

# IMPLEMENTASI RANCANGAN KEAMANAN JARINGAN WIRELESS DENGAN METODE SECURE SOCKET LAYER (SSL) PADA BAPPEDA KABUPATEN BANYUASIN

Reza Aditya  
M. Ukhwarizman

**Jurusan Sistem Informasi**  
**STMIK PalComTech Palembang**

## Abstrak

Dalam merancang dan mengimplementasikan keamanan jaringan *wireless internet hotspot* berbasis mikrotik diperlukan perhatian khusus pada aspek-aspek pemilihan desain jaringan, perangkat keras jaringan, koneksi, media transmisi serta metode pengamanannya. Karena aspek-aspek tersebut sangat berpengaruh terhadap kinerja jaringan secara keseluruhan. Manfaat yang diharapkan dapat membantu kemudahan mengakses *internet* bagi staf dan karyawan dalam memperoleh informasi internet di Bappeda Kabupaten Banyuasin dengan menggunakan perangkat *laptop, handphone, perangkat mobile* lainnya menggunakan fasilitas *wifi* atau *hotspot internet* serta merancang dan mengimplementasikan sistem keamanan *wireless internet hotspot* di lingkungan Bappeda Kabupaten Banyuasin dengan menggunakan metode pengamanan *security Secure Socket Layer (SSL)*.

**Kata Kunci:** *mikrotik, wifi, hotspot, Secure Socket Layer (SSL)*

## PENDAHULUAN

Dunia Teknologi Informasi dan Komunikasi tidak bisa dipisahkan dengan kabel. Perkembangan dunia jaringan komputer sangat cepat, semua komputer diharapkan dapat berkomunikasi satu dengan yang lain dengan medium tertentu. Pada jaringan *Local Area Network* yang kita sebut dengan LAN masih menggunakan kabel sebagai media penghubung agar beberapa komputer dapat saling berkomunikasi. Namun, seiring dengan kemajuan waktu dan teknologi, juga kebutuhan manusia akan mobilitas (mudah berpindah-pindah) dan fleksibilitas yang tinggi menuntut sesuatu yang lebih praktis. Dan teknologi *wireless* memberikan jawaban untuk kebutuhan tersebut. Teknologi *wireless* menawarkan beragam kemudahan, kebebasan dan fleksibilitas yang tinggi. Teknologi *wireless* memiliki cukup banyak kelebihan dibandingkan teknologi kabel yang sudah ada. Teknologi *wireless* sangat nyaman untuk digunakan. Anda bisa mengakses internet di posisi manapun selama masih berada dalam jangkauan *wireless*.

Bappeda Kabupaten Banyuasin terletak di Jalan Lingkaran No.5 Sekojo Telp.0711-7690007 Pangkalan Balai. Badan Perencanaan Pembangunan Daerah dan Penanaman Modal (BAPPEDA-PM) merupakan unsur Pelaksana Tugas tertentu Pemerintahan Daerah dibidang Perencanaan Pembangunan Daerah dan Penanaman Modal BAPPEDA-PM. Bappeda Banyuasin memiliki satu tugas penting yaitu tata ruang perencanaan pembangunan yang mengetahui salah satu titik koordinat pembangunan dan pengukuran suatu wilayah menggunakan GPS (*Global Positioning System*) yang mengambil koordinat langsung ke satelit citra nasional.

Setiap data file informasi atau perencanaan yang dikumpulkan melalui satelit citra nasional untuk perencanaan yang vital, di Bappeda Banyuasin disimpan ke server Bappeda Provinsi Sumatera Selatan melalui internet, biasanya mudah ditembus oleh orang yang tidak bertanggung jawab (*hacker*) untuk kepentingan pribadi atau kelompok yang tidak ingin Kabupaten Banyuasin maju mandiri dan berdaya saing sesuai dengan visi misi Kabupaten Banyuasin. Sistem keamanan fasilitas internet *hotspot* Bappeda Banyuasin memakai sistem

koneksi keamanan. yang terdapat pada *access point* yaitu menggunakan metode *WEP / WPA*. Contoh peristiwa perencanaan pembangunan suatu pabrik tekstil dan karet di kecamatan Maryana Banyuasin 1 yang bertujuan untuk menunjang kemajuan ekonomi di Sumatera Selatan, file perencanaan itu pernah hilang dari data *server* Bappeda Banyuasin sebelum dikirim ke *server* Bappeda Provinsi Sumatera Selatan dan file perencanaan itu menyebar luas kemasyarakat melalui selebaran pembangunan pabrik tekstil di Kecamatan Maryana Banyuasin 1. Seharusnya informasi tersebut tidak boleh diketahui masyarakat sebelum perencanaan tersebut di khawatirkan adanya reaksi penolakan masyarakat sekitar daerah pembangunan. Kejadian seperti ini diharapkan tidak terulang lagi sehingga sistem yang ada ditingkatkan dengan mengganti metode *WEP/WPA* menggunakan metode *SSL*.

Keamanan *wireless hotspot* dengan metode *SSL* dibangun dan dirancang di kantor Bappeda untuk memperkuat sistem keamanan *wireless internet*, hal ini dikarenakan selama ini Bappeda Kabupaten Banyuasin belum memiliki *server gateway* dan sistem keamanan fasilitas internet *hotspot* yang baik dimana metode *WEP / WPA* masih bisa ditembus oleh *software hacking* / penyusup seperti *software backtrack*. Merancang *server gateway* yang berfungsi sebagai *router internet* baik pada jaringan kabel maupun *wireless* merupakan solusi dimana dapat membantu komunikasi antar komputer serta sistem keamanan *internet hotspot* berbasis mikrotik dimana *user* akan melakukan proses *login* terlebih dahulu dengan memasukkan nama *user* dan *password* saat akan mengakses internet dengan menggunakan metode keamanan *Secure Socket Layer (SSL)*.

## LANDASAN TEORI

### Perancangan

Desain atau perancangan adalah penggambaran, perencanaan dan pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah ke dalam satu kesatuan yang utuh dan berfungsi. Proses desain pada umumnya memperhitungkan aspek fungsi dan estetik yang biasanya data didapatkan dari riset, pemikiran, maupun dari desain yang sudah ada sebelumnya. ( John G Burch, 2010).

### MikroTik Router

Menurut Herlambang (2008:20) *Mikrotik* adalah sistem operasi independen berbasis *Linux* khusus untuk komputer yang difungsikan sebagai *Router*, *Mikrotik* didesain untuk memberikan kemudahan bagi penggunaanya. Adminstrasinya bisa dilakukan melalui *Windows application (WinBox)*. Selain itu instalasi dapat dilakukan pada Standard computer PC. PC yang akan dijadikan *router mikrotik* pun tidak memerlukan *resource* yang cukup besar untuk penggunaan standard, misalnya hanya sebagai *gateway*. Untuk keperluan beban yang besar ( *network* yang kompleks, *routing* yang rumit dll) disarankan untuk mempertimbangkan pemilihan *resource* PC yang memadai.

