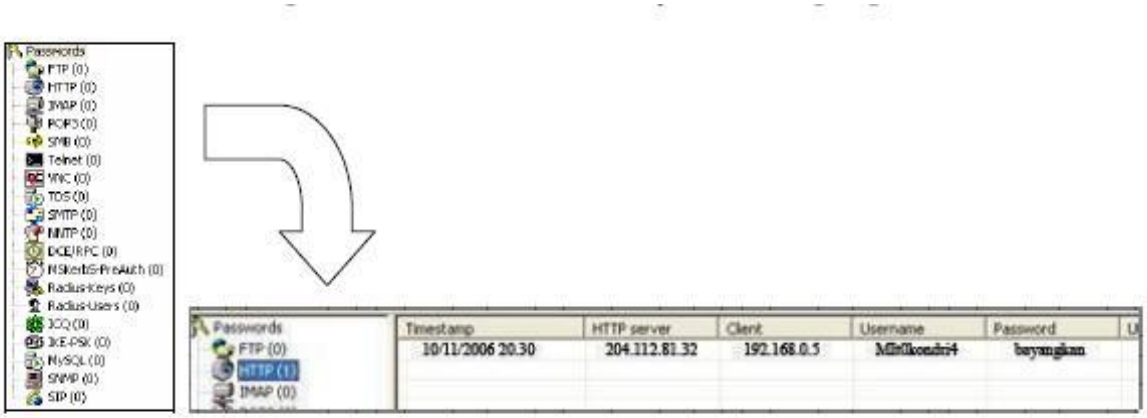
Gambar 4.28 Tampilan *Eternet Card* pada *Cain abel*

3. Jika proses *sniffing* sudah berjalan, bisa melihat hasilnya dengan mengklik pada *sub-tab Password* liat gambah dibawah ini



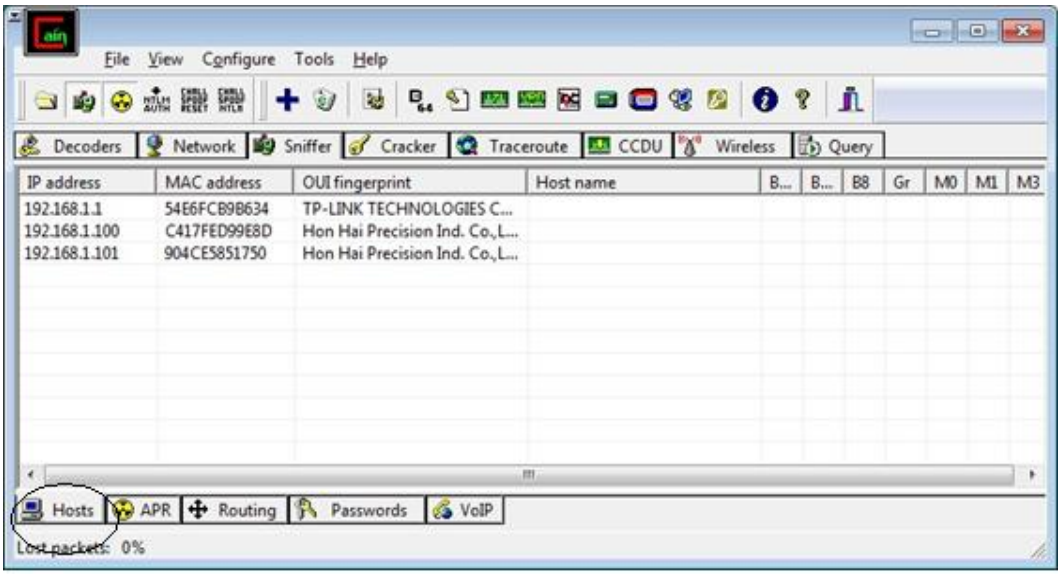
Gambar 4.29 Tampilan Tab *password Cain abel*

4. Kemudian memilih *password* dari aplikasi apa yang ingin di lihat melalui list box pada bagian kiri dan semua daftar *password* beserta *username* akan tampak pada kolom di sebelah kanan,lihat gambar dibawah ini



Gambar 4.30 Tampilan Menu *Capture http*

5.Untuk menyadap komputer dengan ip yang berbeda bisa pilih tab host seperti contoh dibawah ini