### Network Address Translation ( NAT)

Menurut Herlambang (2008:76), *Network Address Translation* atau yang biasa disebut dengan *NAT* adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat *IP*. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat *IP* yang terbatas, kebutuhan akan keamanan (*security*), dan kemudahan serta *fleksibilitas* dalam administrasi jaringan.

### DHCP Server

Menurut Towidjojo (2013:83), *Dynamic Host Configuration Protocol* adalah protokol jaringan yang memungkinkan sebuah perangkat jaringan membagi konfigurasi *IP Address* kepada komputer-komputer user yang membutuhkan. Konfigurasi *IP Address* ini meliputi

IP Address itu sendiri, *subnetmask*, *default gateway* dan DNS Server yang dibutuhkan untuk mengakses internet.

*MySQL*

### **Hotspot Gateway dan User Manager**

Menurut Towidjojo (2013:136), Router mikrotik memiliki fitur-fitur yang lengkap. Salah satu fitur nya adalah Hotspot Gateway. Dengan menggunakan fitur *hotspot gateway* ini, kita akan mendapatkan fasilitas tambahan. Kita dapat mengkonfigurasi jaringan *wireless* yang hanya bisa digunakan dengan *username* dan *password* tertentu serta dapat melakukan manajemen *user-user* tersebut.

### **Tool Wireshark**

Menurut Kurniawan (2012:15), *Wireshark* merupakan *tool* yang ditujukan untuk menganalisis paket data jaringan. *Wireshark* melakukan pengawasan paket secara waktu nyata (*real time*) dan kemudian menangkap data dan menampilkan selengkap mungkin. *Wireshark* bisa digunakan secara gratis karena aplikasi ini berbasis sumber terbuka. Aplikasi *wireshark* dapat berjalan di banyak platform seperti Linux, Windows dan Mac.

## **HASIL DAN PEMBAHASAN**

### **Analisis Kebutuhan**

1. Teknologi *wireless* menawarkan beragam kemudahan, kebebasan dan fleksibilitas yang tinggi. Teknologi *wireless* memiliki cukup banyak kelebihan dibandingkan teknologi kabel yang sudah ada. Teknologi *wireless* sangat nyaman untuk digunakan. Anda bisa mengakses internet di posisi manapun selama masih berada dalam jangkauan *wireless*.
2. Dari hasil pengamatan yang dilakukan penulis di Bappeda Kabupaten Banyuasin belum memiliki sistem keamanan internet hotspot yang baik. Merancang *server gateway* yang berfungsi sebagai *router internet* pada jaringan *wireless* merupakan solusi dimana dapat membantu komunikasi antar komputer serta merancang sistem keamanan *internet hotspot* berbasis mikrotik dimana *user* akan melakukan proses *login* terlebih dahulu dengan memasukkan nama *user* dan *password* saat akan mengakses internet dengan menggunakan metode keamanan SSL (*Secure Socket Layer*).

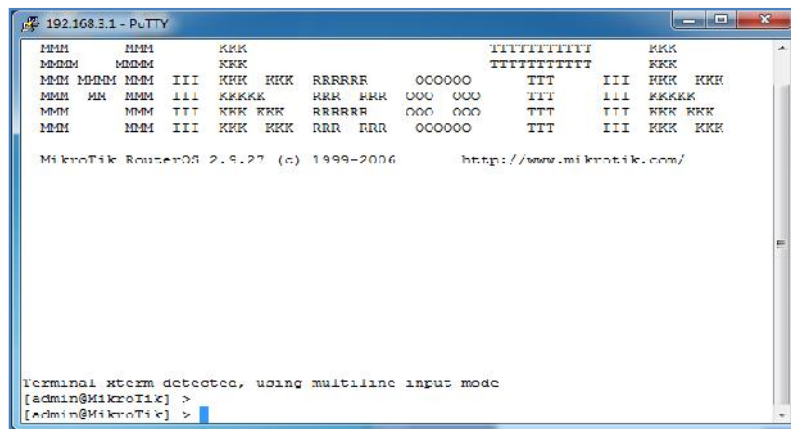
### **Analisis Permasalahan**

Keamanan *wireless hotspot* dengan metode SSL dibangun dan dirancang di kantor Bappeda untuk memperkuat sistem keamanan *wireless internet*, hal ini dikarenakan selama ini Bappeda Kabupaten Banyuasin belum memiliki *server gateway* dan sistem keamanan fasilitas internet *hotspot* yang baik dimana sistem koneksi keamanan internet *hotspot* masih menggunakan fasilitas keamanan yang terdapat pada *access point* yaitu menggunakan metode WEP / WPA yang bisa ditembus oleh *software hacking* / penyusup. merancang *server gateway* yang berfungsi sebagai *router internet* baik pada jaringan kabel maupun *wireless* merupakan solusi dimana dapat membantu komunikasi antar komputer serta sistem keamanan *internet hotspot* berbasis mikrotik dimana *user* akan melakukan proses *login* terlebih dahulu dengan memasukkan nama *user* dan *password* saat akan mengakses internet dengan menggunakan metode keamanan *Secure Socket Layer (SSL)*.

### **Implementasi**

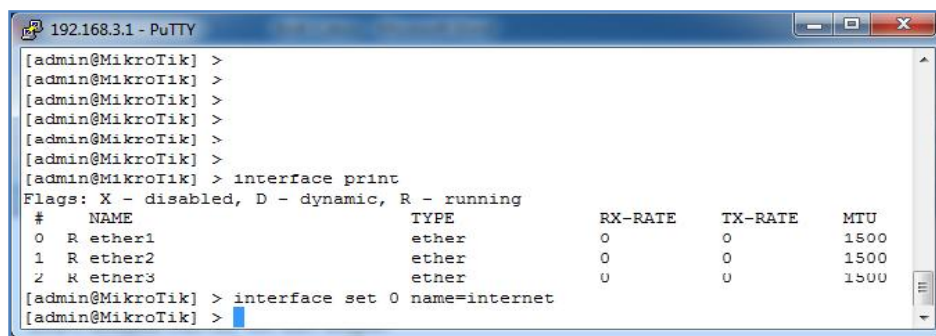
Keamanan *wireless internet hotspot* yang di rancang lingkungan kantor Bappeda Kabupaten Banyuasin menggunakan sistem operasi *Mikrotik Router Versi 2.9.27* . Berikut Langkah-langkah perancangan dan implementasi dari jaringan LAN dan keamanan *Wireless*

*Internet Hotspot*. Sistem Operasi mikrotik terlebih dahulu diinstall pada harddisk dengan mengubah urutan booting di Bios, *First Boot: cdrom*, kemudian masukan cd *master* mikrotik, ikuti petunjuk instalasi.