Gambar 4.31 Tampilan info IP address ketika di scan

4.7.1Penyadapan tanpa vpn di jaringan Tanpa wep dan wpa

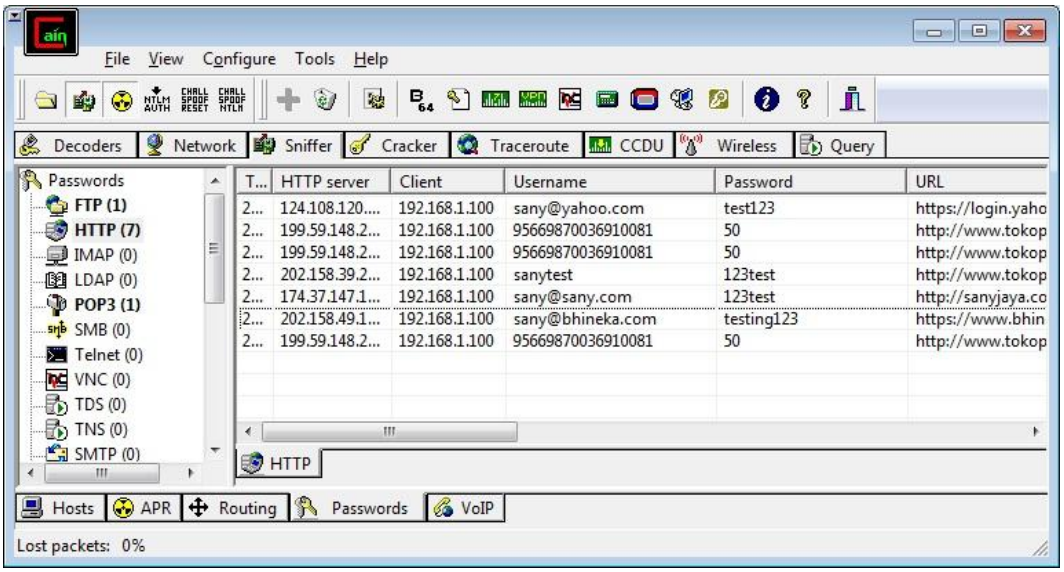
Disini pengujian dilakukan di wifi yang tanpa menggunakan wep,wpa ketika Client melakukan browsing ke

A. www.bhinneka.com

B. www.sanyjaya/saku/sany.com

C. www.yahoo.com

dan di penyadap dipasang *sniffer* cain abel maka hasil nya adalah



Gambar 4.32 Tampilan Cain abel saat penyadapan tanpa wep dan wpa

2.Pengujian dilakukan di wifi dengan WEP

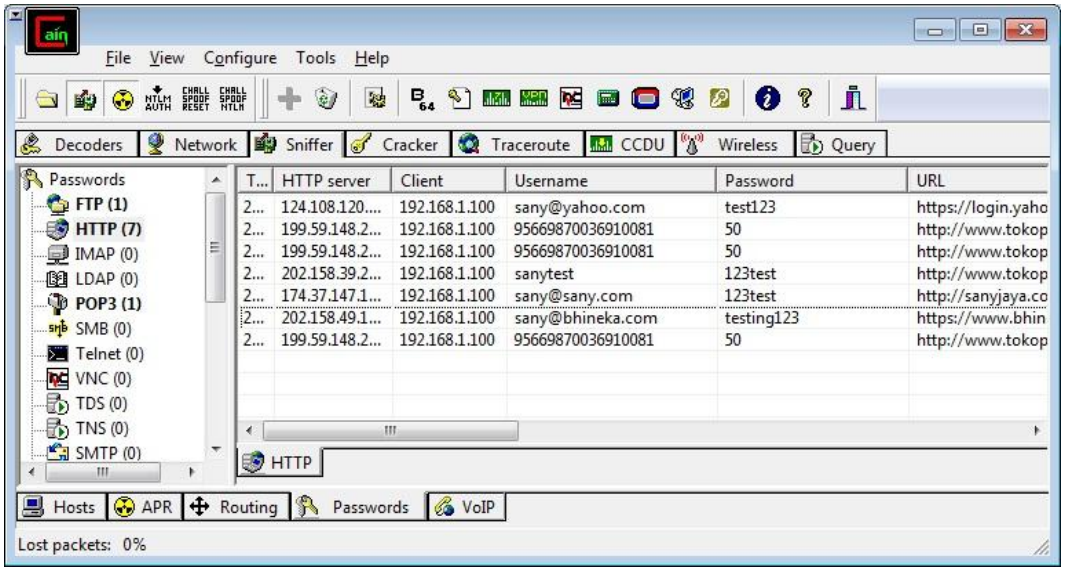
Di client melakukan browsing ke

A. www.bhinneka.com

B. www.sanyjaya/saku/sany.com

C. www.yahoo.com

hasil nya adalah



Gambar 4.33 Tampilan *cain abel* saat penyadapan dengan wep

Dapat di lihat pada gambar *Username* dan *password* dapat tersadap