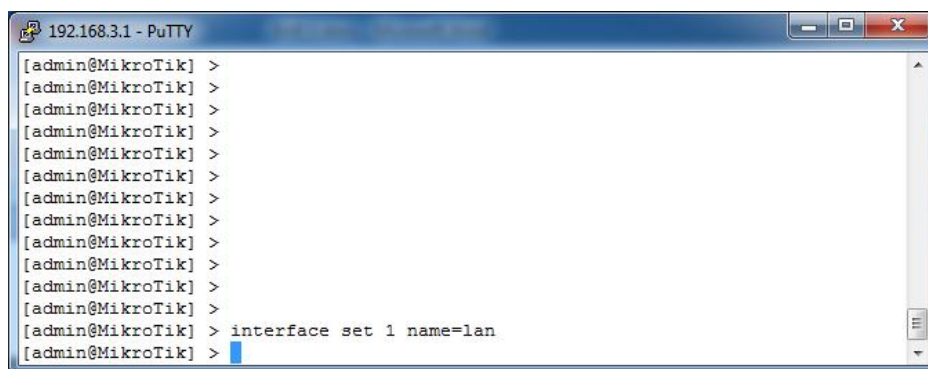


**Gambar 1.** Login awal Mikrotik

Langkah berikutnya mengubah nama masing-masing *interface ether1*, *ether2* dan *ether3* menjadi *internet*, *lan* dan *hotspot* seperti pada gambar 2, 3 dan 4.



**Gambar 2.** Setting nama pada *interface ether 1*

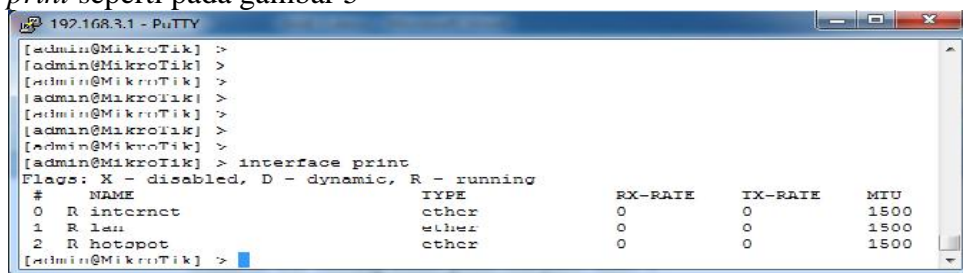


**Gambar 3.** Setting nama pada *interface ether 2*



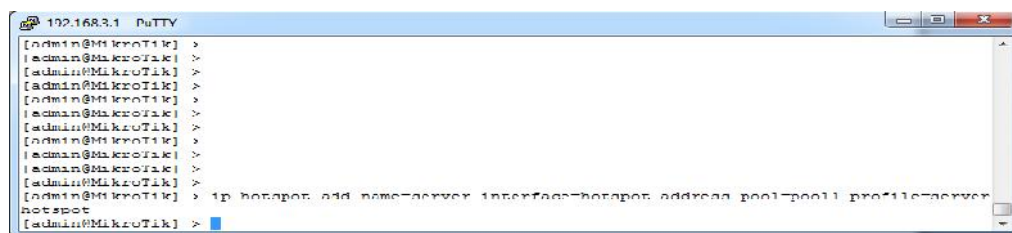
**Gambar 4.** Setting nama pada *interface ether 3*

Menampilkan nama *interface* yang sudah disetting, dengan cara menggunakan perintah *interface print* seperti pada gambar 5



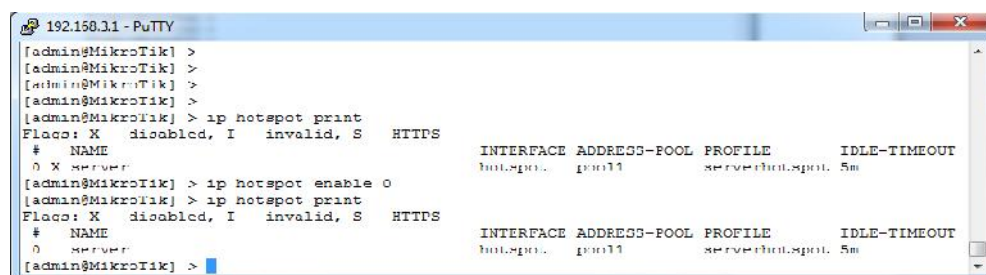
**Gambar 5.** Hasil *Interface Print*

Kemudian menghubungkan *interface hotspot* dengan *profile* yang sudah kita buat seperti pada gambar 6



**Gambar 6.** *Interface hotspot dengan profile*

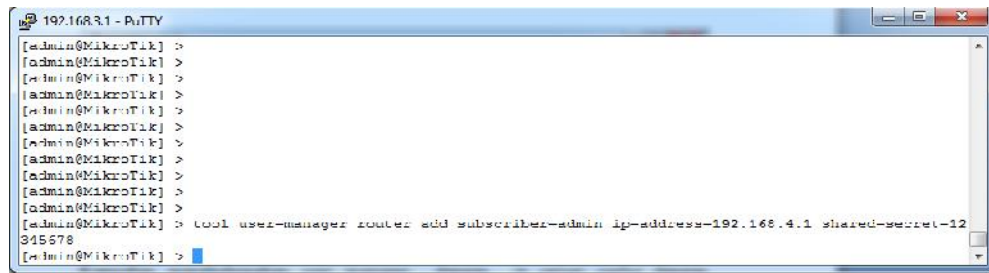
Langkah selanjutnya kita mengaktifkan *ip hotspot* dengan perintah *ip hotspot enable* kemudian menampilkan *ip hotspot* yang telah di *setting* seperti pada gambar 7.



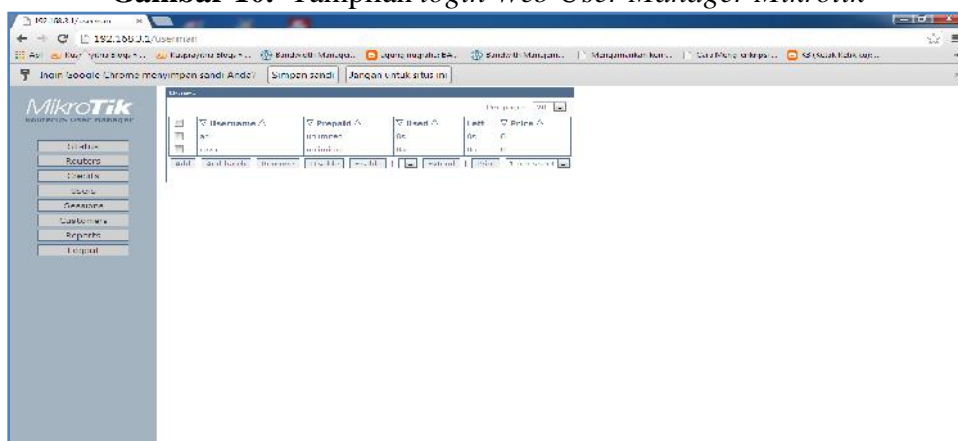
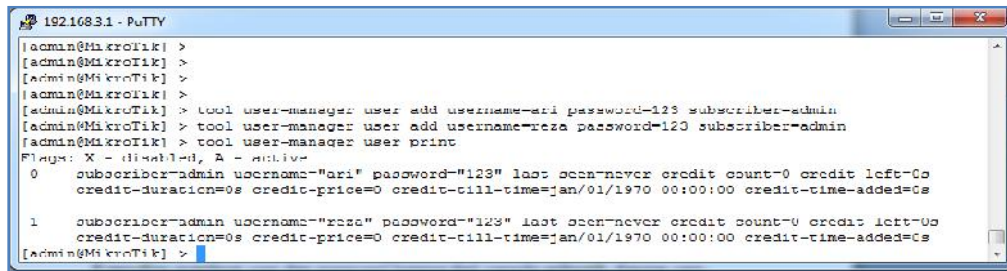
**Gambar 7.** Hasil tampilan *interface hotspot* dengan *profile*

Selanjutnya menggunakan fasilitas *user manager* dengan membuat *user admin* beserta password seperti pada gambar 8.

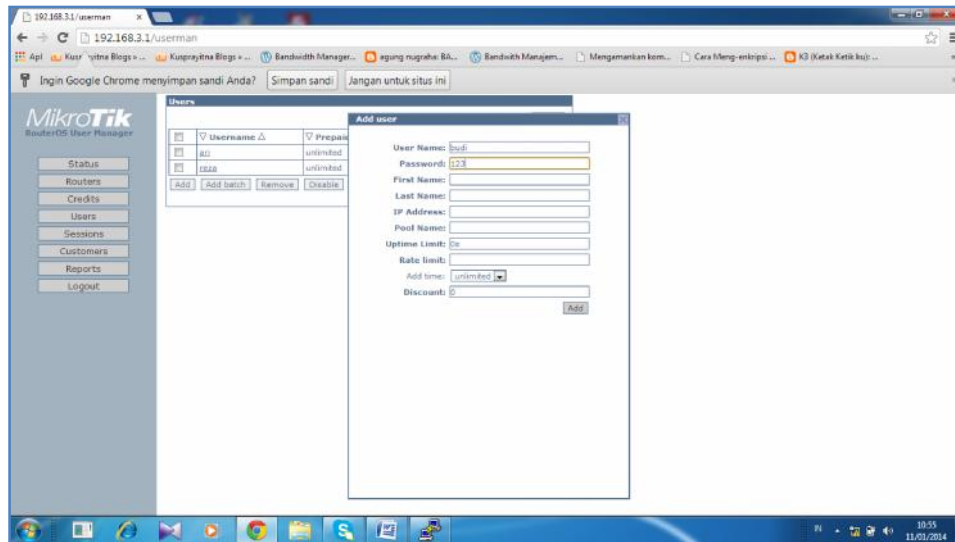
Membuat *user* dan *password* admin pada *userman* kemudian menghubungkan *user manager* dengan *ip server radius* dengan menggunakan keamanan *shared secret*, seperti pada gambar 8



Kemudian membuat *user* dan *password hotspot* dari console mikrotik seperti pada gambar 9.



Langkah selanjutnya membuat *user hotspot via web* dengan menggunakan fasilitas *web user manager* seperti pada gambar 11.



**Gambar 11.** Membuat user baru via user manager mikrotik

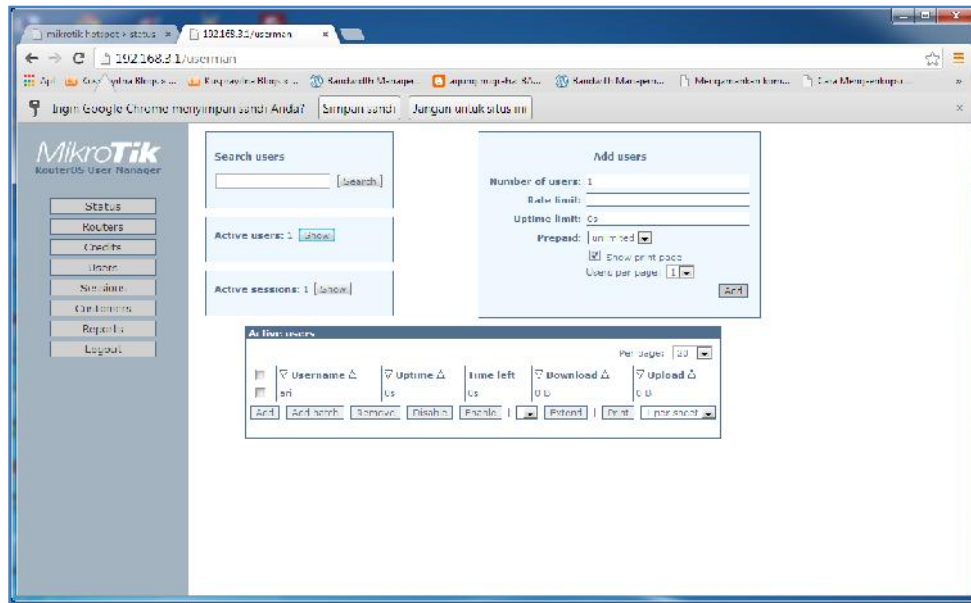
Gambar dibawah ini merupakan hasil penambahan user hotspot mikrotik seperti pada gambar 12



**Gambar 12.** Tampilan hasil penambahan user

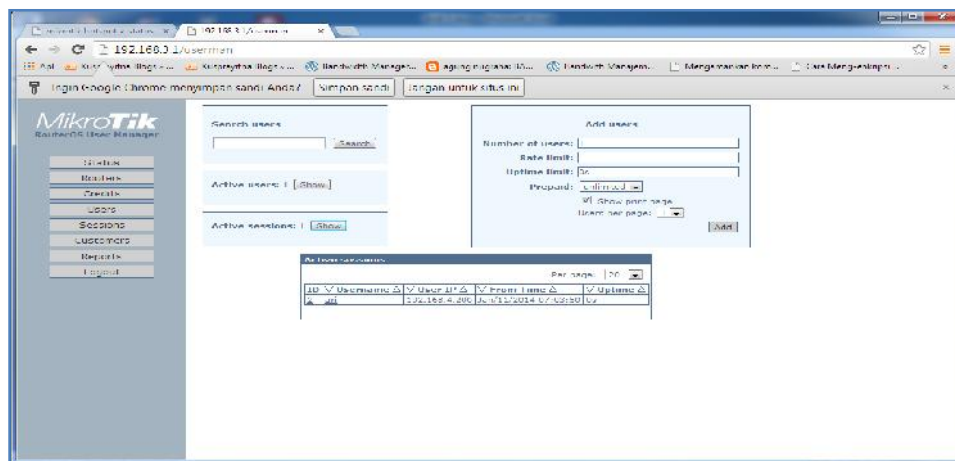
Langkah selanjutnya kita bisa mengamati user hotspot mikrotik yang sedang aktif atau online dengan mengklik tombol show pada bagian active user seperti pada gambar 13.