3. Pengujian dilakukan di *wifi* dengan WPA

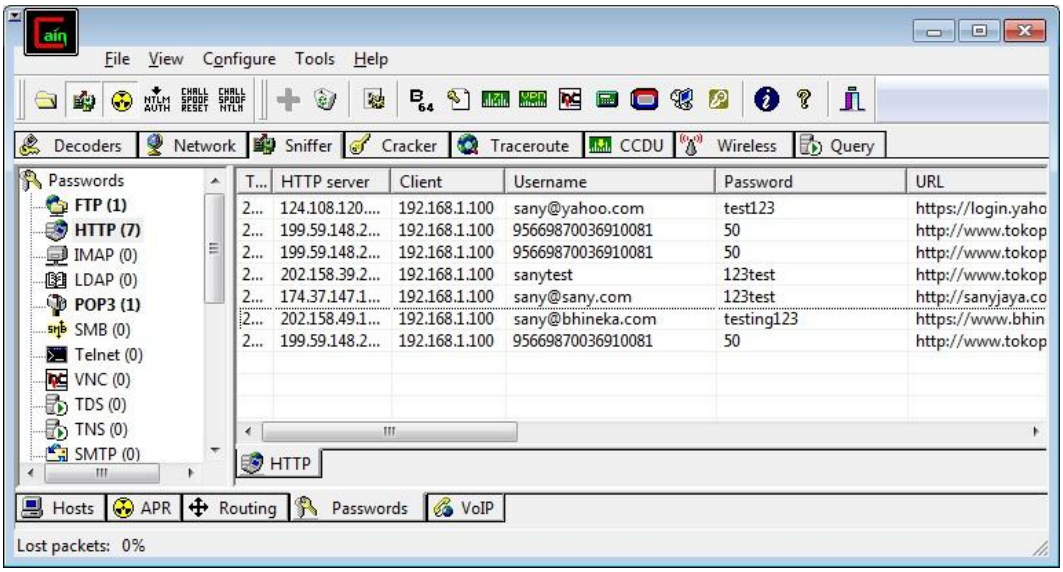
Di client melakukan browsing ke

A. www.bhinneka.com

B. www.sanyjaya/saku/sany.com

C. www.yahoo.com

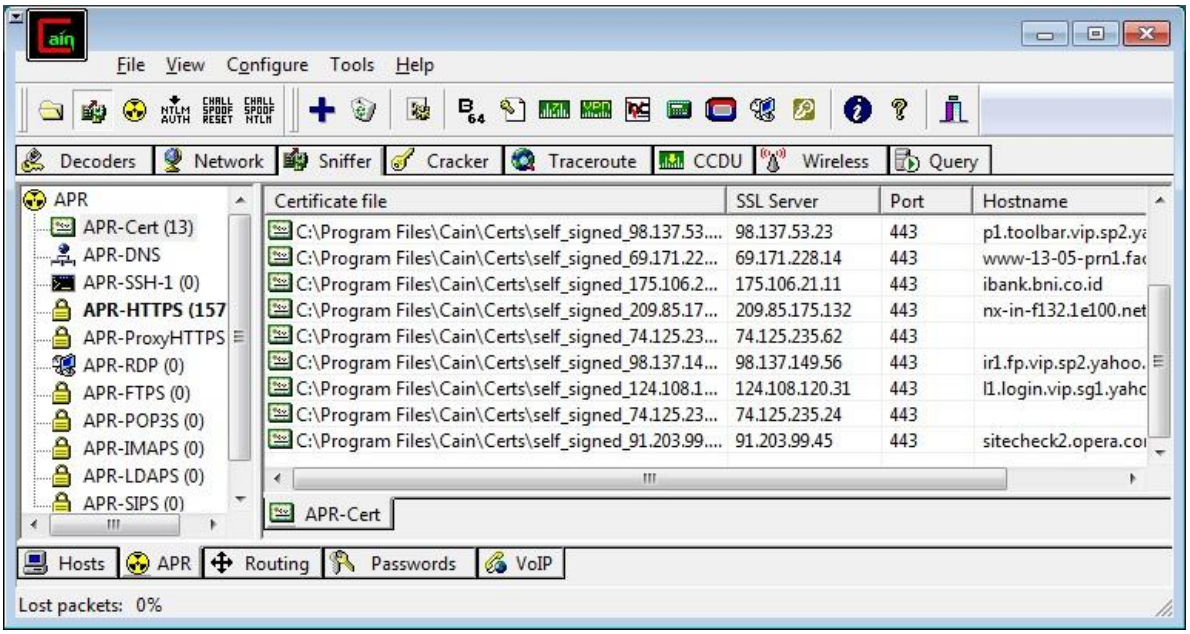
hasil nya adalah



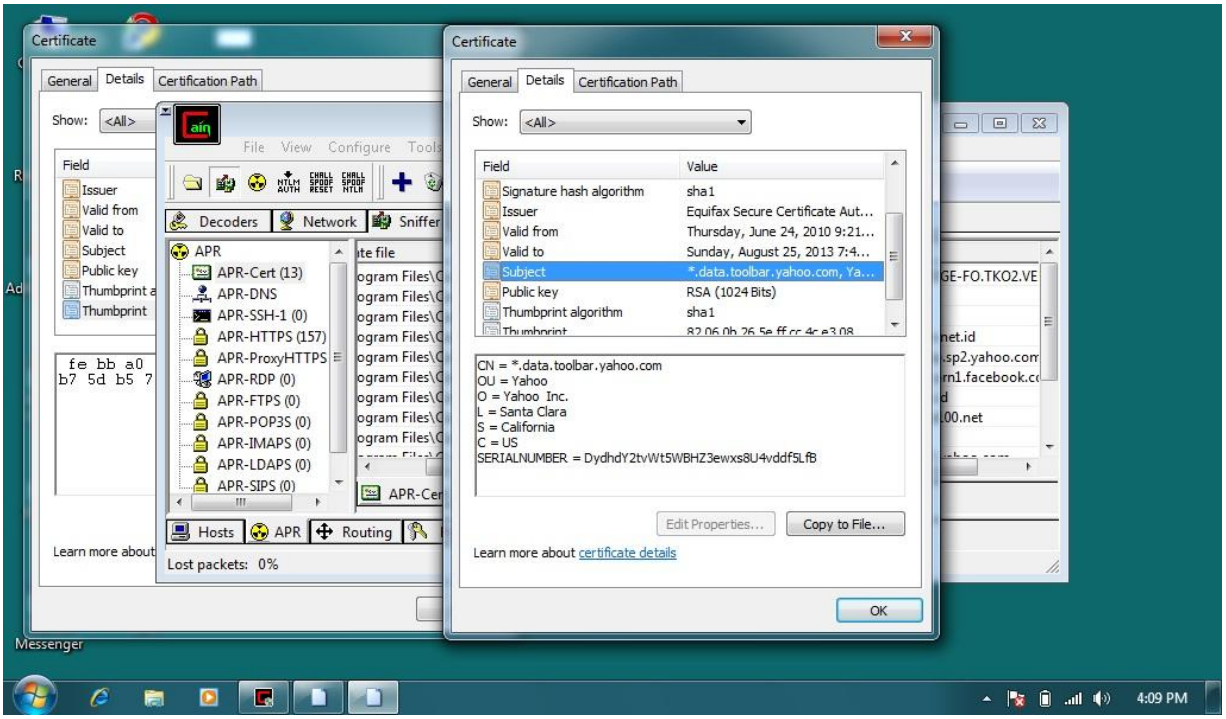
Gambar 4.34 Tampilan cain abel saat penyadapan dengan WPA

A. Pembuatan sertifikat palsu dengan *software cain abel*

Pada bagian ini *software cain abel* membuat Sertifikat palsu agar bisa masuk ke halaman SSL seperti pada gambar dibawah