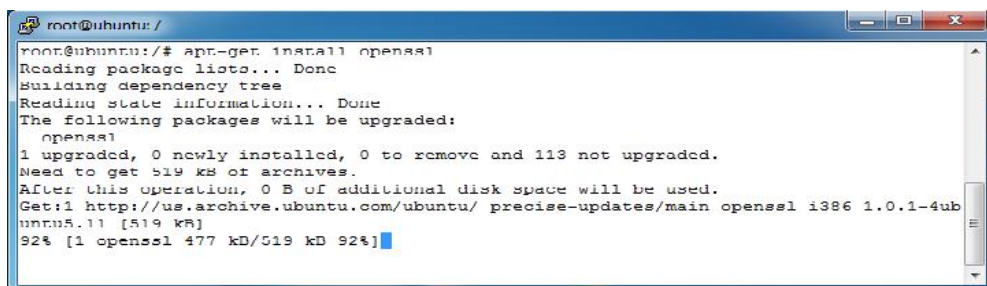
**Gambar 13.** Tampilan status *user* yang aktif

Kemudian pada bagian *active session*, bisa diamati *user hotspot* yang sedang login beserta *ip address* yang diperoleh oleh *client hotspot* dan lama waktu login atau durasi ke *server hotspot* seperti pada gambar 14.



**Gambar 14.** Tampilan *active session*

Langkah selanjutnya kita membuat file sertifikat dan file kunci di sistem operasi linux dengan menggunakan *software openssl*. Untuk dapat membuat sertifikat diperlukan aplikasi *openssl*, maka apabila di OS Linux belum ada diperlukan instalasi *openssl* dengan menggunakan perintah *apt-get install*, dan kemudian membuat kunci hotspot dengan nama *hotspot.key* seperti pada gambar 15 dan 16



**Gambar 15.** Instalasi *Openssl*



```

root@ubuntu: /
root@ubuntu: /# openssl genrsa -des3 -out hotspot.key 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
Enter pass phrase for hotspot.key:
Verifying - Enter pass phrase for hotspot.key:
root@ubuntu: /#

```

**Gambar 16.** Membuat file kunci

Langkah berikutnya membuat *request key* dengan nama file *hotspot.csr* seperti pada gambar 17

```

root@ubuntu: /
root@ubuntu: /# openssl req -new -key hotspot.key -out hotspot.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:id
State or Province Name (full name) [Some-State]:sumsel
Locality Name (eg, city) []:palembang
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Bappeda Banyuasin
Organizational Unit Name (eg, department) []:BDD Banyuasin
Common Name (e.g. server FQDN or YOUR name) []:192.168.4.1
Email Address []:admin@bappedabanyuasin.go.id

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:12345678
An optional company name []:
root@ubuntu: /#

```

**Gambar 17.** Membuat kunci *request*

Kemudian membuat sertifikat *hotspot* seperti pada gambar 18.

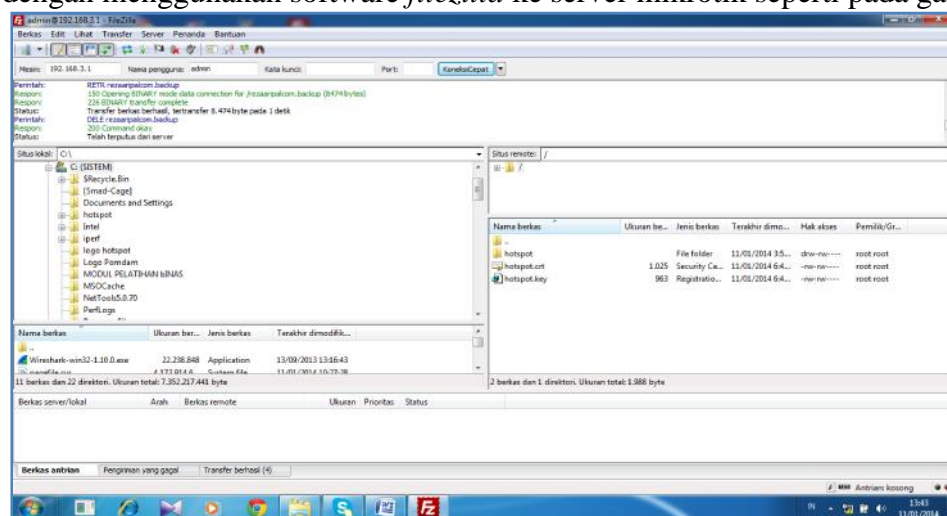
```

root@ubuntu: /
root@ubuntu: /# openssl x509 -req -days 10000 -in hotspot.csr -signkey hotspot.key -out
hotspot.crt
Signature ok
subject=/C=id/ST=sumsel/L=palembang/O=Bappeda Banyuasin/OU=192.168.4.1/CN=192.168.4.1/
emailAddress=admin@bappedabanyuasin.go.id
Getting Private key
Enter pass phrase for hotspot.key:
root@ubuntu: /#

```

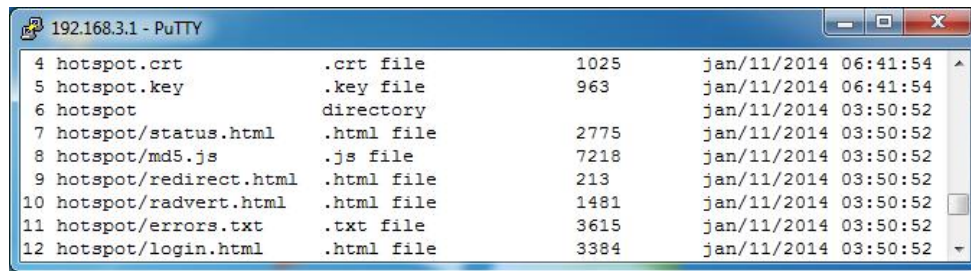
**Gambar 18.** Membuat file sertifikat dan file kunci

Langkah selanjut kita akan mengupload file sertifikat dan file kunci (*key*) yang telah kita buat dengan menggunakan software *filezilla* ke server mikrotik seperti pada gambar 19.



**Gambar 19.** Mengupload *certificate* dan *key security hotspot mikrotik*

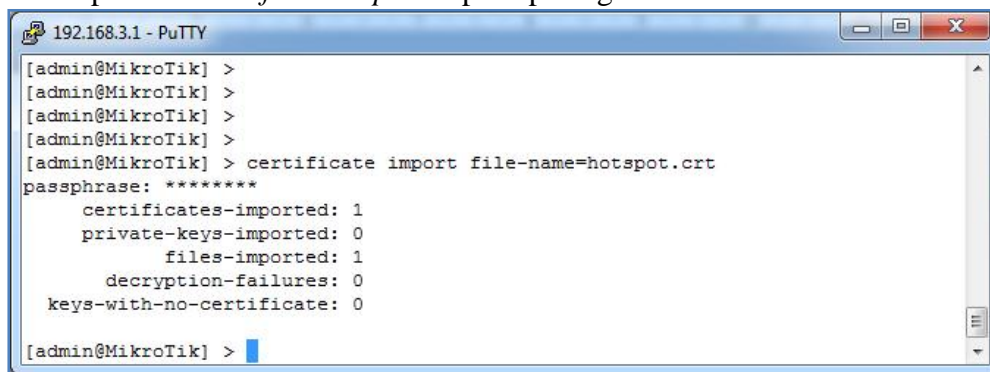
Setelah proses *upload* selesai maka kita menggunakan perintah *file print* untuk melihat hasil *upload* file sertifikat dan file kunci (*key*) diserver mikrotik seperti pada gambar 20.



4	hotspot.crt	.crt file	1025	jan/11/2014 06:41:54
5	hotspot.key	.key file	963	jan/11/2014 06:41:54
6	hotspot	directory		jan/11/2014 03:50:52
7	hotspot/status.html	.html file	2775	jan/11/2014 03:50:52
8	hotspot/md5.js	.js file	7218	jan/11/2014 03:50:52
9	hotspot/redirect.html	.html file	213	jan/11/2014 03:50:52
10	hotspot/radvert.html	.html file	1481	jan/11/2014 03:50:52
11	hotspot/errors.txt	.txt file	3615	jan/11/2014 03:50:52
12	hotspot/login.html	.html file	3384	jan/11/2014 03:50:52

**Gambar 20.** Tampilan *certificate* dan *key security* di terminal

Kemudian installasi file sertifikat yang telah dibuat di mikrotik router dengan menggunakan perintah *certificate import* seperti pada gambar 21.



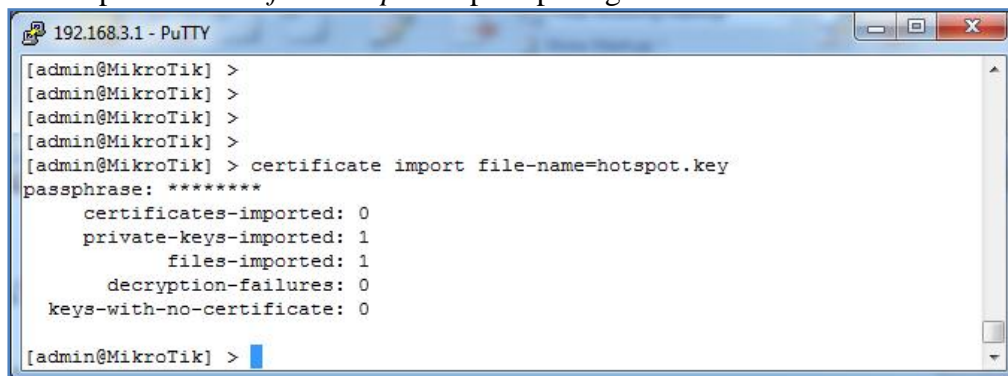
```

[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] > certificate import file-name=hotspot.crt
passphrase: *****
      certificates-imported: 1
      private-keys-imported: 0
           files-imported: 1
      decryption-failures: 0
      keys-with-no-certificate: 0
[admin@MikroTik] >

```

**Gambar 21.** Mengimpor *file certificate*

Kemudian installasi file kunci (*key*) yang telah dibuat di mikrotik router dengan menggunakan perintah *certificate import* seperti pada gambar 22.



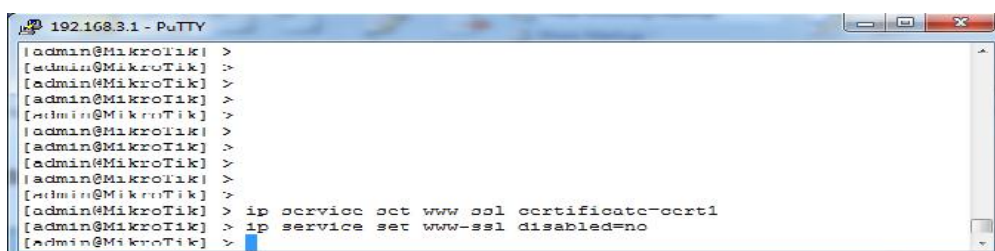
```

[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] > certificate import file-name=hotspot.key
passphrase: *****
      certificates-imported: 0
      private-keys-imported: 1
           files-imported: 1
      decryption-failures: 0
      keys-with-no-certificate: 0
[admin@MikroTik] >

```

**Gambar 22.** Mengimpor *file kunci*

Langkah berikutnya mengaktifkan *service www-ssl* agar server mikrotik *support ssl* setelah itu *setting* menggunakan file sertifikat yang telah kita buat sebelumnya seperti pada gambar 23.



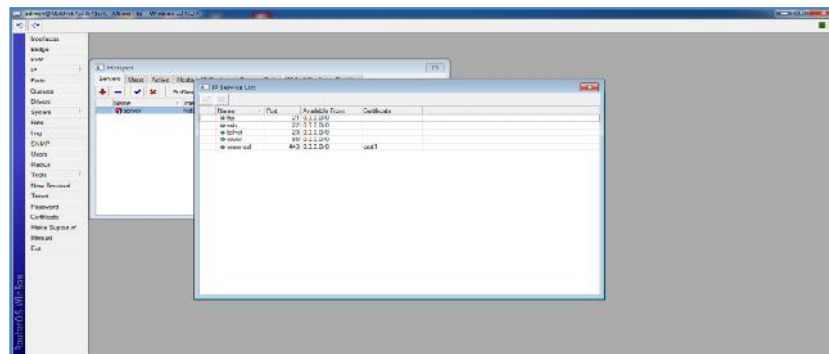
```

[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] > ip service set www ssl certificate=cert1
[admin@MikroTik] > ip service set www-ssl disabled=no
[admin@MikroTik] >

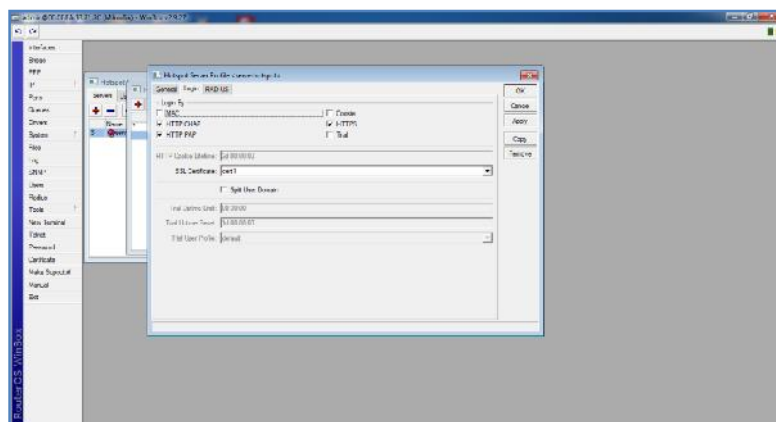
```