Gambar 4.35 Tampilan sertifikat SSL palsu



Gambar 4.36 Tampilan info SSL yang tersadap

4.7.2.Penyadapan ketika menggunakan VPN tanpa WEP dan WPA

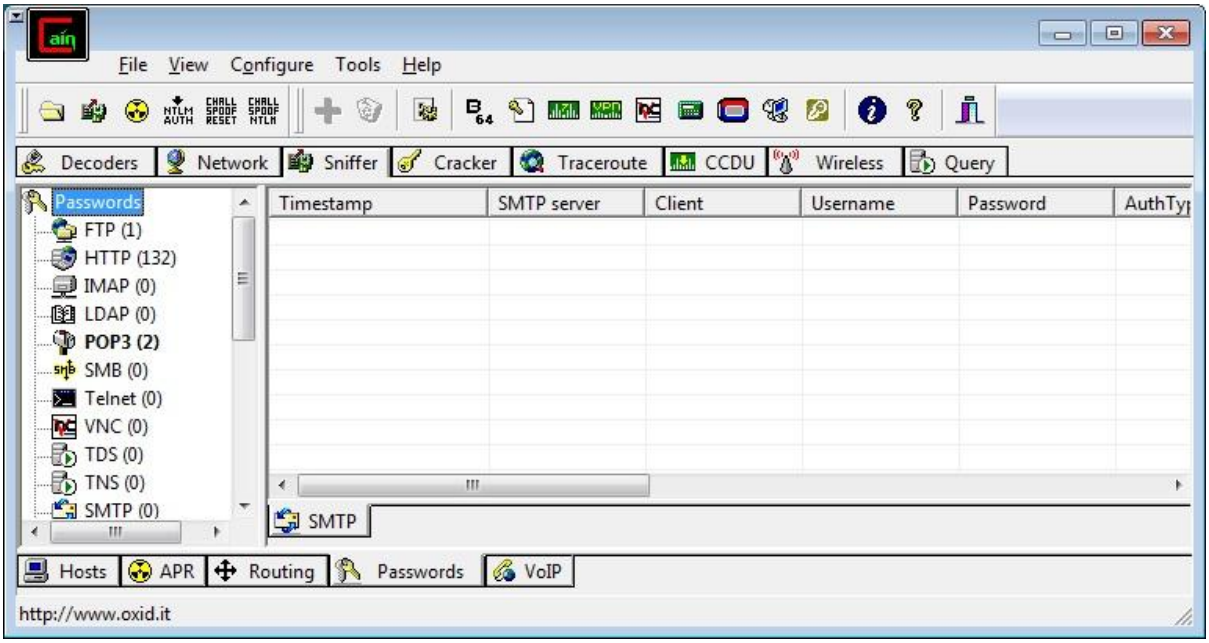
Ketika melakukan browsing ke

A. www.bhinneka.com

B. www.sanyjaya/saku/sany.com

C. www.yahoo.com

Tidak ada paket data yang tertangkap liat gambar



Gambar 4.37 Tampilan penyadapan menggunakan vpn tanpa wep dan wpa

A.Penyadapan ketika menggunakan VPN dan menggunakan WEP

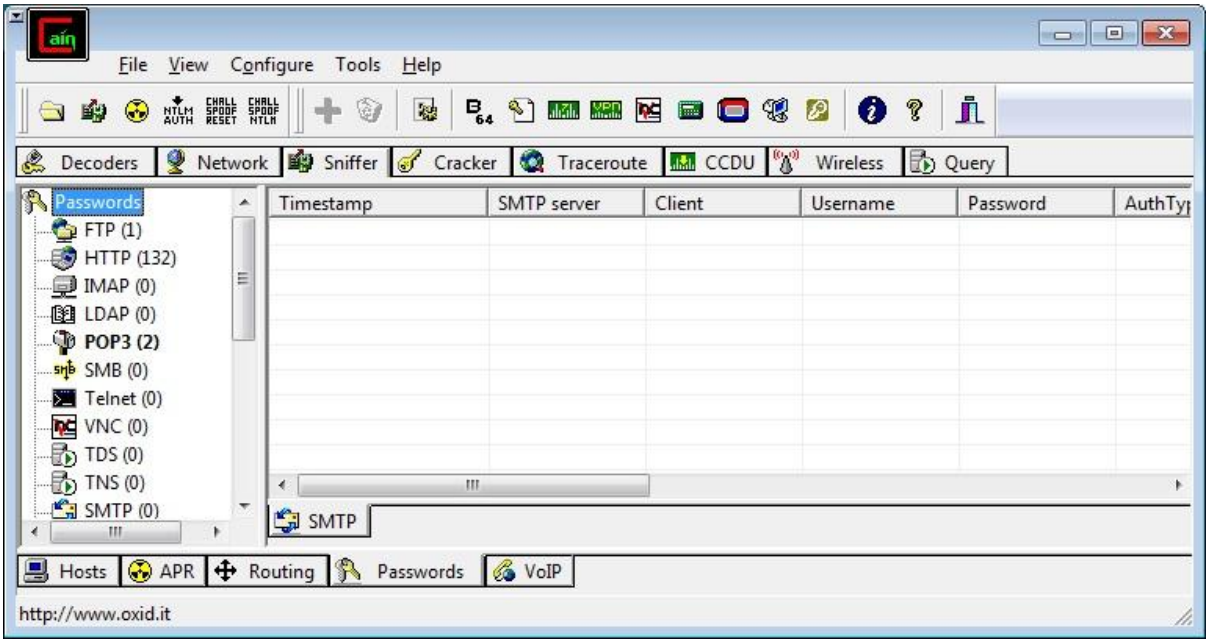
Ketika melakukan browsing ke

A. www.bhinneka.com

B. www.sanyjaya/saku/sany.com

C. www.yahoo.com

tidak ada paket data yang tertangkap liat gambar



Gambar 4.38 Tampilan penyadapan saat menggunakan vpn dengan wep