**Gambar 23.** Mengaktifkan *service ssl* menggunakan *certificate*

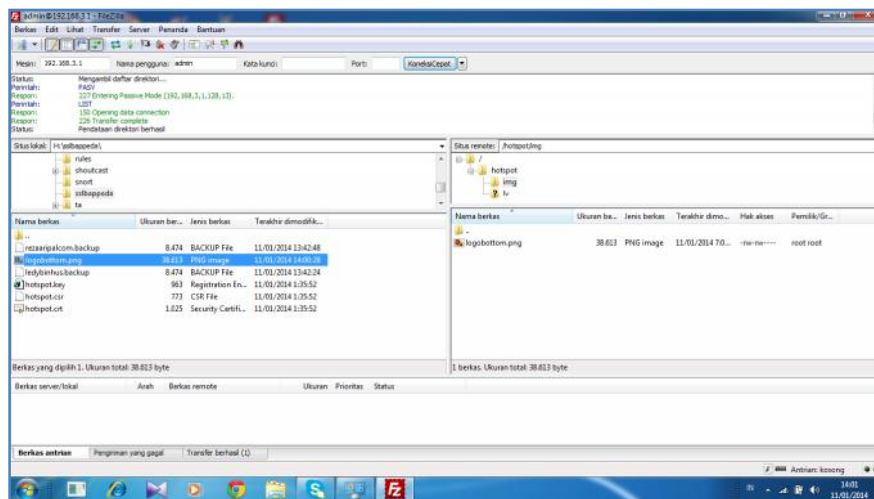
Pada gambar dibawah ini merupakan konfigurasi *service www-ssl* pada *software winbox*. seperti pada gambar 24



**Gambar 24.** Mengaktifkan service ssl menggunakan *certificate* via *winbox*

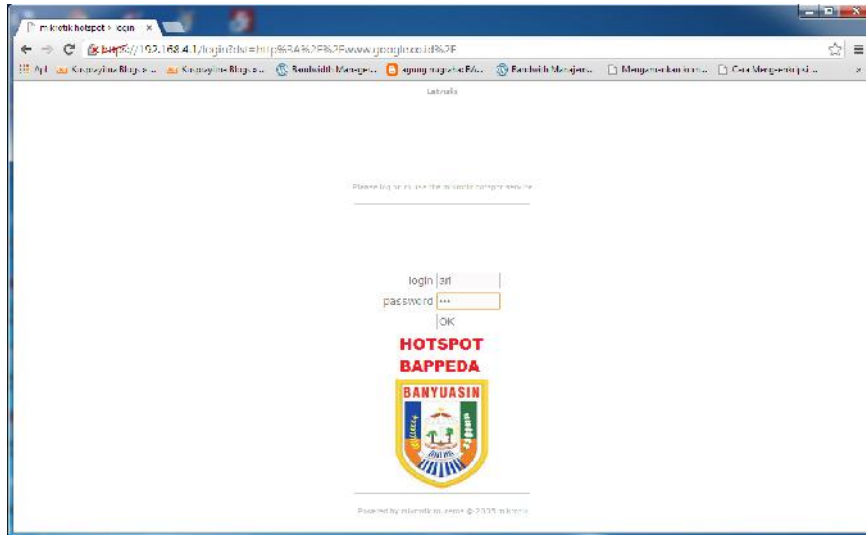


**Gambar 25.** Mengaktifkan service ssl menggunakan *certificate* via *winbox*



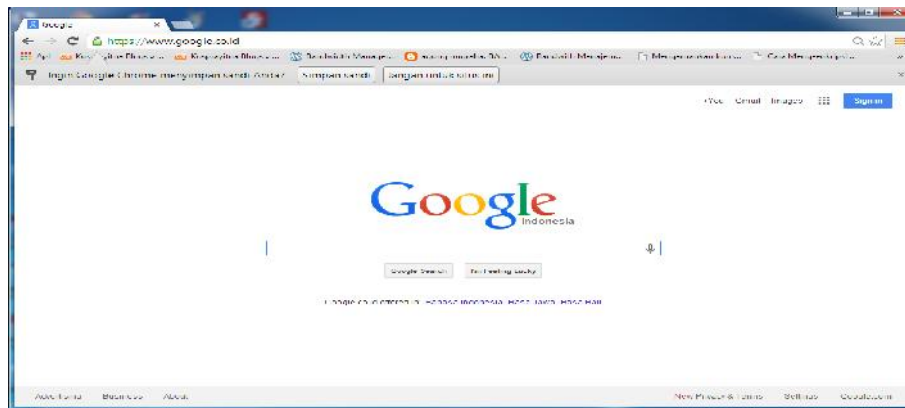
**Gambar 26.** Upload logo Login Hotspot

Selanjutnya buka browser Mozilla atau Google chrome , secara otomatis akan muncul tampilan *login hotspot mikrotik* dengan menggunakan fasilitas *secure socket layer*, hal ini tampak pada url login yaitu *https://192.168.4.1* kemudian isi *user* dan *password hotspot* seperti pada gambar 27.



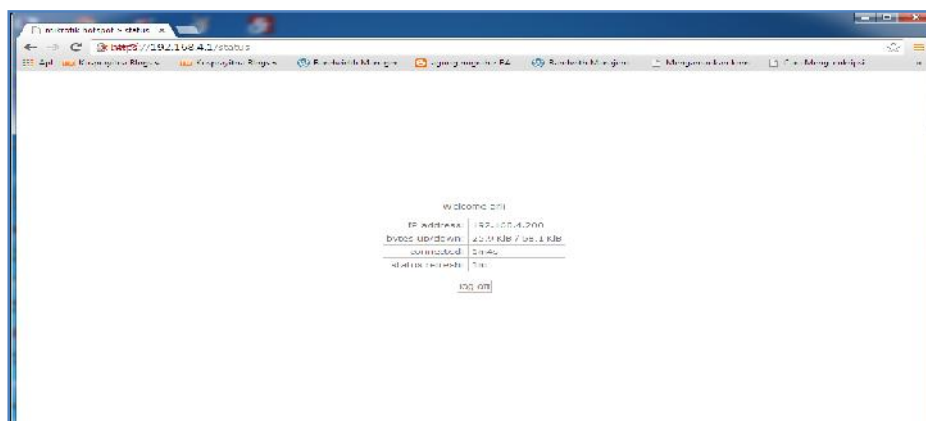
**Gambar 28.** Tampilan *login hotspot* mikrotik

Kemudian setelah *user login* maka *user* bias langsung terkoneksi ke internet melalui web browser seperti gambar 29

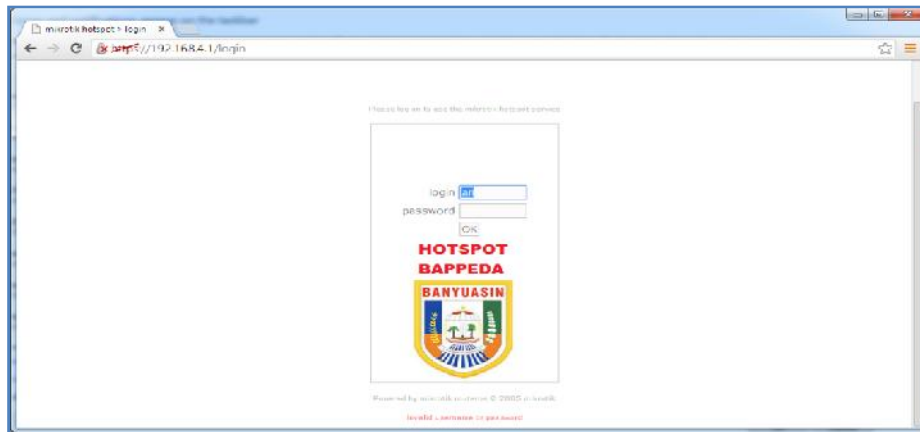


**Gambar 29.** Tampilan koneksi internet

User yang *login* bisa dilihat melalui *url login* yaitu *https://192.168.4.1* yang ditunjukkan pada gambar 30







**Gambar 31.** Penolakan koneksi jika salah *username* atau *password*

Ketika browser Mozilla atau Google chrome dibuka dan *user name* atau *password* yang dimasukkan salah akan tampil seperti gambar 32.