B.Penyadapan ketika menggunakan VPN dan menggunakan WPA

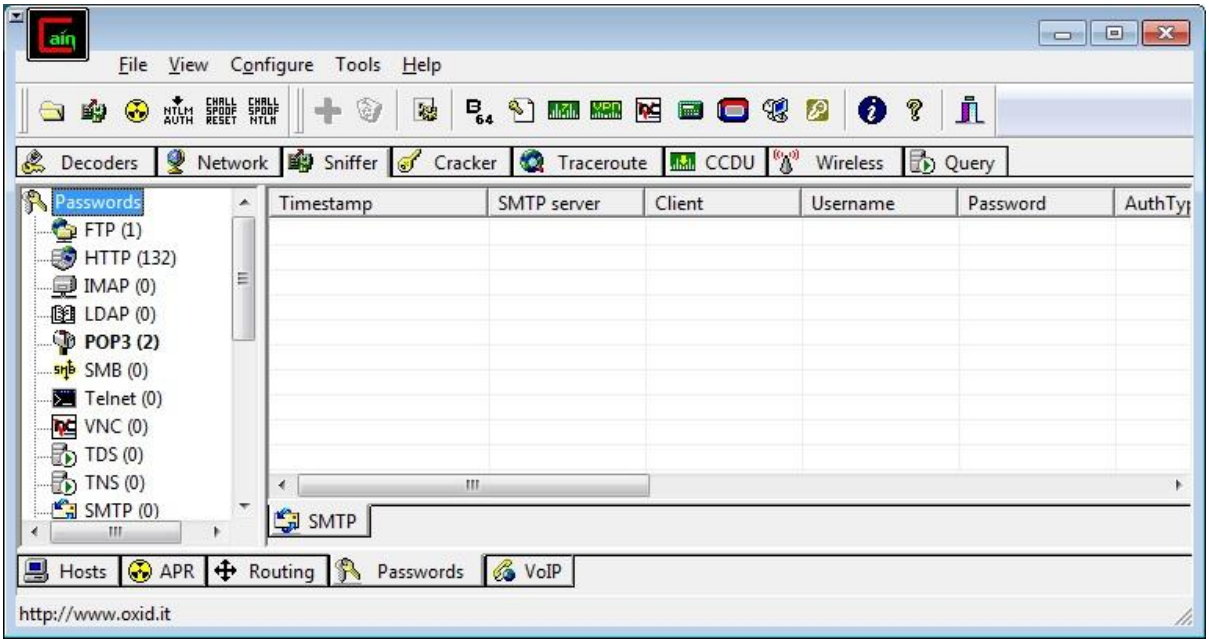
Ketika melakukan browsing ke

A. www.bhinneka.com

B. www.sanyjaya/saku/sany.com

C. www.yahoo.com

tidak ada paket data yang tertangkap liat gambar



Gambar 4.39 Tampilan penyadapan menggunakan vpn tanpa dengan wpa

Pada Gambar dapat diperoleh hasil bahwa dengan menggunakan *remote access* VPN *dengan private virtual server* terbukti data yang ditransfer akan lebih dahulu dilakukan enkripsi, sehingga informasi tentang username, password yang dimiliki oleh *client* tidak dapat diketahui, serta data yang direquest oleh *client* tidak dapat diketahui, sehingga proses transfer data melaui *remote access virtual private network* dengan Virtual Private Server menjadi lebih aman