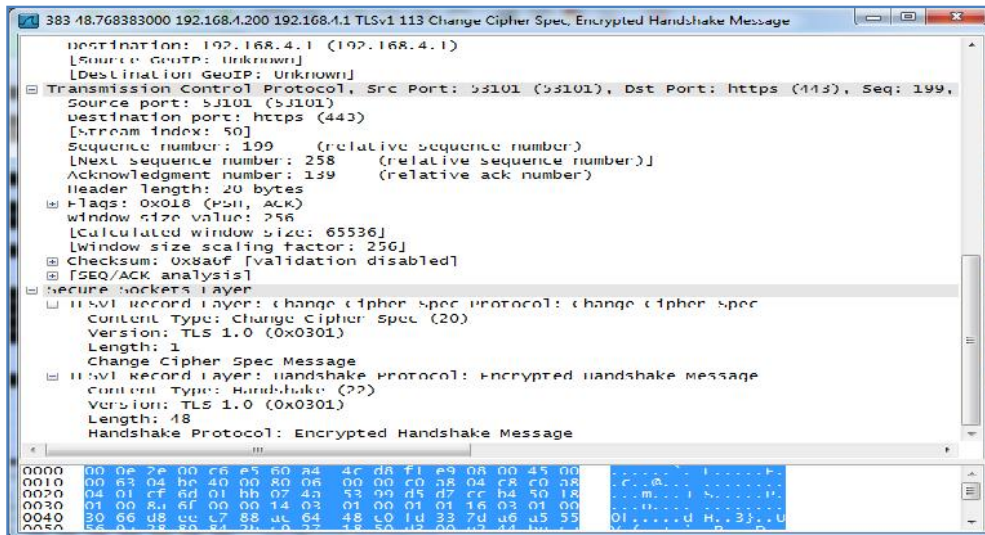
### Evaluasi Hasil dan Pembahasan

Hasil yang didapat dari Implementasi rancangan keamanan jaringan *wireless* dengan metode *Secure Socket Layer* (SSL) pada Bappeda Kabupaten Banyuasin bisa disimpulkan bahwa sistem keamanan ini dapat berjalan dengan baik. Sistem ini mampu menjawab kebutuhan pada jaringan *wireless* yang lebih aman dengan memanfaatkan security *Socket Layer* (SSL), sehingga membuat user menggunakan fasilitas jaringan *wireless* menjadi lebih terkontrol dan sesuai dengan tujuan awal dari perancangan sistem keamanan ini serta memberi kemudahan administrator jaringan dalam melakukan penambahan *user hotspot via browser* melalui fasilitas *user manager*.

Protokol SSL mengotentikasi *server* kepada *client* menggunakan kriptografi kunci publik dan sertifikat digital. Untuk mengaktifkan SSL pada halaman login mikrotik perlu memasang sertifikat SSL yang sesuai dengan server dan halaman web login mikrotik hotspot. Setelah SSL terpasang, maka URL login mikrotik hotspot yang sebelumnya *http://* menjadi *https://*. Pada gambar 32 dan 33 merupakan hasil *capture* menggunakan software *Wireshark*, hasil yang diperoleh adalah *ip address* yang didapat *client hotspot* yaitu 192.168.4.200 kemudian kita dapat melihat paket data yang bertipe SSL sedang melakukan *handshake protocol* yaitu *client hello*. Setelah melakukan *handshake Client Hello*, paket dilanjutkan dengan *server Hello*, kemudian sertifikat dikirim. Paket data jaringan yang telah menggunakan SSL berimplikasi pada terenkripsinya seluruh data yang ditransfer antara *server* dan *client*.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.4.200	192.168.4.1	SSL	55	SSL Connection Data
2	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
3	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
4	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
5	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
6	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
7	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
8	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
9	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
10	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
11	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
12	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
13	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
14	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
15	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
16	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
17	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
18	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
19	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
20	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
21	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
22	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
23	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
24	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
25	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
26	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
27	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
28	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
29	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
30	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
31	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
32	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
33	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
34	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
35	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
36	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
37	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
38	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
39	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
40	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
41	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
42	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
43	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
44	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
45	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
46	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
47	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
48	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
49	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
50	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
51	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
52	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
53	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
54	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
55	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
56	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
57	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
58	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
59	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
60	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
61	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
62	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
63	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
64	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
65	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
66	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
67	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
68	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
69	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
70	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
71	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
72	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
73	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
74	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
75	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
76	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
77	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
78	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
79	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
80	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
81	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
82	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
83	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
84	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
85	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
86	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
87	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
88	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
89	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
90	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
91	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
92	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
93	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
94	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
95	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
96	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
97	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
98	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
99	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello
100	0.000000	192.168.4.200	192.168.4.1	SSL	254	SSL Client Hello

**Gambar 33.** Tampilan *Wireshark*



**Gambar 34.** Tampilan *enkripsi SSL*

## PENUTUP

Keamanan *wireless hotspot* dengan metode SSL dibangun dan dirancang di kantor Bappeda untuk memperkuat sistem keamanan *wireless internet*, hal ini dikarenakan selama ini Bappeda Kabupaten Banyuasin belum memiliki *server gateway* dan sistem keamanan fasilitas internet *hotspot* yang baik dimana metode WEP / WPA masih bisa ditembus oleh *software hacking* / penyusup seperti *software backtrack*. Merancang *server gateway* yang berfungsi sebagai *router internet* baik pada jaringan kabel maupun *wireless* merupakan solusi dimana dapat membantu komunikasi antar komputer serta sistem keamanan *internet hotspot* berbasis mikrotik dimana *user* akan melakukan proses *login* terlebih dahulu dengan memasukkan nama *user* dan *password* saat akan mengakses internet dengan menggunakan metode keamanan *Secure Socket Layer (SSL)*.

## DAFTAR PUSTAKA

- Herlambang. 2008. \_\_\_\_\_. Gava Media : Yogyakarta
- John. G Burch. 2010. \_\_\_\_\_. Andi offset : Yogyakarta
- Kurniawan. 2012. \_\_\_\_\_. Datakom Lintas Buana : Jakarta.
- Towidjojo. 2013. \_\_\_\_\_. Mediakita : Jakarta.